Falting, Endlichkeitssatze für abelsche Varietäten über Zahlkörpern, Inv. Math. 73 (1983), 349–366; Erratum, 75 (1984), p. 381

K: finite ext^n field of $\mathbb{Q}$

A: abelian variety over K, ℓ: a prime number

Thm 3. The representation of $Gal(\bar{K}/K)$ on $T_\ell(A) = \varprojlim_m A[\ell^m](\bar{K})$ is semisimple

Tate conj. for abelian var. over nber fields

Thm 4. $\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \xrightarrow{\sim} \mathrm{End}_{Gal(\bar{K}/K)}(T_\ell(A))$

Thm 5. S = a finite subset of $\Sigma_{K,f}$

There are only finitely many ISOGENY classes of abelian varieties over K of a given dimension g with good reduction outside S

Thm 6 (Shafarevich conjecture) S = a finite subset of $\Sigma_{K,f}$ $g, d > 0$

There are only finitely many isomorphism classes of g-dim^l polarized abelian varieties over K with polarization degree d

Thm 7 (Mordell conjecture) $C_{/K}$ smooth projective curve over K, genus$(C) \geq 2$. Then $C(K)$ is finite

Historical: Mordell. On the rational solutions of the indeterminate equation of third and fourth degree, Proc. Cambridge Phil Soc 21 (1922), 179–192

Weil L'arithmétique sur les courbes algébriques, Acta Math 52 (1928), 281–315

Siegel. Über einige Anwendungen diophantischer Approximationen, Abh. Akad. Wiss. Phys.-Math Kl 1929, No 1

Theorem 5A K: number field. S: a finite subset of $\Sigma_{K,f}$, ℓ: a prime nber

$\exists$ a finite subset $T \subseteq \Sigma_{K,f} \setminus S$ s.t. any semisimple $d>0$

ℓ-adic repr $\rho: \mathrm{Gal}(\bar{K}/K) \to GL_d(\mathbb{Q}_\ell)$ unramified outside S

is determined up to isomorphism by the finite sequence

$\left(\mathrm{Tr}(\rho(\mathrm{Fr}_v))\right)_{v\in T}$

Pf: Hermite thm: Given N, S, $\mathcal{L}_{N,S} := \left\{ L/K \subseteq \bar{K}/K \;\middle|\; [L:K] \le N,\ L/K \text{ Galois unramified outside } S \right\}$

Chebotarev $\Rightarrow$ $\exists$ a finite subset $T_{N,S} \subseteq \Sigma_{K,f} \setminus S$ s.t. $\forall L/K \in \mathcal{L}_{N,S}$

$$\bigcup_{v\in T_{N,S}} \left(\frac{L/K}{v}\right) = \mathrm{Gal}(L/K)$$

Frob. conjugacy class

Take $N = \ell^{2d^2}$.

Claim: $T_{\ell^{2d^2},S}$ satisfies the required property

Suppose $\rho, \rho' : \mathrm{Gal}(\bar{K}/K) \to GL_d(\mathbb{Q}_\ell)$ are semi-simple and unramified outside S

$\rho(\mathrm{Fr}_v) = \rho'(\mathrm{Fr}_v)$ $\forall v \in T_{\ell^{2d^2},S}$

Let $M := \mathrm{Im}\left(\mathbb{Z}_\ell[\mathrm{Gal}(\bar{K}/K)] \xrightarrow[(\rho,\rho')]{} M_d(\mathbb{Q}_\ell)\times M_d(\mathbb{Q}_\ell)\right)$

Will show: The linear form $\delta: M \to \mathbb{Q}_\ell$, $\delta(m_1,m_2) = \mathrm{Tr}(m_1) - \mathrm{Tr}(m_2)$ is 0

Know: $\delta(\rho(\mathrm{Fr}_v), \rho'(\mathrm{Fr}_v)) = 0$ $\forall v \in T$

M is a free $\mathbb{Z}_\ell$-module of rank $\le 2d^2$

$\rightsquigarrow$ $M \otimes_{\mathbb{Z}_\ell} \mathbb{F}_\ell$ is an $\mathbb{F}_\ell$-vector space, $\dim_{\mathbb{F}_\ell}(M\otimes_{\mathbb{Z}_\ell}\mathbb{F}_\ell) \le 2d^2$

$\rightsquigarrow \#\,\mathrm{Im}\left(\mathrm{Gal}(\bar{K}/K) \xrightarrow{(\bar\rho,\bar\rho')} (M\otimes_{\mathbb{Z}_\ell}\mathbb{F}_\ell)^\times\right) \le \ell^{2d^2}$

$$\bigcup_{v\in T_{\ell^{2d^2},S}} (\bar\rho,\bar\rho')\left(\frac{L/K}{v}\right) = \mathrm{Im}\left(\mathrm{Gal}(\bar{K}/K) \xrightarrow{(\bar\rho,\bar\rho')} (M\otimes_{\mathbb{Z}_\ell}\mathbb{F}_\ell)^\times\right)$$

$\Longrightarrow$ The $\mathbb{Z}_\ell$-span of $\bigcup_{v\in T_{\ell^{2d^2},S}} (\rho,\rho')(\text{conjugacy class of } \mathrm{Fr}_v) = M$

Nakayama

$\Rightarrow$ δ vanishes on M $\Longrightarrow$ $\rho \cong \rho'$ QED.

Theorem 5
$\Downarrow$

Corollary Assume Tate conjecture for abelian varieties over number fields

$\# \{$isogeny classes of abelian varieties$/K$ of a given dim. g unramified outside $S\} < \infty$

The proof of Tate conjecture, and the implication Thm 5 $\Rightarrow$ Thm 6, uses the notion of <u>height</u>, or <u>degree</u> of metrized line bundles.

Baby case: Arakelov divisors / metrized line bundles on $\mathrm{Spec}(\mathcal{O}_K)$
K = a number field

<u>Def</u> A <u>compactified divisor</u> on $\mathcal{O}_K$ is a formal finite sum

$$D = \sum_{v\in\Sigma_{K,f}} n_v\,[v] + \sum_{\sigma\in\Sigma_{K,\infty}} \lambda_\sigma\,[\sigma] \qquad n_v\in\mathbb{Z}\ \forall v,\quad \lambda_\sigma\in\mathbb{R}\ \forall\sigma$$

$$\deg(D) := \sum_v n_v\cdot\log q_v + \sum_\sigma \lambda_\sigma$$

principal compactified divisors: $\forall f\in K^\times$, define $\qquad \varepsilon_\sigma = \begin{cases}1 & \sigma \text{ real}\\ 2 & \sigma \text{ cpx}\end{cases}$

$$(f) = \sum_v \mathrm{ord}_v(f)\,[v] - \sum_{\sigma\in\Sigma_{K,\infty}} \varepsilon_\sigma \log|f|_\sigma$$

Note: $|f|_\sigma^2 = \|f\|_\sigma \Leftarrow$ normalized abs. value

Thus: $\iota_\sigma : K \hookrightarrow \mathbb{C}$ $\quad |f|_\sigma = |\iota_\sigma(f)|$ usual abs. value on $\mathbb{C}$

$$\deg : \underset{\substack{\uparrow\\ \text{compactified divisors}}}{\mathrm{Div}_c(\mathcal{O}_K)} \Big/ \underset{\substack{\uparrow\\ \text{principal compactified divisors}}}{\mathrm{Pr}_c(\mathcal{O}_K)} \longrightarrow \mathbb{R}$$

Another point of view: Compactified Picard group

<u>Def</u> A compactified invertible $\mathcal{O}_K$-module is an invertible $\mathcal{O}_K$-module $\mathcal{L}$, endowed with a positive definite Hermitian form on $L_\sigma = L\otimes_{K,\sigma} K_\sigma$ (If you prefer, pick $\iota_\sigma : K_\sigma \hookrightarrow \mathbb{C}$ $\forall\sigma\in\Sigma_{K,\infty}$

Have

$$\begin{array}{ccccccc} \Big(\prod_{\sigma\in\Sigma_{K,\infty}} \mathbb{R}^\times_{>0}\Big)/\mathcal{O}_K^\times & \to & \mathrm{Pic}_c(\mathcal{O}_K) & \longrightarrow & Cl(\mathcal{O}_K) & \longrightarrow & 0\\ & & \cong\uparrow\varphi & & & & \\ & & \mathrm{Div}_c(\mathcal{O}_K)/\mathrm{Pr}_c(\mathcal{O}_K) & & & & \end{array}$$

where $\mathrm{Div}(\mathcal{O}_K) \xrightarrow{\varphi} \mathrm{Pic}_c(\mathcal{O}_K)$

$\sum_v n_v \cdot [v] + \sum_\sigma \lambda_\sigma [\sigma] \mapsto$ the fractional $\mathcal{O}_K$-ideal $\prod_v \mathfrak{p}_v^{-n_v}$ endowed with the Hermitian metrics on K_σ s.t. $|1|_\sigma = \exp\left(-\frac{\lambda_\sigma}{\varepsilon_\sigma}\right)$

To construct φ^{-1}:

Given $\tilde{\mathcal{L}} = (\mathcal{L}, (|\cdot|_\sigma)_{\sigma \in \Sigma_{K,\infty}})$, Pick $s: \mathcal{O}_K \to \mathcal{L}$ a non-zero section of $\mathcal{L}$.

define $\varphi^{-1}(\tilde{\mathcal{L}}) = \sum_{v \in \Sigma_{K,f}} \mathrm{length}_{\mathcal{O}_v}(\mathcal{L} \otimes_{\mathcal{O}} \mathcal{O}_v / \mathcal{O}_v \cdot s) \cdot [v] - \sum_{\sigma \in \Sigma_{K,\infty}} \varepsilon_\sigma \cdot \log |s|_\sigma$ mod $\mathrm{Pr}_c(\mathcal{O}_K)$

Reformulate some classical results in algebraic number theory in this geometric language

Def Given $\tilde{\mathcal{L}} = (\mathcal{L}, (|\cdot|_\sigma)_\sigma)$, define

$$H^0(\tilde{\mathcal{L}}) := \{ s \in \mathcal{L} \mid |s|_\sigma \le 1 \ \forall \sigma \in \Sigma_{K,\infty} \}$$

$$\chi(\tilde{\mathcal{L}}) := -\log \mathrm{vol}\Big(\bigoplus_{\sigma \in \Sigma_{K,\infty}} \mathcal{L}_\sigma / \mathcal{L}\Big)$$

$$\chi'(\tilde{\mathcal{L}}) := \chi(\tilde{\mathcal{L}}) - r_2 \cdot \log\left(\frac{4}{\pi}\right)$$

Prop $$\chi(\tilde{\mathcal{L}}) = -\log(2^{r_1} \cdot \pi^{r_2}) + \log\left(\lim_{t \to 0^+} \frac{\# H^0(\mathcal{L}, (t|\cdot|_\sigma)_{\sigma \in \Sigma_{K,\infty}})}{t^{[K:\mathbb{Q}]}}\right)$$

$$\chi'(\tilde{\mathcal{L}}) = -[K:\mathbb{Q}] \cdot \log 2 + \log\left(\lim_{t \to 0^+} \frac{\# H^0(\mathcal{L}, (t \cdot |\cdot|_\sigma)_{\sigma \in \Sigma_{K,\infty}})}{t^{[K:\mathbb{Q}]}}\right)$$

Ex. $\tilde{\mathcal{O}}_K \overset{\text{def}}{=} (\mathcal{O}_K, |1|_\sigma = 1 \ \forall \sigma \in \Sigma_{K,\infty})$

$$H^0(\tilde{\mathcal{O}}_K) = 0 \sqcup \mathcal{O}_K^\times$$

$$\chi(\tilde{\mathcal{O}}_K) = r_2 \log 2 - \frac{1}{2} \log(|d_K|)$$

$$\chi'(\tilde{\mathcal{O}}_K) = -r_2 \log\left(\frac{2}{\pi}\right) - \frac{1}{2} \log(|d_K|)$$

Lemma 1 (Riemann-Roch)

$$\chi(\tilde{\mathcal{L}}) = \deg \tilde{\mathcal{L}} + \chi(\tilde{\mathcal{O}}_K), \quad \chi'(\tilde{\mathcal{L}}) = \deg \tilde{\mathcal{L}} + \chi'(\tilde{\mathcal{O}}_K)$$

Lemma 2 If $\deg(\hat{\mathcal{L}})<0$, then $H^0(\hat{\mathcal{L}})=(0)$

Lemma 3 If $\deg(\hat{\mathcal{L}})=0$ and $H^0(\hat{\mathcal{L}})\neq(0)$, then $\hat{\mathcal{L}}\cong\hat{\mathcal{O}}_K$

Lemma 4 (Minkowski) If $\deg(\hat{\mathcal{L}})\geq\chi'(\mathcal{O}_K)$, then $H^0(\hat{\mathcal{L}})\neq(0)$

Thm (Hermite–Minkowski) If $[K:\mathbb{Q}]>1$, then $|d_K|>1$, i.e. $\pi_1(\mathrm{Spec}(\mathcal{O}_K))\neq(1)$

<u>**Theorem 1**</u> Given $K/\mathbb{Q}$ number field, $c\in\mathbb{R}$, $g\in\mathbb{N}$

$$\#\left\{\begin{array}{l}\text{isom. classes of}\\ \text{principally polarized } g\text{-dimensional abelian}\\ \text{varieties } A/K \text{ with semiabelian reduction}\\ \text{over } \mathcal{O}_K \text{ s.t. } h(A)\leq c\end{array}\right\}<\infty$$

<u>**Theorem 2**</u> $A/\mathcal{O}_K$ semi-abelian s.t. A_K is an abelian variety

ℓ: prime number

$G/K\subseteq A_K[\ell^\infty]$ an ℓ-divisible subgroup

Then $\left(h(A_K/G[\ell^n])\right)_{n\geq1}$ stabilizes, i.e. $\exists\, n_0$ s.t.

$$h(A_K/G[\ell^n])=h(A_K/G[\ell^m])\quad\forall\, m,n\geq n_0$$

<u>**Proposition**</u> (related to theorem 1) $K=$ number field

$X\to\mathrm{Spec}\,\mathcal{O}_K$ proper, normal $\mathcal{L}$: ample invertible $\mathcal{O}_X$-module

$\cup\!\!\shortmid$ open dense

U

$$\hat{\mathcal{L}}=(\mathcal{L},\langle\,,\rangle)$$

hermitian metric on $\mathcal{L}|_U\otimes_{\mathcal{O}_K}K_\infty$ with logarithmic singularities

Then $\forall c<\mathbb{R}$ $\#\{x\in U(K)\mid h_{\hat{\mathcal{L}}}(x)\leq c\}<\infty$

<u>**Def**</u> $\langle\,,\rangle$ has log. singularities $\exists V$ $I\subseteq\mathcal{O}_X$ ideal s.t. $\mathrm{Spec}(\mathcal{O}_X/I)=(X\setminus Y)_{red}$

$\forall\sigma\in M_{K,\infty}$, $\forall y\in X(K_\infty)\setminus U(K_\infty)$, $\{$ $f_1,\dots,f_m$ local generator of I in V nbd of y in $X(K_\sigma)$ $\exists\, C_1, C_2>0$

$$\left|\frac{\langle\,,\rangle}{\langle\,,\rangle_1}\right|^{\pm1}\leq C_1\max_{x\in V}\{|f_1(x)|,\dots,f_m(x)\}^{C_2}$$

$\langle\,,\rangle_1$: good metric

Lemma (Hermite-Minkowski) K: number field $S \subseteq M_{K,f}$ finite subset
$d > 0$ ⇝ $\#\{L/K \subseteq \bar{\mathbb{Q}}/K \mid [L:K] \le d,\ L/K$ is unramified outside $S\} < \infty$

Pf: Fact: $\forall$ locally compact field k of characteristic 0, $\forall c > 0$
$\#\{F/k \subseteq \bar{k} \mid [F:k] \le c\} < \infty$
(Exer. use Krasner's lemma)

⇝ $\exists c_{1,K,S,d}$ s.t. $\forall L/K$ unramified outside S, $[L:K] \le d$
have $|\mathrm{disc}_{L/K}| \le c_{1,K,S,d}$

Minkowski: $\exists c_2 = c_{2,K,S,d}$ (indep. of L), $\exists x \in \mathcal{O}_L$ s.t.
$\|x\|_{\sigma_1} \le c_2$, $\|x\|_{\sigma_2} < 1, \dots, \|x\|_{\sigma_{r_1+r_2}} < 1$ (⇝ $c_2 > 1$)

If $[L:K(x)] \ge 3$, then $\{\sigma \in M_{L,\infty} \mid \sigma|_{K(x)} = \sigma_1|_{K(x)}\} \ge 2$. contradiction
⇝ $[L:K(x)] \le 2$

There are only a finite number of such ext^n fields $K(x)/K$.
because the heights of coeff. of the min. poly of x
are bounded by some constant $c_{3,K,S,d}$
$L/K(x)$ quadratic ext^n. with $|\mathrm{disc}_{L/K(x)}| \le c_{1,K,S,d}$

$\xrightarrow{\text{class field theory}}$ The number of such quadratic extensions of $L/K(x)$ is finite QED.

Alternative (and more classical) argument, as in Lang, end of Chap V:
- The above argument suffices if L has one real place.
- If L has one complex place $\sigma_{r_1+r_2}$, consider the (additive) lattice

$$\mathcal{O}_L \hookrightarrow \prod_{i=1}^{r_1+r_2} L_{\sigma_i}$$
$$\cup$$
$$B = \left\{ z \;\middle|\; |z_i| < \tfrac{1}{2} \text{ for } i = 1, \dots, r_1+r_2-1,\ \begin{matrix} |z_{r_1+r_2} - \bar{z}_{r_1+r_2}| < c_4 |\mathrm{disc}_{L/K}|^{\frac{1}{2}} \\ |z_{r_1+r_2} + \bar{z}_{r_1+r_2}| < \tfrac{1}{2} \end{matrix} \right\}$$

c_4 large

$\#|B \cap \mathcal{O}_L| \le c_5$ $\wedge$ 0

$[K:\mathbb{Q}] < \infty$

Lemma: A_1, A_2: semiabelian schemes over $\mathcal{O}_K$, $A_{i,K}$: abel. var $i=1,2$

$\phi: A_1 \longrightarrow A_2$ isogeny $\quad G = \mathrm{Ker}(\phi)$ flat and quasi-finite over $\mathcal{O}_K$

Then: $h(A_2) = h(A_1) + \frac{1}{2}\log(\deg(\phi)) - \frac{1}{[K:\mathbb{Q}]}\log(\# \varepsilon^*\Omega^1_{G/R})$

Pf. Consider $\phi^*\omega_{A_2} \xrightarrow{j} \omega_{A_1}$ $\quad \alpha_2 \in \omega_{A_2}$ translation invariant top exterior diff^l form on A_2

$$h(A_2) = \frac{1}{[K:\mathbb{Q}]}\left[\log\#(\omega_{A_2}/\mathcal{O}_K\cdot\alpha_2) - \sum_{\sigma\in M_{K,\infty}}\varepsilon_\sigma\log\left(\left(\frac{1}{2}\right)^g\left(\int_{A_2(\bar{K}_\sigma)}|\alpha_2\wedge\bar{\alpha}_2|_\sigma\right)^{\frac{1}{2}}\right)\right]$$

$$h(A_1) = \frac{1}{[K:\mathbb{Q}]}\left[\log\#(\omega_{A_2}/\mathcal{O}_K\cdot\phi^*\alpha_2) - \sum_{\sigma\in M_{K,\infty}}\varepsilon_\sigma\log\left(\left(\frac{1}{2}\right)^g\int_{A_1(\bar{K}_\sigma)}|\phi^*\alpha_2\wedge\overline{\phi^*\alpha_2}|^{\frac{1}{2}}\right)\right]$$

Cleary: $\displaystyle\int_{A_2(\bar{K}_\sigma)}|\alpha_2\wedge\bar{\alpha}_2|_\sigma = \deg(\phi)^{-1}\cdot\int_{A_1(\bar{K}_\sigma)}|\alpha_1\wedge\bar{\alpha}_1|_\sigma \quad \forall\sigma\in M_{K,\infty}$

The lemma follows from

$$\#(\omega_{A_1}/\mathcal{O}_K\cdot\phi^*\alpha_2) = \#(\omega_{A_1}/\phi^*\omega_2)\cdot\#(\omega_2/\mathcal{O}_K\cdot\alpha_2) \qquad \text{obvious}$$

and the short exact sequence

$$0 \to \varepsilon^*\phi^*\Omega^1_{A_2/\mathcal{O}_K} \longrightarrow \varepsilon^*\Omega^1_{A_1/\mathcal{O}_K} \longrightarrow \varepsilon^*\Omega^1_{G/R} \to 0 \qquad \because G \text{ is a local complete intersection}$$

$$\rightsquigarrow \quad \omega_{A_1}\otimes\phi^*\omega_{A_2}^{-1} \cong \varepsilon^*\Omega^1_{G/R}$$

QED.

Reformulation: Let $\omega_\phi = \omega_{A_1}\otimes\phi^*\omega_{A_2}^{-1} \xleftarrow[\text{can}]{\text{well-defined}} \mathcal{O}_K$

"ω_{A_1/A_2}" $\qquad j(\alpha_2)\otimes\alpha_2^{-1} \longleftarrow 1$

So we have a well-defined "inverse difference ideal" $\mathcal{D}_\phi^{-1}$ s.t. $\mathcal{O}_K \xrightarrow{\text{can}} \omega_{A_1}\otimes\phi^*\omega_{A_2}^{-1}$

and an isom $\omega_{A_1}\otimes\phi^*A_2^{-1} \cong \mathcal{D}_\phi^{-1}$ $\qquad \mathcal{D}_\omega^{-1}$ $\cong$

Under this isom, the section $\mathrm{can}(1)$ of $\omega_{A_1}\otimes\phi^*\omega_{A_2}^{-1}$ correspond to $1\in\mathcal{D}_\phi^{-1}$ $\qquad \mathcal{D}_\phi \subseteq \mathcal{O}_K$ an ideal

Endow $\mathcal{D}_\phi^{-1}$ with the metric $\wedge^{top}\langle\,,\rangle_{A_1}\otimes\phi^*\wedge^{top}\langle\,,\rangle_{A_2}^{-1}$.

$$h(A_1) = h(A_2) + \frac{1}{[K:\mathbb{Q}]}\deg_K(\mathcal{D}_\omega^{-1}, \text{difference metric})$$

Lemma': The section $\mathbb{1}$ of $\mathcal{D}_\phi^{-1}$ satisfy:

$$\begin{cases} \cdot \quad \langle \mathbb{1}, \mathbb{1} \rangle_\sigma = \deg(\phi) \quad \forall \sigma \in M_{K,\infty} \\ \cdot \quad \#(\mathcal{D}_\phi^{-1}/\mathcal{O}_K \cdot \mathbb{1}) = \#(\mathcal{O}_K/\mathcal{D}_\phi) = \#(\omega_{A_1}/\phi^* \omega_{A_2}) \end{cases}$$

$$\Rightarrow \underset{h(A_1) - h(A_2)}{\underset{\parallel}{h(\mathcal{D}_\phi^{-1})}} = \frac{1}{2}\log(\phi) - [K:\mathbb{Q}]^{-1} \log \#(\mathcal{O}_K/\mathcal{D}_\phi)$$

—

Remark: In general, without assuming that $A_{1/K}, A_{2/K}$ have semiabelian reduction, one can still define the inverse difference $\mathcal{D}_\phi^{-1} \supseteq \mathcal{O}_K$ (same def^n as above), the canonical section $\mathbb{1} \in \mathcal{D}_\phi^{-1}$, and an isomorphism $(\omega_{A_1}, \Lambda^{top}\langle , \rangle_{A_1}) \otimes (\omega_{A_2}, \Lambda^{top}\langle , \rangle_{A_2})^{-1}$
$\cong (\mathcal{D}_\phi^{-1}$, difference metric$)$,

but we don't have an isom $\mathcal{D}_\phi^{-1}/\mathcal{O}_K \cong \Lambda^{top} \varepsilon^* \Omega^1_{Ker(\tilde{A}_1^0 \to \tilde{A}_2^0)/R}$

$\uparrow$ connected Néron model

Fact (Without assuming semiabelian reduction)

$$\mathcal{D}_\phi \cdot \mathcal{D}_{\phi^t} = \deg(\phi) \cdot \mathcal{O}_K$$

$$\Rightarrow h(A) = h(A^t)$$

Proposition 8 Let $A_{/\mathcal{O}_K}$ be a semiabelian scheme. Let G_K be a p-divisible subgroup of $A_K[\ell^\infty]$. (ℓ: prime number) Let $v_1, \dots, v_r$ be the places of K above ℓ.

For each $i = 1, \dots, r$ and for each $n \in \mathbb{N}_{\geq 1}$, let $\hat{A}_{\mathcal{O}_{K_{v_i}}}$ = the v_i-adic completion of $A_{/\mathcal{O}}$

$G_{i,n}$ = the Zariski closure of $G_{K_{v_i}} \cap \hat{A}[\ell^n]_{K_{v_i}}$ in $\hat{A}[\ell^n]_{\mathcal{O}_{K_{v_i}}}$

Then $\exists n_0$ s.t. $\forall i = 1, \dots, r$, $(G_{i,n+n_0}/G_{i,n_0})_{/\mathcal{O}_{K_{v_i}}}$ is a p-divisible subgroup of $(\hat{A}_{\mathcal{O}_{K_{v_i}}}/G_{i,n_0})[\ell^\infty]$

Pf: Fix i_0. Prop. 8 follows from Lemma 8a and Proposition 8b below

Lemma 8a Let F be a field, ℓ a prime number, $\ell \neq 0$ in F. Let X be an ℓ-divisible group over F, let Y, Z be ℓ-divisible subgroups of X. Let $H_n = Y[\ell^n] \cap Z[\ell^n]$. $\exists\, n_1 \in \mathbb{N}$ s.t. $(H_{n+n_1}/H_{n_1})_{n \geq 1}$ is a p-divisible subgroup of X/H_{n_1}

Pf: By descent, reduce to intersection of divisible subgroups Y_1, Z_1 in a group $X_1 \cong (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{\oplus h}$

Proposition 8b Let $\mathcal{O}$ be a complete dvr of generic char. 0, residue char. ℓ. Let X be an ℓ-divisible group. Let Y_K be an ℓ-divisible subgroup of X_K. $L = \mathrm{frac}(\mathcal{O})$
Let Y_n = Zariski closure of $Y_K[\ell^n]$ in $X[\ell^n]$. Then $\exists\, n_2 \in \mathbb{N}$ s.t. $(Y_{n+n_2}/Y_{n_2})_{n \geq 1}$ is a p-divisible subgroup of X/Y_{n_2}

Pf. This is proved in Proposition 12 on pp. 181–182 of Tate's "p-divisible groups", 1966 Driebergen Proceedings. 1967, 158–183.

Consider the maps $\to \underset{\mathrm{Spec}\, R_{n+1}}{\underset{\parallel}{Y_{n+1}/Y_n}} \to \underset{\mathrm{Spec}(R_n)}{\underset{\parallel}{Y_n/Y_{n-1}}} \to \cdots$

$\forall i$ $R_i \otimes_{\mathcal{O}} L \xrightarrow{\sim} R_{i+1} \otimes_{\mathcal{O}} L$ = a commutative separable finite dim'l L-algebra D_L.
So each R_i is an $\mathcal{O}$-subalgebra of the maximal order $\mathcal{O}_{D_L}$ in D_L
$\mathcal{O}_{D_L}$ is a finite $\mathcal{O}$-module $\rightsquigarrow$ R_i stabilizes.
Suppose $Y_{n+2}/Y_{n+1} \xrightarrow{\sim} Y_{n+1}/Y_n$ $\forall n \geq n_2$
Let $Z_n \overset{\mathrm{def}}{=} Y_{n+n_0}/Y_{n_0}$ $\forall n \geq 1$

$$\begin{tikzcd}
Z_{n+1} = Y_{n+1+n_0}/Y_{n_0} \arrow[r, "{[\ell]}"] \arrow[d] \arrow[dr] & Y_{n+1+n_0}/Y_{n_0} = Z_{n+1} \\
Y_{n+1+n_0}/Y_{n+n_0} \arrow[r, "\cong", "\beta_n"'] & Y_{1+n_0}/Y_{n_0} = Z_1 \arrow[u, hook]
\end{tikzcd}$$

$\rightsquigarrow$ $\mathrm{Ker}([p^n]_{Z_{n+1}}) = Y_{n+n_0}/Y_{n_0} = Z_n$ $\forall n$
$\Rightarrow (Z_n)_{n \geq 1}$ is an ℓ-divisible group QED

Notation as in Prop. 8 and Lemma 8a

Prop. 8c. $A/_{\mathcal{O}_K}$ semi-abelian $G_K \subseteq A_K[\ell^\infty]$. $v_1, \dots, v_r$ places of K above ℓ

$\forall i = 1, \dots, r$, $\forall n \in \mathbb{N}_{\geq 1}$, $\underset{\substack{\| \\ G_i[\ell^n]}}{G_{i,n}}/_{\mathcal{O}_{K_{v_i}}}$ = Zariski closure of $G_K[\ell^n] \cap \hat{A}_{\mathcal{O}_{v_i}}[\ell^n]$ in $\hat{A}_{\mathcal{O}_{K_{v_i}}}[\ell^n]$

Assume: $(G_{i,n})_{n \geq 1}$ is an ℓ-divisible subgroup G_i of $\hat{A}_{\mathcal{O}_{K_{v_i}}}[\ell^\infty]$ $\forall i$

Then: (a) $\# \varepsilon^* \Omega^1_{G_i[\ell^n]/\mathcal{O}_{K_{v_i}}} = \ell^{n \cdot [K_{v_i}:\mathbb{Q}_\ell] \cdot \dim(G_i)}$

(b) $ht(A_K/G_K[\ell^n]) - ht(A) = \frac{1}{2} ht(G_K) \cdot n \log \ell$

$- n \cdot \log \ell \cdot [K:\mathbb{Q}]^{-1} \cdot \sum_{i=1}^{r} [K_{v_i}:\mathbb{Q}_\ell] \cdot \dim(G_i)$

Pf: (a): $\varepsilon^* \Omega^1_{G_i[\ell^n]/\mathcal{O}_{K_{v_i}}} \cong \omega_{G_i/\mathcal{O}_{v_i}} \otimes_{\mathbb{Z}} (\mathbb{Z}/\ell^n\mathbb{Z})$ $\forall n$

étale ℓ-div. group over $\mathcal{O}_{v_i}$

(b) Over $\mathcal{O}_{v_i} = \mathcal{O}_{K_{v_i}}$, have $\quad = E_i[\ell^n] \times_{\operatorname{Spec} \mathcal{O}_{v_i}} \operatorname{Spec} K_{v_i}$

$$0 \to \hat{A}_{K_{v_i}}[\ell^n] \to A_{K_{v_i}}[\ell^n] \to (\underset{\substack{E_{i,n}/K_{v_i} \\ \|}}{\text{unramified twist}} \text{ of } (\mathbb{Z}/\ell^n\mathbb{Z})^{t_i} \text{ over } K_{v_i}) \to 0$$

$$\leadsto \quad A_{K_{v_i}}/G_i[\ell^n]_{K_{v_i}} = (A_{\mathcal{O}_{v_i}}/G_i[\ell^n])_K$$

$$\cup\!\!\mid$$

$$G_{K_{v_i}}[\ell^n]/G_i[\ell^n]_{K_{v_i}} \hookrightarrow (E_{i,n}/K_{v_i})$$

$\Rightarrow$ The Zariski closure of $G_{K_{v_i}}[\ell^n]/G_i[\ell^n]_{K_{v_i}}$ in $A_{\mathcal{O}_{v_i}}/G_i[\ell^n]$ is a finite étale subgroup of $A_{\mathcal{O}_{v_i}}/G_i[\ell^n]$

$$\leadsto \mathcal{D}_{A_{K_{v_i}}/G_i[\ell^n]_{K_{v_i}} \to A_{K_{v_i}}/G_{K_{v_i}}[\ell^n]} = \mathcal{O}_{v_i}$$

$$\mathcal{D}_{A_{K_{v_i}} \to A_{K_{v_i}}/G_{K_{v_i}}[\ell^n]} = \mathcal{D}_{A_{K_{v_i}} \to A_{K_{v_i}}/G_i[\ell^n]_{K_{v_i}}}$$

Consequently, $\# \mathcal{O}_{v_i}/\mathcal{D}_{A_{K_{v_i}} \to A_{K_{v_i}}/G_{K_{v_i}}[\ell^n]} = \# (\mathcal{O}_{v_i}/\mathcal{D}_{A_{K_{v_i}} \to A_{K_{v_i}}/G_i[\ell^n]_{K_{v_i}}})$

$= \ell^{n \cdot [K_i:\mathbb{Q}_\ell] \cdot \dim(G_i)}$

QED

<u>Proposition 8d</u> Notation and assumption as in Prop 9c

$$2\sum_{i=1}^{r}[K_{v_i}:\mathbb{Q}_\ell]\cdot\dim(G_i) = [K:\mathbb{Q}]\cdot ht(G_K)$$

<u>Pf</u>. Consider the $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$-module $\mathrm{Ind}_{Gal(\bar{\mathbb{Q}}/K)}^{Gal(\bar{\mathbb{Q}}/\mathbb{Q})} T_\ell(A_K) = V$

Let D_ℓ = decomposition group over ℓ in $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$

<u>Consider</u> $\chi = \det(V) : Gal(\mathbb{Q}^{ab}/\mathbb{Q}) \to \mathbb{Z}_\ell^\times$

Mackey's theorem + projection formula

$$\Rightarrow \chi|_{D_\ell} = \prod_{i=1}^{r}\det\left(\mathrm{Ind}_{D_{v_i}}^{D_\ell}(T_\ell(G_i))\right)\cdot\left(\text{finite order}\right)$$

A_{O_K} semi-abelian $\Rightarrow$ χ is unramified outside ℓ and ∞

<u>Weil</u>: χ has motivic weight $-[K:\mathbb{Q}]\cdot ht(G_K)$

(in the sense that $\forall$ prime $p\neq\ell$ s.t. A_K has good reduction at all places above p. $\chi(Fr_p)$ is an algebraic integer (arith. Frob) s.t. $|\sigma(\chi(Fr_p))| = p^{\frac{1}{2}[K:\mathbb{Q}]\cdot ht(G_K)}$

$\forall \sigma : \mathbb{Q}(\chi(Fr_p)) \hookrightarrow \mathbb{C}$)

$$\begin{array}{ccc} & Gal(\mathbb{Q}^{ab}/\mathbb{Q}) \xrightarrow{\ \chi\ } \mathbb{Z}_\ell^\times \\ \ker(\chi) & \uparrow \wr\, rec_{\mathbb{Q}} \\ \cup\!\!\mid & \hat{\mathbb{Z}} \\ \left(\prod_{p\neq\ell}\mathbb{Z}_p^\times\right) & \end{array}$$

<u>So</u> (global CFT): $\chi = \chi_{cyc}^N\cdot(\text{finite order})$ for some $N\in\mathbb{Z}$

χ_{cyc}^N: motivic weight $-2N$

<u>So</u> $N = \frac{1}{2}\cdot[K:\mathbb{Q}]\cdot ht(G_K)$.

<u>Tate</u> $\Rightarrow$ $\det\left(Gal(K_{v_i}^{ab}/K_{v_i})\right) = \chi_{cyc}^{\otimes\dim G_i}$ $\forall i$

$$\rightsquigarrow \mathbb{C}_\ell(\chi) \cong C_\ell\left(\sum_{i=1}^{r}[K_{v_i}:\mathbb{Q}_\ell]\cdot\dim(G_i)\right)$$

Hilbert 90: $\mathbb{C}_p(\text{char. of finite order}) \cong \mathbb{C}_p$ $\rightsquigarrow$ $\mathbb{C}_p\left(\sum_{i=1}^{r}[K_{v_i}:\mathbb{Q}_\ell]\cdot\dim(G_i)\right)$

<u>Tate</u> $\Rightarrow$ $\sum_{i=1}^{r}[K_{v_i}:\mathbb{Q}_\ell]\dim(G_i) = \frac{1}{2}[K:\mathbb{Q}]\cdot ht(G_K)$ $\qquad \cong \mathbb{C}_p\left(\frac{1}{2}[K:\mathbb{Q}]\cdot ht(G_K)\right)$

QED

Thm 2 $\Longleftarrow$ Lemma 8a + Prop. 8b + Prop 8c + Prop 8d.

Alternative way of finishing the proof of Prop 8d:

Raynaud : $\det(T_\ell(G_i)) : \mathrm{Gal}(\bar{K}_{v_i}/K_{v_i}) \to \mathbb{Z}_\ell^\times$

$$\quad \| \qquad\qquad\qquad\qquad \forall i$$
$$\chi_{cycl, K_{v_i}}^{\otimes \dim(G_i)}$$

$$\rightsquigarrow \chi = \chi_{cycl}^{\otimes \sum_{i=1}^{r} [K_{v_i} : \mathbb{Q}_\ell] \cdot \dim(G_i)} \otimes (\text{finite order})$$

global CFT $+ \chi|_{D_\ell}$

$$= \chi_{cycl}^{\frac{1}{2}[K:\mathbb{Q}]\cdot ht(G_K)} \otimes (\text{finite order})$$

Weil

<u>Prop. 9A</u> Admit Thm 1 + Thm 2 $\quad K$: number field

A/K principally polarized, ℓ: a prime number

Let $W \subseteq V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ be a maximal isotropic $\mathbb{Q}_\ell$-vector subspace stable under $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$. Then $\exists$ an idempotent $e \in \mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$ s.t. $e \cdot V_\ell(A) = W$ $\quad (\rightsquigarrow \ (1-e)\cdot V_\ell(A) \oplus W = V_\ell(A))$

clearly stable under $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$

Pf: Let $W_0 = W \cap T_\ell(A)$

$$T_\ell(A) + \ell^{-n} W_0 \supseteq T_\ell(A)$$

Let $G_K \subseteq A[\ell^\infty]$ s.t. $G_K[\ell^n] \longleftrightarrow T_\ell(A) + \ell^{-n} W_0 / T_\ell(A)$

$$\rightsquigarrow T_\ell(A \xrightarrow{\pi_n} \underbrace{A/G_K[\ell^n]}_{\| \atop A_n}) \longleftrightarrow T_\ell(A) \subseteq T_\ell(A) + \ell^{-n} W_0$$

$A_n \leftarrow$ principally polarized

So Thm 1 + Thm 2 $\Rightarrow \exists$ an infinite subset $I \subseteq \mathbb{N}$ s.t.

$$(A_n, \lambda_n) \sim (A_{n_0}, \lambda_{n_0}) \quad \text{where } n_0 = \mathrm{Min}(I)$$

Pick $u_n : (A_{n_0}, \lambda_{n_0}) \xrightarrow{\sim} (A_n, \lambda_n) \quad \forall n \in I$

$$T_\ell(u_n) : T_\ell(A_{n_0}) = T_\ell(A) + \ell^{-n_0} W_0 \xrightarrow{\sim} T_\ell(A) + \ell^{-n} W_0$$

$$\rightsquigarrow T_\ell(\ell^{n-n_0}(u_n)) : T_\ell(A) + \ell^{-n_0} W_0 \xrightarrow{\sim} \ell^{n-n_0} T_\ell(A) + W_0 \qquad \forall n \in I$$

$$\updownarrow$$
$$T_\ell(A)$$

Pick $I' \subseteq I$ infinite s.t. $T_\ell(\ell^{n-n_0}(u_0)) \xrightarrow{\text{converges}} u \in \mathrm{Hom}(A_{n_0}, A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$

$$\rightsquigarrow u \cdot (T_\ell(A) + \ell^{-n_0} W_0) = W_0$$

$$\rightsquigarrow (u \circ \pi_{n_0}) \cdot V_\ell(A) = W$$

Let $u' = u \circ \pi_n \in \underset{\overset{\parallel}{E_\ell}}{\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell}$. Have $\underset{\overset{\parallel}{u' \cdot E_\ell \cdot V_\ell(A)}}{u' \cdot V_\ell(A)} = W$

$E = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a semisimple $\mathbb{Q}$-algebra $\rightsquigarrow$ E_ℓ is a semisimple $\mathbb{Q}_\ell$-alg.

$\rightsquigarrow$ $\exists$ idempotent $e \in E_\ell$ s.t. $u \cdot E_\ell = e \cdot E_\ell$

QED.

Note: Used Weil's result that $\mathrm{End}^\circ(A)$ is semisimple

Admit Thm 1 + Thm 2.

Prop 9B $(A, \lambda)_{/K}$ principally polarized $W \subseteq V_\ell(A)$ $\mathbb{Q}_\ell[\mathrm{Gal}(\bar{\mathbb{Q}}/K)]$-submodule

$\exists$ idempotent $e \in \mathrm{End}_K(A) \otimes \mathbb{Q}_\ell$ s.t. $e \cdot V_\ell(A) = W$

Pf: Pick $a, b, c, d \in \mathbb{Q}_\ell$ s.t. $a^2 + b^2 + c^2 + d^2 = -1$

(Existence: every nondeg. quad. form $/\mathbb{Q}_\ell$ in 5 variables represents 0)

Let $M = \mathbb{Q}_\ell^{\oplus 4}$, $\alpha = \begin{pmatrix} a & -b & -c & -d \\ b & a & d & -c \\ c & -d & a & b \\ d & c & -b & a \end{pmatrix} \in \mathrm{End}_{\mathbb{Q}_\ell}(M)$ $\quad \alpha \cdot {}^t\alpha = {}^t\alpha \cdot \alpha = -1_M$

Let $\langle \ , \ \rangle : T_\ell(A) \times T_\ell(A) \longrightarrow T_\ell(\mathbb{G}_m)$ be the ℓ-adic Weil pairing induced by the principal polarization λ

Consider $(A \otimes_{\mathbb{Z}} M) \times (A \otimes_{\mathbb{Z}} M)$, with principal polarization $(\lambda \otimes 1_M) \times (\lambda \otimes 1_M)$

$$V_\ell((A \otimes_{\mathbb{Z}} M) \times (A \otimes_{\mathbb{Z}} M)) = (V_\ell(A) \otimes_{\mathbb{Z}} M) \oplus (V_\ell(A) \otimes_{\mathbb{Z}} M)$$

Let $W_1 = \{(x, (1 \otimes \alpha)x) \mid x \in W \otimes_{\mathbb{Z}} M\} \oplus \{(y, -(1 \otimes \alpha)y) \mid y \in W^\perp \otimes_{\mathbb{Z}} M\}$

W_1 is a maximal isotropic subspace of $V_\ell((A \otimes_{\mathbb{Z}} M) \times (A \otimes_{\mathbb{Z}} M))$ (Exer.)

Prop 9A $\Longrightarrow$ $\exists\ u \in \mathrm{End}((A \otimes_{\mathbb{Z}} M) \times (A \otimes_{\mathbb{Z}} M)) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \cong \mathrm{End}_{\mathbb{Z}}(M \oplus M) \otimes_{\mathbb{Z}} \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$

s.t. $u \cdot (V_\ell(A) \otimes_{\mathbb{Z}} M \oplus (V_\ell(A) \otimes_{\mathbb{Z}} M)) = W_1$ $\quad \cong M_8(\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell)$

$\rightsquigarrow$ (post-composing with $\begin{array}{ccc} (V_\ell(A) \otimes M) \oplus (V_\ell(A) \otimes M) & \to & V_\ell(A) \otimes M \\ (x_1, \ x_2) & \longmapsto & (1 \otimes \alpha)x_1 + x_2 \end{array}$)

$q : M \twoheadrightarrow \mathbb{Z}$

$u_1, \ldots, u_m \in \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$ s.t. $W = \sum_{i=1}^m u_i V_\ell(A) = \underbrace{\left(\sum_{i=1}^m u_i \cdot \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell\right)}_{\text{a right ideal of } \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell} \cdot V_\ell(A)$

$\mathbb{Q}_\ell$-linear combination of

Let e be an idempotent in $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$ s.t. $e \cdot \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell = \sum_{i=1}^m u_i (\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell)$.

QED.

Prop 9B

$\Rightarrow$ Thm 3 $\forall$ abelian variety $A_{/K}$ K: a number field, ℓ: a prime number the $\mathbb{Q}_\ell[\mathrm{Gal}(\bar{\mathbb{Q}}/K)]$-module $V_\ell(A)$ is semisimple.

Exer G: a group $N \trianglelefteq G$, $[G:N]<\infty$. $\rho: G \to GL_F(V)$
F: a field of characteristic 0 (or, $[G:N]\cdot 1_F \in F^\times$) V: finite dim$^{\ell}$ vector space$/F$
$\rho|_N$: semisimple. Then ρ is semisimple

Proof of Thm 4 Suffices to show:

$$C = \mathrm{End}_{\mathrm{End}(A)\otimes\mathbb{Q}_\ell}(V_\ell(A)) = \mathrm{End}_{\mathbb{Q}_\ell[\mathrm{Gal}(\bar{\mathbb{Q}}/K)]}(V_\ell(A))$$
($\supseteq$ always)

Idea: Encode an element $\beta \in \mathrm{Image}(\mathbb{Q}_\ell[\mathrm{Gal}(\bar{\mathbb{Q}}/K)] \to \mathrm{End}_{\mathbb{Q}_\ell} V_\ell(A)) = F_\ell$
in its graph $\Gamma_\beta = \{(x, \beta(x)) \mid x \in V_\ell(A)\} \subseteq V_\ell(A)\times V_\ell(A)$

Embed C diagonally in $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A)\oplus V_\ell(A)) \cong M_2(\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A)))$
$\quad\|$
commutator of $\mathrm{End}(A\times A)\otimes_{\mathbb{Z}}\mathbb{Q}_\ell \cong M_2(\mathrm{End}(A)\otimes_{\mathbb{Z}}\mathbb{Q}_\ell)$

Γ_β is stable under the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$

$\Longrightarrow \exists\, u \in M_2(\mathrm{End}(A)\otimes_{\mathbb{Z}}\mathbb{Q}_\ell)$ s.t. $u\cdot(V_\ell(A)\oplus V_\ell(A)) = \Gamma_\beta$

$\rightsquigarrow \forall w \in C$, have $w\,\Gamma_\beta = w\cdot u\,(V_\ell(A)\oplus V_\ell(A)) = u w\,(V_\ell(A)\oplus V_\ell(A))$
$\subseteq u\cdot(V_\ell(A)\oplus V_\ell(A)) = \Gamma_\beta$

This means: $\beta(wx) = w\beta(x)$ $\forall x\in V_\ell(A)$ $\forall w \in C$, $\forall \beta\in F_\ell$
i.e. $C \subseteq \mathrm{End}_{F_\ell}(V_\ell(A))$ Q.E.D.

Theorem 5A on p. 2 + Thm 3 + Thm 4 $\Longrightarrow$ Thm 5

Remark: $A_{/\mathcal{O}_K}$ semiabelian $A_K \xrightarrow{\phi} B_K$ isogeny $d = \deg(\phi)$ $G = \mathrm{Ker}(A_{/\mathcal{O}_K} \to B_{/\mathcal{O}_K})$

Then $\exp(2[K:\mathbb{Q}]\cdot(h(B)-h(A))) = \deg(\phi)^{[K:\mathbb{Q}]}\cdot \#\,\varepsilon^*(\Omega^1_{G/\mathcal{O}_K})^{-2}$
is a rational number. Moreover $\forall$ prime number ℓ,

$$\left|\mathrm{ord}_\ell(2[K:\mathbb{Q}]\cdot(h(B)-h(A)))\right| \leq \mathrm{Max}([K:\mathbb{Q}]\,\mathrm{ord}_\ell d,\ 2[K:\mathbb{Q}]\cdot\dim(A)\cdot\mathrm{ord}_\ell(d))$$
$$= 2[K:\mathbb{Q}]\cdot\dim(A)\cdot\mathrm{ord}_\ell(d)$$

(Very inefficient bound)

Consequence If $T_\ell(A)\cong T_\ell(B)$ as $\mathbb{Z}_\ell[\mathrm{Gal}(\bar{\mathbb{Q}}/K)]$-modules,
$\exp(2[K:\mathbb{Q}]\cdot(h(B)-h(A))) \in \mathbb{Z}_{(\ell)}$

Thm 6

Proof of Shafarevich Conj

Given K, $S \underset{\text{finite}}{\subseteq} M_{K,f}$, $g \geq 1$, $d \geq 1$

$\mathcal{S} = \left\{ \begin{array}{l} \text{isom. classes of } g\text{-dim}^{\ell}\ (A,\lambda)_{/K},\ \deg(\lambda)=d \\ \text{with good reduction outside } S \end{array} \right\} < \infty$

Reductions: (i) After base change to a Galois ext^n field $L_{/K}$ unramified outside $S' = \tilde{S} \cup \{\text{places of } L \text{ above } 2 \text{ or } 3\}$, with $[L:K] \leq 4^{2g} \cdot 3^{2g}$, A_L has semistable reduction outside S'

⇝ Hermite-Minkowski + descent may assume A has semistable reduction$/\mathcal{O}_K$

(ii) After a base change to an extension field $L_{1/K}$ which is unramified at all places prime to d, with $[L_1 : K] \leq d$. $\exists$ isogeny $A_{L_1} \to B_{L_1}$ s.t. λ_{L_1} descends to a principal polarization over L_1

⇝ Suffices to prove the case when $d=1$. May assume $d=1$

By Thm 4, there are only a finite number isogeny classes among the prin. polarized abelian varieties in $\mathcal{S}$.

Suffices to show: $\forall [(A,\lambda)] \in \mathcal{S}$, $\#\{[(B,\mu)] \in \mathcal{S} \mid B \text{ is isogenous to } A\} < \infty$

Will show: $\exists$ a constant $C > 0$ s.t. $|h(B) - h(A)| < C$ $\forall [(B,\mu)] \in \mathcal{S}$

Let $Q_1 \subseteq \{\text{prime numbers}\}$ be the following finite set of prime numbers

$Q_1 = \{q : \exists v \in M_K,\ v|\ell, \text{ s.t. } K_v \text{ is ramified over } \mathbb{Q}_\ell\}$
$\quad \cup \{q : \exists v \in M_K,\ v|\ell, \text{ s.t. } A_{K_v} \text{ has bad reduction at } v\}$

Pick $p \notin Q_1$. $\forall h$ with $0 \leq h \leq 2[K:\mathbb{Q}] \cdot \dim(A)$. $\forall \ell \notin \{p\} \cup Q_1$

$$P_h(T) = \det\Big(T - \underset{\text{arith. Frob}}{Fr_p} \,\Big|\, \Lambda^h \operatorname{Ind}_{Gal(\bar{\mathbb{Q}}/K)}^{Gal(\bar{\mathbb{Q}}/\mathbb{Q})}(T_\ell(A))\Big) \in \mathbb{Z}[T], \text{ indep. of } \ell$$

Every root of $P_h(T)$ has cpx abs. values $p^{\frac{h}{2}}$

Let $Q_2 = \left\{ q \text{ prime} : q \,\Big|\, \prod_{\substack{0 \leq h \leq 2[K:\mathbb{Q}]\dim(A) \\ 0 \leq j \leq [K:\mathbb{Q}]\dim(A) \\ j \neq \frac{1}{2}h}} P_h(j) \cdot P_h(-j) \right\}$

Let $Q = \prod_{q \in Q_1 \cup Q_2} q$

Claim 1: $\exists$ a constant C_1 s.t. $\forall [(B,\mu)] \in \mathcal{S}$ $\forall q \in Q$,
$\left|\operatorname{ord}_\ell\big(2[K:\mathbb{Q}] \cdot (h(B) - h(A))\big)\right| \leq C_1$

Claim 1 follows from:

Lemma 1 $\{\text{isomorphism classes of } \mathbb{Q}_q[Gal(\bar{\mathbb{Q}}/K)]\text{-stable lattices in } V_q(A)\} < \infty$

$\Uparrow$

$R_q := \operatorname{Im}\big(\mathbb{Z}_q[Gal(\bar{\mathbb{Q}}/\mathbb{Q})] \to \operatorname{End}_{\mathbb{Z}_q} T_q(A)\big)$ is an order in the semisimple alg $R_q \otimes_{\mathbb{Z}_q} \mathbb{Q}_\ell$. is contained in a maximal order $\tilde{R}_q$ in $R_q \otimes_{\mathbb{Z}_q} \mathbb{Q}_\ell$

+ Fact: Any two $\tilde{R}_q$-stable sublattices in $V_q(A)$ are isomorphic

(Consequence of Thm 18.7(i) of Reiner, Maximal Orders, p.179)

Note: Thm. 18.7(i) of Reiner says:
Let $\mathcal{O}_D$ be a maximal order in a fin. dim$^{\ell}$ central simple algebra D over a complete discretely valued field k. Let M_1 and M_2 be two left $\mathcal{O}_D$-modules which are finite free over $\mathcal{O}_k$. If $\mathrm{rk}_{\mathcal{O}_k} M_1 = \mathrm{rk}_{\mathcal{O}_k} M_2$, then $M_1 \cong M_2$ as $\mathcal{O}_D$-modules

$\rightsquigarrow$ Given any R_q-stable lattice $M \leq V_q(A)$, $[\tilde{R}_q \cdot M : M] \leq [\tilde{R}_q : R_q] \cdot 2\dim(A) \cdot q^{[K:\mathbb{Q}]}$

Claim 2 $\forall [(B,\mu)] \in \mathcal{S}$, $\mathrm{ord}_\ell\left(2[K:\mathbb{Q}]\cdot(h(B)-h(A))\right) = 0 \quad \forall \ell \notin Q$

Suffices to show: $\forall$ subgroup $G_K \leq A_K[\ell]$, $\mathrm{ord}_q\left(2[K:\mathbb{Q}]\cdot(h(A)-h(A/G))\right) = 0$

Let $G_{/\mathcal{O}_K}$ = Zariski closure of G in $A_{/\mathcal{O}}$, $\#G = \ell^h$

$$h(A_K/G_K) - h(A) = \frac{h}{2}\log \ell - \frac{1}{[K:\mathbb{Q}]}\log\underbrace{(\#\varepsilon^*\Omega^1_{G/\mathcal{O}_K})}_{\ell^{\sum_{i=1}^{r}[K_{v_i}:\mathbb{Q}_\ell]\cdot\dim(G_{v_i})}}$$

$\{v_1,\dots,v_r\}$ = places of K above ℓ

Let
$$U_\ell = \ell^{-1}T_\ell(A)/T_\ell(A)$$
$$\cup\!|$$
$$W_\ell = G(\bar{K})$$
Considered as representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$ on $\mathbb{F}_\ell$-vector spaces
$$\tilde{W}_\ell = \mathrm{Ind}_{\mathrm{Gal}(\bar{\mathbb{Q}}/K)}^{\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})} W_\ell \subseteq \mathrm{Ind}_{\mathrm{Gal}(\bar{\mathbb{Q}}/K)}^{\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})} U_\ell$$

Raynaud: The decomposition group $D_{K_{v_i}}$ on W_ℓ via $\chi_{\mathrm{cycl},\mathbb{F}_\ell}^{\dim(G_{v_i})}$

$\rightsquigarrow$ The decomposition group $D_\ell \leq \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ operates on $\Lambda^{[K:\mathbb{Q}]\cdot h}\tilde{W}_\ell$

via $\left(\chi_{\mathrm{cycl},\mathbb{F}_\ell}^{\sum_{i=1}^{r}[K_{v_i}:\mathbb{Q}_\ell]\cdot\dim(G_{v_i})}\cdot\varepsilon^h\right)\Big|_{D_\ell}$

where $\varepsilon = \det(\mathrm{Ind}_{\mathrm{Gal}(\bar{\mathbb{Q}}/K)}^{\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})}\mathbb{Z}) : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \{\pm 1\}$

Let $\chi = \det(\tilde{W}_\ell) : \mathrm{Gal}(\bar{\mathbb{Q}}/K) \longrightarrow \mathbb{F}_\ell^\times$

χ is unramified outside ℓ $\because$ A has semiabelian reduction over $\mathcal{O}_K$

$\rightsquigarrow$ $\chi = \varepsilon^h \cdot \chi_{\mathrm{cycl},\mathbb{F}_\ell}^{\sum_{i=1}^{r}[K_{v_i}:\mathbb{Q}_\ell]\cdot\dim(G_{v_i})}$

Weil conj $\Rightarrow$ $\varepsilon(\mathrm{Fr}_p)^h \cdot p^{\sum_{i=1}^{r}[K_{v_i}:\mathbb{Q}_\ell]\dim(G_{v_i})}$ is a root of $P_h(T)$ mod ℓ

(Fr_p: arith. Frob)

Since $\ell \notin Q_2$, we conclude that $\frac{h}{2} = \sum_{i=1}^{r}[K_{v_i}:\mathbb{Q}_\ell]\cdot\dim(G_{v_i})$.

We have proved claim 2. Claim 1 + Claim 2 $\Rightarrow$ $\#\mathcal{S} < \infty$

QED

Motivation for studying "finite flat p-group schemes of CM type" $\leftarrow$ of type $(p\ldots p)$

Lemma Let K be a local field of char. $(0,p)$ with alg. closed residue field.
Let $\rho: \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}_{gp}(G)$ be a homomorphism, where G is a finite p-group. Suppose that ρ is irreducible. Then
(i) G is killed by p and ρ is tamely ramified ($\because$ wild ramification gp is pro-p)
(ii) $\exists$ a finite field F s.t. G has a structure as a 1-dim^{l} F-vector space, and ρ factors through a homomorphism $\mathrm{Gal}(\bar{K}/K) \to F^\times \subseteq \mathrm{Aut}_{gp}(G)$

Set-up: $q=p^r, r\geq 1$

$\mathbb{Q}(\mu_{q-1})$ unramified above p $\mathfrak{f}$ $\kappa_{\mathfrak{f}} = \mathcal{O}_{\mathfrak{f}}/\mathfrak{f}$ $[\kappa_{\mathfrak{f}}:\mathbb{F}_p]=r$

$\mathbb{Q}$ $r \mid \varphi(q-1)$ p

Let $D = \Gamma(\mathrm{Spec}(\mathcal{O}_{\mathbb{Q}(\mu_{q-1})}) - \{\mathfrak{f}\}, \mathcal{O}_{\mathrm{Spec}(\mathcal{O}_{\mathbb{Q}(\mu_{q-1})})})[\frac{1}{q-1}]$

Thus: D is a Dedekind domain $D[\frac{1}{p}]$ finite over $\mathbb{Z}[\frac{1}{p(q-1)}]$
D has exactly one prime ideal $\mathfrak{f}$ above p. $[\kappa(\mathfrak{f}):\mathbb{F}_p]=r$

F: a finite field, $\cong \mathbb{F}_{p^r}$

Def: A character $F^\times \xrightarrow{\chi} \mu_{q-1} \subseteq D^\times$ is a fundamental character if the extension by 0 of the composition $F^\times \xrightarrow{\chi} \mu_{q-1} \hookrightarrow D^\times \to \kappa(\mathfrak{f})^\times$ is a ring isomorphism

$$\begin{array}{ccc} F^\times & \xrightarrow{\chi} \mu_{q-1} \hookrightarrow D^\times \longrightarrow & \kappa(\mathfrak{f})^\times \\ \cap & & \cap \\ F & \longrightarrow & \kappa(\mathfrak{f}) \end{array}$$

Lemma (i) There are exactly r fundamental characters
(ii) If χ is a fundamental character, then χ^{p^i} is a fundamental character $\forall i \in \mathbb{Z}$, $\chi^{p^i} = \chi^{p^j}$ iff $i \equiv j \pmod r$
(iii) The set J of all fundamental characters from $F^\times$ to $\mu_{q-1} \subseteq D^\times$ has a natural structure as a $(\mathbb{Z}/r\mathbb{Z})$-torsor

Notation Let $(\chi_j)_{j\in J}$ be the set of all fundamental characters.
Then every character can be written in the form $\prod_{j\in J} \chi_j^{a_j}$
$0 \leq a_j \leq r-1$ $\forall j \in J$, unique except $\mathbb{1} = \prod_{j\in J}\chi_j^p = \prod_{j\in J}\chi_j^0$

Equivalent statement: Every character $F^\times \to \mu_{q-1}$ can be written in a unique way in the form $\prod_{j\in J} \chi_j^{p^{a_j}}$,
where $0\leq a_j \leq p-1$ $\forall j \in J$, and not all a_j are equal to $p-1$

(This is a form of p-adic expansion of elements of $\mathbb{Z}/(q-1)\mathbb{Z}$)

$n \equiv \sum_{0\leq i\leq r-1} a_i p^i \pmod{p^r-1}$
$\mathbb{Z}/(q-1)\mathbb{Z}$

If $\chi' = \prod_{j\in J}\chi_j^{a_j'}$, $\chi'' = \prod_{j\in J}\chi_j^{a_j''}$ $0\leq a_j' \leq p-1$ $\forall j$, not all $=p-1$, same for a_j''
and $\chi'\cdot\chi'' = \chi_{j_0}$. Then $\exists! h$, $1\leq h\leq r$ s.t. $a'_{j_0 h} + a''_{j_0 h} = p$, $a'_{j_0-i} + a''_{j_0-i} = p-1$ for $1\leq i\leq h-1$
all other a_j', a_j'''s $=0$

Remark. $\{\chi_j \mid j\in J\}$ $\subseteq \{$ fundamental characters $F^\times \to \mu_{q-1}(D)\}$ provides a "p-adic coordinate system for $M = \mathrm{Hom}_{grp}(F^\times, \mu_{q-1}(D))$

Note: Let χ be a fund char. of $F^\times \to \mu_{q-1}(D)$.
Then χ is a primitive character, i.e. $M = \chi^{\mathbb{Z}}$. Moreover every primitive character is of the form $\chi\circ\varphi$, $\varphi \in \mathrm{Aut}_{grp}(F^\times)$; $\chi\circ\varphi$ is fundamental iff $\varphi\in \mathrm{Aut}_{ring}(F^\times)$

Consider Base scheme: $S_{/\mathrm{Spec}(D)}$ $\quad q = p^r \quad D = \mathcal{O}_{\mathbb{Q}(\mu_{q-1})}[\frac{1}{p(q-1)}]\cap \mathcal{O}_{\mathfrak{p}}$ $\quad \mathfrak{p}$ = a fixed prime ideal of $\mathcal{O}_{\mathbb{Q}(\mu_{q-1})}$ above p

s.t. $S \times_{\mathrm{Spec}(D)} \mathrm{Spec}(\mathbb{Q}(\mu_{q-1}))$ is dense in S

Outline: $(G_{/S},\ F \to \mathrm{End}_S(G))$, G/S finite locally free, $\mathrm{rk}(G) = p^r$

1. Use the $F^\times$-action to decompose the augmentation ideal $\mathcal{I}$ of $\mathcal{O}_G$ and the augmentation ideal $\mathcal{I}'$ of $\mathcal{O}_{G^D}$, and analyze the multiplication and comultiplication maps on $\mathcal{I}_\chi$ and $\mathcal{I}'_\chi$'s, $\chi\in M$

"Most of the "structural constants" of G are independent of G, given by Jacobi sums (for F)

"What determines G are

$$c_j = c_{\underbrace{\chi_j,\dots,\chi_j}_{p}} : \mathcal{I}_{\chi_j^p=\chi_{j+1}} \longrightarrow \underbrace{\mathcal{I}_{\chi_j}\otimes\cdots\otimes\mathcal{I}_{\chi_j}}_{p} = \mathcal{I}_{\chi_j}^{\otimes p} \qquad j\in J \text{ fund. char.}$$

$$d_j = d_{\underbrace{\chi_j,\dots\chi_j}_{p}} : \mathcal{I}_{\chi_j}^{\otimes p} \longrightarrow \mathcal{I}_{\chi_j^p=\chi_{j+1}}$$

$$d_j\circ c_j = w_j = w_{\underbrace{\chi_j,\dots\chi_j}_{p}} = w \quad \text{indep. of } j\in J$$

$$w\in D_1 = D\cap \mathbb{Q}(\mu_{q-1})^{\mathrm{Fr}_p}. \qquad w\equiv p! \pmod{p^2},\ w = pu,\ u\equiv -1 \pmod p$$

Classification theorem:

$$G \longmapsto \left(\mathcal{I}_{\chi_j},\ c_j: \mathcal{I}_{\chi_{j+1}} \to \mathcal{I}_{\chi_j}^{\otimes p},\ d_j: \mathcal{I}_{\chi_j}^{\otimes p} \to \mathcal{I}_{\chi_{j+1}};\ j\in J\right)$$

defines a bijection between

$\left\{\begin{array}{l}\text{isom. classes of commutative}\\ \text{group schemes finite locally}\\ \text{free of rk } p^r \text{ over } S \text{ with}\\ \text{multiplication by } S\end{array}\right\} \longrightarrow$ isom. classes of $\left\{\begin{array}{l}\text{systems } (\mathcal{I}_{\chi_j}, c_j, d_j)_{j\in J}\\ \text{of invertible } \mathcal{O}_S\text{-modules} + \mathcal{O}_S\text{-linear maps}\end{array}\right\}$

$\chi' = \prod_j \chi_j^{a_j}$, $\chi'' = \prod_j \chi_j^{a_j'}$, $0\le a_j, a_j' \le p-1$
$h = \#$ of carries in $\chi'\cdot\chi'' = \chi$
$h(\chi',\chi'')$

Local eq^n: $(X_j^p = \delta_j X_{j+1})_{j\in J}$ $\quad$ comultiplication:

$$c(X_j) = X_j\otimes 1 + 1\otimes X_j + \sum_{\chi'\cdot\chi''=\chi_j} \frac{\delta_{j+h}\cdots\delta_{j-1}}{w_{\chi'}\cdot w_{\chi''}}\cdot\left(\prod_{j\in J} X_j^{a_j}\right)\otimes\left(\prod_{j\in J} X_j^{a_j'}\right)$$

Remark
Generalities on extending a commutative finite group schemes G over $K = \mathrm{frac}(R)$, R = a discrete valuation of mixed char $(0,p)$, to a finite flat commutative group scheme over R

Lemma: Suppose that $\underset{\mathcal{F}}{=} \{ \mathcal{G} :$ finite flat comm group schemes over R s.t. $\underset{= G}{\mathcal{G} \times_{\mathrm{Spec}(R)} \mathrm{Spec}(K)} \}$ is $\neq \phi$, then $\mathcal{F}$ has a unique maximal element and a unique minimal element

2. Careful analysis of the classification result in 1 — R = discrete valuation ring of mixed char. $(0,p)$, $K = \mathrm{Frac}(R)$

Proposition $G_{/K}$ F-vector scheme over K, order $= p^r$

Assume that $G_{/K}$ admits an extension to a finite flat F-vector scheme $/R$

Note: Every extension $\mathcal{G}$ of G corresponds to a system $(\gamma_j, \delta_j)_{j \in J}$ of elements in R s.t. $\gamma_j \cdot \delta_j = w$ $\forall j \in J$.

and $(\gamma_j', \delta_j')_{j\in J}$ corresponds to an isomorphic F-vector scheme over R iff $\exists\, u_j \in R^\times$, $j \in J$, $\delta_j' u_{j+1} = \delta_j u_j^p$ $\forall j \in J$

(1) The maximal extension $\mathcal{G}^+$ of G is characterized by

$$v(\delta_j) \le p-1 \quad \forall j \in J \quad \text{and} \quad \exists j \text{ with } v(\delta_j) < p-1$$

Dually, the minimal ext^n $\mathcal{G}^-$ of G is characterized by

$$v(\delta_j) \geq e-p+1 \quad \forall j \in J, \quad \text{and} \quad \exists j \text{ with } v(\delta_j) > e-p+1$$

(2) Suppose that $e \le p-2$. Then there is a unique ext^n $\mathcal{G}$ of G

(3) Suppose that $e = p-1$, R is henselian, and $G_{/K}$ is simple
Then either $\mathcal{G}^+ = \mathcal{G}^-$ (i.e. there is a unique ext^n of G to a finite flat group scheme over R, and the F-vector scheme structure extends)
or $\mathcal{G}^+$ is étale, $\mathcal{G}^-$ is multiplicative, and these are the only finite flat extensions of $(G, F \to \mathrm{End}_{grp}(G))$ to R

Cor. Suppose that R is strictly henselian d.v.r with mixed char. $(0,p)$ $e \le p-1$. Let $\mathcal{G}$ be a comm finite flat group scheme over R killed by some power of p. Then $\mathcal{G}$ admits a composition series s.t. each successive quotient has a structure as a F-vector scheme of CM type for some suitable finite field $F \supseteq \mathbb{F}_p$

Recall: $D = \mathcal{O}_{\mathbb{Q}(\mu_{p^r-1})}[\frac{1}{p}] \cap \mathcal{O}_{\mathfrak{q}}$ $\quad \mathfrak{q} \subseteq \mathcal{O}_{\bar{\mathbb{Q}}(\mu_{q-1})}$ prime ideal above p $\quad F \cong \mathbb{F}_q \quad q = p^r$

$G/_S$ finite locally free commutative group scheme, with $F \to \mathrm{End}_{grp}(G)$ and $\mathrm{order}(G) = p^r$

$S \to D \qquad S \times_{\mathrm{Spec}\, D} \mathrm{Spec}(\mathcal{O}_{\mathbb{Q}(\mu_{q-1})}) \underset{\text{dense}}{\subseteq} S$

$G = \underline{\mathrm{Spec}}_S(A), \qquad G^D = \underline{\mathrm{Spec}}_S(A') \qquad A' = \underline{\mathrm{Hom}}_{\mathcal{O}_S}(A, \mathcal{O}_S)$

$\varepsilon^* : A \to \mathcal{O}_S$ zero section of G, $\mathcal{I} = \mathrm{Ker}(\varepsilon^*)$ augmentation ideal $\rightsquigarrow A = \mathcal{I} \oplus \mathcal{O}_S$

$\forall \chi \in M \quad i_\chi = \frac{1}{q-1} \sum_{\lambda \in F^\times} \chi^{-1}(\lambda) [\lambda]^*$ endomorphism of A $\qquad M = \mathrm{Hom}_{grp}(F^\times, \mu_{q-1})$

$\underset{F^\times}{[\mu]^*} i_\chi(f) = \frac{1}{q-1} \sum_{\lambda \in F^\times} \chi^{-1}(\lambda\mu)\, \chi(\mu) [\lambda\mu]^* = \chi(\mu)\, i_\chi(f) \quad \forall f \in A, \forall \mu \in F^\times$

$i_\chi^{\,2} = \frac{1}{(q-1)^2} \sum_{\lambda, \mu \in F^\times} \chi^{-1}(\lambda\mu) [\lambda\mu]^* = \frac{1}{q-1} \sum_{\nu \in F^\times} [\nu]^* = i_\chi$

$\chi' \neq \chi'' \rightsquigarrow i_\chi \circ i_{\chi'} = \frac{1}{(q-1)^2} \sum_{\lambda, \mu \in F^\times} (\chi')^{-1}(\mu)\, (\chi'')^{-1}(\nu)\, [\mu\nu]^* = 0$

$\because \sum_{t \in F^\times} (\chi')^{-1}(\mu t)\, (\chi'')^{-1}(t^{-1}\nu) = (\chi')^{-1}(\mu) \cdot (\chi'')^{-1}(\nu) \cdot \sum_{t \in F^\times} (\chi'' \cdot \chi'^{-1})(t) = 0$

$\rightsquigarrow \mathcal{I}_\chi \overset{\text{def}}{=} \mathrm{Im}(\mathcal{I} \xrightarrow{i_\chi} \mathcal{I}) \qquad \mathcal{I} = \bigoplus_{\chi \in M} \mathcal{I}_\chi$

$G \times_S S_{\mathbb{Q}(\mu_{q-1})}$ étale $\Rightarrow \mathcal{I}_\chi$ is an invertible $\mathcal{O}_S$-module $\forall \chi \in M$

The multiplication $A \otimes_{\mathcal{O}_S} A \xrightarrow{d} A$ and comultiplication $A \xrightarrow{c} A \otimes_{\mathcal{O}_S} A$ are determined by their eigen-component

$$d_{\chi', \chi''} : \mathcal{I}_{\chi'} \otimes_{\mathcal{O}_S} \mathcal{I}_{\chi''} \longrightarrow \mathcal{I}_{\chi', \chi''} \quad \text{and} \quad c_{\chi', \chi''} : \mathcal{I}_{\chi' \cdot \chi''} \longrightarrow \mathcal{I}_{\chi'} \otimes \mathcal{I}_{\chi''} \qquad \chi', \chi'' \in M$$

Better: For $\chi_1, \dots, \chi_n \in M$, have iterated

$$d_{\chi_1, \dots, \chi_n} : \mathcal{I}_{\chi_1} \otimes_{\mathcal{O}_S} \cdots \otimes_{\mathcal{O}_S} \mathcal{I}_{\chi_n} \longrightarrow \mathcal{I}_{\prod_{i=1}^n \chi_i} \quad \text{and} \quad c_{\chi_1, \dots, \chi_n} : \mathcal{I}_{\prod_{i=1}^n \chi_i} \longrightarrow \mathcal{I}_{\chi_1} \otimes_{\mathcal{O}_S} \cdots \otimes_{\mathcal{O}_S} \mathcal{I}_{\chi_n}$$

associativity of d and c

For $\chi' = \chi_1' \cdots \chi_n'$, $\chi'' = \chi_1'' \cdots \chi_m''$, $\chi_1', \dots, \chi_n', \chi_1'', \dots, \chi_m'' \in M$

$$\begin{cases} c_{\chi_1', \dots, \chi_n', \chi_1'', \dots, \chi_m''} = (c_{\chi_1', \dots, \chi_n'} \otimes c_{\chi_1'', \dots, \chi_m''}) \circ c_{\chi', \chi''} \\ d_{\chi_1', \dots, \chi_n', \chi_1'', \dots, \chi_m''} = d_{\chi', \chi''} \circ (d_{\chi_1', \dots, \chi_n'} \otimes d_{\chi_1'', \dots, \chi_m''}) \end{cases} \qquad \text{associativity}$$

<u>Def^n</u> $\forall \chi_1, \dots, \chi_n \in M$, define $w_{\chi_1, \dots, \chi_n} \in \Gamma(S, \mathcal{O}_S)$ by

$$w_{\chi_1, \dots, \chi_n} = d_{\chi_1, \dots, \chi_n} \circ c_{\chi_1, \dots, \chi_n} \in \mathrm{Hom}(\mathcal{I}_{\prod_{i=1}^n \chi_i}, \mathcal{I}_{\prod_{i=1}^n \chi_i}) = \Gamma(S, \mathcal{O}_S)$$

The above associativity gives:

$$w_{\chi_1', \dots, \chi_n', \chi_1'', \dots, \chi_m''} = w_{\chi', \chi''}\, w_{\chi_1', \dots, \chi_n'} \cdot w_{\chi_1'', \dots, \chi_m''} \qquad \text{with } \chi' = \chi_1' \cdots \chi_n', \ \chi'' = \chi_1'' \cdots \chi_m''$$

Since $\exists\ T \xrightarrow[\text{finite étale}]{} S_{\mathbb{Q}(\mu_{q-1})}$ s.t $G \times_S T$ is constant, compatibility of the $w_{\chi_1,\dots,\chi_n}$'s with arbitrary base chang implie

Lemma: $w_{\chi_1,\dots,\chi_n} \in D \quad \forall \chi_1,\dots,\chi_n \in M$

Consider
$$\begin{tikzcd} G\times G \arrow[r, "{[\lambda]\times[\mu]}"] & G\times G \arrow[d, "\mu_G"] \\ G \arrow[u, "\Delta"] \arrow[r, "{[\lambda+\mu]}"] & G \end{tikzcd} \quad \forall \lambda,\mu\in F \quad \rightsquigarrow \quad [\lambda+\mu]^* = d\circ([\lambda]^*\otimes[\mu]^*)\circ c$$

Apply this to $\mathcal{I}_\chi$ to get:

$$\chi(\lambda+\mu) = \chi(\lambda)+\chi(\mu)+\sum_{\substack{\chi',\chi''\in M\\ \chi'\cdot\chi''=\chi}} \chi'(\lambda)\cdot\chi''(\mu)\cdot w_{\chi',\chi''} \qquad \forall \lambda,\mu\in F$$

when $\lambda+\mu=0$, $\chi(\lambda+\mu)=0$ by convention

Let $\chi_1,\chi_2\in M$ with $\chi_1\cdot\chi_2=\chi$, multiply both sides of above equation by $\chi_1^{-1}(\lambda)\,\chi_2^{-1}(\mu)$ and sum over λ,μ to get

$$\sum_{\lambda,\mu\in F^\times} \chi_1^{-1}(\lambda)\,\chi_2^{-1}(\mu)\,\chi(\lambda+\mu) \overset{\chi=\chi_1\cdot\chi_2}{=} \sum_{\lambda,\mu\in F^\times}\left(\chi_2(\lambda\mu^{-1})+\chi_1(\mu\lambda^{-1})\right) + (q-1)^2 w_{\chi_1,\chi_2}$$

$\big\Vert$ $\lambda=ut$, $\mu=vt$, $u+v=1$

$$(q-1)\sum_{\substack{u+v=1\\u,v\in F^\times}} \chi_1^{-1}(u)\,\chi_2^{-1}(v) \qquad = (q-1)\sum_{t\in F^\times}\left(\chi_1(t)+\chi_2(t)\right) + (q-1)^2 w_{\chi_1,\chi_2}$$

$$(q-1)\,w_{\chi_1,\chi_2} = \sum_{\substack{u+v=1\\u,v\in F^\times}} \chi_1^{-1}(u)\,\chi_2^{-1}(v) - \sum_{t\in F^\times}\left(\chi_1(t)+\chi_2(t)\right)$$

Explicitly:

1) If $\chi_1\neq \mathbb{1}\neq\chi_2$, then
$$w_{\chi_1,\chi_2} = \frac{1}{q-1}\sum_{u+v=1}\chi_1^{-1}(u)\,\chi_2^{-1}(v) = \frac{(\chi_1\chi_2)(-1)}{q-1}\sum_{z+w+1=0}\chi_1^{-1}(z)\,\chi_2^{-1}(w) = \frac{(\chi_1\cdot\chi_2)(-1)}{q-1}\,j(\chi_1^{-1},\chi_2^{-1})$$

(Recall def^n of Jacobi sum for the finite field F
$$j(\chi,\chi') = \sum_{\substack{z+w+1=0\\ z,w\in F^\times}} \chi(z)\,\chi(w)\ )$$

2) $\chi_1=\mathbb{1},\ \chi_2=\chi\neq\mathbb{1}$
$$w_{1,\chi}=w_{\chi,1}=\frac{1}{q-1}\left[\sum_{\substack{u+v=1\\u\in F^\times}}\chi^{-1}(v) - (q-1)\right] = -\frac{q}{q-1}$$

3) $\chi_1=\chi_2=\mathbb{1}$
$$w_{1,1} = \frac{1}{q-1}\left((q-2)-2(q-1)\right) = -\frac{q}{q-1}$$

Notation / definition

(a) For $\chi = \prod_{j\in J} \chi_j^{a_j}$ $\quad 0 \le a_j \le p-1$ $\quad a_j$'s not all equal to 0

define $\quad c_\chi = c_{\underbrace{\chi_{j_0}\cdots\chi_{j_0}}_{a_{j_0}},\ \underbrace{\chi_{j_0+1},\cdots\chi_{j_0+1}}_{a_{j_1}},\ \dots,\ \underbrace{\chi_{j_0+r-1},\cdots\chi_{j_0+r-1}}_{a_{j_0+r-1}}} : \mathcal{I}_\chi \longrightarrow \bigotimes_{j\in J} \mathcal{I}_{\chi_j}^{\otimes a_j}$

Similarly have $\quad d_\chi : \bigotimes_{j\in J} \mathcal{I}_{\chi_j}^{\otimes a_j} \longrightarrow \mathcal{I}_\chi$

$$w_\chi := d_\chi \circ c_\chi \quad \in \Gamma(S, \mathcal{O}_S)$$

(b) $\forall$ fundamental character χ_j, $j \in J$.

let $\quad c_j = c_{\underbrace{\chi_j,\dots,\chi_j}_{p}} : \mathcal{I}_{\chi_{j+1}} \longrightarrow \mathcal{I}_{\chi_j}^{\otimes p}, \qquad d_j = d_{\underbrace{\chi_j,\dots,\chi_j}_{p}} : \mathcal{I}_{\chi_j}^{\otimes p} \longrightarrow \mathcal{I}_{\chi_{j+1}}$

$$w_j = d_j \circ c_j \quad \in \Gamma(S, \mathcal{O}_S)$$

As already remarked, $w_{\chi_1,\dots,\chi_n}$ can be computed from the generic fiber of G, which is étale over $S_{\mathbb{Q}(\mu_{q-1})}$. Therefore the structural constants $w_{\chi_1,\dots,\chi_n}$. Thus one can compute these structural constants $w_{\chi_1,\dots,\chi_n}$ in the case of $G = (F,+)_{/\mathbb{Q}(\mu_{q-1})}$, which is isomorphic to G^D over $\mathbb{Q}(\mu_{q-1})$

In this case, pick a nontrivial additive character $\psi : (F,+) \longrightarrow \mu_p$

$\left(\text{e.g. } (F,+) \xrightarrow{\mathrm{Tr}_{F/\mathbb{F}_p}} (\mathbb{F}_p,+) \longrightarrow \mu_p \right)$
$\qquad\qquad a \bmod p \longmapsto \zeta_p^a$

ψ defines a isomorphism $\quad \underline{(F,+)}_{\mathbb{Q}(\mu_p)} \xrightarrow{\varphi} \underline{(F,+)}^D_{\mathbb{Q}(\mu_p)} \quad$ over $\mathbb{Q}(\mu_{q-1})$

$$a \longmapsto a\cdot\psi \qquad \forall a \in F$$

On A,
$[\lambda]^*\delta_a = \delta_{\lambda^{-1}a}$
$\forall \lambda \in F^\times$
$[0]^*\delta_a = 0$
$\forall a \in F^\times$

$$A = \left\{ \begin{matrix} \mathbb{Q}(\mu_p)\text{-valued} \\ \text{functions on } F \end{matrix} \right\} \xleftarrow{\varphi^*} A' = \mathbb{Q}(\mu_p)[F] = \bigoplus_{b\in F} \mathbb{Q}(\mu_p)\cdot[b]$$

$$= \bigoplus_{a\in F} \delta_a \qquad \sum_{a\in F} \psi(ab)\delta_a \longleftarrow [b]$$

On A',
$[\lambda]^*[b] = [\lambda b]$
$\forall \lambda \in F$

Let $\quad \varepsilon_\chi \overset{\text{def}}{=} \sum_{a\in F^\times} \chi(a)\,\delta_a$

$$\left\{ \begin{aligned} e_\chi &= \sum_{b\in F^\times} \chi^{-1}(b)\,[b] \quad \text{if } \chi \ne 1 \\ e_{\mathbb{1}} &= \Big(\sum_{b\in F} [b]\Big) - q\cdot[0] \end{aligned} \right.$$

Note. $e_{\mathbb{1}}\cdot e_{\mathbb{1}} = -q\, e_{\mathbb{1}}$

$\rightsquigarrow \quad I_\chi = \mathbb{Q}(\mu_p)\cdot\delta_a$

$$\varphi^*(e_\chi) = \sum_{\substack{b\in F^\times \\ a\in F}} \chi^{-1}(b)\,\psi(ab)\,\delta_a = \sum_{\substack{a\in F^\times \\ b\in F^\times}} \overset{\shortparallel}{\chi^{-1}(ab)\,\psi(ab)\,\chi(a)\,\delta_a} + \overbrace{\sum_{b\in F^\times} \chi^{-1}(b)}^{\overset{0}{\shortparallel}} \quad \text{if } \chi \ne \mathbb{1}$$

$$= g(\chi,\psi)\cdot\varepsilon_\chi \qquad \text{if } \chi \ne \mathbb{1}$$

If $\chi = \mathbb{1}$ $\quad \varphi^*(e_{\mathbb{1}}) = \sum_{a,b\in F} \psi(ab)\,\delta_a - q\underbrace{\sum_{a\in F}\delta_a}_{\overset{\shortparallel}{1}} = -q\cdot\sum_{a\in F^\times}\delta_a = -q\cdot\varepsilon_{\mathbb{1}}$

$\varphi^*(e_\chi) = g_\psi(\chi)\cdot \varepsilon_\chi$ if $\chi \neq \mathbb{1}$

$\varphi^*(e_{\mathbb{1}}) = -q\cdot \varepsilon_{\mathbb{1}}$

$\begin{cases} \varepsilon_\chi = \sum_{b\in F^\times} \chi^{-1}(b)\,[b] & \text{if } \chi\neq \mathbb{1} \\ \varepsilon_{\mathbb{1}} = \left(\sum_{b\in F}[b]\right) - q\cdot[0] \end{cases}$ in $A' = \mathbb{Q}(\mu_p)[F]$

$e_\chi = \sum_{a\in F} \chi(a)\,\delta_a$

in $A = \mathrm{Fnc}(F, \mathbb{Q}(\mu_p))$

augmentation on A':

$\sum_{a\in F} n_a[a] \mapsto \sum_{a\in F} n_a$

$$\begin{aligned} A &\xrightarrow{\varepsilon^*} \mathbb{Q}(\mu_p) \\ f &\mapsto f(0) \end{aligned}$$

$$g_\psi(\chi) \overset{\text{def}}{:=} \sum_{a\in F^\times} \chi^{-1}(a)\,\psi(a)$$

comultiplication on $A' = \mathbb{Q}(\mu_{q-1})$: $[a]\mapsto [a]\otimes[a]$ $\forall a\in F$

Cartier duality $G\times G^D \to \mathbb{G}_m$:

$A\otimes A' \leftarrow \mathcal{O}_S[T, T^{-1}]$

$\forall$ scheme S'/S $\quad G(S') = \mathrm{Hom}_{\mathcal{O}_S\text{-alg}}(A\otimes_{\mathcal{O}_S}\mathcal{O}_{S'}, \mathcal{O}_{S'}) \hookrightarrow \mathrm{Hom}_{\mathcal{O}_{S'}\text{-module}}(A\otimes_{\mathcal{O}_S}\mathcal{O}_{S'}, \mathcal{O}_{S'}) = \Gamma(S', A'\otimes_{\mathcal{O}_{S'}}\mathcal{O}_{S'})$

$\cup$

$\simeq$ $\left\{ g : A'\otimes_{\mathcal{O}_S}\mathcal{O}_{S'} \;\middle|\; \begin{array}{l} g \text{ is } \mathcal{O}_S\text{-linear},\ g\in (A'\otimes_{\mathcal{O}_S}\mathcal{O}_{S'})^\times \\ c_{A'}(g) = g\otimes g \end{array} \right\}$

g corresponds to an $\mathcal{O}_{S'}$-alg. homomorphism

g has an inverse (in G)

co-multiplication on $A' = \mathrm{Fnc}(F, \mathbb{Q}(\mu_{q-1}))$:

$$\delta_a \mapsto \sum_{\substack{b,c\in F\\ b+c=a}} \delta_b\otimes\delta_c$$

- On A, have
  (i) $\varepsilon_{\chi'}\cdot\varepsilon_{\chi''} = \varepsilon_{\chi'\cdot\chi''}$ $\quad\forall \chi',\chi''\in M$

  Check: $\left(\sum_{a\in F^\times}\chi'(a)\,\delta_a\right)\cdot\left(\sum_{b\in F^\times}\chi''(b)\,\delta_b\right) = \sum_{a\in F^\times}(\chi'\cdot\chi'')(a)\,\delta_a$ $\quad \left(\delta_a\cdot\delta_b = \begin{cases}0 & a\neq b\\ 1 & a=b\end{cases}\right)$

  So from the definition of $w_{\chi',\chi''}$ get

  (ii) $c(\varepsilon_\chi) = \varepsilon_\chi\otimes 1 + 1\otimes\varepsilon_\chi + \sum_{\substack{\chi',\chi''\in M\\ \chi'\cdot\chi''=\chi}} w_{\chi',\chi''}\,\varepsilon_{\chi'}\otimes\varepsilon_{\chi''}$ $\qquad c: A\to A\otimes A$

- On A', $\{[a] : a\in F\}$ is the dual basis of $\{\delta_a\}_{a\in F}$

  $\rightsquigarrow$ $\left\{ e_{\mathbb{1}} = \left(\sum_{b\in F}[b]\right) - q\cdot[0],\ e_\chi = \sum_{b\in F^\times}\chi^{-1}(b)\,[b] \right\}$ is the dual basis of $\left\{(q-1)^{-1}\cdot\varepsilon_\chi\right\}_{\chi\in M}$

  basis of I

So, $\varepsilon_{\chi'}\cdot\varepsilon_{\chi''} = \varepsilon_{\chi'\cdot\chi''}$ dualize to:

(ii)' $c'(e_\chi) = e_\chi\otimes 1 + 1\otimes e_\chi + \frac{1}{q-1}\sum_{\substack{\chi'\cdot\chi''=\chi\\ \chi',\chi''\in M}} e_{\chi'}\otimes e_{\chi''}$

on A'

and (ii) dualize to

(i)' $e_{\chi'}\cdot e_{\chi''} = (q-1)\, w_{\chi',\chi''}\, e_{\chi'\cdot\chi''}$ $\quad\forall \chi',\chi''\in M$

Look at $\varphi^*: A' \longrightarrow A$ $\qquad \varphi^* : [b] \longmapsto \sum_{a\in F} \psi(ab)\,\delta_a$

$$\varphi^*(e_\chi) = \begin{cases} g_\psi(\chi)\,\varepsilon_\chi & \text{if } \chi \neq 1 \\ -q\cdot \varepsilon_1 & \text{if } \chi = 1 \end{cases} = g_\psi(\chi)\,\varepsilon_\chi \quad \text{if we } \underline{\text{define}}\ g_\psi(1) := -q$$

$$\varphi^*(e_{\chi'}\cdot e_{\chi''}) = \varphi^*\left((q-1)\,w_{\chi',\chi''}\,e_{\chi'\cdot\chi''}\right)$$
$$\parallel$$
$$\varphi^*(e_{\chi'})\cdot\varphi^*(e_{\chi''})$$

$\rightsquigarrow$ $\forall \chi', \chi'' \in M$, have $w_{\chi',\chi''} = \dfrac{1}{q-1}\,\dfrac{g_\psi(\chi')\cdot g_\psi(\chi'')}{g_\psi(\chi'\cdot\chi'')}$ $\qquad$ recall: $g_\psi(\chi) = \sum_{a\in F^\times} \chi^{-1}(a)\,\psi(a)$

$\rightsquigarrow$ $\forall \chi_1,\dots,\chi_n \in M$,
$$\begin{cases} w_{\chi_1,\dots,\chi_n} = \dfrac{1}{(q-1)^{n-1}}\,\dfrac{g_\psi(\chi_1)\cdots g_\psi(\chi_n)}{g_\psi(\prod_{i=1}^n \chi_i)} & (1) \\[2ex] w_{\chi_1,\dots,\chi_n,\chi_1^{-1},\dots,\chi_n^{-1}} = \dfrac{q^{n-1}}{(q-1)^{2n-2}} \quad \text{if } \chi_i \neq 1 \ \ \forall i=1,\dots,n & (2) \end{cases}$$

$\uparrow$ associativity for these structural constants

$$\because\ g_\psi(\chi)\cdot g_\psi(\chi^{-1}) = q\cdot\chi(-1)$$ elementary. also: Lang p.92 GS2

Lang, p.93 : $\quad g_\psi(\chi^p) = g_\psi(\chi) \quad \forall \chi \in M$ $\qquad$ Lang, p.93 GS5

$$\rightsquigarrow\ w_{\chi_1^p,\dots,\chi_n^p} = w_{\chi_1,\dots,\chi_n} \qquad \forall \chi_1,\dots,\chi_n \in M \qquad (3)$$

$\underline{\text{Lemma:}}$ $w_{\chi_1,\dots,\chi_n} \in \mathbb{Q}(\mu_{q-1})^{\mathrm{Fr}_p} \cap D =: D_1$ $\quad \forall \chi_1,\dots,\chi_n \in M$

Recall that $\forall j \in J$, $\quad w_j := w_{\underbrace{\chi_j,\dots,\chi_j}_{p}}$

$$(3) \Rightarrow \quad w_j = w_{j'} =: w \qquad \forall j, j' \in J$$

$$w = \frac{1}{(q-1)^{p-1}}\,\frac{g_\psi(\chi_j)^p}{g_\psi(\chi_j^p)} = \frac{1}{(q-1)^{p-1}}\,g_\psi(\chi_j)^{p-1}$$

Use properties about p-adic valuation of Gauss sums $\quad$ (or explore the case $G = (F,+)_{\mathbb{Q}(\mu_{q-1})}$)

Lang, p.94, Thm 9

$$\chi = \prod_{j\in J} \chi_j^{a_j} \qquad 0 \le a_j \le p-1, \text{ not all } a_j \text{ equal to } 0$$

$\tilde{\mathfrak{p}} \subseteq \tilde{D}$ = integral closure of D in $\mathbb{Q}(\mu_{q-1},\mu_p)$

$\mathfrak{p} \subseteq D$ $\quad$ totally ramified above $\mathfrak{p}$

$\underline{\text{Thm}}$ $\qquad \dfrac{g_\psi(\chi)}{(\zeta_p - 1)^{\sum_{j\in J} a_j}} \in \tilde{D} \qquad$ and $\qquad \dfrac{g_\psi(\chi)}{(\zeta_p-1)^{\sum_j a_j}} \equiv \prod_{j\in J} a_j! \pmod{\tilde{\mathfrak{p}}\tilde{D}}$

$\underline{\text{Note}}$: Use p-adic coordinates for $M = \mathrm{Hom}(F^\times, \mu_{q-1})$ given by fundamental characters for a prime ideal $\mathfrak{p}$ of $\mathcal{O}_{\mathbb{Q}(\mu_{q-1})}$ above p to get congruence information of $g_\psi(\chi)$ at $\mathfrak{p}$!

<u>Proposition</u>: 1) For $\chi = \prod_{j\in J} \chi_j^{a_j}$ $\quad 0 \le a_j \le p-1$, not all equal to 0

Then $w_\chi \in D_1^\times$, where $D_1 = D_1 \cap \mathcal{O}_{\mathbb{Q}(\mu_{q-1})}^{Fr_p}$, and

$$w_\chi \equiv \prod_{j\in M} a_j! \quad (\text{mod } pD_1)$$

2) $w = w_{\underbrace{\chi_j \cdots \chi_j}_{p}} \in pD_1^\times$ $\quad w = pu$, $u \in D_1^\times$ with $u \equiv -1$ (mod pD_1)

equiv. $w = p!$ (mod $p^2 D_1$) in D_1

This proposition follows from results on Gauss sums for finite fields; see Lang, p. 94.

Alternative direct proof, using $G = (F,+)_D$ $\quad A = \{\text{functions } F \to D\}$

$$= \bigoplus_{a\in F} D\cdot\delta_a$$

$$A = D \oplus \bigoplus_{\chi\in M} D\,\varepsilon_\chi \qquad \varepsilon_\chi = \sum_{a\in F^\times} \chi(a)\,\delta_a$$

$$\begin{cases} \varepsilon_{\chi'}\cdot\varepsilon_{\chi''} = \varepsilon_{\chi'\cdot\chi''} \quad \forall\, \chi',\chi'' \in M \\ c(\varepsilon_\chi) = \varepsilon_\chi \otimes 1 + 1\otimes \varepsilon_\chi + \sum\limits_{\substack{\chi',\chi''\in M \\ \chi'\cdot\chi'' = \chi}} w_{\chi',\chi''}\, \varepsilon_{\chi'}\otimes\varepsilon_{\chi''} \end{cases}$$

$$A' = D \oplus \bigoplus_{\chi\in M} D\cdot e_\chi \qquad e_\chi = \sum_{b\in F^\times} \chi^{-1}(b)\cdot[b], \quad e_1 = \Big(\sum_{b\in F}[b]\Big) - q\cdot[0]$$

$$\mathrm{Lie}\,(G^D \times_{\operatorname{Spec} D} \operatorname{Spec} \underset{\substack{\| \\ k}}{\kappa(\mathfrak{z})}) = G^D(k[\varepsilon]/(\varepsilon^2)) = \mathrm{Hom}_{grp}((F,+), (k[\varepsilon]/(\varepsilon^2))^\times) \circlearrowleft F^\times$$

$$= \bigoplus_{\chi} k\cdot(\text{eigenvector } v_\chi \text{ for some } \chi\in M)$$

$v_\chi(0) = 1$, $\quad v_\chi = 1 + \varepsilon\, h_\chi \pmod{\varepsilon^2}$

$h_\chi : (F,+) \to (k,+)$ homomorphism, normalized by $h_\chi(1) = 1$

$\rightsquigarrow$ $h_\chi(\underset{\substack{\uparrow \\ F^\times}}{a}) = \chi(a)$

$1 + \varepsilon h_\chi(a+b) \equiv (1+\varepsilon h_\chi(a))\,(1+\varepsilon h_\chi(b)) \pmod{\varepsilon^2}$ $\quad \forall a,b$

$\rightsquigarrow$ $h_\chi : F \to k$ is a ring homom

$$\rightsquigarrow \quad \mathrm{Lie}\,(G^D \times_{\operatorname{Spec} D} \operatorname{Spec}(\kappa(\mathfrak{z}))) = \bigoplus_{\chi\in J} k\cdot(1+\varepsilon\chi)$$

is a fundamental character

$$\Rightarrow \quad I'/(I')^2 = \text{dual of } \mathrm{Lie}(G^D \times_{\operatorname{Spec} D} \operatorname{Spec}(\kappa(\mathfrak{z}))) = \bigoplus_{j\in J} \kappa(\mathfrak{z})\cdot \bar{e}_{\chi_j}$$

image of e_{χ_j} in $I'/(I')^2$

<u>Fact</u> for multiplicative group killed by p:

$$A' \otimes_D \kappa(\mathfrak{z}) \underset{\text{as algebras}}{\cong} \operatorname{Sym}^\bullet_{\kappa(\mathfrak{z})} \underset{\deg = 1}{I'/(I')^2} \Big/ \left(\begin{matrix}\text{p-th powers of} \\ \text{elements of } I'/(I')^2\end{matrix}\right)$$

Equivalently $A' \otimes_D \kappa(\mathfrak{z})$ is generated by $\bar{e}_{\chi_j}$, $j\in J$, with relations $\bar{e}_{\chi_j}^{\,p} = 0$ $\quad \forall j \in J$

Notation / def^n

$\chi', \chi'' \in M$. $\chi' = \prod_{j\in J} \chi_j^{a_j'}$, $\chi'' = \prod_{j\in J} \chi_j^{a_j''}$ $0 \le a_j' \le p-1$, not all 0
$0 \le a_j'' \le p-1$, not all 0.

If $\chi' \cdot \chi'' = \chi_{j_0}$ $j_0 \in J$, define $h = h_{\chi',\chi''}$ by:

$0 < h_{\chi',\chi''} \le r$, $a'_{j_0-h} + a'_{j_0-h} = p$ $\rightsquigarrow \chi_j = \chi_{j-h}^{p} \cdot \chi_{j-h-1}^{p-1} \cdots \chi_{j-1}^{p-1}$

$a'_{j_0-k} + a''_{j_0-k} = p-1$ for all k s.t. $0 < k < h_{\chi',\chi''}$

<u>and</u> $a_j' = a_j''$ for all other j's, i.e $j \ne i_0 - k$ for every k with $0 < k \le h$

Thus $h(\chi', \chi'') =$ # of carries in $\chi' \cdot \chi'' =$ a fundamental character χ_{j_0}

Continue from p. 25:

$$\begin{cases} e_{\chi'} \cdot e_{\chi''} = (q-1)\, w_{\chi',\chi''}\, e_{\chi'\cdot\chi''} \\ c'(e_\chi) = e_\chi \otimes 1 + 1 \otimes e_\chi + \frac{1}{q-1} \sum_{\chi'\cdot\chi''=\chi} e_{\chi'} \otimes e_{\chi''} \end{cases} \quad \text{on } A'$$

— Use multiplication on A':

For $\chi = \prod_{j\in J} \chi_j^{a_j}$ $0 \le a_j \le p-1$, not all $=0$

$$\underset{\substack{\#\\0}}{\prod_{j\in J} (e_{\chi_j})^{a_j}} \equiv (-1)^{(\sum_j a_j)-1} w_\chi\, e_\chi \pmod{\mathfrak{p}} \implies w_\chi \not\equiv 0 \pmod{\mathfrak{p}} \ \forall \chi \in M$$

i.e. $w_\chi \in D^\times$

Similarly, $\forall j \in M$

$$\underset{\substack{|||\\ 0 \ (\mathrm{mod}\ \mathfrak{p})}}{(e_{\chi_j})^p} \equiv (q-1)^{p-1} w_j\, e_{\chi_{j+1}} \implies w \equiv 0 \pmod{\mathfrak{p}}$$

— Use comultiplication on A

$c_n = n$-th iterate of $c: A \longrightarrow \underbrace{A \otimes \cdots \otimes A}_{n}$

For $\chi = \prod_{j\in J} \chi_j^{a_j}$, $0 \le a_j \le p-1$, not all $a_j = 0$

Compute $c_n(\varepsilon_\chi)$, $n = \sum_j a_j$ $\quad \begin{cases} \varepsilon_{\chi'} \cdot \varepsilon_{\chi''} = \varepsilon_{\chi'\cdot\chi''} \quad \forall \chi', \chi'' \in M \\ c(\varepsilon_\chi) = \varepsilon_\chi \otimes 1 + 1 \otimes \varepsilon_\chi + \sum_{\chi'\cdot\chi''=\chi} w_{\chi',\chi''}\, \varepsilon_{\chi'} \otimes \varepsilon_{\chi''} \end{cases}$

$\quad \overset{\shortparallel}{\prod_{j\in M} \varepsilon_{\chi_j}^{a_j}}$

$\rightsquigarrow$ In $c_n(\varepsilon_\chi) = \bigotimes_{j\in M} c_n(\chi_j)^{a_j}$, the coefficient of $\bigotimes_{j\in J} (\underbrace{\varepsilon_{\chi_j} \otimes \cdots \otimes \varepsilon_{\chi_j}}_{a_j})$ is

$$\equiv \prod_{j\in J} a_j! \pmod{p}$$

for $j \in J$

Similarly, in $c_p(\varepsilon_{\chi_{j+1}}) = c_p(\varepsilon_{\chi_j}^p) = c_p(\varepsilon_{\chi_j})^p$, the coefficient of $\underbrace{\varepsilon_{\chi_j} \otimes \cdots \otimes \varepsilon_{\chi_j}}_{p}$ is

$$\equiv p! \pmod{p^2}$$

This finishes the alternative / direct proof of the Proposition on p. 25

Classification theorem

$$\bar d_j \circ \bar c_j = w \cdot id_{\mathcal{L}_{j+1}} \quad \forall j$$

$$\left\{\begin{matrix}\text{commutative finite locally}\\ \text{free rank-one } F\text{-vector scheme}\end{matrix}\right\} \longrightarrow \left\{\left(\mathcal{L}_j,\ \mathcal{L}_{j+1} \xrightarrow{\bar c_j} \mathcal{L}_j^{\otimes p},\ \mathcal{L}_j^{\otimes p} \xrightarrow{\bar d_j} \mathcal{L}_{j+1}\right)_{j\in J}\right\}$$

$$G \longmapsto \left(\mathcal{I}_j,\ c_j : \mathcal{I}_{\chi_{j+1}} \to \mathcal{I}_{\chi_j}^{\otimes p},\ d_j : \mathcal{I}_{\chi_j}^{\otimes p} \to \mathcal{I}_{\chi_{j+1}}\right)$$

is an equivalence of categories

(Re) construct G from $(\mathcal{I}_j, \bar c_j, \bar d_j)_{j\in J}$:

Define (i) $A := \bigoplus_{\underline{a}=(a_j)_{j\in J}\in\mathbb{N}^J} \underbrace{\bigotimes_{j\in M} \mathcal{L}_j^{\otimes a_j}}_{\mathcal{L}^{\otimes \underline{a}}} \Big/ \left(\mathrm{Im}\left(\mathcal{L}_j^{\otimes p} \xrightarrow[id_{\mathcal{L}_j^{\otimes p}} - d_j]{} \mathcal{L}_j^{\otimes p} \oplus \mathcal{L}_{j+1}\right)\right)_{j\in J}$

$$\uparrow\simeq$$

$$\bigoplus_{\substack{\underline{a}=(a_j)_j\\ 0\le a_j\le p-1\ \forall j}} \bigotimes_{j\in J} \mathcal{L}_j^{\otimes a_j}$$

Have define A as an $\mathcal{O}_S$-algebra

Let $\mathcal{I} \overset{\text{def}}{=} \bigoplus_{\substack{\underline{a}\neq 0\\ 0\le a_j\le p-1}} \bigotimes_{j\in J} \mathcal{L}_j^{\otimes a_j}$ augmentation ideal

(ii) Define $c : A \longrightarrow A\otimes A = \mathcal{O}_S \oplus (\mathcal{I}\otimes\mathcal{O}_S) \oplus (\mathcal{O}_S\otimes\mathcal{I}) \oplus \sum_{\substack{\underline{a},\underline{b}\neq 0\\ 0\le a_j,b_j\le p-1}} \underbrace{\left(\bigotimes_{j\in J}\mathcal{L}_j^{a_j}\right)\otimes\left(\bigotimes_{j\in J}\mathcal{L}_j^{\otimes b_j}\right)}_{\mathcal{L}^{\otimes\underline{a}}\otimes\mathcal{L}^{\otimes\underline{b}}}$

$$\mathcal{L}^{\otimes\underline{a}}\otimes\mathcal{L}^{\otimes\underline{b}} \xrightarrow{\pi_{\underline{a},\underline{b}}} \mathcal{L}^{\otimes\underline{a}}\otimes\mathcal{L}^{\otimes\underline{b}}$$

$\pi_{\underline{a}',\underline{a}''}\circ c(\mathcal{L}_{\underline{a}}) \neq 0$ if $\left(\prod_j \chi_j^{a_j'}\right)\cdot\left(\prod_j \chi_j^{a_j''}\right) \neq \prod_j \chi_j^{a_j}$

- Define $c|_{\mathcal{L}_{j+1}} : \mathcal{L}_{j+1} \longrightarrow \mathcal{L}_j^{\otimes p}$ to be $\bar c_j$ $\forall j\in M$

- $\forall\, \underline{a},\underline{b}$ with $0\le a_j, b_j\le p-1$, $\underline{a},\underline{b}\neq\underline{0}$, s.t. $\left(\prod_j \chi_j^{a_j}\right)\left(\prod_j \chi_j^{b_j}\right) = \chi_j$ $h = h(\underline{a},\underline{b})$, $0<h\le r$

define $c_{\underline{a},\underline{b}} : \mathcal{L}_{j_0} \longrightarrow \mathcal{L}^{\otimes\underline{a}}\otimes\mathcal{L}^{\otimes\underline{b}}$ by

$a_{j_0-h} + b_{j_0-h} = p$, $a_{j_0-k} + b_{j_0-k} = p-1$ for $0<k<h$

$0 = a_{j'} = b_{j'}$ if $j' \neq j-k$ for some k with $0<k\le h$

$$\begin{tikzcd}
\mathcal{L}_{j_0} \arrow[r, "\bar c_{j-1}"] \arrow[ddr, "c_{\underline{a},\underline{b}}"'] & \mathcal{L}_{j_0-1}^{\otimes p} = \mathcal{L}_{j_0-1}^{\otimes p-1}\otimes\mathcal{L}_{j_0-1} \arrow[r, "1\otimes\bar c_{j-2}"] & \mathcal{L}_{j_0-1}^{\otimes p-1}\otimes\mathcal{L}_{j_0-2}^{p} = \mathcal{L}_{j_0-1}^{\otimes p-1}\otimes\mathcal{L}_{j_0-2}^{\otimes p-1}\otimes\mathcal{L}_{j_0-2} \arrow[d] \\
& & \vdots \arrow[d] \\
& \mathcal{L}^{\otimes\underline{a}}\otimes\mathcal{L}^{\otimes\underline{b}} \arrow[r, "w_{\underline{a}}\cdot w_{\underline{b}}"] & \mathcal{L}^{\otimes\underline{a}}\otimes\mathcal{L}^{\otimes\underline{b}} = \mathcal{L}_{j_0-1}^{\otimes p-1}\otimes\mathcal{L}_{j_0-2}^{\otimes p-1}\otimes\cdots\otimes\mathcal{L}_{j_0-h+1}^{\otimes p-1}\otimes\mathcal{L}_{j_0-h}^{\otimes p}
\end{tikzcd}$$

Shorthand :

$$c_{\underline{a},\underline{b}} = \frac{\bar c_{j_0-h}\circ\cdots\circ\bar c_{j-1}}{w_{\underline{a}}\cdot w_{\underline{b}}}$$

$$w_{\underline{a}} = w_{\prod_j \chi_j^{a_j}},\quad w_{\underline{b}} = w_{\prod_j \chi_j^{b_j}}$$

Define $c|_{\mathcal{L}_{j_0}} : \mathcal{L}_{j_0} \longrightarrow A$ by :

$$c(\lambda) = \lambda\otimes 1 + 1\otimes\lambda + \sum_{\substack{\underline{a},\underline{b}\neq 0\\ 0\le a_j,b_j\le p-1\ \forall j\\ \prod_j\chi_j^{a_j}\cdot\prod_j\chi_j^{b_j}=\chi_{j_0}}} c_{\underline{a},\underline{b}}(\lambda)$$

$\leadsto$ define $c|_{\mathcal{L}^{\underline{a}}} = \bigotimes_{j\in J} \left(c|_{\mathcal{L}_j}\right)^{\otimes a_j}$

$\forall\, \underline{a}\neq 0$ with $0\le a_j\le p-1$ $\forall j$

(Re) construction continued: Given $(\mathcal{L}_j, \bar{c}_j, \bar{d}_j)_{j\in J}$, have construct an $\mathcal{O}_S$-alg. A over S

and an $\mathcal{O}_S$-module homom $c: A \to A \otimes_{\mathcal{O}_S} A$

Need to show: c is an $\mathcal{O}_S$-algebra homomorphism, and is co-associative (co-commutativity is obvious)

Zariski localization: reduce to the case when each $\mathcal{L}_j$ is $\mathcal{O}_S$

$\leadsto$ Suffices to check the universal situation, with

$S = \mathrm{Spec}\, D[U_j, V_j : j\in J]/(U_jV_j - W)_{j\in J} = \mathrm{Spec}(E)$ u_j = image of U_j in E, v_j = image of V_j in E

$A = E[X_j : j\in J]/(X_j^p - v_j X_{j+1})_{j\in J}$ free E-module

E is faithfully flat over D

With $c: A \to A \otimes_D A$ E-module homomorphism

To check the c is an algebra homorphism and is co-associative, it suffices to show that the equalities in question hold after inverting p

Pick $j_0 \in J$

Lemma: Let $E' = E[T]/(T^{p^r-1} - v_{j_0+1}^{p^{r-1}} v_{j_0+2}^{p^{r-2}} \cdots v_{j_0+r})$ $S' = \mathrm{Spec}(E')$

$H := (\mathbb{F},+)_{/S'}$ Then c is an $\mathcal{O}_S$-alg. homomorphism and is co-associative, giving $G = \mathrm{Spec}(A)$ a structure as a rank-one $\mathbb{F}$-vector scheme. Moreover we have an $\mathbb{F}$-linear homomorphism $\varphi: H_{S'_{(p)}} \to G \times_S S'_{(p)}$ of rank-one $\mathbb{F}$-vector schemes, where $S'_{(p)} = \mathrm{Spec}(E'[\frac{1}{p}])$

$B = \{$functions from $\mathbb{F}$ to $E'\}$

pf: Will define a E'-alg homom $A \otimes_E E' \to B$

Consider syst of eq $(X_j^p - v_j X_{j+1})_{j\in J}$ $\leadsto$ $X_{j_0+1}^{p^r} = v_{j_0+1}^{p^{r-1}} \cdot X_{j_0+2}^{p^{r-1}} = v_{j_0+1}^{p^{r-1}} \cdot v_{j_0+2}^{p^{r-2}} X_{j_0+2}^{p^{r-2}} = \cdots = v_{j_0+1}^{p^{r-1}} \cdot v_{j_0+2}^{p^{r-2}} \cdots v_{j_0+r} \underset{X_{j_0+1}}{\underset{\parallel}{X_{j_0+r+1}}}$

$X_{j_0+1} \mapsto t \leftarrow$ image of T

$X_{j_0+2} \mapsto t^p \cdot v_{j_0+1}^{-1}$, $X_{j_0+3} \mapsto (X_{j_0+2})^p \cdot v_{j_0+2}^{-1} = t^{p^2} \cdot v_{j_0+1}^{-p} v_{j_0+2}$, etc.

$\leadsto$ get a E'-linear ring homomorphism $A \otimes_E E' \to E'$, $X_j \mapsto t_j$ $j\in M$

Define $A \otimes_E E' \xrightarrow{\alpha} B$

$X_j \mapsto t_j \varepsilon_{\chi_j}$ $\forall j \in M$

Recall: $\varepsilon_{\chi_j} = \sum_{a\in\mathbb{F}^\times} \chi_j(a)\,\delta_a$ $\forall j\in M$

Note: ε_χ evaluated at the point $1 \in \mathbb{F}^\times$ $\forall \chi\in M$

This means: α corresponds to a map $H_{S'_{(p)}} \to G_{S'_{(p)}}$ where the section 1 of H goes to the section $(X_j \mapsto t_j\ \forall j\in J)$ of G

Proposition R: strictly henselian dvr, $K = \mathrm{frac}(R)$, $I_t = \mathrm{Gal}(\bar{K}/K)$ $k = \bar{k}$ alg. closed residue field

$G_{/R}$: rank-one $\overset{\cong \mathbb{F}_q \quad q = p^r}{F}$-vector scheme $\longleftrightarrow \left((\gamma_j, \delta_j) \mid \gamma_j \cdot \delta_j = w_j\right)_{j \in J}$

Let $\rho_G : I_t \to F^\times$ be the associated character

Then: $\rho_G = \prod_{j \in M} \psi_{j+1}^{v(\delta_j)} \circ \jmath_q$, where $\jmath_q : I_t \twoheadrightarrow \mu_{q-1} \leftarrow \mathrm{Gal}(K_n/K)$

$\chi_j^{-1} =: \psi_j : \mu_{q-1} \xrightarrow{\sim} F^\times$

Note

$$\begin{tikzcd} F^\times \arrow[r, "\chi_j"] \arrow[d, "="] & \mu_{q-1} \arrow[d, "{[p]}"] \\ F^\times \arrow[r, "\chi_{j+1}"] & \mu_{q-1} \end{tikzcd}$$

$\leadsto \psi_{j+1} = \psi_j \circ [p^{-1}]$

i.e. $\psi_{j+1}^p = \psi_j \quad \forall j \in J$

Pf: Equation of G is $x_j^p = \delta_j x_{i+1} \quad \forall j \in J$

$\leadsto x_j^q = a_j x_j \quad \forall$

where $a_j = \delta_j^{p^{r-1}} \cdot \delta_{j+1}^{p^{r-2}} \cdots \delta_{j+r-1} = \prod_{h=0}^{r-1} \delta_{j+h}^{p^{r-1-h}}$

The assertion means: $\forall \sigma \in I_t$, $\forall x \in G(\bar{K})$, ${}^\sigma x = \left(\prod_j \psi_{j+1}^{v(\delta_j)}\right)(\jmath(\sigma)) \cdot x$

for the F-vector scheme structure of x

Cor. $\det_G : I_t \to F^\times$ is given by

$$\det_G = \left(\prod_{j \in M} \psi_j\right)^{\sum_{j \in J} v(\delta_j)} = \tau_p^{\sum_{j \in J} v(\delta_j)} \qquad \tau_p : I_t \twoheadrightarrow \mu_{p-1}$$

Tate's paper on p-divisible groups: $\mathcal{O}_K$: complete dvr, $k = \mathcal{O}_K/\mathfrak{m}_K$ perfect, char. $(0,p)$

Hodge-Tate decomposition of $T_p(G)$ $\quad G = (G_\nu)_{\nu \geq 1}$ over $\mathcal{O}_{\hat{K}}$

$$G(\mathcal{O}_{\hat{K}}) = \varprojlim_i \varinjlim_\nu G_\nu(\mathcal{O}_{\hat{K}}/\mathfrak{m}^{i+1}_{\mathcal{O}_{\hat{K}}}) \quad \text{divisible}$$

$$\leadsto \begin{tikzcd} T_p(G^t) \times G(\mathcal{O}_{\hat{K}}) \arrow[r] \arrow[d, "1 \times \log_G"] & \mu_{p^\infty}(\mathcal{O}_{\hat{K}}) = \mathcal{O}^\times_{\hat{K},1} =: U \arrow[d, "\log_{\hat{K}}"] \\ T_p(G^t) \times t_G(\hat{K}) \arrow[r] & \hat{K} \end{tikzcd}$$

$$\leadsto \begin{tikzcd} 0 \arrow[r] & T_p(G) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \arrow[r] \arrow[d, "\alpha_0", "\cong \text{(by Cartier duality)}"'] & G(\mathcal{O}_{\hat{K}}) \arrow[r] \arrow[d, "\alpha"] & t_G(\hat{K}) \arrow[r] \arrow[d, "d\alpha"] & 0 \\ 0 \arrow[r] & \mathrm{Hom}_{\mathbb{Z}_p}(T_p(G^t), U_{tors}) \arrow[r] & \mathrm{Hom}_{\mathbb{Z}_p}(T_p(G^t), \mathcal{O}^\times_{\hat{K},1}) \arrow[r] & \mathrm{Hom}_{\mathbb{Z}_p}(T_p(G^t), \hat{K}) \arrow[r] & 0 \end{tikzcd}$$

exact rows (kernels are torsion subgroups of the middle terms)

(1) α_0 is $\cong$ $\Rightarrow$ $\mathrm{Ker}(\alpha) \cong \mathrm{Ker}(d\alpha)$, $\mathrm{Coker}(\alpha) \cong \mathrm{Coker}(d\alpha)$ $\Big\}$ $\hat{K}$-vector spaces

$\leadsto$ $\mathrm{Ker}(\alpha)$ and $\mathrm{Coker}(\alpha)$ are vector spaces over $\mathbb{Q}_p$

$\because \hat{K}^{\mathrm{Gal}(\bar{K}/K)} = K \leadsto G(\mathcal{O}_K) = G(\mathcal{O}_{\hat{K}})^{\mathrm{Gal}(\bar{K}/K)}$ and $t_G(K) = t_G(\hat{K})^{\mathrm{Gal}(\bar{K}/K)}$

(2) $\alpha|_{G(R)} : G(O_K) \longrightarrow \mathrm{Hom}_{\mathbb{Z}_p}(T_p(G^t), O^{\times}_{\bar{K},1})^{\mathrm{Gal}(\hat{\bar{K}}/K)}$ is injective

$\mathrm{Ker}(\alpha|_{G(O_K)}) = \mathrm{Ker}(\alpha)^{\mathrm{Gal}(\hat{\bar{K}}/K)}$ is a $\mathbb{Q}_p$-vector space, hence uniquely divisible

$\mathrm{Ker}(\alpha|_{G(O_K)}) = \mathrm{Ker}(\alpha) \cap G(O_K)$

$\rightsquigarrow \mathrm{Ker}(\alpha) \cap G(O_K) = \bigcap_{i \geq 1} p^i(\mathrm{Ker}(\alpha) \cap G(O_K)) \subseteq \bigcap_{i \geq 1} p^i G(O_K) \cap G^\circ(O_K)$ $\longleftarrow$ $\because G(O_K)/G^\circ(O_K)$ is torsion

$\because \bigcap_{i \geq 1} p^i G^\circ(O_K) = (0)$

$\rightsquigarrow \mathrm{Ker}(\alpha) \cap G^\circ(O_K) = (0)$

(3) $d\alpha|_{t_G(K)} : t_G(K) \rightarrow \mathrm{Hom}_{\mathbb{Z}_p}(T_p(G^t), O^{\times}_{\hat{\bar{K}},1})^{\mathrm{Gal}(\bar{K}/K)}$ is injective

(formal consequence of (2))

$\rightsquigarrow d\alpha = d\alpha|_{t_G(K)} \otimes_K \hat{\bar{K}}$ is injective

using Tate's result on finite dim^l $\hat{\bar{K}}$-vector spaces with semi-linear $\mathrm{Gal}(\hat{\bar{K}}/K)$-action

<u>Conclude</u> α and $d\alpha$ are both injective

<u>and</u>

<u>Theorem</u> $G(O_K) \xrightarrow[\alpha]{\sim} \mathrm{Hom}_{\mathrm{Gal}(\bar{K}/K)}(T_p(G^t), U)$

$t_G(K) \xrightarrow[d\alpha]{\sim} \mathrm{Hom}_{\mathrm{Gal}(\bar{K}/K)}(T_p(G^t), \hat{\bar{K}})$

dimension count, using Tate's number-theoretic result modern version $\varepsilon > 0$

Roth thm: K: number field, $\underset{\text{finite}}{S} \subseteq M_K$ $\forall v \in S$, let $\alpha_v \in \overline{K} \cap K_v$ be given

$$\# \left\{ \beta \in K \;\middle|\; \prod_{v \in S} \min(1, |\beta - \alpha_v|_v) \leq H(\beta)^{-2-\varepsilon} \right\} < \infty$$

History: Thue 1909. Siegel 1970, Ges. Abh IV, paper 91, p 140–166 (Also, Landau Vorlesungen)
Siegel 1921 (the first two paper in his Gesammelte Abhandungen vol I)
Roth 1955
Schmidt 1972

Subspace Theorem: K: number field $S \subseteq M_K$ a finite subset

$\forall v \in S$, let $L_{v,1}(\underline{x}), \ldots, L_{v,m_v}(\underline{x}) \in \overline{\mathbb{Q}}[X_0, \ldots, X_n]$ be linear forms <u>in general position</u>, i.e. every subset of $\{L_{v,1}(\underline{x}), \ldots, L_{v,m_v}(\underline{x})\}$ with cardinality $\leq n+1$ is linearly independent over $\overline{\mathbb{Q}}$

$\forall \varepsilon > 0$, $\exists$ a finite number $T_1, \ldots, T_h$ of hyperplanes in $\mathbb{P}^n(K)$ s.t.

$$\left\{ x \in \mathbb{P}^n(K) \;\middle|\; \prod_{v \in S} \prod_{i=1}^{m_v} \min_{0 \leq j \leq n} \left| \frac{L_{v,i}(\underline{x})}{x_j} \right|_v < H(\underline{x})^{-n-1-\varepsilon} \right\}$$

is contained in $T_1 \cup \cdots \cup T_h$

Archimedes $3\frac{10}{71} < \pi < 3\frac{1}{7}$

Tsu Chúng-Chih $\pi \sim \frac{355}{113}$ A.D. 430–501

Brahmagupta solution of $x^2 - dy^2 = 1$

Euler (1737) real quadratic irrationals are periodic continued fraction
Converse: Lagrange 1770

Dirichlet (1842). Given $(\alpha_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ $\alpha_{ij} \in \mathbb{R}$ $\forall i,j$ $Q > 1$, $Q \in \mathbb{N}$

$\exists$ integers $q_1, \ldots, q_n, p_1, \ldots, p_m$ with $1 \leq \max_j (|q_j|) < Q^{n/m}$

s.t. $\left| \sum_j \alpha_{ij} q_j - p_i \right| \leq Q^{-1}$ $\forall i = 1, \ldots, m$

Minkowski (1896) $(\beta_{ij}) \in M_n(\mathbb{R})$, $\det(\beta_{ij}) = \pm 1$, $A_1, \ldots, A_n \in \mathbb{R}^\times_{>0}$, $\prod_i A_i = 1$

Then $\exists$ $\underset{0 \neq}{\underline{x}} = (x_1, \ldots, x_n) \in \mathbb{Z}^n$ s.t.

$$\left| \sum_j \beta_{ij} x_j \right| < A_i \quad \forall i = 1, \ldots, n-1$$

Minkowski linear form thm

and

$$\left| \sum_j \beta_{nj} x_j \right| \leq A_n$$

F : number field

$M_F \ni v$ Use normalized valuation

$|x|_{v,F} = \|x\|_{F_v}^{\frac{1}{[F:\mathbb{Q}]}}$ $\forall x \in F$, where $\|x\|_{F_v}$ defined using Haar measures on F_v

Explicitly: if $p \mid v$, $|x|_{v,F} = |\mathrm{Nm}_{F_v/\mathbb{Q}_p}(x)|_{\mathbb{Q}_p}^{\frac{1}{[F:\mathbb{Q}]}}$

if v is arch $|x|_{v,F} = |\mathrm{Nm}_{F_v/\mathbb{R}}(x)|_{\mathbb{R}}^{\frac{1}{[F:\mathbb{Q}]}}$

Define height on $\overline{\mathbb{Q}}$: $\overline{\mathbb{Q}} \supseteq F \ni x$, $F/\mathbb{Q}$ finite

$$H(x) = \prod_{v \in M_F} \max(1, |x|_v), \quad h(x) = \sum_{v \in M_F} \log^+ |x|_v$$

height on $\mathbb{P}^n(\overline{\mathbb{Q}}) \supseteq \mathbb{P}^n(F) \ni x = [x_0 : \cdots x_n]$ $x_i \in F$

$$\leadsto H(x) = \prod_{v \in M_F} \max(|x_0|_v, \dots, |x_n|_v), \quad h(x) = \log H(x)$$

Classical Liouville thm:

$\alpha \in \overline{\mathbb{Q}} \setminus \mathbb{Q}$, $\exists$ const $c(\alpha) > 0$ s.t. $\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^n}$ $\forall \frac{p}{q} \in \mathbb{Q}$ $p, q \in \mathbb{Z}$

$n = [\mathbb{Q}(\alpha) : \mathbb{Q}]$

Modern version $K \in L \subseteq \overline{\mathbb{Q}}$, $\alpha \in L$, $\beta \in K$ $\alpha \neq \beta$, $S \subseteq M_L$ finite subset

nber fields

Then

$$(2H(\alpha)H(\beta))^{-1} \leq \prod_{w \in S} |\alpha - \beta|_{w,L} \leq 2H(\alpha) \cdot H(\beta)$$

Lemma: $\forall x \in L \setminus (0)$, $-h(x) \leq \sum_{w \in S} \log |x|_{w,L} \leq h(x)$ "fundamental ineq"

Lemma $h(x+y) \leq h(x) + h(y) + \log 2$ ← arch. contribution

Pf of modern version $S \subseteq M_K$ finite subset

Fund. ineq $\Rightarrow$ $-h(\alpha)-h(\beta)-2 \leq -h(\alpha-\beta) \leq \sum_{w \in S} |\alpha-\beta|_{w,L} \leq h(\alpha-\beta) \leq h(\alpha)+h(\beta)+2$

Remark: $w \mid v$, L / F: $|\alpha-\beta|_{w,L} = |\alpha-\beta|_{v,K}^{\frac{1}{[L:K]}}$, so the exponent n in the classical version of Liouville theorem disappeared in the modern version.

Modern version': $\alpha \in L$, $\beta \in K$, $S \subseteq M_K$ finite subset

$$(2H(\alpha)H(\beta))^{\frac{1}{[L:K]}} \leq \sum_{v \in M_K} |\alpha - \beta|_{v,L} \leq (2H(\alpha)H(\beta))^{[L:K]}$$

Minkowski 2^{nd} convex body theorem (1907)

$B \subseteq \mathbb{R}^n$ convex compact, symmetric about $\vec{0} \in \mathbb{R}^n$, $\vec{0} \in$ interior(B).

$0 < \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$: successive minima of K.

$$\lambda_1 = \inf \{ \lambda \in \mathbb{R}_{>0} \mid \lambda K \cap \mathbb{Z}^n \neq \{\vec{0}\} \}$$

$$\lambda_j = \inf \{ \lambda \in \mathbb{R}_{>0} \mid \lambda K \cap \mathbb{Z}^n \text{ contains } j \text{ linearly indep. lattice points} \}$$

$$\frac{2^n}{n!} \leq \lambda_1 \cdots \lambda_n \cdot vol(K) \leq 2^n$$

(Minkowski's first theorm says: $\lambda_1^n \, vol(K) \leq 2^n$)

Rmk The above are (mostly) upper bounds of errors in approximation

i.e. $\exists$ good approximation

Lower bounds of error in approximation

- Liouville's theorem (1844) $\left|\alpha - \frac{p}{q}\right| > c(\alpha)\, q^{-[\mathbb{Q}(\alpha):\mathbb{Q}]}$ $\forall \alpha \in (\overline{\mathbb{Q}} \setminus \mathbb{Q}) \cap \mathbb{R}$
- Thue 1909
  Given $\mu > \frac{1}{2}[\mathbb{Q}(\alpha):\mathbb{Q}]+1$ $\quad \# \{ \frac{p}{q} \in \mathbb{Q} : \left|\alpha - \frac{p}{q}\right| < q^{-\mu} \} < \infty$
- Siegel 1921 : same statement, with $\mu > 2\sqrt{d}$ $\quad d = [\mathbb{Q}(\alpha):\mathbb{Q}]$
- Dyson 1947 $\quad \mu > \sqrt{2d}$
- Roth 1955 $\quad \mu > 2$
- Schmidt 1972 (consequence of subspace theorem)

  Given $\alpha \in \overline{\mathbb{Q}} \subseteq \mathbb{C}$, $\varepsilon > 0$, k

$$\# \{ \beta \in \overline{\mathbb{Q}} \,;\, [\mathbb{Q}(\beta):\mathbb{Q}] \leq k : |\alpha - \beta| < H(\beta)^{-(k+1+\varepsilon)} \} < \infty$$

Related : $\mathcal{L} \overset{def}{=} \exp^{-1}(\overline{\mathbb{Q}}^\times) = \{ \lambda \in \mathbb{C} \mid e^\lambda \in \overline{\mathbb{Q}}^\times \}$

Baker (1966) $\lambda_1, \ldots, \lambda_n \in \mathcal{L}$, linearly indep over $\mathbb{Q}$ $\Longrightarrow$ $1, \lambda_1, \ldots, \lambda_n$ are lin. indep over $\overline{\mathbb{Q}}$

Roth Theorem

K: number field, $[F:K] < \infty$ $\quad S \subseteq M_K$ finite set of places of K

Given $\alpha_v \in F$ $\forall v \in S$, extend $|\cdot|_v$ to F

Given $\kappa > 2$

$$\# \{ \beta \in K \mid \prod_{v \in S} \min(1, |\beta - \alpha_v|_v) \leq H(\beta)^{-\kappa} \} < \infty$$

Sketch of the steps of Roth Theorem for $K=\mathbb{Q}$. $S=\{\infty\}\in M_{\mathbb{Q}}$

Suppose $\exists$ infinitely many $\frac{p}{q} \in \mathbb{Q}$, $q\in\mathbb{N}_{>0}$ with $\left|\alpha-\frac{p}{q}\right| \leq q^{-\kappa}$

$\forall$ large constants $L, M>0$, $\forall m \in \mathbb{N}_{>0}$

$\rightsquigarrow$ Find a sequence $\frac{p_j}{q_j}$ $j=1,\dots,m$ s.t. $\left|\alpha-\frac{p_j}{q_j}\right| \leq q_j^{-\kappa}$

$$q_1 > L, \quad \log q_{j+1}/\log q_j > M \quad \forall j=1,\dots,m-1$$

Call such a finite sequence (L,M)-indep.

Let D be a large real number

Let $d_j = \lfloor D/\log q_j \rfloor$, $j=1,\dots,m$ (So that $d_1 > d_2 > \cdots > d_m$ decreasing rapidly)

step 1. Use Siegel's lemma (pigeon-hole principle) to construct an "auxiliary polynomial" $P(X_1,\dots,X_m)$, $\deg_{X_j} P \leq d_j$ $\forall j=1,\dots,m$

s.t. $\operatorname{ind}(P,(d_1,\dots,d_m),(\alpha,\dots,\alpha)) \geq t$ t large

and $h(P) \leq \underset{\text{Constant}>0}{C_1} \cdot \frac{D}{L}$

step2 Prove that $\exists (\mu_1,\dots,\mu_m)\in\mathbb{N}^m$ with $\sum \frac{\mu_i}{d_j}$ small s.t. ($= \operatorname{ind}(P,(d_1,\dots,d_m),(\frac{p_1}{q_1},\dots,\frac{p_m}{q_m}))$)

Uses Roth's Lemma

$$\underbrace{\left(\prod_{i=1}^m \frac{1}{\mu_i!}\partial_{X_i}^{\mu_i}\right)(P)}_{Q}\left(\frac{p_1}{q_1},\dots,\frac{p_m}{q_m}\right) \neq 0$$

step3. Use Taylor expansion to get an upper bound for $\left|Q\left(\frac{p_1}{q_1},\dots,\frac{p_m}{q_m}\right)\right|$

$$\left|Q\left(\frac{p_1}{q_1},\dots,\frac{p_m}{q_m}\right)\right| \leq C^{d_1+\dots+d_m} \max_j q_j^{-\kappa t d_j}$$

$\left(\begin{array}{c}\kappa t \leq m + O(\frac{1}{M}) \\ t = (\frac{1}{2}-\varepsilon)\end{array}\right)$

step. Comparing with Liouvill's lower bound to find. $\kappa \leq \frac{1}{\frac{1}{2}-\varepsilon}$

<u>Roth's Lemma</u> $0 \neq P(X_1,\dots,X_m)\in\overline{\mathbb{Q}}[X_1,\dots,X_m]$, $\deg_{X_j} P \leq d_j$ $\forall i$

Given $\xi=(\xi_1,\dots,\xi_m)\in\overline{\mathbb{Q}}$, $0<\sigma<\frac{1}{2}$

Suppose: (a) $d_{j+1}/d_j \leq \sigma$ ("$d_1 > d_2 > \cdots > d_m$ decreasing rapidly")

(b) $\min_j d_j h(\xi_j) \geq \sigma^{-1}(h(P)+4m d_1)$ ("all components of ξ have large height")

Then $\operatorname{ind}(P; \underset{(d_1,\dots,d_m)}{d}, \underset{(\xi_1,\dots,\xi_m)}{\xi}) \leq 2m\,\sigma^{\frac{1}{2^{m-1}}}$

$\|$

$$\min_{\mu=(\mu_1,\dots,\mu_m)} \left\{ \frac{\mu_1}{d_1}+\dots+\frac{\mu_m}{d_m} \;\middle|\; \underbrace{\left(\prod_j \frac{1}{\mu_j!}\partial_{X_j}^{\mu_j}\right)}_{\partial_\mu} P(\xi_1,\dots,\xi_m)\neq 0\right)$$

Note: Case $m=1$. $P(x) = (x-\xi_1)^{d_1 \cdot ind(P,d,\xi)} \cdot q(x)$

Recall: General inequality $\vec{x} = (x_1, \dots, x_m)$

$$-d \log 2 + \sum_{i=1}^{n} h(f_i) \le h(f_1(\vec{x}) \cdots f_n(\vec{x})) \le d \log 2 + \sum_{i=1}^{n} h(f_i)$$

where $d = \sum_{j=1}^{m} \deg_{x_j}(f_1 \cdots f_n)$

So
$$ind(P,d,\xi) \cdot d_1 \cdot h(\xi_1) \le h(P) + d_1 \log 2$$

The above $\le$ + the assumption $d_1 h(\xi_1) \ge \sigma^{-1}(h(P) + 4d_1)$

$$\Rightarrow ind(P,d,\xi) \le \frac{h(P) + d_1 \log 2}{\sigma^{-1}(h(P)+4d_1)} < \sigma$$ (So better than the asserted $ind(P,d,\xi) \le 2\sigma$)

pf of Roth's Lemma:

Write $P(x_1, \dots, x_m) = \sum_{j=0}^{s} f_j(x_1, \dots, x_{m-1}) \cdot g_j(x_m)$ with s minimum

$\leadsto$ $(f_0, \dots, f_s)$ and $(g_0, \dots, g_s)$ are both linearly indep

$\leadsto$ $s \le d_m$

$\Rightarrow \exists\, \mu_0, \dots, \mu_s \in \mathbb{N}^{m-1}$ with $|\mu_i| \le i$ $\forall i = 0, 1, \dots, s$ $\leadsto$ $|\mu_i| \le d_m$ $\forall i = 0, 1, \dots, s$

and $\nu_0, \dots, \nu_s \in \mathbb{N}$ with $\nu_i \le i$ $\forall i = 0, 1, \dots, s$

s.t.

$$U(x_1, \dots, x_{m-1}) \overset{def}{=} \det\left(\partial_{\mu_i} f_j\right)_{0 \le i, j \le s} \neq 0$$

and
$$V(x_m) \overset{def}{=} \det\left(\partial_i g_j\right)_{0 \le i \le j \le s} \neq 0$$

$$U(x_1, \dots, x_{m-1}) \cdot V(x_m) = \det\left(\partial_{\mu_i, j} P\right)_{0 \le i, j \le s} =: W(x_1, \dots, x_m) \in \overline{\mathbb{Q}}[x_1, \dots, x_m]$$

W is a sum of $(s+1)!$ product of $s+1$ terms; each of the $s+1$ terms is $\partial_{\mu_i, \nu_j} P$ for some (i,j)

Similarly for $U(x_1, \dots, x_{m-1})$ and $V(x_m)$ $\quad \sum_{i=1}^{m-1} \deg_{x_i} U \le (s+1)(d_1 + \dots + d_{m-1})$

$\deg_{x_m} V \le (s+1) \cdot s \le (s+1) d_m$

Estimate $h(W)$ using $W = \det(\partial_{\mu_i, j} P)_{0 \le i, j \le n}$

$$h(W) \le \underbrace{\sum_{v \in M_K} \max_{\pi \in S_{n+1}} \log \left| \prod_{i=0}^{s} \partial_{\mu_i, \pi(i)} P \right|_v}_{= h\left(\prod_{i=0}^{s} \partial_{\mu_i, \pi(i)} P\right)} + \log (s+1)!$$

$\left(\because h(Q_1 + \dots + Q_t) \le \sum_i h(P_i) + \log t \right)$

Note $(s+1)! \le (d_m + 1)^{s+1}$ $\quad \because s \le d_m$

$$h\left(\prod_{i=0}^{s} \partial_{\mu_i, \pi(i)} P\right) \le \sum_{i=0}^{s} \underbrace{h(\partial_{\mu_i, \pi(i)} P)}_{\le h(P) + \left(\sum_{i=1}^{m} d_i\right) \cdot \log 2} + \left(\sum_{i=1}^{m} d_i\right) \cdot \log 2$$

$\because \sum_{i=0}^{N} \binom{N}{i} = 2^N$

$$\le (s+1) h(P) + (s+2) \cdot \left(\sum_{i=1}^{m} d_i\right)$$

$$\Rightarrow h(W) \le (s+1) h(P) + (s+2) \cdot \left(\sum_{i=1}^{m} d_i\right) \cdot \log 2 + (s+1) \cdot \log(d_m + 1)$$

$$\le (s+1)\left(h(P) + 4d_1\right)$$

$d_1 + \dots + d_m \le 2d_1$

$\because \log(d_m + 1) \le d_m \le \frac{1}{2} d_1$

Clearly
$$ind(W, d, \xi) = ind(U, (d_1, \ldots, d_{m-1}), (\xi_1, \ldots, \xi_{m-1})) + ind(V, d_m, \xi_m)$$

Have upper bounds for $ind(U, (d_1, \ldots d_{m-1}), (\xi_0, \ldots, \xi_{m-1}))$
and $ind(V, d_m, \xi_m)$ by induction

From general inequalities for ind
$$\begin{cases} ind(Q_1 + Q_2; \underline{d}, \underline{\alpha}) \geq \min(ind(Q_1; \underline{d}; \alpha), ind(Q_2; \underline{d}, \alpha)) \\ ind(Q_1 \cdot Q_2; \underline{d}, \underline{\alpha}) = ind(Q_1; \underline{d}; \underline{\alpha}) + ind(Q_2; \underline{d}, \alpha) \\ ind(\partial_{\underline{\mu}} Q, \underline{d}, \underline{\alpha}) \geq ind(Q; \underline{\mu}, \underline{\alpha}) - \sum_{i=1}^{m} \frac{\mu_i}{d_i} \end{cases}$$

One checks easily that the conditions for U and V are satisfied with $(s+1) d_j$ in place of d_j ($\because$ each is an $(s+1) \times (s+1)$ determinant)

One gets
$$(*) \quad \begin{cases} ind(U, (d_1, \ldots, d_{m-1}), (\xi_0, \ldots, \xi_{m-1})) \leq 2(m-1)(s+1)\,\sigma^{\frac{1}{2^{m-2}}} \\ ind(V, d_m, \xi_m) \leq (s+1)\sigma \end{cases}$$

(The factor $(s+1)$ appears because of the weights) are scaled by $s+1$.

To get a lower bound of $ind(W, d, \xi)$, we expand the determinant $\det(\partial_{\mu_{i,j}} P)$ to get a lower bound of $ind(W, d, \xi)$

$$W(x_1, \ldots x_m) = \sum_{\pi \in S_{n+1}} \prod_{i=0}^{s} \partial_{\mu_{i}, \pi_i} P$$

$$\begin{aligned} ind(\partial_{\mu_{i,\pi(i)}} P, d, \xi) &\geq ind(P, d, \xi) - \frac{\mu_{i,1}}{d_1} - \cdots - \frac{\mu_{i,m-1}}{d_{m-1}} - \frac{\pi(i)}{d_m} \\ &\geq ind(P) - \frac{d_m}{d_{m-1}} - \frac{\pi(i)}{d_m} \qquad \because \mu_{i,1} + \cdots + \mu_{i,m-1} \leq s \leq d_m \\ &\geq ind(P) - \frac{\pi(i)}{d_m} - \sigma \end{aligned}$$

$$\rightsquigarrow ind(\partial_{\mu_{i,\pi(i)}} P, d, \xi) \geq \operatorname{Max}\left(ind(P, d, \xi) - \frac{\pi(i)}{d_m}, 0\right) - \sigma$$

$$\rightsquigarrow \quad ind(W, d, \xi) \geq \operatorname*{Min}_{\pi \in S_{n+1}} \left(\sum_{i=0}^{s} ind(\partial_{\mu_{i}, \pi(i)} P) \right)$$

$$\underset{\text{use the above estimate}}{\geq} \operatorname*{Min}_{\pi} \left(\sum_{i=0}^{s} \max\left(ind(P) - \frac{\pi(i)}{d_m}, 0\right) - \sigma \right)$$

$$(**) \quad = \sum_{i=0}^{s} \left(\max\left(ind(P) - \frac{i}{d_m}, 0\right) - \sigma \right)$$

$$\geq (s+1) \min\left(\tfrac{1}{2} ind(P), \tfrac{1}{2} ind(P)^2\right)$$

use $\sum_{i=0}^{s} \max\left(t - \frac{i}{s}, 0\right) \geq (s+1) \min\left(\frac{1}{2}t, \frac{1}{2}t^2\right)$

simple, discuss cases $t \geq 1$ and $t < 1$

Combine (*) with (**) to get

$$\min\left(\mathrm{ind}(P),\ \mathrm{ind}(P)^2\right) \leq 4(m-1)\,\sigma^{\frac{1}{2^{m-2}}} + 4\sigma$$

$$\leadsto \quad \mathrm{ind}(P) \leq m$$

Then: $\mathrm{ind}(P)^2 \leq m \cdot \min\left(\mathrm{ind}(P),\ \mathrm{ind}(P^2)\right)$

$$\leq 4m(m-1)\,\sigma^{\frac{1}{2^{m-2}}} + 4m\sigma \leq 4m^2\,\sigma^{\frac{1}{2^{m-2}}}$$

QED