arXiv:2301.00518v1 [math.NT] 2 Jan 2023

全局函数域上椭圆曲线的弗罗贝尼乌斯扭曲

KI-SENG TAN

Abstract. 对于定义在特征为 $p>0$ 的全局函数域 K 上的椭圆曲线 A，其弗罗贝尼乌斯扭曲 $A^{(p)}$ 的 p-塞尔默群的阶往往大于 A 的阶。本文旨在探讨这一现象。

1. Introduction

对于定义在特征为$p>0$的全局函数域 K 上的椭圆曲线 A，其弗罗贝尼乌斯扭曲的 p-塞尔默群的阶往往大于 A 的阶。本文旨在探讨这一现象。

弗罗贝尼乌斯扭曲 $A^{(p)}$ 是沿绝对弗罗贝尼乌斯 Frob_p 的基变换 $A\times_K K$：$K\longrightarrow K,\quad x\mapsto x^p$。

1.1. 主要结果。我们假设 A/K 是普通的，且处处具有半稳定约化。令 $\Delta_{A/K}$ 表示 A/K的全局极小判别式除子。比较两条曲线的定义方程可得

$$\Delta_{A^{(p)}/K}=p\cdot\Delta_{A/K}. \tag{1}$$

令 A_{p^ν} 为 A 上乘以 p^ν 的核，并令

$$\mathrm{Sel}_{p^\nu}(A/K)\subset \mathrm{H}^1(K,A_{p^\nu})$$

表示 A/K的 p^ν-塞尔默群。若 $p=2$，令 $\mathfrak{d}'$ 为 K 中满足以下条件的赋值集合：A 具有非分裂乘法约化，且其分支群的阶为偶数；否则，令 $\mathfrak{d}'=\emptyset$。令 S_b 表示 A/K的坏约化处集合。记

$$S_b=\mathfrak{d}'\sqcup\mathfrak{d}.$$

令 $k=K(A_p^{(p)}(\bar{K}^s))$，并令 $\mathfrak{d}_0\subset\mathfrak{d}$ 为在 k上完全分裂的赋值子集。令 $\hbar$ 表示由以下同态组成的 $\mathrm{Hom}(\mathrm{Gal}(k^s/k)\ \mathbb{Z}/p\mathbb{Z})$子群的 p-秩：这些同态处处非分歧，且在 k中位于 $\mathfrak{d}$之上的每个赋值处局部平凡。我们的主要结果如下。令 q 表示 K 的常数域的阶。

命题 1. 存在一个整数 ϵ_1, $2\hbar+1+|\mathfrak{d}_0|\geq\epsilon_1\geq-|\mathfrak{d}_0|$，使得

$$\log_p|\mathrm{Sel}_p(A^{(p)}/K)|=\frac{(p-1)\deg\Delta_{A/K}}{12}\cdot\log_p q+\epsilon_1.$$

致谢：本研究部分得到了台湾科技部 MOST 109-2115-M-002-008-MY2 项目的支持。作者感谢 F. Trihan 提供的许多宝贵建议，尤其感谢他帮助作者完成引理 3.1.1 的证明。

命题 2. 存在一个整数 ϵ_2, $2\hbar+1+|\eth_0| \geq \epsilon_2 \geq -2\hbar-3|\eth_0|$，使得对于每个正整数 ν，

$$\log_p |\operatorname{Sel}_{p^{\nu+1}}(A^{(p)}/K)| = \frac{(p-1)\deg \Delta_{A/K}}{12} \cdot \log_p q + \log_p |\operatorname{Sel}_{p^\nu}(A/K)| + \epsilon_2.$$

注意，$\frac{\deg \Delta_{A/K}}{12}$ 是一个非负整数（参见 [LLTT16, §2.2.1]）；当且仅当 A/K 是等变的时，它为零。令 $Ш_{p^\infty}(A/K)$ 表示 A/K的 Tate-Shafarevich 群的 p-主部分，令 $Ш_{div}(A/K)$ 表示其 p-可除子群，并将 p-余扭

$$\overline{Ш}(A/K) := Ш_{p^\infty}(A/K)/Ш_{div}(A/K) = \operatorname{Sel}_{p^\infty}(A/K)/\operatorname{Sel}_{div}(A/K),$$

其中 $\operatorname{Sel}_{div}(A/K)$ 是 $\operatorname{Sel}_{p^\infty}(A/K)$ 的 p-可除子群。令 r 表示 $\operatorname{Sel}_{div}(A/K)$ 的$\mathbb{Z}_p$-余秩。若 ν 大于 $Ш(A/K)$ 和 $Ш(A^{(p)}/K)$ 的指数，则

$$|\operatorname{Sel}_{p^\nu}(A/K)| = |\overline{Ш}(A/K)| \cdot p^{r\nu} \text{ and } |\operatorname{Sel}_{p^{\nu+1}}(A^{(p)}/K)| = |\overline{Ш}(A^{(p)}/K)| \cdot p^{r(\nu+1)}.$$

由命题 2 可得

$$\log_p |\overline{Ш}(A^{(p)}/K)| + r = \frac{(p-1)\deg \Delta_{A/K}}{12} \cdot \log_p q + \log_p |\overline{Ш}(A/K)| + \epsilon_2.$$

这类公式受到 Birch–Swinnerton-Dyer 猜想公式的启发（参见 [Ta66, Tan95]），该猜想分别适用于 $A^{(p)}/K$ 和 A/K。

接下来，设 L/K 是 A/K的一个 $\mathbb{Z}_p^d$-扩张，且仅在有限多个普通素点处分歧。记 $\Gamma := \operatorname{Gal}(L/K)$，并记 $\Lambda_\Gamma := \mathbb{Z}_p[[\Gamma]]$。设 Z 是一个有限生成的挠 Λ_Γ-模，则存在一个正合列

$$0 \longrightarrow \bigoplus_{i=1}^m \Lambda_\Gamma/(p^{\alpha_i}) \oplus \bigoplus_{j=1}^n \Lambda_\Gamma/(\eta_j^{\beta_j}) \longrightarrow Z \longrightarrow N \longrightarrow 0, \tag{2}$$

其中 α_1、...、α_m、β_1、...、β_n 均为正整数，η_1、...、$\eta_n \in \Lambda_\Gamma$ 均不可约，且与 p 互素；N 为伪零。尽管该正合列并非典范的，模 $\bigoplus_{i=1}^m \Lambda_\Gamma/(p^{\alpha_i})$ 和 $\bigoplus_{j=1}^n \Lambda_\Gamma/(\eta_j^{\beta_j})$ 由 Z 唯一确定，我们称它们分别为 Z 的 p部分和非-p部分；称 p^{α_1}、...、p^{α_m} 为初等 μ-不变量，并称 m 为 Z 的 μ-秩。若 Z 非挠，则将 μ-秩定义为 ∞。

考虑 $\operatorname{Sel}_{p^\infty}(A/L)$、$\operatorname{Sel}_{p^\infty}(A^{(p)}/L)$ 的庞特里亚金对偶 X、$X^{(p)}$。它们在 Λ_Γ 上有限生成（见 [Tan14]）。令

$$\eth_1 := \{v \in \eth \mid v \text{ splits completely over } kL\}.$$

命题 3. $X^{(p)}$ 的 μ-秩至少为 $\frac{(p-1)\text{ 的度}}{12}\Delta_{A/K} \cdot \log_p q - |\eth_1|$。

若 L 包含 $K_p^{(\infty)}$，即 K上的常数 $\mathbb{Z}_p$-扩张，则在此情形下，X 和 $X^{(p)}$ 是挠[OT09, Tan14], $|\eth_1| = 0$。

命题 4. 若 L 包含 $K_p^{(\infty)}$，则 $X^{(p)}$的 μ-秩 m 等于 $(p-1)$ 次 $\Delta_{A/K} \cdot \log_p q$。此外，若 $p^{\alpha_1}, ..., p^{\alpha_m}$, $\alpha_1 \geq \cdots \geq \alpha_m$ 是 $X^{(p)}$ 的初等 μ- 不变量，则 X 的初等不变量为 $p^{\alpha_1-1}, ..., p^{\alpha_{m'}-1}$，其中 m' 是满足$\alpha_i > 1$的最大 i。

对于有限扩张 F/K，记 $\mathfrak{w}_F$ 为 kF的除子类群的 p-完备化；对于 L/K的一个 $\mathbb{Z}_p^e$子扩张 M/K，令 $\mathfrak{w}_M:=\varprojlim_{K\subset F\subset M}\mathfrak{w}_F$，它是 $\Lambda_{\mathrm{Gal}(kM/k)}$上的有限生成挠模。实际上，根据 [Crw87], ， $\mathfrak{w}_M$的特征理想有一个生成元 $\Theta_M:=\varprojlim_{F}\Theta_F$，其中基本上对每个 F， $\Theta_F\in\mathbb{Z}_p[\mathrm{Gal}(kF/k)]$ 都是 [Ta84, §V.1.1], 中定义的 Stickelberger 元。特别地，我们有

$$p_{L/M}(\Theta_L)=\Theta_M\cdot *, \tag{3}$$

其中 $p_{L/M}:\Lambda_{\mathrm{Gal}(Lk/k)}\longrightarrow\Lambda_{\mathrm{Gal}(Mk/k)}$ 是连续的 $\mathbb{Z}_p$-代数同态，它扩张了商映射 Gal(Lk/k) $\longrightarrow$ Gal(Mk/k)，而 $*\in\Lambda_{\mathrm{Gal}(Mk/k)}$ 是一个不能被 p 整除的修正因子。

为简便起见，我们将 $\Lambda_{\mathrm{Gal}(Mk/k)}$ 与 $\Lambda_{\mathrm{Gal}(M/K)}$ 等同，并将 Θ_L、 $\mathfrak{w}_L$ 视为定义在 Λ_Γ 上的对象。在 $L=K_p^{(\infty)}$ 的特殊情形下，模 $\mathfrak{w}_L$ 的 μ-秩为零，因此 Θ_L 不能被 p 整除。为此，令 $\mathcal{Y}$ 为定义在 k 的常数域上的完备光滑曲线，其函数域为 k 。对于 L/K 的每个有限子扩张 F/K ，我们有正合列

$$0\longrightarrow\mathfrak{w}_F^0\longrightarrow\mathfrak{w}_F\xrightarrow{\deg}\mathbb{Z}_p\longrightarrow 0$$

且 $\mathfrak{w}_F^0[p]$ 包含于 $\mathcal{Y}$ 的雅可比簇的 p-除点子群中。因此，$\mathfrak{w}_F^0[p]$ 的阶有界，从而 $\mathfrak{w}_L[p]=0$。一般而言，(3) 表明，若 L 包含 $K_p^{(\infty)}$，则 Θ_L 不能被 p 整除。此外，在此情形下，$\eth_1=\emptyset$。因此，命题 4 是下述命题的特殊情形。

命题 5. 若 Θ_L 不能被 p 和 $\eth_1=\emptyset$整除，则 $X^{(p)}$的 μ-秩 m 等于 $\frac{(p-1)\deg}{12}^{\Delta_{A/K}}\cdot\log_p q$。~~此外，若~~ $p^{\alpha_1},...,p^{\alpha_m}$, $\alpha_1\geq\cdots\geq\alpha_m$是 $X^{(p)}$的初等 μ-不变量，则 X的初等不变量为 $p^{\alpha_1-1},...,p^{\alpha_{m'}-1}$，其中 m'是满足 $\alpha_i>1$的最大 i 。

由于弗罗贝尼乌斯和 Verschiebung 在 X 和 $X^{(p)}$的非-p 部分之间诱导伪同构，该命题推出 $X^{(p)}$的特征理想是 X的特征理想的 $q_{(p-1)\deg 12}^{\Delta_{A/K}}$倍。若 $L=K_p^{(\infty)}$，~~这也~~可由 [LLTT16]的主定理推出。

1.2. 记号。对于域 F，令 F和 F^s分别表示其代数闭包和可分闭包，并将 $G_F=$记作 Gal(F^s/F)。对于赋值 v，令 $\mathcal{O}_v$、 π_v和 $\mathbb{F}_v$分别表示整数环、统一化元和剩余域。将 q_v 记作 $|\mathbb{F}_v|$。

令 S_{ss} 表示 K 中 A具有超奇异约化的赋值 v 所构成的集合。对于 K 的赋值集合 S 及代数扩张 F，令 $S(F)$表示 F 中位于 S之上的赋值集合。对于阿贝尔群 H 的端同态 φ ，令 $H[\varphi]$表示其核。用 $^\vee$ 表示庞特里亚金对偶，用 $\sim$ 表示伪同构。

本文使用平坦上同调或伽罗瓦上同调。令

$$\mathsf{F}:A\longrightarrow A^{(p)}\ \text{ and }\ \mathsf{V}:A^{(p)}\longrightarrow A$$

分别为弗罗贝尼乌斯和 Verschiebung 同态。我们有以下正合列

$$0 \longrightarrow C_p \longrightarrow A_p \xrightarrow{\mathsf{F}} E_p^{(p)} \longrightarrow 0, \tag{4}$$

以及

$$0 \longrightarrow E_p^{(p)} \longrightarrow A_p^{(p)} \xrightarrow{\mathsf{V}} C_p \longrightarrow 0, \tag{5}$$

其中 $C_p = \ker \mathsf{F}$ 连通，而 $E_p^{(p)} = \ker \mathsf{V}$，$'$为 étale（见 [LSc10]）。对于包含 K 的域 F，有 $A_p^{(p)}(F) = E_p^{(p)}(F)$。特别地，$k = K(E_p^{(p)}(\bar{K}^s))$。注意，对于 $p = 2$，$k = K$，因为 $E_p^{(p)}(\bar{K}^s)$ 的非平凡点是其唯一的伽罗瓦共轭。

1.3. 证明。命题 1 的证明中的关键要素是局部的，涉及自然映射 $\mathrm{H}^1(K_v, E_p^{(p)}) \longrightarrow \mathrm{H}^1(K_v, A^{(p)})$ 的核，尤其是当 v 为超奇异约化的赋值时。引理 2.2.1、引理 2.2.2 和引理 2.3.3 讨论了不同类型的约化，并根据相应的循环扩张在 k_v 上的导子，为判定 $\mathrm{H}^1(K_v, E_p^{(p)})$ 中的元素是否属于该核提供了准则。

利用现有的局部判据，并借助整体类域论，我们在命题 3.2.5 中确定了 $\mathrm{Sel}(E_p^{(p)}/K)$ 的阶，即 $\mathrm{Sel}_p(A^{(p)}/K)$ 的 $E_p^{(p)}$-部分。在此过程中，我们发现一个有趣的现象：式 (1) 所述的两个判别式之间的差异完全由超奇异处造成（见 (27)）。接下来，在命题 3.2.6 中，我们利用 Poitou-Tate 对偶 [Ces15] 确定了 $\mathrm{Sel}(C_p/K)$ 的阶，即 $\mathrm{Sel}_p(A/K)$ 的C_p-部分。随后，作为上述两个命题的推论，命题 1 在 §3.2 末尾得以证明。命题 2 则通过应用 Cassels-Tate对偶性在 §3.3 中得以证明。

在 §3.4 中，我们利用 Monsky定理 [Mon81]，建立了一种方法，将命题 3、5 的证明归约到 $d = 1$ 情形。由于该方法可应用于更一般的情况，我们放宽了该小节中的条件，允许A 为定义在全局域 K 上的普通阿贝尔簇。主要结果总结在引理 3.4.4 中。作为该引理及命题 1、2 的推论，命题 3、5 的证明在最后一个小节 §3.5 中给出。

2. Local fields

在 K 的每个赋值 v 处，我们有长正合列

$$\cdots \longrightarrow A^{(p)}(K_v) \xrightarrow{\mathsf{V}_*} A(K_v) \xrightarrow{\partial} \mathrm{H}^1(K_v, E_p^{(p)}) \xrightarrow{j_v} \mathrm{H}^1(K_v, A^{(p)}) \longrightarrow \cdots \tag{6}$$

由 $0 \longrightarrow E_p^{(p)} \xrightarrow{j} A^{(p)} \mathsf{V} \succ A \longrightarrow 0$ 导出。本节旨在确定 $\ker(j_v) = \mathrm{coker}(\mathsf{V}_*)$。对于位于 v 之上的赋值 w，阿贝尔群 k

$$\mathrm{H}^1(k_w, E_p^{(p)}) = \mathrm{Hom}(G_{k_w}, \mathbb{Z}/p\mathbb{Z}) = \mathrm{Hom}(k_w^*/(k_w^*)^p, \mathbb{Z}/p\mathbb{Z}), \tag{7}$$

因此，每个 $\xi \in \mathrm{H}^1(k_w, E_p^{(p)})$ 都确定一个次数为 p 的循环扩张 $k_w,\ \xi/k_w$。

令 ord_v 表示定义在.....上的赋值 $\bar{K}_v$ 满足 $\mathrm{ord}_v(\pi_v) = 1$。

2.1. 弗罗贝尼乌斯与 Verschiebung。令 $\mathscr{F}$（分别为 $\mathscr{F}^{(p)}$）表示与 A（分别为 $A^{(p)}$）相关联的形式群律，其定义在 K_v 上。由于 A 具有半稳定约化，$\mathscr{F}$ 在局部域扩张下是稳定的。令 A 表示 A 在 v处的约化。对于 K的代数扩张 F 中位于 v之上的赋值 w，在约化映射 $A(F_w) \longrightarrow A(\mathbb{F}_w)$ 下，$0 \in A(\mathbb{F}_w)$ 的原像 $A_o(F_w)$ 可通过双射 ι与 $\mathscr{F}(\mathfrak{m}_w)$ 识别。令 $\iota^{(p)}$ 为与 $A_o^{(p)}(F_w)$ 相关联的对应双射。

Le令 t $\mathscr{P} \in \mathcal{O}_v[[t]]$ 为满足交换图的唯一幂级数 m

$$\begin{array}{ccccc} \mathscr{F}(\mathfrak{m}_w) & \xrightarrow{\mathrm{Frob}_p} & \mathscr{F}^{(p)}(\mathfrak{m}_w) & \xrightarrow{\mathscr{P}} & \mathscr{F}(\mathfrak{m}_w) \\ \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle \iota^{(p)}} & & \downarrow{\scriptstyle \iota} \\ A_o(F_w) & \xrightarrow{\mathsf{F}} & A_o^{(p)}(F_w) & \xrightarrow{\mathsf{V}} & A_o(F_w). \end{array} \tag{8}$$

元素 $\xi \in \mathfrak{m}_w$ 满足 $\mathscr{P}(\xi) = 0$，当且仅当 $\iota^{(p)}(\xi) \in E_p^{(p)}(F_w) \cap A_o^{(p)}(F_w)$。

设 $\mathscr{F}$（分别地，$\mathscr{F}^{(p)}$）的形式群律由 $\mathcal{O}_v$ 系数的幂级数 $f(X,Y)$（分别地，$f^{(p)}(X,Y)$）给出。

若 t_i 是方程 $\mathscr{P}(t) = 0$的解，则 $\mathscr{P}(f^{(p)}(t,t_i)) = \mathscr{P}(t)$；此外，由于$A/K_v$ 是普通的，根据 [Sil86, §IV.7.2]，$\mathscr{P}'(0) \neq 0$，因此 $\mathscr{P}'(t_i) \neq 0$也成立。

引理 2.1.1. 我们有 $\mathscr{P}(t) = u(t) \cdot P(t)$，其中 $u(t)$ 是 $\mathcal{O}_v[[t]]$ 中的一个单位，而 $P(t)$是相应的 distinguished 多项式。多项式 $P(t)$ 可分，且 $P(0) = 0$。若 v 是超奇异处，则 deg $P = p$；若 v 是普通的，则$P(t) = t$。

证明。第一个断言由以下结论推出：π_v 不整除 $\mathscr{P}(t)$。对于普通的 v，由于 $E_p^{(p)}(\bar{K}_v) \cap A_o^{(p)}(\bar{K}_v) = \{0\}$，我们知道，在 K_v中，0是$P(t)$的唯一根。这意味着 distinguished 多项式 $P(t) = t$。对于超奇异的 v，群 $E_p^{(p)}(\bar{K}_v) \cap A_o^{(p)}(\bar{K}_v) \simeq \mathbb{Z}/p\mathbb{Z}$，因此 deg $P(t) = p$；此外，由于$\mathscr{P}(t_i) = 0$ 且 $\mathscr{P}'(t_i) \neq 0$，我们有 $P(t_i) = 0$ 且 $P'(t_i) \neq 0$。

为证明该结论，我们先考虑 v 是良约化赋值的情形。$\bar{}$ $\bar{}$与 A 相关联的形式群律为 $f(X,Y) := f(X,Y) \pmod{(\pi_v)}$，$\bar{}$其高度为1或2，因此 $\mathscr{P} := \mathscr{P} \pmod{(\pi_v)}$非零。这就证明了该结论。

对于乘法位置 v，我们通过证明 Verschiebung 导出一个同构 $\mathscr{F}^{(p)}(\mathfrak{m}_v) \longrightarrow \mathscr{F}(\mathfrak{m}_v)$ 来证明该断言。如果 v 是分裂乘法约化点，且 $\tilde{Q}$ 是 A 的局部泰特周期，那么 $\tilde{Q}^p$ 是 $A^{(p)}$ 的局部泰特周期，而 Verschiebung 由 $K_v^*/\tilde{Q}^{p\mathbb{Z}} \longrightarrow K_v^*/\tilde{Q}^{\mathbb{Z}}$ 给出，它由 K_v^* 上的恒等映射诱导而来。这意味着 $\mathscr{F}_{(p)}(\mathfrak{m}_v) \longrightarrow \mathscr{F}(\mathfrak{m}_v)$ 是一个同构，因此该断言得证。

若 v 是非分裂乘法的，则 A/K_v 是分裂乘法椭圆曲线 B/K_v 在非分歧二次扩张 L_w/K_v下的扭曲。令 Z_v 为范数映射 N_{L_w/K_v}：$\mathcal{O}_w^* \longrightarrow \mathcal{O}_v^*$ 的核。则 $\mathscr{F}^{(p)}(\mathfrak{m}_v) \longrightarrow \mathscr{F}(\mathfrak{m}_v)$ 由恒等映射 $\mathrm{Z}_v \longrightarrow \mathrm{Z}_v$ 给出，因此它是一个同构。

□

2.2. 普通位置。引理 2.1.1 的证明表明，若 v 是分裂乘法赋值，则 V_* 由 $K_v^*/\tilde{Q}^{p\mathbb{Z}} \longrightarrow K_v^*/\tilde{Q}^{\mathbb{Z}}$给出，因而是满射，所以由 (6) 得 $\ker(j_v) = 0$。

引理 2.2.1. 设 v 是一个乘法位置。则 $\ker(j_v) = 0$，除非 $v \in \eth'$；在这种情况下，$\ker(j_v)$ 的阶为 $2 = p$，由 $\xi \in \mathrm{H}^1(K_v, E_p^{(p)})$ 组成，其中 $K_{v,\ \xi}/K_v$非分歧。

注意，如果 $p = 2$，那么 $k = K$，因此 $K_{v,\ \xi}$ 有定义。

证明。假设 v 是非分裂乘法的，并令 B/K_v 和 L_w/K_v 如引理 2.1.1 的证明中所设。由于 A/L_w 是分裂乘法的，我们有单射 $\mathrm{H}^1(L_w, E_p^{(p)}) \longrightarrow \mathrm{H}^1(L_w, A^{(p)})$，因此

$$\ker(j_v) = \ker(\mathrm{H}^1(L_w/K_v, E_p^{(p)}(L_w)) \longrightarrow \mathrm{H}^1(L_w/K_v, A^{(p)}(L_w))).$$

对于 $p \neq 2$，我们有 $\mathrm{H}^1(L_w/K_v, E_p^{(p)}(L_w)) = 0$，所以 $\ker(j_v) = 0$。记 $G = \mathrm{Gal}(L_w/K_v)$，我们有交换图

$$\begin{array}{ccc} \mathrm{H}^1(L_w/K_v, E_p^{(p)}(L_w)) & \longrightarrow & \mathrm{H}^1(L_w/K_v, A^{(p)}(L_w)) \\ \downarrow \simeq & & \downarrow \simeq \\ \mathrm{Hom}(G, \mathbb{Z}/2\mathbb{Z}) & \longrightarrow & B^{(p)}(K_v)/\,\mathrm{N}_{L_w/K_v}(B^{(p)}(L_w)). \end{array}$$

$\mathrm{Hom}(G, \mathbb{Z}/2\mathbb{Z})$ 的非平凡元素将 G 的生成元映射到由 B/K_v 的 Tate 局部周期 Q_v 得到的 $B^{(p)}(K_v)$ 中的点；当且仅当 $Q_v \in \mathrm{N}^{L_w/K_v}(L_w^*)$ 时，该元素对应于 $\ker(j_v)$ 的一个元素，等价地说，$\mathrm{ord}_v Q_v$ 为偶数。

□

引理 2.2.2. 假设 v 是一个良好普通赋值，且 w 是位于 k 上方的 v 的一个赋值。那么 $\ker(j_w)$ 的阶为 p，由满足 $k_{w,\xi}/k_w$ 非分歧的 $\xi \in \mathrm{H}^1(k_w, E_p^{(p)})$ 构成。若 $K_v \neq k_w$，则 $\ker(j_v)$ 是平凡的。

证明. 根据图表（8），引理 2.1.1 表明 $A_o^{(p)}(k_w) \sim \mathrm{V} \succ A_o(k_w)$。我们需要确定由此诱导的 $\bar{\mathrm{V}} : \bar{A}^{(p)}(\mathbb{F}_w) \longrightarrow \bar{A}(\mathbb{F}_w)$ 的余核。Frobenius $\bar{\mathrm{F}}$ 将 $\bar{A}^{(p)}(\mathbb{F}_w)$ 与 $\bar{A}(\mathbb{F}_w)$ 等同，在此对应下，$\bar{\mathrm{V}}$ 对应于乘以 p。所讨论的余核同构于

$$\bar{A}(\mathbb{F}_w)/p\bar{A}(\mathbb{F}_w) \simeq \bar{A}_p(\mathbb{F}_w) = \bar{E}_p^{(p)}(\mathbb{F}_w).$$

将蛇引理应用于该图表

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_o^{(p)}(k_w) & \longrightarrow & A^{(p)}(k_w) & \longrightarrow & \bar{A}^{(p)}(\mathbb{F}_w) & \longrightarrow & 0 \\ & & \simeq \downarrow \mathrm{V} & & \downarrow \mathrm{V} & & \downarrow \bar{\mathrm{V}} & & \\ 0 & \longrightarrow & A_o(k_w) & \longrightarrow & A(k_w) & \longrightarrow & \bar{A}(\mathbb{F}_w) & \longrightarrow & 0 \end{array}$$

这意味着约化映射 $E_p^{(p)}(k_w) \longrightarrow \bar{E}_p^{(p)}(\mathbb{F}_w)$ 是一个同构，因此 $\ker(j_w)$ 的阶为 p；根据 [Mil06, §I.3.8], ，它由所有非分歧 ξ 构成。若 $K_v \neq k_w$，则 $\bar{E}_p^{(p)}(\mathbb{F}_v) = E_p^{(p)}(K_v) = 0$，类似的论证表明 $\ker(j_v)$ 是平凡的。

□

2.3. 超奇异处。设 v 是超奇异的。取一个非零的 $t_1 \in \mathfrak{m}_w$（属于某个 F_w），使得 $\iota^{(p)}(t_1) \in E_p^{(p)}(F_w)$。令 $[u]$ 表示 $A^{(p)}$ 上乘以 u 的映射。由于 t_u:
$= \iota^{(p)^{-1}} \circ [u] \circ \iota^{(p)}(t_1) = ut_1 +$高阶项，若 $p \nmid u$，则 $\mathrm{ord}_v\, t_u = \mathrm{ord}_v\, t_1$。记

$$n_v := \sum_{i \in \mathbb{F}_p^*} \mathrm{ord}_v\, t_i = (p-1)\,\mathrm{ord}_v(t_u),\ \text{for } (u,p) = 1. \tag{9}$$

写作

$$P(t) = t^p + z_{p-1}t^{p-1} + \cdot + z_1 t,$$

with

$$\mathrm{ord}_v\, z_1 = n_v. \tag{10}$$

对于 $s, t \in \mathfrak{m}$，记 $s \boxplus t$ 为 $\mathscr{F}^{(p)}(s,t)$。则 $\iota^{(p)}(s \boxplus t) = \iota^{(p)}(s) + \iota^{(p)}(t)$。图表（8）表明，对于给定的 $b \in \mathfrak{m}_v$，若 $a_0 \in \mathfrak{m}_w$ 是 $\mathscr{P}(t) - b = 0$ 的一个根，则所有其他根都等于 $a_u := a_0 \boxplus t_u = \mathscr{F}^{(p)}(a_0, t_u)$，$u = 1, ..., p-1$。令 $Q(t)$ 为与 $\mathscr{P}(t) - b$ 相关联的 distinguished 多项式，其根也为 $a_0, ..., a_{p-1}$。由于 $Q(0) = -b \cdot \xi$，对于某个 $\xi \in \mathcal{O}_v^*$,

$$\sum_{u=0}^{p-1} \mathrm{ord}_v\, a_u = \mathrm{ord}_v\, b. \tag{11}$$

由于 $\mathscr{F}_{(p)}(X, 0) = \mathscr{F}^{(p)}(0, X) = X$，我们可以写成 $\mathscr{F}_{(p)}(X, Y) = X + Y + XY \cdot g(X, Y)$。由此可得 $a_u = a_0 + t_u +$ 高次项。因此

$$\mathrm{ord}_v(a_u - a_{u'}) = \frac{n_v}{p-1}. \tag{12}$$

引理 2.3.1. 对于每个 $b \in \mathfrak{m}_v$（满足 $\mathrm{ord}_v\, b > \frac{pn_v}{p-1}$），存在一个元素 $a \in \mathfrak{m}_v$（满足 $\mathrm{ord}_v\, a > \frac{n_v}{p-1}$），使得 $\mathscr{P}(a) = b$。反之，对于 $a \in \mathfrak{m}_v$（满足 $\mathrm{ord}_v\, a > \frac{n_v}{p-1}$），元素 $b = \mathscr{P}(a) \in \mathfrak{m}_v$ 的赋值为 $\mathrm{ord}_v\, b = \mathrm{ord}_v\, a + n_v > \frac{pn_v}{p-1}$。

证明. 如果 $b \in \mathfrak{m}_v$ 和 a_0 是 $\mathscr{P}(t) = b$的一个解，且 $\mathrm{ord}_v(a_0) > \frac{n_v}{p-1}$，那么根据（12），其他解 a_u的赋值为 $\mathrm{ord}_v\, a_u = \frac{n_v}{p-1}$。因此，如果 $a \in \mathfrak{m}_v$（满足 $\mathrm{ord}_v\, a > \frac{n_v}{p-1}$），且 $b = \mathscr{P}(a)$，那么根据（11），$\mathrm{ord}_v\, b = \mathrm{ord}_v\, a + n_v$。反之，如果 $b \in \mathfrak{m}_v$，$\mathrm{ord}_v\, b > \frac{pn_v}{p-1}$，则根据（11），存在一个解 a，满足 $\mathscr{P}(t) = b$，且 $\mathrm{ord}_v\, a > \frac{n_v}{p-1}$。比较这些赋值，我们得出 a 是其自身唯一的伽罗瓦共轭，从而 $a \in \mathfrak{m}_v$。

□

引理 2.3.2. 若 v 是 A/K的超奇异处，则其余核的

$$A^{(p)}(K_v) \xrightarrow{\mathsf{V}_*} A(K_v)$$

阶为 $p^{\epsilon_v} \cdot q_v^{n_v}$，其中若 $k_v = K_v$，$\epsilon_v = 1$；否则，$\epsilon = 0$。

证明。由于 $A(\mathbb{F}_v)$ 的阶与 p 互素，根据图表（8），我们需要证明 $\mathscr{F}^{(p)}(\mathfrak{m}_v) \overset{\mathscr{P}}{\succ} \mathscr{F}(\mathfrak{m}_v)$ 的余核具有所需的阶。

设 $\beta = [\frac{1}{p-1} n_v] + 1$。引理 2.3.1 表明，$\mathscr{P}$ 将 $\mathscr{F}_{(p)}(\mathfrak{m}^{\beta})$ 映到 $\mathscr{F}(\mathfrak{m}^{\beta+n_v})$ 上。因此，只需检验诱导同态的余核

$$\bar{\mathscr{P}} : \mathscr{F}^{(p)}(\mathfrak{m})/\mathscr{F}^{(p)}(\mathfrak{m}^{\beta}) \longrightarrow \mathscr{F}(\mathfrak{m})/\mathscr{F}(\mathfrak{m}^{\beta+n_v}).$$

由于 $\mathscr{P}$ 的核的阶为 p^{ϵ_v}，计数即可完成证明。 □

引理 2.3.2 表明

$$|\ker(j_v)| = p^{\epsilon_v} \cdot q_v^{n_v}. \tag{13}$$

引理 2.3.3. 设 v 是 K 的一个赋值，w 是位于 v上方的 k 的一个赋值。群 $\ker(j_w)$由所有满足 $k_{w,\,\xi}/k_w$ 且导子至多为 $\frac{pn_w}{p-1}$ 的 ξ 组成。

证明. 元素 $\xi \in \ker(j_w)$ 可写为 ∂x，其中某个 $x \in A$满足 (k_w)。由于 $_A(\mathbb{F}_w)$ 的阶与 p互素，我们可以选取 $x = \iota(b) \in A_o(k_w)$，其中某个 $b \in \mathfrak{m}_{w^o}$ 设 $a_0, ..., a_{p-1}$是 $\mathscr{P}(t) = b$的解。那么所有 a_u都是 $\mathcal{O}_w$上的整元，并且 $k_{w,\,\xi} = k_w(a_0)$。由 (12) 可知，若 Disc 是 $k_{w,\,\xi}/k_w$的判别式，则

$$\mathrm{ord}_w(\mathrm{Disc}) \leq p \cdot n_w.$$

这意味着 $k_{w,\xi}/k_w$ 的导子至多为 $\frac{pn_w}{p-1}$。 $\xi \in \mathrm{H}^1(k_w, E_p^{(p)})$ 中$k_{w,\xi}/k_w$ 非分歧的类属于 $\ker(j_w)$（参见 [Mil06, I.3.8]）。它们构成一个阶为 p 的子群。根据局部类域论，k_w 的次数为 p 且导子至多为 m 的分歧循环扩张，由群 D_m/D_m^p, $D_m :$ $= \mathcal{O}_w^*/1 + \pi_w^m \mathcal{O}_w$ 刻画。在我们的情形中，$m = \frac{pn_w}{p-1}$ 是一个可被 p 整除的整数（由 (9) 可知，因为每个 $t_u \in k_w$）。由于$\mathcal{O}_w = \mathbb{F}_w[[\pi_w]]$，映射

$$D_{\frac{m}{p}} \longrightarrow D_m^p, \quad x \mapsto x^p,$$

是一个双射。因此 $|D_m/D_m^p| = q_w^{m-1} \cdot (q_w - 1)/q_w^{\frac{m}{p}-1} \cdot (q_w - 1) = q_w^{n_w}$。结合 (13)，计数即可完成证明。

□

该引理实际上由（7）说明，

$$\ker(j_w) = \mathrm{Hom}(k_w^*/(1 + \pi_w^{\frac{pn_w}{p-1}} \mathcal{O}_w) \cdot (k_w^*)^p, \mathbb{Z}/p\mathbb{Z}). \tag{14}$$

3. Global fields

令 $\mathcal{X}/\mathbb{F}_q$ 为以 K 为其函数域的完备光滑曲线。令 $\mathcal{X}_g$、$\mathcal{X}_{go}$ 分别表示由 A 具有良约化、良普通约化的赋值所组成的开集。

3.1. Poitou-Tate 对偶。我们首先回顾以下内容。

引理 3.1.1. 设 $\mathrm{f} : B/K \longrightarrow B'/K$ 是椭圆曲线之间的一个给定同源，并且在所有 $v \in \mathcal{X}_g$ 处均具有良约化；设 $\mathrm{f} : \mathcal{B} \longrightarrow \mathcal{B}'$ 是将 f 延拓到 $\mathcal{X}_g$上的 N´eron 模型之间的同态。那么，$\mathcal{N} :$ $= \ker$ [f] 是 $\mathcal{X}_g$上的有限平坦群概形。此外，若 $\hat{}\mathcal{N}$ 表示同态 $\hat{}\mathrm{f} : \mathcal{B}' \longrightarrow \mathcal{B}$ 的核，其中该同态延拓了对偶同源 $\hat{}\mathrm{f} : B' \longrightarrow B$，则 $\mathcal{N}$ 与 $\hat{}\mathcal{N}$ 互为 Cartier 对偶。

$\hat{}$ 注意，f 和 f 的存在性与唯一性源于 N´eron 映射性质，参见 [BLR90, §1.2]。

证明。由于 $\mathcal{B}/\mathcal{X}_g$ 是阿贝尔概形，态射 f 是适当的。因此$\mathcal{N}/\mathcal{X}_g$ 是适当且拟有限的，故为有限态射 [EGA IV, part 4, 8.12.4] 且是平坦的[Mil06, III.C.8]。正合列

$$0 \longrightarrow \mathcal{N} \longrightarrow \mathcal{B} \xrightarrow{\mathbf{f}} \mathcal{B}' \longrightarrow 0$$

以及同构（参见 [SGA 7I, VIII.7.1], [BBM82] 或 [Mil06, III.C.14]）

$$\mathcal{B}/\mathcal{X}_g \simeq \mathscr{E}xt^1_{\mathcal{X}_g}(\mathcal{B}, \mathbb{G}_m)$$

导出正合列

$$\cdots \longrightarrow \mathscr{H}om_{\mathcal{X}_g}(\mathcal{B}, \mathbb{G}_m) \longrightarrow \mathscr{H}om_{\mathcal{X}_g}(\mathcal{N}, \mathbb{G}_m) \longrightarrow \mathcal{B}' \xrightarrow{\hat{\mathbf{f}}} \mathcal{B} \longrightarrow \cdots.$$

这里我们应用交换图

$$\begin{array}{ccc} \mathscr{E}xt^1_{\mathcal{X}_g}(\mathcal{B}', \mathbb{G}_m) & \xrightarrow{\mathbf{f}^*} & \mathscr{E}xt^1_{\mathcal{X}_g}(\mathcal{B}, \mathbb{G}_m) \\ \| & & \| \\ \mathcal{B}' & \xrightarrow{\hat{\mathbf{f}}} & \mathcal{B} \end{array}$$

它扩展了在一般纤维上已知的图。接着，我们利用如下事实逐纤维验证等式 $\mathscr{H}om^{\mathcal{X}_g}(\mathcal{B}, \mathbb{G}_m) = 0$：在域上，从阿贝尔簇到 $\mathbb{G}_m$ 的任何同态都是平凡的。

□

沿用引理 3.1.1 中的记号，并令 N 表示 $\mathcal{N}$ 的一般纤维。对于$v \in \mathcal{X}_g$，我们有（参见 [Mil06, §III.7]）

$$\mathrm{H}^1(\mathcal{O}_v, \mathcal{N}) \hookrightarrow \mathrm{H}^1(K_v, N)\ . \tag{15}$$

引理 3.1.2. 采用上述记号。对于 $v \in \mathcal{X}_g$，我们有

$$\mathrm{H}^1(\mathcal{O}_v, \mathcal{N}) = \ker(\mathrm{H}^1(K_v, \mathrm{N}) \longrightarrow \mathrm{H}^1(K_v, B)).$$

证明。该引理由以下事实 $\mathrm{H}^1(\mathcal{O}_v, \mathcal{B}) = 0$ (见 [Mil06, §III.2.1]) 以及由正合列构成的交换图得出

$$\begin{array}{ccccccc} \mathcal{B}(\mathcal{O}_v) & \longrightarrow & \mathcal{B}'(\mathcal{O}_v) & \longrightarrow & \mathrm{H}^1(\mathcal{O}_v, \mathcal{N}) & \longrightarrow & \mathrm{H}^1(\mathcal{O}_v, \mathcal{B}) \\ \| & & \| & & \downarrow & & \downarrow \\ B(K_v) & \longrightarrow & B'(K_v) & \longrightarrow & \mathrm{H}^1(K_v, \mathrm{N}) & \longrightarrow & \mathrm{H}^1(K_v, B). \end{array}$$

□

设 $\mathcal{U} \subset \mathcal{X}$ 是一个开子概形。定义

$$\mathcal{S}(N/\mathcal{U}) := \ker(\mathrm{H}^1(K, N) \longrightarrow \prod_{v \in \mathcal{U}} \mathrm{H}^1(K_v, B)).$$

记 $\mathrm{Sel}(N/K) := \mathcal{S}(N/\mathcal{X})$，它是以下映射的核

$$\mathcal{S}(N/\mathcal{U}) \longrightarrow \textstyle\bigoplus_{v \notin \mathcal{U}} \mathrm{H}^1(K_v, B)\ .$$

令 Q($N/\mathcal{U}$) 表示局部化映射的余核

$$\mathcal{S}(N/\mathcal{U}) \xrightarrow{\mathcal{L}_{N/K}} \bigoplus_{v\notin\mathcal{U}} \mathrm{H}^1(K_v, N)\ .$$

引理 3.1.3. 若 $\mathcal{U}\subset\mathcal{X}_g$，则 $\mathrm{H}^1(\mathcal{U},\mathcal{N}) = \mathcal{S}(N/\mathcal{U})$。

证明. 设 $\mathcal{V}\subset\mathcal{U}$ 是一个开仿射子概形。由局部化正合列 [Mil06, III.0.3(c)] 以及 [Mil06, III.7], 开头的计算，我们得到正合列

$$0 \longrightarrow \mathrm{H}^1(\mathcal{U},\mathcal{N}) \longrightarrow \mathrm{H}^1(\mathcal{V},\mathcal{N}) \longrightarrow \bigoplus_{v\in\mathcal{U}\setminus\mathcal{V}} \mathrm{H}^1(K_v,N)/\,\mathrm{H}^1(\mathcal{O}_v,\mathcal{N}).$$

[Gon09, 引理 4.2] 表明，自然映射 $\mathrm{H}^1(\mathcal{V},\mathcal{N}) \longrightarrow \mathrm{H}^1(K,N)$ 是单射。正合列表明 $\mathrm{H}^1(\mathcal{U},\mathcal{N}) \subset \mathcal{S}(N/\mathcal{U})$。根据 [Gon09, 引理 2.3],, $\mathcal{S}(N/\mathcal{U})$ 中的一个元素可由某个 $\mathcal{V}\subset\mathcal{U}$ 对应的 $\mathrm{H}^1(\mathcal{V},\mathcal{N})$ 得到，而正合列表明它属于 $\mathrm{H}^1(\mathcal{U},\mathcal{N})$。

□

对于 $\mathcal{U}\neq\mathcal{X}$，应用局部对偶 [Mil06, §III.6.10] ，并考虑复合映射

$$\mathcal{S}(C_p/\mathcal{U}) \xhookrightarrow{\mathcal{L}_{C_p/\mathcal{U}}} \bigoplus_{v\notin\mathcal{U}} \mathrm{H}^1(K_v,C_p) \xrightarrow{\sim} \prod_{v\notin\mathcal{U}} \mathrm{H}^1(K_v,E_p^{(p)})^\vee, \qquad (16)$$

其中， $\mathcal{L}_{C_p/\mathcal{U}}$ 的单射性归因于 [GoT12，主定理]。

引理 3.1.4. 若 $\mathcal{U}\subset\mathcal{X}_g$ 且 $\mathcal{U}\neq\mathcal{X}$，则在 (16) 下，群 $\mathcal{S}(C_p/\mathcal{U})$ 是 $Q(E_p^{(p)}/\mathcal{U})$ 的庞特里亚金对偶。

证明. 将 F 和 V 扩张到 $\mathcal{F}\colon\mathcal{A}\longrightarrow\mathcal{A}^{(p)}$ 和 $\mathcal{V}\colon\mathcal{A}^{(p)}\longrightarrow\mathcal{A}$ 上，定义于 $\mathcal{X}_g$。Deno te

$$\mathcal{C}_p = \ker(\mathcal{F}) \ \text{ and } \ \mathcal{E}_p^{(p)} = \ker(\mathcal{V}).$$

它们互为 Cartier 对偶。由引理 3.1.3，我们将 $\mathrm{H}^1(\mathcal{U},\mathcal{C}_p)$ 与$\mathcal{S}(C_p/\mathcal{U})$ 等同。于是该引理由 Poitou-Tate 对偶 [Ces15, (5.1.2)] 得出。□

鉴于引理 3.1.2，以下引理推广了这样一个事实：对于任意赋值$v\in\mathcal{X}_g$，局部对偶将 $\mathrm{H}^1(\mathcal{O}_v,\mathcal{C}_p)\subset\mathrm{H}^1(K_v,C_p)$ 等同于 $\mathrm{H}^1(\mathcal{O}_w,\mathcal{E}_p^{(p)})\subset\mathrm{H}^1(K_v,E_p^{(p)})$ 的湮灭子 [Mil06, §III, 定理 7.1]。

引理 3.1.5. 对 K 的每个赋值 v，在对偶 $\mathrm{H}^1(K_v,C_p) = \mathrm{H}^1(K_v,E_p^{(p)})^\vee$[Mil06, §III. Theorem 6.10], 下， $j_v'\colon\mathrm{H}^1(K_v,C_p)\longrightarrow\mathrm{H}^1(K_v,A)$ 的核，作为 $\mathrm{H}^1(K_v,C_p)$ 的子群，恰好是 $\ker(j_v)\subset\mathrm{H}^1(K_v,E_p^{(p)})$ 的湮灭子。

我们将上述内容简记为

$$\ker(j_v') = \ker(j_v)^\perp. \qquad (17)$$

证明。令 ∂ 表示长正合列中的连接同态

$$\cdots\longrightarrow A(K_v)\xrightarrow{\mathsf{F}} A^{(p)}(K_v)\xrightarrow{\partial}\mathrm{H}^1(K_v,C_p)\xrightarrow{j_v'}\mathrm{H}^1(K_v,A)\longrightarrow\cdots, \qquad (18)$$

¯由于 $p = \mathsf{F} \circ \mathsf{V}$，因此在图表中诱导出同态 ∂

$$\begin{array}{ccc} A^{(p)}(K_v)/p \cdot A^{(p)}(K_v) & \xrightarrow{\bar{\partial}} & \mathrm{H}^1(K_v, C_p) \\ \big\downarrow{\scriptstyle i} & & \| \\ \mathrm{H}^1(K_v, A_p^{(p)}) & \xrightarrow{\mathsf{V}_*} & \mathrm{H}^1(K_v, C_p), \end{array} \tag{19}$$

其中，左下箭头由 (5) 给出，左侧向下箭头 i 由长正合列诱导

$$A_p^{(p)}(K_v) \longrightarrow A^{(p)}(K_v) \xrightarrow{[p]} A^{(p)}(K_v) \longrightarrow \mathrm{H}^1(K_v, A_p^{(p)}) \longrightarrow \cdots .$$

我们断言图 (19) 交换，因此交换图

$$\begin{array}{ccc} \mathrm{H}^1(K_v, A_p^{(p)}) \times \mathrm{H}^1(K_v, A_p^{(p)}) & \xrightarrow{(-,-)_v} & \mathbb{Q}/\mathbb{Z} \\ \mathsf{V}_*\big\downarrow \quad \big\uparrow j_v & & \| \\ \mathrm{H}^1(K_v, C_p) \times \mathrm{H}^1(K_v, E_p^{(p)}) & \xrightarrow{(-,-)_v} & \mathbb{Q}/\mathbb{Z}, \end{array}$$

其中左侧箭头为局部配对，得到交换图（参见 [Mil06, §III, Theorem 7.8]）

$$\begin{array}{ccc} A^{(p)}(K_v) \times \mathrm{H}^1(K_v, A^{(p)}) & \xrightarrow{(-,-)_{A^{(p)}/K_v}} & \mathbb{Q}/\mathbb{Z} \\ \partial\big\downarrow \quad \big\uparrow j_v & & \| \\ \mathrm{H}^1(K_v, C_p) \times \mathrm{H}^1(K_v, E_p^{(p)}) & \xrightarrow{(-,-)_v} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

这表明 $\ker(j_v)^\perp = \mathrm{Im}(\partial_v) = \ker(j_v')$。为证明这一断言，我们使用 Čech 余循环（参见 [Mil80, §III.2.10]）。设 $x \in A^{(p)}(K_v)$，并记其在 $A^{(p)}(K_v)/p \cdot A^{(p)}(K_v)$ 中的像为 $\bar{x}$。设 $y \in A^{(p)}(K_w') = \mathrm{Hom}(\mathrm{Spec}(K_w'), A^{(p)})$ 是 x 在有限扩张 K_w' 上的一个 p-除点。令 pr_l, $l = 1, 2$ 为投影

$$\mathrm{Spec}(K_w') \times_{\mathrm{Spec}(K_v)} \mathrm{Spec}(K_w') \longrightarrow \mathrm{Spec}(K_w')$$

到第 l 个因子。于是，$\xi := y \circ pr_1 - y \circ pr_2$ 是一个 1-上循环，表示类 $i(\bar{x})$。令 $z = \mathsf{V}(y) \in \mathrm{Hom}(\mathrm{Spec}(K_w'), A)$，使得 $\mathsf{F}(z) = x$。那么 $\mathsf{V} \circ \xi$ 是一个 1-上循环 ¯，同时表示 $\partial(\bar{x})$ 和 $\mathsf{V}_*(i(\bar{x}))$。

□

3.2. 导子。回顾一下，$k = K(E_p^{(p)}(\bar{K}^s))$，因此 $E_p^{(p)}(\bar{K}^s) = E_p^{(p)}(k)$，其上的伽罗瓦群 $\Phi := \mathrm{Gal}(k/K)$ 的作用由一个单射特征给出

$$c : \Phi \longrightarrow \mathbb{F}_p^*$$

使得 ${}^g x = c(g) \cdot x$，对于 $g \in \Phi$, $x \in E_p^{(p)}(k)$。由于 Φ 的阶与 p互素，霍赫希尔德-塞尔谱序列（参见 [Mil80, §II.2.21(a)]）给出

$$\mathrm{H}^1(K, E_p^{(p)}) \xrightarrow{\sim} \mathrm{H}^1(k, E_p^{(p)})^\Phi = \mathrm{Hom}(G_k, E_p^{(p)}(k))^\Phi . \tag{20}$$

对于 $w \in S_{ss}(k)$，令 $\iota^{(p)}(t_1)$ 为 §2.3 中所述的 $E_p^{(p)}(k_w)$ 的一个非零元素。设

$$M_w := \begin{cases} (1+t_1^p\mathcal{O}_w)\cdot(\mathcal{O}_w^*)^p, & \text{if } w \in S_{ss}(k); \\ k_w^*, & \text{if } w \in \eth(k); \\ \mathcal{O}_w^*, & \text{otherwise.} \end{cases}$$

令 $\mathbb{A}_k^*$ 表示 k 的幂等元群，$\mathscr{W}$ 表示 $k^*\backslash\mathbb{A}_k^*/\prod_w M_w$ 的 p-完备化。

引理 3.2.1. 我们有 $\mathrm{Sel}(E_p^{(p)}/k) = \mathrm{Hom}(\mathscr{W}, E_p^{(p)}(k))$。

证明。根据全局类域论，$\mathrm{Hom}(\mathscr{W}, E_p^{(p)}(k)) \subset \mathrm{Hom}(G_k, E_p^{(p)}(k))$ 由在 $w \in \eth(k)$ 处局部平凡、在超奇异处 w 的导子不大于 $\mathrm{ord}_w(t_1^p)$，且在其他处非分歧的元素组成。该引理由引理 2.2.1、2.2.2 和 2.3.3 得出。 □

每个 pro-p Φ-模 Y 都可以分解为 $Y = \bigoplus_{\chi\in\hat{\Phi}} Y^\chi$，其中对每个 χ，Y^χ 表示 χ-特征子空间 $\{y \in Y \mid {}^g y = \chi(g)\cdot y\}$。由 (20) 和引理 3.2.1，

$$\mathrm{Sel}(E_p^{(p)}/K) = \mathrm{Hom}(\mathscr{W}, E_p^{(p)}(k))^\Phi = \mathrm{Hom}(\mathscr{W}^c, \mathbb{Z}/p\mathbb{Z}). \tag{21}$$

对于 $v \in S_{ss}$，令 $W_v := \bigoplus_{w|v} k_w^*/((k_w^*)^p \cdot M_w)$，并令 $U_v := \bigoplus_{w|v} \mathcal{O}_w^*/M_w$，将其视为 W_v 的子群。

引理 3.2.2. 若 $v \in S_{ss}$，则 $|U_v^c| = q_v^{n_v}$。

证明. 再次利用霍赫希尔德-塞尔谱序列

$$\mathrm{H}^1(K_v, E_p^{(p)}) \xrightarrow{\sim} (\textstyle\bigoplus_{w|v} \mathrm{H}^1(k_w, E_p^{(p)}))^\Phi = (\bigoplus_{w|v} \mathrm{Hom}(G_{k_w}, E_p^{(p)}(k)))^\Phi. \tag{22}$$

因此，引理 2.3.3 蕴含 $\ker(j_v) \simeq \mathrm{Hom}(W_v^c, \mathbb{Z}/p\mathbb{Z})$。由此，利用 (13) 即可推出该引理，因为若 $k_w \neq K_v$，则 $W_v^c = U_v^c$；若 $k_w = K_v$，则有分裂正合列

$$0 \longrightarrow U_v^c \longrightarrow W_v^c \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0.$$

□

3.2.1. 幂等元计算。仅在本小节中，我们考虑这样的一般情形：对于 $w \in S_{ss}(k)$，前一小节中的 M_w 被替换为

$$M_w := (1+\pi_w^{a_v}\mathcal{O}_w)\cdot(\mathcal{O}_w^*)^p,$$

其中 v 是位于 w 下方的 K 的一个赋值，a_v 是一个仅取决于 v 的选定整数；对于其他 w，我们保持 M_w 不变。记 $\mathfrak{a} := (a_v)_{v\in S_{ss}}$。接着令 $\mathscr{W}_\mathfrak{a}$ 为 $k^*\backslash\mathbb{A}_k^*/\prod_w M_w$ 的 p-完备化，使得 $\mathscr{W} = \mathscr{W}_\mathfrak{o}$，其中 $\mathfrak{o} := (p\cdot\mathrm{ord}_w\, t_v)_{v\in S_{ss}}$。令 $U_\mathfrak{a} := \bigoplus_{w\in S_{ss}} \mathcal{O}_w^*/M_w$，$W_\mathfrak{a} := \bigoplus_{w\in S_{ss}} k_w^*/((k_w^*)^p\cdot M_w)$。假设

$$|U_\mathfrak{a}^c| = \prod_{v\in S_{ss}} q_v^{\rho_v}. \tag{23}$$

令 $U_\mathfrak{a}^c$ 表示自然映射的像

$$\varsigma_\mathfrak{a}^c : U_\mathfrak{a}^c \longrightarrow \mathscr{W}_\mathfrak{a}^c.$$

令 V 为 k 的 $\mathfrak{d}(k)$-单位群。那么 $\ker(\varsigma^c)$ 等于

由局部化映射 $V \longrightarrow \prod_{w\in S_{ss}(k)} \mathcal{O}_w^c : (V/pV)^c \longrightarrow U_{\mathfrak{a}}^c$ 诱导。V 的扭部是有限的，且其阶与 p 互素。映射 $V \longrightarrow \prod_{v\in\mathfrak{d}} R_v$（其中 $R_v := \prod_{w|v} k_w^*/\mathcal{O}_w^*$）在 V 的自由部分上是单射。模 R_v 由分解子群 Φ_v 固定，且是 Φ/Φ_v 的正则表示。如果 $k = K$，则 $(\mathbb{Z}_p \otimes_{\mathbb{Z}} V)^c$ 的 $\mathbb{Z}_p$-秩为 $\max\{|\mathfrak{d}_0| - 1, 0\}$；否则为 $|\mathfrak{d}_0|$，因此

$$|\ker(\varsigma_{\mathfrak{a}}^c)| = |\operatorname{Im}\varrho_{\mathfrak{a}}^c| \leq p^{|\mathfrak{d}_0|}. \tag{24}$$

如果 $\mathfrak{d} = \emptyset$，令 $\daleth$ 表示 k 的除子类群的 p-完备化；否则，令 $\daleth$ 为 $\mathfrak{d}(k)$-类群。于是 $\hbar$ 是 $\daleth$ 的 p-秩。正合列

$$0 \longrightarrow \bar{U}_{\mathfrak{a}}^c \longrightarrow \mathscr{W}_{\mathfrak{a}}^c \longrightarrow \daleth^c \longrightarrow 0$$

导出

$$0 \longrightarrow \bar{U}_{\mathfrak{a}}^c \longrightarrow \mathscr{W}_{\mathfrak{a}}^c[p] \xrightarrow{\varkappa^c} \daleth^c[p] \tag{25}$$

Put

$$\tau := \begin{cases} \log_p |\operatorname{Im}(\varkappa^c)| + 1, & \text{if } \mathfrak{d} = \emptyset \text{ and } k = K; \\ \log_p |\operatorname{Im}(\varkappa^c)|, & \text{otherwise.} \end{cases} \tag{26}$$

由 (20)，我们将 $\mathrm{H}^1(K, E_p^{(p)})$ 与 $\mathrm{Hom}(G_k, E_p^{(p)}(k))^\Phi$ 等同，因此其元素在每个赋值 v 处的导子都有定义。令 $\mathcal{X}_o \subset \mathcal{X}$ 为 S_{ss} 的补集。

定义 3.2.3。定义 $\mathrm{Sel}_{\mathfrak{a}}(E_p^{(p)}/K)$ 为 $\mathcal{S}(E_p^{(p)}/\mathcal{X}_o)$ 中由在每个 $v \in S_{ss}$ 处导子不大于 a_v 的元素组成的子群。

引理 3.2.4。假设 (23) 成立，则

$$\log_p |\operatorname{Sel}_{\mathfrak{a}}(E_p^{(p)}/K)| = \sum_{v\in S_{ss}} \rho_v \cdot \deg v + \tilde{\varepsilon}_1 - \tilde{\varepsilon}_2,$$

其中 $\tilde{\varepsilon}_1 = \tau \leq \hbar + 1$, $\tilde{\varepsilon}_2 = \log_p |\ker(\varsigma_{\mathfrak{a}}^c)| \leq |\mathfrak{d}_0| \leq |S_b|$。

证明。与 (21) 类似，$\mathrm{Sel}_{\mathfrak{a}}(E_p^{(p)}/K) = \mathrm{Hom}(\mathscr{W}_{\mathfrak{a}}^c, \mathbb{Z}/p\mathbb{Z})$。我们将 $\mathscr{W}_{\mathfrak{a}}$ 写成加法形式。若 $\mathfrak{d} \neq \emptyset$ 或 $k \neq K$，则 $\mathscr{W}_{\mathfrak{a}}^c$ 是有限的，且 $|\mathscr{W}_{\mathfrak{a}}^c/p\mathscr{W}_{\mathfrak{a}}^c| = |\mathscr{W}_{\mathfrak{a}}^c[p]|$；否则，$\mathscr{W}_{\mathfrak{a}}^c$ 在 $\mathbb{Z}_p$ 上有限生成，秩为 1，因此 $|\mathscr{W}_{\mathfrak{a}}^c/p\mathscr{W}_{\mathfrak{a}}^c| = p \cdot |\mathscr{W}_{\mathfrak{a}}^c[p]|$。由 (23)、(24)、(25) 和 (26) 即得该引理。□

命题 3.2.5. 我们有

$$\log_p |\operatorname{Sel}(E_p^{(p)}/K)| = \frac{(p-1)\deg \Delta_{A/K}}{12} \cdot \log_p q + \tilde{\varepsilon}_1 - \tilde{\varepsilon}_2,$$

其中 $\tilde{\varepsilon}_1 = \tau \leq \hbar + 1$, $\tilde{\varepsilon}_2 = \log_p |\ker(\varsigma_{\mathfrak{o}}^c)| \leq |\mathfrak{d}_0| \leq |S_b|$。

证明。鉴于 (21)、引理 3.2.2 和引理 3.2.4，我们需要证明

$$\sum_{v\in S_{ss}} n_v \cdot \deg v = \frac{(p-1)\deg \Delta_{A/K}}{12}. \tag{27}$$

令 ω 为 A/K 的一个不变微分，并对每个赋值 v，令 $\omega_{0,v}$ 和 $\omega_{0\,v}^{(p)}$,分别为 A 和 $A^{(p)}$的局部 N´eron 微分。根据 [Sil86, §IV. Corollary 4.3],

$$\mathrm{ord}_v(\mathrm{V}^*\omega_{0,v}/\omega_{0,v}^{(p)}) = \mathrm{ord}_v \frac{d\mathscr{P}(t)}{dt}\mid_{t=0},$$

由此结合引理 2.1.1 和 (10) 可得

$$\sum_{v\in S_{ss}} n_v \cdot \deg v = \sum_{\text{all } v} \mathrm{ord}_v(\mathrm{V}^*\omega_{0,v}/\omega_{0,v}^{(p)}) \cdot \deg v. \tag{28}$$

现在， [Tan95]中的公式 (8) 表明

$$\frac{\deg \Delta_{A/K}}{12} = \sum_{\text{all } v} \mathrm{ord}_v(\frac{\omega}{\omega_{0,v}}) \cdot \deg v = \sum_{\text{all } v} \mathrm{ord}_v(V^*(\frac{\omega}{\omega_{0,v}})) \cdot \deg v,$$

and

$$\frac{p\cdot \deg \Delta_{A/K}}{12} = \frac{\deg \Delta_{A^{(p)}/K}}{12} = \sum_{\text{all } v} \mathrm{ord}_v(\frac{V^*\omega}{\omega_{0,v}^{(p)}}) \cdot \deg v.$$

由此以及 (28) 可得所需的等式。

□

3.2.2. 计算 $\mathcal{S}(C_p/\mathcal{U})$。接下来，我们研究 $\mathcal{S}(C_p/\mathcal{U})$，其中 $\mathcal{U} = \mathcal{X}_{go}$、 $\mathcal{X}_g$ 或 $\mathcal{X}$。令 S_{ngo} 为 $\mathcal{X}_{go}$ 在 $\mathcal{X}$ 中的补集， $S'_{ngo} := \mathcal{U}\cap S_{ngo}$, $S'_{ss} := \mathcal{U}\cap S_{ss}$, 并令 † 为 $\mathcal{U}$ 在 $\mathcal{X}$ 中的补集。记 ‡ 为 †∪ð。我们先讨论 $\mathcal{X}_{go} \neq \mathcal{X}$ 的情形，或者等价地， A/K 不是等变的情形[1]。令

$$\bar{W} := \prod_{w\in S_{ngo}(k)} k_w^*/(k_w^*)^p$$

and

$$\bar{\mathscr{W}} := k^*\backslash \mathbb{A}_k^*/(\prod_{w\in \mathcal{X}_{go}(k)} \mathcal{O}_w^* \times \prod_{w\in S_{ngo}(k)} (k^*)^p).$$

若 ℓ_c 和 $\ell_{c^{-1}}$ 分别表示 Φ 在 $\mathbb{F}_p[\Phi]$ 上的正则表示的 c 和 c^{-1} 特征子空间，则 $E_p^{(p)}(k) = \ell_c$。因此

$$\prod_{w\in S_{ngo}(k)} \mathrm{H}^1(k_w, E_p^{(p)}) = \mathrm{Hom}(\bar{W}, \ell_c) = \mathrm{Hom}(\bar{W}\otimes_{\mathbb{F}_p} \ell_{c^{-1}}, \mathbb{Z}/p\mathbb{Z}) = (\bar{W}\otimes_{\mathbb{F}_p} \ell_{c^{-1}})^\vee,$$

and

$$\mathcal{S}(E_p^{(p)}/\mathcal{X}_{go}\times \mathrm{Spec}\, k) = \mathrm{Hom}(\bar{\mathscr{W}}, \ell_c) = ((\bar{\mathscr{W}}^c/p\bar{\mathscr{W}})\otimes_{\mathbb{F}_p} \ell_{c^{-1}})^\vee.$$

鉴于 (16) 和引理 3.1.4,

$$\mathcal{S}(C_p/\mathcal{X}_{go}\times \mathrm{Spec}\, k) = \ker(\bar{W} \longrightarrow \bar{\mathscr{W}}/p\bar{\mathscr{W}}).$$

因此，再次由霍赫希尔德-塞尔谱序列可得,

$$\mathcal{S}(C_p/\mathcal{X}_{go}) = \mathcal{S}(C_p/\mathcal{X}_{go}\times \mathrm{Spec}\, k)^\Phi = \ker(\bar{W}^c \longrightarrow \bar{\mathscr{W}}^c/p\bar{\mathscr{W}}^c).$$

对每个 w，令

$$\overline{M}_w := M_w/M_w\cap (k_w^*)^p = M_w\cdot (k_w^*)^p/(k_w^*)^p.$$

[1]回想一下， A/K 假设为普通，且处处具有半稳定约化。

引理 3.1.5 给出了以下交换图的左侧部分

$$\begin{array}{ccccccc} \mathrm{H}^1(k_w, C_p) & \xrightarrow{\sim} & \mathrm{H}^1(k_w, E_p^{(p)})^\vee & \xrightarrow{\sim} & \mathrm{Hom}(k_w^*/(k_w^*)^p, \mathbb{Z}/p\mathbb{Z})^\vee & \xrightarrow{\sim} & k_w^*/(k_w^*)^p \\ \uparrow & & \uparrow & & \uparrow & & \uparrow \\ \ker(j_w') & \xrightarrow{\sim} & \ker(j_w)^\perp & \xrightarrow{\sim} & \mathrm{Hom}(k_w^*/M_w \cdot (k_w^*)^p, \mathbb{Z}/p\mathbb{Z})^\perp & \xrightarrow{\sim} & \overline{M}_w. \end{array}$$

中间块由对交换图取对偶得到

$$\begin{array}{ccc} \mathrm{H}^1(k_w, E_p^{(p)}) & \xrightarrow{\sim} & \mathrm{Hom}(k_w^*/(k_w^*)^p, \mathbb{Z}_p/p\mathbb{Z}_p) \\ \uparrow & & \uparrow \\ \ker(j_w) & \xrightarrow{\sim} & \mathrm{Hom}(k_w^*/(k_w^*)^p \cdot M_w, \mathbb{Z}_p/p\mathbb{Z}_p), \end{array} \tag{29}$$

这归因于引理 2.3.3 以及局部类域论（见 (7) 和 (14)），而右侧块则是对偶的直接推论。

$^-$表明，若 $\mathscr{M} = \prod_{w\in\dagger(k)} k_w^*/(k_w^*)^p \times \prod_{w\in S'_{ngo}(k)} \overline{M}_w$，则

$$\mathcal{S}(C_p/\mathcal{U}) = \ker(\bar{\mathscr{M}}^c \longrightarrow \bar{\mathscr{W}}^c/p\bar{\mathscr{W}}^c). \tag{30}$$

为进一步推进，我们引入

$$\tilde{\mathscr{M}} = \prod_{w\in\dagger(k)} k_w^*/(\mathcal{O}_p^*)^p \times \prod_{w\in S'_{ngo}(k)} M_w \cdot (\mathcal{O}_p^*)^p/(\mathcal{O}_p^*)^p$$

and

$$\tilde{\mathscr{W}} := k^*\backslash\mathbb{A}_k^*/\Big(\prod_{w\in\mathcal{X}_{go}(k)} \mathcal{O}_w^* \times \prod_{w\in S_{ngo}(k)} (\mathcal{O}_w^*)^p\Big).$$

$^-$ $^\sim$ $^\sim$ $^\sim$ $^-$ $^\sim$于是 $\mathscr{M} = \mathscr{M}/p\mathscr{M}$，并且由于 $\mathscr{W} \twoheadrightarrow \mathscr{W}$的核包含于 $p\mathscr{W}$ 中，我们还有$^-$ $^-$ $^\sim$ $^\sim\mathscr{W}/p\mathscr{W} = \mathscr{W}/p\mathscr{W}$。因此 (30) 蕴含

$$\mathcal{S}(C_p/\mathcal{U}) = \ker(\tilde{\mathscr{M}}^c/p\tilde{\mathscr{M}}^c \longrightarrow \tilde{\mathscr{W}}^c/p\tilde{\mathscr{W}}^c). \tag{31}$$

$^\sim$ $^\sim$令 $\mathscr{V}$ 和 $\mathscr{M}$ 分别表示自然映射 $\tilde{\varsigma}\colon \mathscr{M} \longrightarrow \mathscr{W}$.$^\sim$ $^\sim$的核和像。令 $\xi \in \mathscr{V}$，并令 ξ为 ξ到$\prod_{w\in\dagger(k)} k_w^* \times \prod_{w\in S'_{ngo}(k)} M_w \cdot (\mathcal{O}_p^*)^p$的一个提升。那么存在 $\alpha \in k^*$ 和 $\theta \in \prod_{w\in\mathcal{X}_{go}(k)} \mathcal{O}_w^* \times \prod_{w\in S_{ngo}(k)} (\mathcal{O}_w^*)^p$，使得

$$\xi = \alpha \cdot \theta. \tag{32}$$

令 $V_\ddagger$ 表示 k 的 $\ddagger(k)$-单位群。等式 (32) 表明，α 属于子群 $V'_\ddagger \subset V_\ddagger$，该子群由所有满足以下条件的元素组成：对于所有 $w \in S'_{ss}(k)$，这些元素都位于 $M_w \cdot (\mathcal{O}_w^*)^p$ 内。假设还存在另一种表达式 $\xi = \alpha' \cdot \theta'$。那么 $\alpha'\alpha^{-1}$ 实际上属于全局单位群 $\mathbb{F}_k^*$。由于 $S_{ngo} = \dagger \sqcup S'_{ngo}$，对应关系$\xi \leftrightarrow \alpha$ (模 $\mathbb{F}_k^*$) 导出一个同构

$$\mathscr{V} \simeq V'_\ddagger/\mathbb{F}_k^*.$$

$^\sim$正合列 $0 \longrightarrow \mathscr{V} \longrightarrow \mathscr{M} \longrightarrow \mathscr{M} \longrightarrow 0$ 导出正合列

$$\tilde{\mathscr{M}}[p] \longrightarrow \mathscr{M}[p] \xrightarrow{\partial} \mathscr{V}/p\mathscr{V} \longrightarrow \tilde{\mathscr{M}}/p\tilde{\mathscr{M}} \longrightarrow \mathscr{M}/p\mathscr{M} \longrightarrow 0\ .$$

˜对于一个 $h \in \mathscr{M}[p]$，令 $\tilde{\eta}$ 为它在 $\mathscr{M}$ 中的一个原像，并令 η 为 $\tilde{\eta}$ 到$\prod_{w\in\dagger(k)} k_w^* \times \prod_{w\in S'_{ngo}(k)} M_w \cdot (\mathcal{O}_p^*)^p$的一个提升。令 $\xi = \eta^p$，则存在某个 α 和θ使得 (32) 成立，而 $\partial(h)$ 由 α表示。在这种情况下，由于 ξ 是一个 p次幂，$\alpha \in (k_w^*)^p$ 在所有 $w \in S_{ngo}(k)$处都成立；这些点非空，因此由局部 Leopoldt 猜想，[K是93],$\alpha = \beta^p$，其中某个 $\beta \in V_{\ddagger}$。由于 $pV_{\ddagger} \subset V'_{\ddagger}$，我们得出

$$\ker(\tilde{\mathscr{M}}^c/p\tilde{\mathscr{M}}^c \longrightarrow \mathscr{M}^c/p\mathscr{M}^c) = (V'_{\ddagger}/pV_{\ddagger})^c. \tag{33}$$

记

$$\beth := \tilde{\mathscr{W}}/\mathscr{M} = k^*\backslash\mathbb{A}_k^*/(\prod_{w\in\mathcal{X}_{go}(k)} \mathcal{O}_w^* \times \prod_{w\in\dagger(k)} k_w^* \times \prod_{w\in S'_{ngo}(k)} M_w \cdot (\mathcal{O}_p^*)^p.$$

于是我们有正合列

$$\tilde{\mathscr{W}}[p] \longrightarrow \beth[p] \longrightarrow \mathscr{M}/p\mathscr{M} \longrightarrow \tilde{\mathscr{W}}/p\tilde{\mathscr{W}}\ . \tag{34}$$

˜若 $y \in \mathscr{W}[p]$ 由一个 idele $\zeta = (\zeta_w)_w$表示，则存在 $\alpha \in k^*$ 和 $\theta \in \prod_{w\in\mathcal{X}_{go}(k)} \mathcal{O}_w^* \cdot \prod_{w\in S_{ngo}(k)} (\mathcal{O}_w^*)^p$，使得

$$\zeta^p = \alpha \cdot \theta.$$

于是，在 $w \in S_{ngo}(k)$ 处，$\alpha \in (k_w^*)^p$，因此再次由局部 Leopoldt 猜想，$\alpha = \beta^p$,$\beta \in k^*$。由于 y 也由 $\zeta \cdot \beta^{-1}$表示，我们有同构

$$\prod_{w\in S_{ngo}(k)} \mathcal{O}_w^*/(\mathcal{O}_w^*)^p \xrightarrow{\sim} \tilde{\mathscr{W}}[p].$$

由于 $\gimel$ 等于 $\prod_{w\in S_{ngo}(k)} \mathcal{O}_w^*/(\mathcal{O}_w^*)^p \longrightarrow \beth$的余核，上述同构与 (34) 一起推出

$$\ker(\mathscr{M}^c/p\mathscr{M}^c \longrightarrow \tilde{\mathscr{W}}^c/p\tilde{\mathscr{W}}^c) = \mathrm{Im}(\beth[p]^c \longrightarrow \gimel[p]^c) \subset \gimel]p]^c \tag{35}$$

我们有 $\hbar = \gimel[p]$ 和

$$\log_p |(V'_{\ddagger}/p\cdot V_{\ddagger})^c| \le \log_p |\mathbb{Z}_p \otimes_{\mathbb{Z}} V_{\ddagger}^c/p\cdot\mathbb{Z}_p \otimes_{\mathbb{Z}} V_{\ddagger}^c| = \begin{cases} 0, & \text{if } \ddagger = \emptyset; \\ |\ddagger_0 - 1|, & \text{if } \ddagger \neq \emptyset \text{ and } k = K; \\ |\ddagger_0|, & \text{otherwise,} \end{cases}$$

因此由 (33) 和 (35),

$$\log_p |\mathcal{S}(C_p/\mathcal{U})| \le \log_p |(V'_{\ddagger}/p\cdot V_{\ddagger})^c| + \log_p |\gimel^c[p]| \le |\ddagger_0| + \hbar. \tag{36}$$

假设 A/K 是等变的。则 $S_b = S_{ss} = \emptyset$。若 $k \neq K$，选取一个不在 k/K 上完全分裂的赋值 v；否则，任取一个 v。令 $\natural := \{v\}$。令 U 为 $\natural$的补集。置

$$\bar{W} := \prod_{w\in\natural(k)} k_w^*/(k^*)^p$$

并记

$$\bar{\mathscr{W}} := k^*\backslash\mathbb{A}_k^*/(\prod_{w\in\mathsf{U}(k)} \mathcal{O}_w^* \cdot \prod_{w\in\natural(k)} (k^*)^p),$$

使得 $\mathrm{H}^1(K_v, E_p^{(p)}) = \mathrm{Hom}(\bar{W}^c, \mathbb{Z}/p\mathbb{Z})$ 且 $\mathcal{S}(E_p^{(p)}/\mathrm{U}) = \mathrm{Hom}(\bar{\mathscr{W}^c}/p\bar{\mathscr{W}^c}, \mathbb{Z}/p\mathbb{Z})$。因此，由 (16) 和引理 3.1.4 可知，若 $\mathscr{M} := \prod_{w\in\natural(k)} \mathcal{O}_w^*/(\mathcal{O}_w^*)^p$，则

$$\mathcal{S}(C_p/\mathcal{X}) = \ker(\bar{\mathscr{M}^c} \longrightarrow \bar{\mathscr{W}^c}/p\bar{\mathscr{W}^c}).$$

$\bar{\mathscr{M}} \longrightarrow \bar{\mathscr{W}}$ 的核包含于 $V_\natural$的像中，即 k的 $\natural(k)$-单位。由于我们选择了 $(\mathbb{Z}_p \otimes_{\mathbb{Z}} V_\natural)^c = 0$，因此 $\bar{\mathscr{M}^c} \longrightarrow \bar{\mathscr{W}^c}$ 是单射。

S与前一种情形类似，在 $w \in \natural$处的局部 Leopoldt 猜想(k)蕴含

$$\prod_{w\in\natural(k)} k_w^*/(k_w^*)^p \twoheadrightarrow \bar{\mathscr{W}}[p].$$

由于$(\prod_{w\in\natural(k)} k_w^*/(k_w^*)^p)^c = 0$，我们有 $\bar{\mathscr{W}}[p] = 0$。现在，$(\mathscr{W}/\mathscr{M})[p] = \text{ℶ}[p]$，其中 ℶ是 k的除子类群。由正合列可知

$$\bar{\mathscr{W}^c}[p] \longrightarrow \text{ℶ}^c[p] \longrightarrow \bar{\mathscr{M}^c} \longrightarrow \bar{\mathscr{W}^c}/p\bar{\mathscr{W}^c}$$

that

$$|\mathcal{S}(C_p/\mathcal{X})| = |\text{ℶ}^c[p]|.$$

因此，以下命题得证。

命题 3.2.6. 对于 $\mathcal{U} = \mathcal{X}_{go}$、 $\mathcal{X}_g$或 $\mathcal{X}$,

$$\log_p |\mathcal{S}(C_p/\mathcal{U})| \le |\text{ǂ}_0| + \hbar.$$

特别是,

$$\log_p |\,\mathrm{Sel}(C_p/K)| \le |\eth_0| + \hbar.$$

命题 1 的证明。该命题是命题 3.2.5 和命题 3.2.6 的推论，因为我们有如下正合列的交换图

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Sel}(E_p^{(p)}/K) & \longrightarrow & \mathrm{Sel}_p(A^{(p)}/K) & \longrightarrow & \mathrm{Sel}(C_p/K) \\
\| & & \downarrow & & \downarrow & & \downarrow \\
C_p(K) & \longrightarrow & \mathrm{H}^1(K, E_p^{(p)}) & \longrightarrow & \mathrm{H}^1(K, A_p^{(p)}) & \xrightarrow{\mathsf{V}_*} & \mathrm{H}^1(K, C_p) \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & \bigoplus_v \mathrm{H}^1(K_v, A^{(p)}) & = & \bigoplus_v \mathrm{H}^1(K_v, A^{(p)}) & \xrightarrow{\mathsf{V}_*} & \bigoplus_v \mathrm{H}^1(K_v, A),
\end{array}$$

其中，中间的长正合列由 (5) 导出。 □

3.3. Cassels-Tate对偶性。Cassels-Tate配对诱导出完美配对（见 [Mil06, III.9.5]）

$$\langle -, - \rangle_{A/K} : \overline{\text{Ш}}(A/K) \times \overline{\text{Ш}}(A/K) \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p.$$

If $\varphi :\ A \longrightarrow B$ 是一个同源，其对偶同源为 φ^t，则交换图

$$\begin{array}{ccc}
\overline{\text{Ш}}(A/K) \times \overline{\text{Ш}}(A/K) & \xrightarrow{\langle -,-\rangle_{A/K}} & \mathbb{Q}_p/\mathbb{Z}_p \\
{\scriptstyle \varphi_\natural}\downarrow \quad \uparrow{\scriptstyle \varphi_\natural^t} & & \| \\
\overline{\text{Ш}}(B/K) \times \overline{\text{Ш}}(B/K) & \xrightarrow{\langle -,-\rangle_{B/K}} & \mathbb{Q}_p/\mathbb{Z}_p
\end{array}$$

给出了$Ш(A/K)/\ker(\varphi_\natural)$与$\overline{Ш(B/K)/\ker(\varphi_\natural^t)}$之间的对偶。特别地

$$|(\overline{Ш}(A/K)/\ker(\varphi_\natural))[p^\nu]| = |(\overline{Ш}(B/K)/\ker(\varphi_\natural^t))[p^\nu]|, \tag{37}$$

因为 $|G/p^\nu G| = |G[p^\nu]|$ 对有限阿贝尔群 G成立。

命题 2 的证明。考虑正合列

$$0 \longrightarrow \ker(\mathsf{F}_\natural) \longrightarrow \overline{Ш}(A/K)[p^\nu] \longrightarrow (\overline{Ш}(A/K)/\ker(\mathsf{F}_\natural))[p^\nu] \xrightarrow{\cdot p^\nu} \ker(\mathsf{F}_\natural) \cap p^\nu \overline{Ш}(A/K) \longrightarrow 0,$$

其中态射 $\cdot p^\nu$ 由乘以 p^ν 导出。这意味着

$$\log_p |\overline{Ш}(A/K)[p^\nu]| = \log_p |(\overline{Ш}(A/K)/\ker(\mathsf{F}_\natural))[p^\nu]| + \delta_1, \tag{38}$$

其中 $\log_p|\mathrm{Sel}(C_p/K)| \geq \log_p|\ker(\mathsf{F}_\natural)| \geq \delta_1 \geq 0$。此外，考虑正合列

$$0 \longrightarrow \ker(\mathsf{V}_\natural) \longrightarrow (\overline{Ш}(A^{(p)}/K)/\ker(\mathsf{V}_\natural))[p^\nu] \xrightarrow{\cdot p^\nu} (\overline{Ш}(A^{(p)}/K)/\overline{Ш}(A^{(p)}/K)[p])[p^\nu] \longrightarrow \mathsf{T} \longrightarrow 0,$$

其中 $\mathsf{T} = (\mathrm{X}(\overline{A^{(p)}}/K)[p]/\ker(\mathsf{V}_\natural)) \cap p^\nu(\mathrm{X}(\overline{A^{(p)}}/K)/\ker(\mathsf{V}_\natural))$。结合 (37) 和 (38)，可得

$$\log_p |\overline{Ш}(A/K)[p^\nu]| = \log_p |(\overline{Ш}(A^{(p)}/K)/\overline{Ш}(A^{(p)}/K)[p])[p^\nu]| + \delta_1 + \delta_2, \tag{39}$$

with

$$\log_p|\mathrm{Sel}(C_p/K)| \geq \log_p|\ker(\mathsf{F}_\natural)| \geq \log_p|\mathsf{V}_\natural(\overline{Ш}(A^{(p)}/K)[p])| \geq \delta_2 \geq 0.$$

Now

$$(\overline{Ш}(A^{(p)}/K)/\overline{Ш}(A^{(p)}/K)[p])[p^\nu] = \overline{Ш}(A^{(p)}/K)[p^{\nu+1}]/\overline{Ш}(A^{(p)}/K)[p].$$

回想一下， r 表示 $\mathrm{Sel}_{div}(A/K) \simeq \mathrm{Sel}_{div}(A^{(p)}/K)$ 的余秩，因此

$$\log_p |\overline{Ш}(A/K)[p^\nu]| = \log_p |\mathrm{Sel}_{p^\nu}(A/K)| - r\nu,$$

并且对 $A^{(p)}$也有类似的公式。因此，

$$\log_p|\mathrm{Sel}_{p^\nu}(A/K)| = \log_p|\mathrm{Sel}_{p^{\nu+1}}(A^{(p)}/K)| - \log_p|\mathrm{Sel}_p(A^{(p)}/K)| + \delta_1 + \delta_2.$$

然后我们应用命题 1 和命题 3.2.6。

□

3.4. 特殊化方法。仅在本节中，我们假设 A/K是定义在全局域上的普通阿贝尔簇。与前面一样，设 L/K 是一个 $\mathbb{Z}_p^d$-扩张，在 K的有限多个赋值之外非分歧。设 Γ 为伽罗瓦群，Λ_Γ 为岩泽代数。

在 μ_{p^∞} 上赋予离散拓扑，并记 $\hat{\Gamma}$ 为所有连续特征 $\Gamma \longrightarrow \mu_{p^\infty}$ 构成的群。令 $\hat{\mathcal{O}}$ 为 $\mathbb{Q}_p(\mu_{p^\infty})$ 的整数环。每个特征 $\hat{\chi} \in \Gamma$ 都唯一地延拓为连续的 $\mathbb{Z}_p$-代数同态 $\chi\colon \Lambda_\Gamma \longrightarrow \mathcal{O}$。

对于不被 p 整除的 $g \in \Lambda_\Gamma$，根据 Monsky [Mon81，定理 2.3]，，集合

$$\nabla_g := \{\chi \in \hat{\Gamma} \mid \chi(g) \in p \cdot \mathcal{O}\}$$

要么是 $\emptyset$，要么包含于 $T_1 \cup \cdots \cup T_n$，其中对每个 i，存在 $\zeta_{i,\,1}$，……，$\zeta_{i,\,\nu_i} \in \mu_{p^\infty}$、$\nu_i > 0$，以及 $\sigma_{i,\,1}$，……，$\sigma_{i,\,\nu_i} \in \Gamma$，它们可扩充为 Γ 的一组 $\mathbb{Z}_p$-基，使得

$$T_i := \{\chi \in \hat{\Gamma} \mid \chi(\sigma_{i,j}) = \zeta_{i,j},\ \text{for } j = 1, ..., \nu_i\}.$$

对于一个可扩充为 Γ 的 $\mathbb{Z}_p$-基的元素 $\psi \in \Gamma$，令

$$T_\psi := \{\chi \in \hat{\Gamma} \mid \chi(\psi) = 1\}.$$

那么，除非 $\nu_i = 1$、$\zeta_{i,\,1} = 1$ 和 $\sigma_{i,\,1}$、ψ 在拓扑意义下生成 Γ 的同一个闭子群，否则 $T_\psi \subset T_i$ 不成立；在这种情况下，实际上有 $T_\psi = T_i$。因此，Γ 中秩一 $\mathbb{Z}_p$-子模只有有限多个，使得若 ψ 选取时避开它们，则

$$T_\psi \subsetneq \nabla_g. \tag{40}$$

对于 L/K 的一个 $\mathbb{Z}_p^e$-子扩张 L'/K，记 $\Gamma' = \mathrm{Gal}(L'/K)$。商映射$\Gamma \longrightarrow \Gamma'$ 唯一地连续延拓为一个 $\mathbb{Z}_p$-代数同态

$$p_{L/L'} : \Lambda_\Gamma \longrightarrow \Lambda_{\Gamma'}.$$

记 $\Psi := \mathrm{Gal}(L/L')$，使得 $\Gamma' = \Gamma/\Psi$。令 $\mathscr{I}_\Psi := \ker(p_{L/L'})$。

设 $\mathfrak{b}$ 是 K 的一个有限素点集。对于 L/K 的一个子扩张 M，令 $\mathfrak{b}_M \subset \mathfrak{b}$ 表示由在 M 上完全分裂的素点组成的子集。

引理 3.4.1. 假设 $d \geq 2$。设 Z_ℓ, $\ell = 1$,.., s, 为有限生成的挠 Λ_Γ-模，θ 是 Λ_Γ 中一个不可被 p 整除的元素，且 $\mathfrak{b}$ 是 K 的有限素点集。存在一个元素 $\psi \in \Gamma$，可扩充为一个 $\mathbb{Z}_p$-基，使得若 L' 是 ψ 的不动域，则 $\mathfrak{b}_{L'} = \mathfrak{b}_L$, $p_{L/L'}(\theta)$ 不被 p 整除，并且每个 $\Lambda_{\Gamma'}$-模 $Z'_\ell := Z_\ell/\mathscr{I}_\Psi Z_\ell$ 都是挠模，具有与 Z_ℓ 在 Λ_Γ 上相同的初等 μ-不变量。

证明. 对于每个具有非平凡分解子群 Γ_v 的 $v \in \mathfrak{b}$，如果 $\psi \notin \Gamma_v$ 或 Γ_v 的 $\mathbb{Z}_p$-秩大于一，则 v 不在 L' 上完全分裂。为了得到 $\mathfrak{b}_{L'} = \mathfrak{b}_L$，我们只需选取一个避开所有秩一 Γ_v, $v \in \mathfrak{b}$ 的 ψ。

与（2）类似，我们有

$$0 \longrightarrow \bigoplus_{i=1}^{m_\ell} \Lambda_\Gamma/(p^{\alpha_{\ell,i}}) \oplus \bigoplus_{j=1}^{n_\ell} \Lambda_\Gamma/(\eta_{\ell,j}^{\beta_{\ell,j}}) \longrightarrow Z_\ell \longrightarrow N_\ell \longrightarrow 0, \tag{41}$$

其中 N_ℓ 是伪零的，并且每个 $\eta_{\ell,\,j}$ 都不能被 p整除。对每个 ℓ，选取一个 $h_\ell \in \Lambda_\Gamma$ 作为 N_ℓ的湮灭子，且不能被 p整除，并令

$$g := \theta \cdot \prod_{\ell=1}^{s} h_\ell \cdot \eta_{\ell,1} \cdot \cdots \cdot \eta_{\ell,n_\ell}.$$

^ ^ 我们还选择满足 (40) 的 ψ 。由于 $\Gamma' = T_\psi$，存在 $\chi \in \Gamma'$ 使得 $\chi(p_{L/L'}(g)) \notin p \cdot \mathcal{O}$，因此 $p_{L/L'}(g) \notin p \cdot \Lambda_{\Gamma'}$。因为 $p^\alpha \cdot g^\beta \cdot Z_\ell = 0$，对于某个 α，$\beta \in \mathbb{Z}$，我们有 $p^\alpha \cdot p_{L/L'}(g^\beta) \cdot Z'_\ell = 0$。因此，$Z'_\ell$ 在 $\Lambda_{\Gamma'}$ 上是挠的。

为了比较 Z_ℓ 和 Z'_ℓ 的初等 μ-不变量，我们将乘以 $\psi - 1$ 的映射应用于 (41)，并使用蛇引理得到正合列

$$N_\ell[\psi - 1] \longrightarrow \bigoplus_{i=1}^{m_\ell} \Lambda_{\Gamma'}/(p^{\alpha_{\ell,i}}) \oplus \bigoplus_{j=1}^{n_\ell} \Lambda_{\Gamma'}/(p_{L/L'}(\eta_{\ell,j})^{\beta_{\ell,j}}) \longrightarrow Z'_\ell \longrightarrow N_\ell/\mathscr{I}_\Psi N_\ell. \quad (42)$$

由于 $N_\ell[\psi - 1]$ 被 $p_{L/L'}(g)$ 消去，且该元素与 p 互素，正合列中的第二个箭头在 $\bigoplus_{i=1}^{m_\ell} \Lambda_{\Gamma'}/(p^{\alpha_{\ell,\,i}})$ 上是单射。通过比较该列中各项特征理想的 p 次幂因子，我们即可完成证明。

□

在引理 3.4.1 中，域 L' 是 $\mathbb{Z}_p^{d-1}$ 关于 K 的扩张。反复应用该引理，可得如下序列

$$L \supset L' \supset \cdots \supset L^{(d-1)}, \quad (43)$$

并且，对每个 ℓ,

$$Z_\ell \longrightarrow Z'_\ell \longrightarrow \cdots \longrightarrow Z_\ell^{(d-1)}. \quad (44)$$

令 $\Psi_0 = \Psi$, $\Psi_i =$ 伽罗瓦群$(L/L^{(i+1)})$，且 $\Gamma^{(i+1)} =$ 伽罗瓦群$(L^{(i+1)}/K) = \Gamma/\Psi_i$。则 $L^{(d-1)}$ 是 $\mathbb{Z}_p$ 关于 K 的扩张，其中 $\mathfrak{b}_{L^{(d-1)}} = \mathfrak{b}_L$, $p_{L/L^{(d-1)}}(\theta)$ 不被 p 整除；并且对每个ℓ，$\Lambda_{\Gamma^{(d-1)}}$-模 $Z_\ell^{(d-1)} = Z_\ell/\mathscr{I}_{\Psi_{d-2}} Z_\ell$ 与 Z_ℓ 在 Λ_Γ 上具有相同的初等 μ-不变量。这些初等 μ-不变量 $p^{\alpha_{\ell,\,1}}$，...，$p^{\alpha_{\ell,\,m_\ell}}$可通过下面的计数公式求得。对每个 ν，定义

$$\alpha_{\ell,i,\nu} = \min\{\nu, \alpha_{\ell,i}\}.$$

令 $\sigma \in \Gamma^{(d-1)}$ 为一个拓扑生成元，并令 $x = \sigma - 1$。令 $\mathscr{I}_{\nu,\,n}$ 表示由 p^ν 和 $(x+1)^{p^n} - 1$ 生成的 $\Lambda_{\Gamma^{(d-1)}}$ 的理想。

引理 3.4.2. 设记号同上，则

$$\log_p |Z_\ell^{(d-1)}/\mathscr{I}_{\nu,n} Z_\ell^{(d-1)}| = p^n \cdot \sum_{i=1}^{m_\ell} \alpha_{\ell,i,\nu} + \mathrm{O}(1).$$

*Pro*取 (2) 中的 $Z = Z_\ell^{(d-1)}/p^\nu Z_\ell^{(d-1)}$，我们可推出以下正合列 ,

$$0 \longrightarrow \textstyle\bigoplus_{i=1}^{m_\ell} \Lambda_{\Gamma^{(d-1)}}/(p^{\alpha_{\ell,i,\nu}}) \longrightarrow Z_\ell^{(d-1)}/p^\nu Z_\ell^{(d-1)} \longrightarrow N_{\ell,\nu} \longrightarrow 0, \quad (45)$$

其中 $N_{\ell,\ \nu}$ 是有限的，因为另外两项伪同构。记 R_α 为$\mathbb{Z}_p/p^\alpha\mathbb{Z}_p$。该引理可由 (45) 导出的正合列得到:

$$N_0[\sigma^{p^n}-1]\longrightarrow \bigoplus_{i=1}^{m_\ell} R_{\alpha_{\ell,i,\nu}}[x]/((x+1)^{p^n}-1)\longrightarrow Z_\ell^{(d-1)}/\mathscr{J}_{\nu,n}Z_\ell^{(d-1)}$$

$$N_0/(\sigma^{p^n}-1)N_0.$$

□

为将上述结果应用于对偶塞尔默群，我们需要以下简化的控制引理。对于 $K\subset F\subset L$, 考虑限制映射

$$\mathrm{res}^{(\nu)}_{L/F}:\mathrm{Sel}_{p^\nu}(A/F)\longrightarrow \mathrm{Sel}_{p^\nu}(A/L)^{\mathrm{Gal}(L/F)}.$$

令 $\mathtt{K}^{(n)}$ 表示 $\mathbb{Z}_p$-扩张 $L^{(d-1)}/K$ 的第 n 层。令 $\mathfrak{r}$ 表示 L/K 的分歧轨迹，假设它是有限的。

引理 3.4.3. 设 $L^{(d-1)}/K$ 是 L/K 的一个中间 $\mathbb{Z}_p$-扩张。假设 $\mathfrak{r}$ 仅包含 A 具有良普通约化或乘法约化的素点，且 $\mathfrak{b}_{L^{(d-1)}}=\mathfrak{b}_L$；并且 $\mathfrak{b}$ 包含 $\mathfrak{r}$ 以及所有 A 具有坏约化的素点。对于给定的 ν，当 n 变化时，$\ker(\mathrm{res}^{(\nu)}_{L/\mathtt{K}^{(n)}})$ 和 $\mathrm{coker}(\mathrm{res}^{(\nu)}_{L/\mathtt{K}^{(n)}})$ 的阶有界。

证明. 对某个有限子扩张 K'/K，令 $M=A_{p^\nu}(L)=A_{p^\nu}(K')$。记 $\mathtt{K}'^{(n)}$ 为 $\mathtt{K}^{(n)}K'$。根据 Tan10，引理 3.2.1] 表明，对于 $i=0,\ 1,2,$

$$|\,\mathrm{H}^i(L/\mathtt{K}'^{(n)},M)|\le |M|^{d^i}.$$

由于 $[\mathtt{K}'^{(n)}:\ \mathtt{K}^{(n)}]\le[K':\ K]$，通过计算余链的数量，我们可得

$$|\,\mathrm{H}^i(\mathtt{K}'^{(n)}/\mathtt{K}^{(n)},M)|\le |M|^{[K':K]^i}.$$

这给出了 $|\ker(\mathrm{res}^{(\nu)}_{L/\mathtt{K}^{(n)}})|$ 的上界。要给出 $|\mathrm{coker}(\mathrm{res}^{(\nu)}_{L/\mathtt{K}^{(n)}})|$ 的上界，根据霍赫希尔德-塞尔谱序列，我们需要给出以下量的上界（参见 [Tan10 定理 4] 的证明）

$$|\bigoplus_{\text{all } v}\prod_{w|v}\mathrm{H}^1(L_w/\mathtt{K}_w^{(n)},A(L_w))[p^\nu]|.$$

记 $\mathscr{H}_{(\nu)w}$ 为 $\mathrm{H}^1(L_w/\mathtt{K}_w^{(n)},A(L_w))[p^\nu]$。若 $v\notin\mathfrak{b}$，则对所有 $w\mid v$，均有 $\mathscr{H}_{(w^\nu}=0$ [Mil06, I.3.8]。此外，对于所有位于 $\mathfrak{b}_L$ 上方的 w，也有 $\mathscr{H}_{(\nu)w}=0$，因为 $\mathtt{K}_w^{(n)}=L_w$。

假设 $v\in\mathfrak{b}$ 但 $v\notin\mathfrak{b}_L=\mathfrak{b}_{L^{(d-1)}}$。位于 v之上的 $\mathtt{K}^{(n)}$ 的赋值数目随着 n 变化而有界。我们需要对所有 $w\mid v$，界定 $\mathscr{H}_{(\nu)w}$ 的阶。如果 A 在 v处有良普通约化，根据 [Tan10、(3) 和定理 2], ， $\mathscr{H}_w^{(\nu)}$的阶由 $p^{2\nu(d+1)\text{维数}\,A}$所界。众所周知（例如，见 [Tan10]的最后两段），若 A 在 v处有分裂乘法约化，则 $\mathscr{H}_w^{(\nu)}$的阶由 $p^{\nu d\text{维数}\,A}$所界。一般而言，若 A在 v处有乘法约化，则经过某个非分歧扩张 K'_v/K_v后， A的约化会变为分裂乘法约化。

由于 $\mathscr{H}_{(\nu)w} \subset \mathrm{H}^1(L_wK'_v/\mathtt{K}_v, A(L_wK'_v))$，记 $\mathtt{K}_vK'_v$, $L_wK'_v$为 $\mathtt{K}'_v$, L'_w，我们利用正合列结束证明

$$\mathrm{H}^1(\mathtt{K}'_v/\mathtt{K}_v, A(\mathtt{K}'_v)) \hookrightarrow \mathrm{H}^1(L'_w/\mathtt{K}_v, A(L'_w)) \longrightarrow \mathrm{H}^1(L'_w/\mathtt{K}'_v, A(L'_w))$$

以及 A/K'_v 的分支群的 p-秩被 $\dim A$所界定这一事实（见 [BX96，命题 5.2]），因此根据 [Mil06，命题 I.3.8]，$\mathrm{H}^1(\mathtt{K}'_v/\mathtt{K}_v, A(\mathtt{K}'_v))$ 的阶是有界的。

□

引理 3.4.4。设 $\theta \in \Lambda_\Gamma$ 是一个不被 p 整除的元素。设 A_ℓ、$\ell = 1$、...、s 是定义在 K 上的普通阿贝尔簇，使得所有 $Z_\ell := \mathrm{Sel}_{p^\infty}(A_\ell/L)^\vee$ 在 Λ_Γ 上都是挠的，并且分歧轨迹 $\mathfrak{r}$ 只包含这样的赋值：对每个 A_ℓ，其具有良普通约化或乘法约化。设 $\mathfrak{b}$ 是 K 的一个有限赋值集，其中包含 $\mathfrak{r}$ 以及某个 A_ℓ 具有坏约化的所有赋值。假设 $p^{\alpha_{\ell,1}}$、...、$p^{\alpha_{\ell,m_\ell}}$ 是 Z_ℓ 的初等 μ-不变量。则存在一个 L/K 的中间 μ-扩张 $L^{(d-1)}/K$，使得以下结论成立：

(a) $p_{L/L^{(d-1)}}(\theta) \notin p\Lambda_{\Gamma^{(d-1)}}$，其中 $\Gamma^{(d-1)} = \mathrm{Gal}(L^{(d-1)}/K)$。(b) $\mathfrak{b}_{L^{(d-1)}} = \mathfrak{b}_L$。(c) 对每个 ℓ，$\mathrm{Sel}_{p^\infty}(A_\ell/L^{(d-1)})^\vee$ 在 $\Lambda_{\Gamma^{(d-1)}}$ 上的初等 μ-不变量与 Z_ℓ 在 Λ_Γ上的初等不变量相同。(d) 特别地，若 L/K 是一个 $\mathbb{Z}_p$-扩张，且 $K^{(n)}$ 表示第 n 层，则

$$\log_p |\mathrm{Sel}_{p^\nu}(A_\ell/K^{(n)})| = p^n \cdot \sum_{i=1}^{m_\ell} \alpha_{\ell,i,\nu} + \mathrm{O}(1). \tag{46}$$

证明。(a) 和 (b) 由引理 3.4.1 得出。注意，$Z_\ell^{(d-1)}/\mathscr{J}_{\nu,n}Z^{(d-1)}$ 不过是 $\mathrm{Sel}_{p^\nu}(A_\ell/L)^{\mathrm{Gal}(L/\mathtt{K}^{(n)})}$ 的庞特里亚金对偶，因此由引理 3.4.2、3.4.3 可得

$$\log_p |\mathrm{Sel}_{p^\nu}(A_\ell/\mathtt{K}^{(n)})| = p^n \cdot \sum_{i=1}^{m_\ell} \alpha_{\ell,i,\nu} + \mathrm{O}(1). \tag{47}$$

在 (d) 的情形下，$L = L^{(d-1)}$，因此 (46) 成立。为证明 (c)，我们假设 $\mathrm{Sel}_{p^\infty}(A_\ell/L^{(d-1)})^\vee$ 在 $\Lambda_{\Gamma^{(d-1)}}$上的初等 μ-不变量为 $p^{\alpha'_{\ell,1}}$，...，$p^{\alpha'_{\ell,w_\ell}}$。将 (d) 应用于 $L^{(d-1)}/K$，得到

$$\log_p |\mathrm{Sel}_{p^\nu}(A_\ell/\mathtt{K}^{(n)})| = p^n \cdot \sum_{i=1}^{w_\ell} \alpha'_{\ell,i,\nu} + \mathrm{O}(1),$$

其中，与前面一样，$\alpha'_{\ell,i,\nu} := \min\{\alpha'_{\ell,i}, \nu\}$。由此及式 (47) 可得

$$\sum_{i=1}^{w_\ell} \alpha'_{\ell,i,\nu} = \sum_{i=1}^{m_\ell} \alpha_{\ell,i,\nu},$$

对所有 ν 均成立。我们得出，$w_\ell = m_\ell$和 $p^{\alpha'_{\ell,1}}$，...，$p^{\alpha'_{\ell,w_\ell}}$与 $p^{\alpha_{\ell,1}}$，...，$p^{\alpha_{\ell,m_\ell}}$相同。

□

3.5. 初等 μ-不变量。本节中，我们完成命题 3 和命题 5 的证明。对于 L/K 的每个 $\mathbb{Z}_p$-子扩张 F/K，记

$$S_b(F) = \eth'_F \sqcup \eth_F,$$

其中，若 $p = 2$, $\eth'_F$ 是 A/K 具有非分裂乘法约化且分支群阶为偶数的素点集合；若 $p \neq 2$, $\eth'_F = \emptyset$。对于位于 $v \in S_b$ 上的 $w \in S_b(F)$，若 $w \in \eth'_F$ 和 $v \in \eth$，或 $w \in \eth_F$ 和 $v \in \eth'$，则 $F_w \neq K_v$，因此位于 v 上方的 F 的素点只有有限多个。

命题 3 的证明。我们应用引理 3.4.4，取 $s = 1$, $Z_1 = X^{(p)}$, $\mathfrak{b} = \mathfrak{r} \cup S_b$。令 $\mathtt{K}^{(n)}$ 为 $L^{(d-1)}/K$的第 n层。由于 k/K 和 $\mathtt{K}^{(n)}/K$ 的次数互素，可知 K 的一个素点 v 在 k中完全分裂，当且仅当 $\mathtt{K}^{(n)}$ 中所有位于 v 上方的素点都在 $k\mathtt{K}^{(n)}$中完全分裂，因为这两个断言都等价于分解子群 $\mathrm{Gal}(k\mathtt{K}^{(n)}/K)_v$ 在 $\mathrm{Gal}(k\mathtt{K}^{(n)}/\mathtt{K}^{(n)})$中不含非平凡元素，因此包含于 $\mathrm{Gal}(k\mathtt{K}^{(n)}/k)$中。令

$$\eth_{0,n} := \{w \in \eth_{\mathtt{K}^{(n)}} \mid w \text{ splits completely over } k\mathtt{K}^{(n)}\}.$$

那么，根据本节开头的讨论，

$$|\eth_{0,n}| = |\eth_0(\mathtt{K}^{(n)})| + \mathrm{O}(1) = p^n \cdot |\eth_1| + \mathrm{O}(1).$$

如果 $\mathbb{F}_{q^{(n)}}$ 表示 $\mathtt{K}^{(n)}$的常数域，那么

$$\deg \Delta_{A/\mathtt{K}^{(n)}} \cdot \log_p q^{(n)} = p^n \cdot \deg \Delta_{A/K} \cdot \log_p q.$$

因此，引理 3.4.4(d)和命题 1表明，如果 m 是 μ的秩，那么

$$p^n \cdot m = \log_p |\operatorname{Sel}_p(A^{(p)}/\mathtt{K}^{(n)})| + \mathrm{O}(1) \geq p^n \cdot (\frac{(p-1)\deg \Delta_{A/K}}{12} \cdot \log_p q - |\eth_1|) + \mathrm{O}(1).$$

这就证明了该命题。 □

命题 5 的证明。取 $s = 2$、 $Z_1 = X^{(p)}$、 $Z_2 = X$、 $\mathfrak{b} = S_b \cup \mathfrak{r}$、 $\theta = \Theta_L$，使得 $m = m_1$，并且对于 $i = 1$, ..., m，有 $\alpha_i = \alpha_{1,\, i,}$。由引理 3.4.4， $\mathfrak{b}_{L^{(d-1)}} = \mathfrak{b}_L = \emptyset$和$\Theta_{L^{(d-1)}}$ 不被 p整除。因此，我们可以假设 $d = 1$。

令 $K^{(n)}$ 表示 L/K的第 n层。如果 $L = K_p^{(\infty)}$，我们已在 §1.1 中证明$|\mathfrak{w}_{K^{(n)}}[p]| = \mathrm{O}(1)$；否则，当 n 充分大时， $L/K^{(n)}$ 在某个赋值处全分歧，从而 Hom(伽罗瓦群($L/K^{(n)}$) $\mathbb{Q}_p/\mathbb{Z}_p$) $\cap$ Hom($\mathfrak{w}_{K^{(n)}}$, $\mathbb{Q}_p/\mathbb{Z}_p$) $= \{0\}$。因此，Hom($\mathfrak{w}_{K^{(n)}}$, $\mathbb{Q}_p/\mathbb{Z}_p$) $\longrightarrow$ Hom($\mathfrak{w}_L$, $\mathbb{Q}_p/\mathbb{Z}_p$) 是单射，或者等价地，对于充分大的 n，映射 $\mathfrak{w}_L \longrightarrow \mathfrak{w}_{K^{(n)}}$ 是满射。由于 $p \nmid \Theta_L$， $\mathfrak{w}_L$ 的 p- 部分是平凡的，$\mathfrak{w}_{K^{(n)}}[p]$ 的阶必须有界。该假设表明

$$|S_b(K^{(n)})| = \mathrm{O}(1).$$

因此，由引理 3.4.4(d) 和命题 1，我们得到

$$\begin{aligned} p^n \cdot m &= p^n \cdot \textstyle\sum_{i=1}^m \alpha_{1,i,1} \\ &= \log_p |\operatorname{Sel}_p(A^{(p)}/K^{(n)})| + \mathrm{O}(1) \\ &= p^n \cdot \tfrac{(p-1)\deg \Delta_{A/K}}{12} \cdot \log_p q + \mathrm{O}(1), \end{aligned}$$

这就证明了第一个断言。接着，由引理 3.4.4(d) 和命题 2 可得

$$\begin{aligned} p^n \cdot \textstyle\sum_{i=1}^{m_2} \alpha_{2,i,\nu} &= \log_p |\operatorname{Sel}_{p^\nu}(A/K^{(n)})| + \mathrm{O}(1) \\ &= p^n \cdot (\log_p |\operatorname{Sel}_{p^{\nu+1}}(A^{(p)}/K^{(n)})| - \tfrac{(p-1)\deg \Delta_{A/K}}{12} \cdot \log_p q) + \mathrm{O}(1) \\ &= p^n \cdot \textstyle\sum_{i=1}^{m} (\alpha_{1,i,\nu+1} - 1) + \mathrm{O}(1), \end{aligned}$$

这对每个 ν 都成立，因此命题得证。

□

References

[BBM82] P. Berthelot、L. Breen 和 W. Messing，《Dieudonné 晶体理论》II，数学讲义 930。Springer-Verlag，1982。[BLR90] S. Bosch、W. Lütkebohmert 和 M. Raynaud，《Néron 模型》，Springer-Verlag 柏林—海德堡，1990。[BX96] S. Bosch、X. Xarles，《通过刚性一致化研究 Néron 模型的分支群》，《数学年刊》306（1996），459–486。[Ces15] K. Česnavičius，《不对阶数加以限制的 Poitou-Tate》，《数学研究快报》22（2015），第 6 期，1621–1666。[Crw87] R. Crew，《p 进特征的 L 函数与几何岩泽理论》，《数学发明》88（1987），395–403。[Gon09] C.D. González-Avilés，《函数域上 1-动机的算术对偶定理》，《纯粹与应用数学杂志》632（2009），203–231。[GoT12] C.D. González-Avilés、K.-S. Tan，《全局函数域上有限群概形的 Hasse 原理》，《数学研究快报》19（2012），第 02 期，453–460。[EGA IV，第 A 部分 4] A. Grothendieck 和 J. Dieudonné，《代数几何要素 IV》，高等科学研究所数学出版物 32（1967）。[SGA 7I] A. Grothendieck，《代数几何中的单值群 I》，《布瓦-马里代数几何研讨班 1967–1969》（SGA 7 I）。数学讲义 288。Springer，海德堡，1972。[Kis93] H. Kisilevsky，《函数域中的乘法独立性》，《数论杂志》44（1993），352–355。[LLTT16] K.F. Lai、I. Longhi、K.-S. Tan 和 F. Trihan，《函数域上半稳定阿贝尔簇的岩泽主猜想》，《数学杂志》282（2016），第 1 期，485–510。[LSc10] C. Liedtke、S. Schröer，《Igusa 曲线上的 Néron 模型》，《数论杂志》130（2010），2157–2197。[Mil80] J.S. Milne，《étale 上同调》，普林斯顿大学出版社，普林斯顿，1980。[Mil06] J.S. Milne，《算术对偶定理》，第二版（电子版），2006。[Mon81] P. Monsky，《关于 p-进幂级数》，《数学年刊》255（1981），第 2 期，217–227。[OT09] T. Ochiai 和 F. Trihan，《特征为 $p > 0$ 的函数域上阿贝尔簇的岩泽主猜想》，《剑桥哲学学会数学论文集》146（2009），23–43。[Sil86] J. H. Silverman，《椭圆曲线算术》，Springer Verlag，柏林，1986。[Tan95] K.-S. Tan，《Birch–Swinnerton-Dyer 型精细定理》，《傅里叶研究所年刊》，格勒诺布尔 45（1995），317–374。[Tan10] K.-S. Tan，《广义 Mazur 定理及其应用》，《美国数学会会刊》362（2010），第 8 期，4433–4450。[Tan14] K.-S. Tan，《 $\mathbb{Z}_p^d$-扩张上的塞尔默群》，《数学年刊》359（2014），1025–1075。[Ta66]J. Tate，《关于 Birch–Swinnerton-Dyer 猜想及其几何类比》，《布尔巴基研讨班》第 9 号（1966），415–440。[Ta84] J. Tate，《Stark 关于 L 中 Artin 函数的猜想》（Birkhäuser，波士顿，1984）。

Department of Mathematics, National Taiwan University, Taipei 10764, Taiwan
*E*电子邮件地址：tan@math.ntu.edu.tw