On local root numbers of abelian varieties

Lukas Melninkas

Thèse

INSTITUT DE RECHERCHE MATHÉMATIQUE AVANCÉE

UMR 7501

Strasbourg

présentée pour obtenir le grade de docteur de l'Université de Strasbourg
Spécialité MATHÉMATIQUES

Lukas Melninkas

Autour des signes locaux de variétés abéliennes

Soutenue le 6 Juillet 2021
devant la commission d'examen

Kęstutis Česnavičius, rapporteur
Olivier Fouquet, examinateur
Céline Maistret, examinatrice
Adriano Marmora, directeur de thèse
Rutger Noot, directeur de thèse
Takeshi Saito, rapporteur
Yichao Tian, examinateur

irma.math.unistra.fr

IRMA
Institut de Recherche Mathématique Avancée

cnrs

Université de Strasbourg

Autour des signes locaux de variétés abéliennes

Thèse de doctorat

présentée par

Lukas Melninkas

sous la direction de

Adriano Marmora et Rutger Noot

à

l'Université de Strasbourg

2021

Lukas Melninkas

Institut de recherche mathématique avancée UMR 7501,
Université de Strasbourg,
7 rue René Descartes,
67084 Strasbourg Cedex, France

Email address: melninkas@math.unistra.fr

2020 *Mathematics Subject Classification.* 11-02, 11G07, 11G10, 11G20, 11G40, 14G20, 14K15

Remerciements, Thanks, Ačiū

Tout d'abord, ma reconnaissance énorme va à mes deux directeurs de thèse Adriano Marmora et Rutger Noot. Votre disponibilité, vos soutiens et vos conseils ont été absolument essentiels pour la réussite de ce travail. Je vous remercie pour les innombrables heures de nos discussions, ainsi que pour le temps que vous avez passé en lisant les montagnes de texte que je vous envoyais.

Mes remerciements les plus sincères vont à Kęstutis Česnavičius et à Takeshi Saito pour avoir acceptés d'être rapporteurs de cette thèse ainsi que pour leurs commentaires et suggestions multiples concernant le manuscrit. Je remercie également Olivier Fouquet, Céline Maistret et Yichao Tian qui me font l'honneur de siéger dans le jury.

Pendant mes cinq années à l'Université de Strasbourg j'ai rencontré de nombreuses personnes que j'ai eu le plaisir d'appeler collègues. Je dis merci à mes partenaires d'enseignement Michel Coornaert, Sylvain Porret-Blanc, Hans-Werner Henn et toute l'équipe MSV avec Michaël Gutnic en tête, sans qui mon année ATER-Covid-rédaction aurait été beaucoup moins supportable. Je voudrais aussi remercier les chercheurs de l'IRMA avec qui j'ai eu des discussions mathématiques très intéressantes, notamment Giuseppe Ancona.

J'ai eu la fortune de discuter et partager un repas/verre avec plusieures générations de doctorants et post-docs en mathématiques. Pour un accueil très chalereux je dis merci à Guillaume D., Laura M. et Marie H. de l'équipe MoCo. Je veux bien remercier mes chers cobureaux dinosaures Elena, Firat, François, Giosué et Valeria, ainsi que les jeunes padawans Adam et Greta. Je remercie également les occupants du bureau-frère 114, notamment Ciccio, Djibril, Martin, P.-A., Sonia, Valdo et Yohann. Je remercie aussi Alex T., Cuong, Georgios, Fred et tous les autres qui ne sont pas mentionnés par leur prénom ici. Un grand merci particulier va à mes amis doctorants en géométrie arithmétique et fanboys de Deligne, Grothendieck, Serre et Tate. Ce sont donc Antoine, Archia, Hao et Kien à Strasbourg, Félix à London (Canada) et Yoël à Orsay.

I would like to thank Johannes and Kristina in London and Matthew and Simone in Bristol for the opportunities to present my research in their respective Number Theory seminars.

Merci à mes potes Camille et Lucile. My warmest thanks also goes to the people of StrasAir association of international students of which I was once a member and through which I have met many inspiring people.

No PhD student experience in Strasburgo would be complete without a swarm of Italians buzzing around. I believe the people of this lovely Mediteranean country have mistaken me for one of their own. Among many more, my particular thank-you's go to Alessandro, Antonella, Betta, Cosimino, Edo, Emanuela, Francesca, Giulia, Guido, Matteoandrea, Natascia, Roberto, and Valentina. Grazie a questi bomberi e bomberine, oggi sono orgoglioso di essere un cittadino onorario della Repubblica Italiana.

My dearest zio Lorenzo, you are a friend for life. I cannot thank you enough. Honestly, I really don't see how this thesis could have been completed without our skiing trips, and especially without that sweet sweet trip to Sardegna.

Labai dėkoju Julytei, ne tik už tai, kad pasikvietė į Strasbūrą ir surado darbą, bet ir už visas superines vakarienes ir intelektualines (ar nelabai) diskusijas.

Ačiū biznioplanui. Jūs, draugai, esat saulelės. Mūsų Simpioziumas, Workation Drobuose ir Du Ski yra geriausia kas man yra nutikę gyvenime. Ačiū, Mildute, Pijukai ir Vladukai, kad aplankėt.

Ačiū Mamai ir Tėtei už tai, kad užaugino tokį nevisiškai žioplą, ir už beribį ir besąlygišką palaikymą visame kame. Ačiū Martynukui už visas geiminimo sesijas, už pasaulio gelbėjimo diskusijas ir už nuotykius abipus Lamanšo ir Tsugaru. Ačiū Močiutei už reklamą ir palaikymą. Ačiū Vidai už viską, kuri, deja, nebesulaukė šios tezės pabaigos.

Contents

Introduction

On commence par introduire les objets centraux d'étude de cette thèse ainsi qu'expliquer leur intérêt. Ensuite, on présentera les résultats principaux obtenus par l'auteur.

1. Signes locaux

Soient p un nombre premier, $K/\mathbb{Q}_p$ une extension finie et $k/\mathbb{F}_p$ l'extension des corps résiduels induite. On notera $|k|$ le cardinal de k. On choisit une clôture algébrique $\overline{K}$ de K. Par convention, toute extension algébrique de K considérée dans ce texte sera contenue dans $\overline{K}$. Soit $\Gamma_K := \mathrm{Gal}(\overline{K}/K)$ le groupe de Galois absolu, $I_K \subset \Gamma_K$ le sous-groupe d'inertie et $K^{\mathrm{ur}} := \overline{K}^{I_K}$ l'extension maximale non-ramifiée de K. Le corps résiduel de K^{ur}, noté $\overline{k}$, est une clôture algébrique de k. On choisit $\varphi \in \Gamma_K$ un relèvement du Frobenius géométrique de $\mathrm{Gal}(\overline{k}/k) \cong \Gamma_K/I_K$. On définit le groupe de Weil de K par

$$W_K := \{i\varphi^n \mid i \in I_K,\, n \in \mathbb{Z}\} \subset \Gamma_K.$$

Le groupe W_K ne dépend pas du choix de φ et a une structure de produit semi-direct $W_K = I_K \rtimes \varphi^{\mathbb{Z}}$.

On désigne par $\left(\frac{\cdot}{k}\right)$ le symbole de Legendre sur $k^\times$ et par $(\cdot,\cdot)_K$ le symbole quadratique de Hilbert sur $K^\times \times K^\times$.

1.1. Représentations ℓ-adiques. Soient $\ell \neq p$ un nombre premier et V_ℓ un $\mathbb{Q}_\ell$-espace vectoriel de dimension finie muni de la topologie ℓ-adique. Une représentation ℓ-adique de Γ_K sur V_ℓ est un morphisme continu de groupes $\rho_\ell \colon \Gamma_K \to \mathrm{GL}(V_\ell)$.

1.2. Représentations de Weil. Le groupe W_K est muni de la topologie engendrée par les sous-groupes ouverts de I_K. Une représentation de Weil est un morphisme continu de groupes $\rho \colon W_K \to \mathrm{GL}(V)$ où V est un $\mathbb{C}$-espace vectoriel de dimension finie et $\mathrm{GL}(V)$ est muni de la topologie discrète. La continuité de ρ et équivalente à la finitude de l'image $\rho(I_K)$. On note $\mathrm{Rep}_{\mathbb{C}}(W_K)$ la catégorie des représentations de Weil et $\mathbb{1}_{W_K}$ la représentation triviale.

1.3. Représentations de Weil–Deligne. Par une représentation de Weil–Deligne on entend un couple $\rho' = (\rho, N)$ d'une représentation $\rho \in \mathrm{Rep}_{\mathbb{C}}(W_K)$ avec espace sous-jacent V et d'une application linéaire $N \in \mathrm{End}(V)$ nilpotente,

telle que N commute avec $\rho(I_K)$, et $\rho(\varphi)N\rho(\varphi)^{-1} = |k|^{-1}N$. L'application N est parfois appelée l'opérateur de monodromie.

1.4. Monodromie ℓ-adique. Soit ρ_ℓ une représentation ℓ-adique avec espace sous-jacent V_ℓ. En général, l'image $\rho_\ell(I_K)$ n'est pas finie. En suivant Grothendieck (voir [Del73, Thm. 8.2]) on peut associer à ρ_ℓ une représentation de Weil–Deligne de manière fonctorielle. En effet, on choisit un morphisme continu non-trivial $t_\ell\colon I_K \to \mathbb{Q}_\ell$ et un plongement $\iota : \mathbb{Q}_\ell \hookrightarrow \mathbb{C}$. Alors il existe une extension finie L/K et une unique application nilpotente $N \in \mathrm{End}(V_\ell \otimes_\iota \mathbb{C})$ telles que pour tout $i \in I_L$ on a $\rho_\ell(i) = \exp(\iota \circ t_\ell(i)N)$. Pour tout $i\varphi^n \in W_K$ on pose

$$\rho(i\varphi^n) := (\rho_\ell(i\varphi^n) \otimes_\iota \mathbb{C}) \cdot \exp(-\iota \circ t_\ell(i)N).$$

Alors (ρ, N) est une représentation de Weil–Deligne dont classe d'isomorphisme ne dépend pas des choix de φ et t_ℓ. À priori, elle dépend de ι.

En particulier, si $\rho_\ell(I_K)$ est fini, alors $\rho = \rho_\ell|_{W_K} \otimes_\iota \mathbb{C}$ et $N = 0$.

1.5. Cohomologie ℓ-adique. Soit X une variété lisse et propre sur K, qu'on notera X/K. Pour toute extension L/K on notera X_L ou $X \times_K L$ le changement de base de X à L. Pour tout entier $i \geqslant 0$, l'action de Γ_K sur $H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_\ell)$ définit une représentation ℓ-adique. Dans ce texte on va étudier les variétés abéliennes A/K et les représentations ℓ-adiques associées

$$\rho_\ell\colon \Gamma_K \to \mathrm{GL}\big(H^1_{\text{ét}}(A_{\overline{K}}, \mathbb{Q}_\ell)\big).$$

Das ce cas, $\dim \rho_\ell = 2 \dim A$ et la représentation duale ρ_ℓ^* est induite par la Γ_K-action sur le module de Tate $T_\ell A := \varprojlim A[\ell^n]$. De plus, la classe d'isomorphisme de la représentation de Weil–Deligne associée à ρ_ℓ ne dépend pas des choix de ℓ et de ι (fait dans 1.4), voir, p. ex., [Sab07, Cor. 1.15].

1.6. Facteurs epsilon. On se donne une représentation de Weil–Deligne $\rho' = (\rho, N)$ avec espace sous-jacent V. On fixe un caractère additif localement constant $\psi\colon K \to \mathbb{C}^\times$ et une mesure de Haar $\mathrm{d}x$ sur K. Soit Ind l'opérateur d'induction sur les représentations linéaires de groupes. Pour toute extension finie L/K on désigne par $\mathrm{Tr}_{L/K}\colon L \to K$ l'application de trace. En suivant [Roh94, §11] on définit le facteur epsilon de ρ' comme

$$\epsilon(\rho', \psi, \mathrm{d}x) := \epsilon(\rho, \psi, \mathrm{d}x)\delta(\rho'),$$

avec

$$\delta(\rho') := \det\left(-\rho(\varphi)\Big| V^{I_K}\Big/(\ker N)^{I_K}\right)$$

et où $\epsilon(\rho, \psi, \mathrm{d}x) \in \mathbb{C}^\times$ est l'unique nombre satisfaisant les axiomes suivants :

(i) si $0 \to \rho_1 \to \rho_2 \to \rho_3 \to 0$ est une suite exacte dans $\mathrm{Rep}_{\mathbb{C}}(W_K)$ alors $\epsilon(\rho_2, \psi, \mathrm{d}x) = \epsilon(\rho_1, \psi, \mathrm{d}x)\epsilon(\rho_3, \psi, \mathrm{d}x)$,

(ii) pour toute extension finie L/K, toute mesure de Haar $\mathrm{d}x_L$ sur L et toute $\rho \in \mathrm{Rep}_{\mathbb{C}}(W_L)$ on a

$$\epsilon(\mathrm{Ind}_{W_L}^{W_K}\rho, \psi, \mathrm{d}x) = \epsilon(\rho, \psi \circ \mathrm{Tr}_{L/K}, \mathrm{d}x_L) \left(\frac{\epsilon(\mathrm{Ind}_{W_L}^{W_K} \mathbb{1}_{W_L}, \psi, \mathrm{d}x)}{\epsilon(\mathbb{1}_{W_L}, \psi \circ \mathrm{Tr}_{L/K}, \mathrm{d}x_L)} \right)^{\dim \rho},$$

(iii) pour toute extension finie L/K, tout caractère additif $\psi_L \colon L \to \mathbb{C}^\times$, toute mesure de Haar $\mathrm{d}x_L$ sur L et toute $\xi \in \mathrm{Rep}_{\mathbb{C}}(W_L)$ de dimension 1, le nombre $\epsilon(\xi, \psi_L, \mathrm{d}x_L)$ est le coefficient de l'équation fonctionnelle de Tate associée à ξ, voir [Tat79, §3.2], [Roh94, §11] ou I.1.18.

Remarque 1.7. Les facteurs ϵ généralisent la notion de sommes de Gauss. En effet, pour un caractère modérément ramifié $\xi \in \mathrm{Rep}_{\mathbb{C}}(W_K)$, le facteur $\epsilon(\xi, \psi, \mathrm{d}x)$ est donné par une somme de Gauss classique sur $k^\times$, voir, p. ex., [AS10, Prop. 8.7.(i)].

1.8. Signe local. Pour une représentation de Weil–Deligne ρ' on définit le signe local

$$w(\rho', \psi) := \frac{\epsilon(\rho', \psi, \mathrm{d}x)}{|\epsilon(\rho', \psi, \mathrm{d}x)|}.$$

Il résulte des propriétés basiques des facteurs epsilon (voir [Roh94, §11, Prop.]) que $w(\rho', \psi)$ ne dépend pas du choix de $\mathrm{d}x$.

Soit A/K une variété abélienne. On définit son signe local par $w(A/K) := w(\rho', \psi)$ où ρ' est la représentation de Weil–Deligne obtenue à partir de la représentation ℓ-adique sur $H^1_{\text{ét}}(A_{\overline{K}}, \mathbb{Q}_\ell)$ comme dans 1.5. Dans ce cas, accouplement de Weil sur $H^1_{\text{ét}}(A_{\overline{K}}, \mathbb{Q}_\ell)$ induit une structure symplectique sur ρ' qui implique que $w(A/K) \in \{\pm 1\}$ et que $w(A/K)$ ne dépend pas du choix de ψ (voir [Roh94, §12]).

2. Conjectures autour des signes globaux

Soient $\mathcal{K}$ un corps de nombres et $A/\mathcal{K}$ une variété abélienne définie sur $\mathcal{K}$.

2.1. Signe global. Pour chaque place v de $\mathcal{K}$ on considère le complété $\mathcal{K}_v$ en v et la variété abélienne induite $A_v/\mathcal{K}_v$. En toute place infinie on définit $w(A_v/\mathcal{K}_v) := (-1)^{\dim A}$. Pour les places finies v, les signes locaux $w(A_v/\mathcal{K}_v)$ ont été définis dans 1.8. Pour toute place finie v où la réduction de $A_v/\mathcal{K}_v$ est bonne (voir tableau 1 plus bas) on a $w(A_v/\mathcal{K}_v) = 1$. Le nombre de places de $\mathcal{K}$ où la réduction n'est pas bonne est fini et on peut définir le signe global comme $w(A/\mathcal{K}) := \prod_v w(A_v/\mathcal{K}_v)$, le produit parcourt toutes les places v de $\mathcal{K}$.

2.2. Conjecture de parité. La conjecture de Hasse–Weil prédit que la fonction L complétée de $A/\mathcal{K}$, notée Λ, se prolonge analytiquement sur $\mathbb{C}$ et satisfait l'équation fonctionnelle

$$\Lambda(A/\mathcal{K}, s) = w(A/\mathcal{K})\Lambda(A/\mathcal{K}, 2-s).$$

Elle implique, en particulier, que

$$w(A/\mathcal{K}) = (-1)^{\operatorname{ord}_{s=1}\Lambda(A/\mathcal{K},s)}.$$

L'entier $\operatorname{ord}_{s=1}\Lambda(A/\mathcal{K},s)$ est appelé le rang analytique de $A/\mathcal{K}$. Le rang de Mordel–Weil de $A/\mathcal{K}$ est défini comme le rang du groupe des points rationnels $A(\mathcal{K})$. La conjecture de Birch et Swinnerton-Dyer affirme que

$$\operatorname{ord}_{s=1}\Lambda(A/\mathcal{K},s) = \operatorname{rk} A(\mathcal{K}).$$

La combinaison des deux conjectures implique que

$$(-1)^{\operatorname{rk} A(\mathcal{K})} = w(A/\mathcal{K}).$$

Cette dernière équation est appelée la conjecture de parité. En particulier, elle implique que si $w(A/\mathcal{K}) = -1$, alors le groupe $A(\mathcal{K})$ contient un élément d'ordre infini.

2.3. Conjecture de p-parité. Pour tout nombre premier p, il est conjecturé que la partie de p^∞-torsion du groupe de Shafarevich–Tate de $A/\mathcal{K}$ est fini. Si c'est le cas, l'entier $\operatorname{rk} A(\mathcal{K})$ est égal au co-rang $\operatorname{rk}_p(A/\mathcal{K})$ du groupe de Selmer $\varinjlim \operatorname{Sel}^{(p^n)}(A/\mathcal{K})$, voir [Dok13, §2]. On peut donc espérer que l'égalité

$$(-1)^{\operatorname{rk}_p(A/\mathcal{K})} = w(A/\mathcal{K})$$

est valable indépendamment des conjectures mentionnées ci-dessus. On l'appelle la conjecture de p-parité. Si $A/\mathcal{K}$ admet une isogénie de degré $p^{\dim A}$ et satisfait d'autres hypothèses techniques (voir [CFKS10, Thm. 2.3]), alors on peut décomposer $(-1)^{\operatorname{rk}_p(A/\mathcal{K})}$ en un produit infini de facteurs locaux indexés par toutes les places v de $\mathcal{K}$. En comparant chaque facteur local avec le signe local $w(A_v/\mathcal{K}_v)$ on peut tenter de démontrer la conjecture de p-parité. Plusieurs preuves de cas particuliers adoptent cette stratégie et utilisent des formules de signes locaux.

3. Quelques invariants classiques

Dans cette section on va introduire quelques invariants associés à une variété abélienne A définie sur une extension finie $K/\mathbb{Q}_p$. Ils figurent dans les formules de signes locaux connues précédemment ainsi que dans les résultats de cette thèse. On note v_K la valuation de K normalisée par $v_K(K^\times) = \mathbb{Z}$. Soit $\mathcal{O}_K$ son anneau des entiers.

Parmi les invariants d'une représentation de Weil–Deligne nous avons son conducteur d'Artin, noté $a(\cdot)$. Soient ρ_ℓ une représentation ℓ-adique et $\rho' = (\rho, N)$ la représentation de Weil–Deligne attachée comme expliqué dans 1.4. On pose $a(\rho_\ell) := a(\rho')$. Si maintenant ρ_ℓ est associée à une variété abélienne A/K comme dans 1.5, alors $a(\rho_\ell)$ est indépendant du choix de ℓ et on définit $a(A/K) := a(\rho_\ell)$.

Soit $\mathscr{A}/\mathcal{O}_K$ le modèle de Néron de A/K. On note $\mathscr{A}_k$ sa fibre spéciale et $\mathscr{A}_k^\circ$ la composante neutre de cette dernière. Le groupe $\Phi := \mathscr{A}_k/\mathscr{A}_k^\circ$ est fini et on pose $c(A/K) := |\Phi(k)|$. On l'appelle le nombre de Tamagawa local. En général, $\mathscr{A}_k^\circ$ est une extension d'une variété abélienne B par le produit d'un tore T et d'un groupe unipotent U. Les dimensions de B, T et U sont respectivement appelées les rangs abélien, torique et unipotent de A/K.

On définit les types de réduction de A/K selon le tableau 1.

Tableau 1. Types de réduction de A/K.

Réduction	Condition
bonne	$\dim U = \dim T = 0$
torique	$\dim U = \dim B = 0$
additive	$\dim T = \dim B = 0$
semi-stable	$\dim U = 0$

Rappelons que la construction de $\mathscr{A}/\mathcal{O}_K$ ne commute pas avec un changement de base quelconque. On dit que A/K a réduction potentiellement de type $*$ s'il existe une extension finie L/K telle que A_L/L a réduction de type $*$. D'après le théorème de réduction semi-stable de Grothendieck, toute variété abélienne A/K a réduction potentiellement semi-stable. En général, en passant à une extension finie de K le rang unipotent décroit est les rangs abélien et torique augmentent.

Grothendieck a aussi établi un critère de réduction semi-stable en termes des représentations ℓ-adiques. En effet, A/K a réduction semi-stable si et seulement si tout élément de $\rho_\ell(I_K)$ est unipotent. Le critère de Néron–Ogg–Shafarevich affirme que $\rho_\ell(I_K)$ est trivial si et seulement si A/K a bonne réduction. En particulier, A/K a potentiellement bonne réduction si et seulement si $\rho_\ell(I_K)$ est fini. Dans ce cas, si on note $I_K^{\mathrm{w}} \subset I_K$ le sous-groupe de ramification sauvage, alors $\rho_\ell(I_K)$ est une extension d'un groupe cyclique fini d'ordre premier à p par le p-groupe fini $\rho_\ell(I_K^{\mathrm{w}})$. D'après Serre–Tate [ST68, p. 497, Cor. 2], si $\rho_\ell(I_K^{\mathrm{w}})$ est non-trivial, alors $p \leqslant 2\dim A + 1$.

Supposons que J/K est la jacobienne d'une courbe projective lisse C/K de genre g. Alors $\dim \rho_\ell = 2\dim J = 2g$. La courbe C/K admet un unique modèle minimal régulier (projectif, plat) $\mathscr{C}/\mathcal{O}_K$. On note $m(C/K)$ le nombre des composantes irréductibles de la fibre spéciale géométrique $\mathscr{C}_{\overline{k}}$ de $\mathscr{C}$. Si C/K est une courbe hyperelliptique, alors elle admet une équation de Weierstrass $Y^2 = P(X)$ avec $P \in K[X]$ de degré $2g+1$ ou $2g+2$. Pour une telle équation on définit son discriminant $\Delta \in K^\times$ en suivant Liu [Liu96, §2] (voir aussi II.2.2 pour le cas $g = 2$). La classe de Δ dans $K^\times/(K^\times)^2$ ne dépend pas du choix de l'équation de Weierstrass. Pour une courbe elliptique il existe une équation de Weierstrass minimale dont le discriminant $\Delta_{\min}$ est appelé minimal. La valuation $v_K(\Delta_{\min})$ ne dépend pas de l'équation minimale choisie. Dans le cas

général des courbes hyperelliptiques, il y a plusieurs façons non-équivalentes de définir un discriminant minimal. Dans le cas de genre 2 les relations entre des discriminants minimaux ont été étudiées par Liu [Liu94a].

4. Résultats précédents sur les signes locaux

4.1. Résultats généraux. La théorie des facteurs epsilon a été développée par Tate [Tat67], Dwork [Dwo56], Langlands [Lan70] et Deligne [Del73].

Quelques formules pour les facteurs epsilon et les signes locaux ont été établies par Fröhlich–Queyrut [FQ73, Thm. 3] et Abbes–Saito [AS10, §8].

Le résultat principal de Rohrlich [Roh11] montre que si ρ est une représentation de Weil (complexe) avec une certaine structure symplectique, alors son signe local est égal à ceux de ses conjuguées par l'action de $\mathrm{Aut}(\mathbb{C})$.

4.2. Courbes elliptiques. Le signe local d'une courbe elliptique E/K sur un corps p-adique K avec $p \geqslant 5$ a été calculé par Rohrlich [Roh93; Roh96]. Les cas de réduction potentiellement torique et de potentiellement bonne réduction sont traités séparément. Dans le dernier cas le signe local dépend seulement du corps résiduel k et de l'entier $|\rho_\ell(I_K)| = \frac{12}{\mathrm{pgcd}(v_K(\Delta_{\min}),12)}$, voir aussi [DD10, Thm. 3.1].

Pour une courbe elliptique définie sur $\mathbb{Q}$, Connell [Con94] a établi des formules pour le signe local en 2 et en 3 sous certaines hypothèses. Dans le même contexte, Halberstadt [Hal98] a produit des tableaux complets pour déterminer le signe local à partir d'une équation de Weierstrass minimale de la courbe. Sa méthode est indirecte : en utilisant les résultats de modularité on calcule d'abord le signe global et puis on détermine les signes locaux inconnus via le produit infini.

Le cas d'une courbe elliptique sur un corps 3-adique général a été étudié par Kobayashi [Kob02]. Le signe local est déterminé en termes du type de Kodaira–Néron et d'une équation de Weierstrass particulière dans le cas où ρ_ℓ est sauvagement ramifiée (i.e. $|\rho_\ell(I_K^{\mathrm{w}})|$ est non-trivial). On reformule ce résultat dans Thm. 7.1 en termes qui ne réfèrent pas directement aux équations de Weierstrass.

Dans le cas d'une courbe elliptique 2-adique générale, les résultats de Dokchitser–Dokchitser [DD08] permettent de calculer le signe local en calculant des signes locaux de caractères explicites associés à l'extension de rationalité des points de 3-torsion. Combiné avec les résultats mentionnés ci-dessus ça permet de déterminer le signe local d'une courbe elliptique E/K quelconque. Par conséquent, on peut calculer le signe global de toute courbe elliptique définie sur un corps de nombres. La procédure complète a été mise en œuvre sur Magma par T. Dokchitser.

Enfin, Sabitova [Sab14] montre comment les signes locaux d'une courbe elliptique se comportent par rapport à un changement du corps de base.

4.3. Variétés abéliennes. Sabitova [Sab07, Prop. 1.10] montre qu'afin de déterminer le signe local d'une variété abélienne A/K on peut se ramener à calculer le signe local d'une variété abélienne de potentiellement bonne réduction et le signe local d'une représentation de Galois provenant d'un tore.

Les travaux de Brumer–Kramer–Sabitova [BKS18] permettent de calculer les signes locaux des variétés abéliennes avec réduction additive potentiellement torique et des jacobiennes de courbes stables. Dans ce dernier cas, les formules sont données en termes de la géométrie de la fibre spéciale d'un modèle stable.

La formule de Česnavičius [Čes18, Thm. 1.6] montre comment le signe local de A/K varie par rapport à un changement de base non-ramifié. Ce changement est controlé par le degré de l'extension non-ramifiée en question et le conducteur $a(A/K)$.

Dans le cas où $\rho_\ell(I_K^{\mathrm{w}})$ est trivial, Bisatt [Bis19] a obtenu des formules pour le signe local en comptant les valeurs propres de l'image par ρ_ℓ d'un générateur topologique de I_K/I_K^{w}.

Récemment, Bisatt [Bis21] a produit des formules pour les signes locaux associés aux jacobiennes de courbes hyperelliptiques de genre $g = \frac{p-1}{2}$ ayant ramification maximale (i.e. $|\rho_\ell(I_K)| = 2(p-1)p$) généralisant les résultats de Kobayashi. Ses formules dépendent d'une équation particulière de Weierstrass.

5. Multiplication réelle

Ici on présente les résultats du chapitre I de cette thèse. Ils font l'objet de la prépublication [Mel19].

5.1. Les hypothèses. Soit A/K une variété abélienne de dimension g définie sur un corps p-adique $K/\mathbb{Q}_p$ avec $p \neq 2$. On suppose que A/K a multiplication réelle, i.e. qu'il existe une involution de Rosati, un corps de nombres $F/\mathbb{Q}$ totalement réel de degré g et un plongement d'anneaux $i\colon F \to \mathrm{End}_K(A)\otimes_{\mathbb{Z}}\mathbb{Q}$ tels que $i(F)$ est fixé par l'involution. Sous l'hypothèse additionnelle que $\rho_\ell(I_K)$ est abélien on donne des formules pour le signe local en termes des invariants classiques de A/K introduits dans la section 3. Pour cela on s'inspire des méthodes développées par Rohrlich dans le cas de courbes elliptiques.

Théorème 5.2 (Prop. I.3.12, Cor. I.4.8). *Supposons que A/K a multiplication réelle et que sa réduction est potentiellement bonne. Désignons par $ep^r = |\rho_\ell(I_K)|$ avec $p \nmid e$, et par $a(A/K)$ le conducteur d'Artin de A/K.*

(1) *Si g est pair, alors $w(A/K) = 1$;*
(2) *Si $\rho_\ell(\Gamma_K)$ est commutatif, alors $\frac{|k|-1}{e} \in \mathbb{Z}$ et*

$$w(A/K) = (-1)^{g\frac{|k|-1}{e}};$$

(3) *Si* $\rho_\ell(\Gamma_K)$ *est non-commutatif et* $\rho_\ell(I_K)$ *est commutatif, alors* $\frac{a(A/K)}{2g} \in \mathbb{Z}$, $\frac{|k|+1}{e} \in \mathbb{Z}$ *et*

$$w(A/K) = (-1)^{\frac{a(A/K)}{2} + g\frac{|k|+1}{e}}.$$

5.3. Conséquences géométriques. On montre dans la Prop. I.2.6 que l'hypothèse de multiplication réelle donne une trichotomie géométrique sur A/K : sa réduction est soit bonne, soit torique, soit additive. De plus, si la réduction est additive, alors elle est soit potentiellement bonne, soit potentiellement torique. Ces résultats généralisent la situation observée dans le cas de courbes elliptiques. Dans le cas où A/K a réduction torique, la composante neutre de la fibre spéciale du modèle de Néron est un tore T. Si $T \simeq \mathbb{G}_m^g$ on dit que la réduction est torique déployée, sinon on dit que la réduction est torique non-déployée. Il suit de I.5.2 que soit $T \simeq \mathbb{G}_m^g$, soit T ne contient aucune copie de $\mathbb{G}_m$.

Théorème 5.4 (Prop. I.5.1, Cor. I.5.4). *Supposons que* A/K *a multiplication réelle et que sa réduction n'est pas potentiellement bonne. Alors* A/K *a réduction potentiellement torique et*

$$w(A/K) = \begin{cases} (-1)^g & \text{si la réduction est torique déployée;} \\ 1 & \text{si la réduction est torique non-déployée;} \\ \left(\frac{-1}{k}\right)^g & \text{si la réduction est additive.} \end{cases}$$

De plus, ces trois cas sont les seuls possibles.

Remarque 5.5. Comme conséquence de théorèmes ci-dessus on obtient $w(A/K) = 1$ pour toute variété abélienne A/K avec multiplication réelle et de dimension paire. Il suit que pour toute variété abélienne $A/\mathcal{K}$ de dimension paire définie sur un corps de nombres $\mathcal{K}$ avec multiplication réelle, son signe global est $w(A/\mathcal{K}) = 1$.

5.6. Esquisse de la preuve. Soit F le corps totalement réel de la définition de multiplication réele 5.1. On montre dans Prop. I.3.3 et I.5.2 que ρ_ℓ est $F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$-linéaire et que les polynômes caractéristiques de $\rho_\ell(W_K)$ sont à coefficients dans F. Il s'ensuit que la représentation de Weil–Deligne complexe ρ' associée se décompose en g facteurs directs qui sont conjugués pour l'action de $\mathrm{Aut}(\mathbb{C})$. On montre dans Prop. I.3.4 que ces facteurs ont des propriétés qui ressemblent à celles de représentations provenant de courbes elliptiques. D'après le théorème de Rohrlich [Roh11, Thm. 1] les signes locaux de ces facteurs sont tous égaux. Dans le cas de potentiellement bonne réduction on sépare l'analyse en deux cas selon la commutativité de $\rho_\ell(\Gamma_K)$. Le cas commutatif peut être traité directement, voir Thm. I.4.1. Dans le cas non-commutatif on se ramène à calculer le signe local d'un caractère. Celui-ci est calculé grâce au théorème de Fröhlich–Queyrut, voir Thm. I.4.6.

6. Surfaces jacobiennes et ramification maximale

Ici on présente le résultat principal du chapitre II. Ces travaux font l'objet de [Mel21].

6.1. Le cadre. Soit C/K une courbe hyperelliptique de genre 2 définie sur une extension finie $K/\mathbb{Q}_p$. On suppose que sa jacobienne J/K a potentiellement bonne réduction et que $\rho_\ell(I_K^{\mathrm{w}})$ est non-triviale. On a vu dans la section 3 qu'alors $p \leqslant 5$. Pour simplifier on suppose dans cette section et dans la plupart du chapitre II que $p = 5$. Liu [Liu93, Cor. 4.1] montre que C/K a potentiellement bonne réduction, i.e. il existe une extension finie L/K pour laquelle le modèle minimal régulier $\mathscr{C}'$ de C_L est lisse sur $\mathcal{O}_L$. Liu [Liu94b, §5.1] donne également un analogue pour l'algorithme de Tate : il existe un modèle de Weierstrass de C/K donné par l'équation

$$Y^2 = P(X) = X^5 + a_2X^4 + a_3X^3 + a_4X^2 + a_5X + a_6 \tag{6.1.1}$$

telle que $P(X) \in \mathcal{O}_K[X]$ est irréductible et $1 \leqslant v_K(a_6) \leqslant 9$, $v_K(a_6) \neq 5$. En outre, l'entier $v_K(a_6)$ détermine complètement le type de la fibre spéciale géométrique $\mathscr{C}_{\overline{k}}$ de $\mathscr{C}/\mathcal{O}_K$ en suivant la classification due à Namikawa–Ueno [NU73]. En particulier, $v_K(a_6)$ détermine $m(C/K)$, le nombre des composantes irréductibles de $\mathscr{C}_{\overline{k}}$.

6.2. L'action d'inertie maximale. Sous les hypothèses de 6.1, on montre dans II.3.5 que $\rho_\ell(I_K^{\mathrm{w}})$ est d'ordre 5 et que $\rho_\ell(I_K)$ est isomorphe à un sous-groupe de produit semi-direct $C_5 \rtimes C_8$ où C_8 agit sur C_5 à travers de $C_8 \twoheadrightarrow C_4 \simeq \mathrm{Aut}(C_5)$. Grâce à la Prop. II.3.13, le quotient $\rho_\ell(I_K)/\rho_\ell(I_K^{\mathrm{w}})$ dépend seulement de la valuation $v_K(\Delta)$ d'un discriminant Δ de C/K (voir II.2.2 pour la définition), et donc l'entier $v_K(\Delta)$ détermine la structure exacte de $\rho_\ell(I_K)$. On s'intéresse au cas où $\rho_\ell(I_K) \simeq C_5 \rtimes C_8$. On montre dans Prop. II.5.1 que cette condition est équivalente à la condition que la valuation $v_K(\Delta)$ est impaire et également à la condition que le conducteur $a(J/K)$ est impair.

Theorem 6.3 (Thm. II.6.1). *Soit $p = 5$ et soit C/K une courbe hyperelliptique de genre 2. On suppose que ρ_ℓ est sauvagement ramifiée et que pour un discriminant Δ de C/K la valuation $v_K(\Delta)$ est impaire. Étant donné une équation de Weierstrass comme dans (6.1.1), le signe local est donné par*

$$w(C/K) = -(-1)^{[k:\mathbb{F}_5]} \cdot \left(\frac{m(C/K)+3}{k}\right) \cdot (\Delta, a_6)_K. \tag{6.3.1}$$

Remarque 6.4. Le choix de Δ ci-dessus n'est pas important car sa classe dans $K^\times/(K^\times)^2$ ne dépend pas de ce choix. Par contre, il est nécessaire d'avoir $5 \nmid v_K(a_6)$.

6.5. Esquisse de la preuve. On utilise une approche analogue à celle de Kobayashi [Kob02]. La représentation de Weil ρ associée à A/K est induite par un caractère χ du W_H avec $H = K(\sqrt[4]{-\Delta})$. Dans II.6.2 on montre comment se ramener au calcul du signe local $w(\chi, \psi)$, avec un caractère additif $\psi\colon K \to \mathbb{C}^\times$ bien choisi. Une ψ-jauge de χ est un élément de $H^\times$ qui permet de comparer le caractère multiplicatif χ avec le caractère additif ψ (voir II.1.3). Dans Cor. II.1.9 on exprime $w(\chi, \psi)$ en termes d'une ψ-jauge explicite c en utilisant la théorie explicite des corps de classes locaux due à Serre. On explique dans II.6.4 comment choisir c en fonction de l'équation (6.1.1). Il reste à calculer $\chi(c)$, ici on a identifié χ avec un pseudo-caractère de $H^\times$ en utilisant le morphisme de réciprocité d'Artin. Pour ce faire, il faut étudier la configuration des racines de P. On choisit une extension L/K explicite pour laquelle C_L/L a bonne réduction, i.e. son modèle minimal régulier $\mathscr{C}'/\mathcal{O}_L$ est lisse. On étudie la fibre spéciale $\mathscr{C}'_{k_L}$ grâce à la théorie d'Artin–Schreier et on détermine $\mathrm{Tr}(\rho)$ en comptant les points sur $\mathscr{C}'_{k_L}$, voir Prop. II.4.8. Dans le cas où $[k_K : \mathbb{F}_5]$ est pair on utilise un résultat de Yelton [Yel15] sur le corps de rationalité $K(J[4])$ des points de 4-torsion de J. Dans le cas où $[k_K : \mathbb{F}_5]$ est impair, une analyse plus fine est nécessaire. On exploite un lien entre le choix de χ, le choix de L, et la configuration des racines de P (voir Prop. II.4.10, Lemme II.6.7).

L'invariant $m(C/K)$ dans la formule du Thm. 6.3 vient de la congruence $v_K(a_6) \equiv (m(C/K)+3) \bmod (\mathbb{F}_5^\times)^2$ pour le coefficient a_6 de l'équation (6.1.1), qui est démontrée dans le Cor. II.3.21.

7. Courbes elliptiques revisitées

On présente le résultat principal de la section II.8 qui fait partie de [Mel21].

Soit E/K une courbe elliptique ayant potentiellement bonne réduction. On suppose que l'image $\rho_\ell(I_K)$ n'est pas abélienne. Alors $\rho_\ell(I_K^{\mathrm{w}})$ est non-triviale, d'où $p = 2$ ou $p = 3$. Dans le cas où $p = 3$ les signes locaux ont été déterminés par Kobayashi [Kob02] en termes d'une équation de Weierstrass particulière, analogue à (6.1.1). Nous donnons une caractérisation plus géométrique en termes des invariants introduits dans la section 3.

Théorème 7.1 (Thm. II.8.10). *Soient $K/\mathbb{Q}_3$ une extension finie et E/K une courbe elliptique de potentiellement bonne réduction pour laquelle $\rho_\ell(I_K)$ est non-abélienne. Soit $H = K(\sqrt{\Delta})$ pour un discriminant Δ de E/K. On note $\lfloor\cdot\rfloor$ la fonction partie entière sur $\mathbb{R}$ et v_3 la valuation 3-adique sur $\mathbb{Q}$. Alors $a(E/K)$ et $m(E/K)$ sont impairs, $c(E/H)$ est 1 ou 3, et on a*

$$w(E/K) = (-1)^{v_3(c(E/H))} \cdot \left(\frac{-1}{k}\right)^{\frac{a(E/K)+m(E/K)}{2}+\lfloor\frac{m(E/K)+1}{6}\rfloor}.$$

Remarque 7.2.

(1) La condition que $\rho_\ell(I_K)$ est non-commutative est équivalente à la condition que la valuation $v_K(\Delta)$ est impaire et $a(E/K) \geqslant 3$.

(2) L'extension H/K ne dépend pas du choix de Δ. Sous les hypothèses du Thm. 7.1 le corps de rationalité $K(E[2])$ des points de 2-torsion de E définit une extension totalement ramifiée de K de degré 6. Dans ce cas H/K est l'unique sous-extension quadratique de $K(E[2])/K$.
(3) Sous les hypothèses du Thm. 7.1 l'entier $c(E/H)$ vaut 1 ou 3. Le symbole de Kodaira–Néron de E/K (voir [Sil94, IV.8.2]) est II, II^*, IV ou IV^* et $\lfloor \frac{m(E/K)+1}{6} \rfloor$ vaut 1 si «*» apparaît dans le symbole et 0 sinon.

7.3. Preuves. On donne deux preuves du Thm. 7.1. Pour la première (voir page 70) on commence avec la formule originale de Kobayashi et on applique l'algorithme de Tate afin de déterminer le nombre de Tamagawa sur H à partir d'une équation de Weierstrass sur K. Pour la deuxième (voir page 72) on utilise la formule des Dokchister [DD11, Thm. 6.3] et on se ramène à calculer les différentielles de Néron de E sur certaines extensions finies de K.

8. Lien avec des nombres de Tamagawa

Le théorème présenté ici est le résultat principal du chapitre III.

Reprenons pour l'instant le cadre 6.1. Partant de la formule obtenue dans le Thm. 6.3, on voudrait remplacer le facteur $(\Delta, a_6)_K$ par un terme plus géométrique. La démonstration du Thm. 7.1 suggère que le nombre de Tamagawa $c(J/H)$ sur une extension H/K bien choisie pourrait jouer ce rôle. On montre une formule qui généralise cette idée pour des courbes hyperelliptiques plus générales. Soient $p > 2$ un nombre premier et $K/\mathbb{Q}_p$ une extension finie.

THÉORÈME 8.1 (Prop. III.1.2, Prop. III.4.1). *Soit C/K une courbe hyperelliptique de genre $g = \frac{p-1}{2}$ telle que ρ_ℓ est sauvagement ramifiée. Alors sa jacobienne J/K a potentiellement bonne réduction et C/K est définie par une équation*

$$Y^2 = P(X) = X^p + \ldots + a_0 \tag{8.1.1}$$

avec $P \in \mathcal{O}_K[X]$ irréductible, $0 < v_K(a_0) < 2p$ et $v_K(a_0) \neq p$.

On suppose que $v_K(\Delta)$ est impaire pour un discriminant Δ de C/K. Soit $H := K(\sqrt{\Delta})$. Alors

$$(\Delta, a_0)_K \cdot \left(\frac{-1}{k}\right)^{v_K(a_0)} = -(-1)^{v_p(c(J/H))}. \tag{8.1.2}$$

REMARQUE 8.2. L'extension H/K ne dépend pas du choix de Δ. De plus, si $K(J[2])/K$ désigne l'extension de rationalité des points de 2-torsion de J, alors, sous les hypothèses du théorème, $K(J[2])/K$ est totalement ramifiée de degré pair $(p-1)p$. L'extension $K(J[2])/K$ contient une unique sous-extension quadratique, qui est H/K.

8.3. Esquisse de la preuve. L'existence de l'équation (8.1.1) généralise le résultat de Liu [Liu94b, §5.1] produisant l'équation (6.1.1). Notre preuve suit l'approche de Liu, voir Prop. III.1.2. Pour montrer l'égalité (8.1.2) on construit

d'abord un modèle régulier explicite de C/K. On utilise l'algorithme général de Dokchitser [Dok18] qui produit un modèle à croisements normaux en fonction du polytope de Newton de (8.1.1). La fibre spéciale géométrique $\mathscr{C}_{\overline{k}}$ de ce modèle, avec l'action de Galois, est décrite dans III.2.15. Ensuite, dans Prop. III.3.3 on explicite la matrice d'incidence de $\mathscr{C}_{\overline{k}}$. Cette information est suffisante pour appliquer les résultats de Bosch–Liu [BL99] et pour montrer (voir Thm. III.3.1) la formule

$$c(J/K) = \begin{cases} p & \text{si } a_0 \in (K^\times)^2; \\ 1 & \text{sinon.} \end{cases} \tag{8.3.1}$$

L'égalité (8.1.2) est une conséquence de (8.3.1).

8.4. Applications aux signes locaux. On utilise (8.1.2) pour réécrire la formule (6.3.1) sans référence directe à une équation de Weierstrass particulière, voir Cor. III.4.3.

De manière similaire, l'équation (8.1.2) peut être utilisée pour donner une autre preuve du Thm. 7.1, et aussi pour reformuler le résultat de Bisatt [Bis21, Thm. 2.1] en termes plus géométriques.

Chapter I

On the root numbers of abelian varieties with real multiplication

Abstract. Let A/K be an abelian variety with real multiplication defined over a p-adic field K with $p > 2$. We show that A/K must have either potentially good or potentially totally toric reduction. In the former case we give formulas of the local root number of A/K under the condition that inertia acts via an abelian quotient on the associated Tate module; in the latter we produce formulas without additional hypotheses.

Introduction

Let A be an abelian variety defined over a number field $\mathcal{K}$. The Hasse–Weil conjecture (see, e.g., [Ser70, §4.1]) predicts that its completed L-function $\Lambda(A/\mathcal{K}, s)$ has a meromorphic continuation to the whole of $\mathbb{C}$ and satisfies a functional equation

$$\Lambda(A/\mathcal{K}, s) = w(A/\mathcal{K})\Lambda(A/\mathcal{K}, 2-s).$$

The coefficient $w(A/\mathcal{K})$ is called the global root number. A straightforward consequence of the conjecture is the equality $w(A/\mathcal{K}) = (-1)^{\operatorname{ord}_{s=1}\Lambda(A/\mathcal{K},s)}$. On the other hand, the Mordel–Weil theorem tells us that the group of rational points $A(\mathcal{K})$ is finitely generated. Its rank $\operatorname{rk}(A/\mathcal{K})$ is notably hard to compute in general and, granting analytic continuation of Λ at $s = 1$, is predicted to be equal to $\operatorname{ord}_{s=1}\Lambda(A/\mathcal{K}, s)$ by the Birch and Swinnerton-Dyer conjecture. As a consequence of the two aforementioned conjectures, we get a third one, the Parity Conjecture, which is the equality

$$(-1)^{\operatorname{rk}(A/\mathcal{K})} = w(A/\mathcal{K}).$$

Deligne [Del73] shows that the global root number can be defined unconditionally as the product of local factors $\prod_v w(A_v/\mathcal{K}_v)$ where v runs through all the places of $\mathcal{K}$ and all but finitely many factors are 1. For each v, the local root number $w(A_v/\mathcal{K}_v)$ is defined via the respective local complex Weil–Deligne representation by using the theory of ϵ-factors, see [Del73, §4]. It is expected that the geometric properties of A impose enough conditions on the associated Weil–Deligne representations to allow a complete and explicit determination of the root number. Let us briefly review the existing formulas in the next paragraphs.

For each infinite place, the Weil–Deligne representation is defined using the Hodge decomposition of $H^1(A(\mathbb{C}),\mathbb{C})$ and the root number is always $(-1)^{\dim A}$ (see [Sab07, Lemma 2.1]).

For a finite place v of residual characteristic p the Weil–Deligne representation is obtained via an ℓ-adic Galois representation for any $\ell \neq p$ (or even for $\ell = p$ following Fontaine). We know that $w(A_v/\mathcal{K}_v) = 1$ if A has good reduction at v. In general, the existence of the Weil pairing forces $w(A_v/\mathcal{K}_v) = \pm 1$.

Let $K/\mathbb{Q}_p$ be a finite extension and let A/K be an elliptic curve. When $p \geqslant 5$, the local root number was computed by Rohrlich [Roh96]. In this case, the root number is essentially determined by the Néron–Kodaira reduction type of A/K. Kobayashi [Kob02] has extended Rohrlich's results to include the case $p = 3$, where we find a dependancy on the Artin conductor $a(A/K)$. Kobayashi's general formula also includes some coefficients of a Weierstrass equation. The case $p = 2$ has been studied by Connell [Con94] and the Dokchitsers [DD08].

For a general abelian variety, a framework for studying the associated Weil–Deligne representation and its root number was developed by Sabitova [Sab07]. Under the condition that the inertia action on the Tate module is tame, Bisatt [Bis19] gives explicit formulas.

0.1. The setup and results. Let p be a prime and let $K/\mathbb{Q}_p$ be a finite extension. Let A/K be abelian variety of dimension g together with a polarization $\lambda\colon A \to A^\vee$ defined over K. Let $\cdot^\dagger$ denote the corresponding Rosati involution on $\mathrm{End}_K^0(A) := \mathrm{End}_K(A) \rtimes_{\mathbb{Z}} \mathbb{Q}$. If there exists a totally real field F of degree $[F : \mathbb{Q}] = g$ and an inclusion of rings $F \to \mathrm{End}_K^0(A)$ such that the image of F is fixed by $\cdot^\dagger$, then we say that A has real multiplication (RM) by F over K. For example, every elliptic curve has real multiplication by $\mathbb{Q}$. In this chapter we generalize the methods used in the case of elliptic curves for the RM setting and produce formulas for local root numbers $w(A/K)$ that extend previously known results. Let $\Gamma_K = \mathrm{Gal}(\overline{K}/K)$, I_K, and q_K be respectively the absolute Galois group, the inertia subgroup, and the order of the residue field of K. We fix a prime $\ell \neq p$ and we denote by ρ_ℓ the ℓ-adic Galois representation of Γ_K on $H^1_{\text{ét}}(A_{\overline{K}},\mathbb{Q}_\ell)$. By $a(A/K)$ we denote the Artin conductor of ρ_ℓ, which is independent of ℓ. The main results of this chapter are the following.

Theorem 0.2 (Cor. 4.8). *Let A/K be an abelian variety of dimension g with real multiplication. Let us suppose that $p \neq 2$ and that A/K has potentially good reduction, so that $\rho_\ell(I_K)$ is a finite group of some order ep^r with $p \nmid e$.*

(1) *If $\rho_\ell(\Gamma_K)$ is commutative, then $\frac{q_K-1}{e} \in \mathbb{Z}$ and*

$$w(A/K) = (-1)^{\frac{g(q_K-1)}{e}};$$

(2) *If $\rho_\ell(\Gamma_K)$ is non-commutative and $\rho_\ell(I_K)$ is commutative, then $\frac{a(A/K)}{2g}$ and $\frac{q_K+1}{e}$ are integers, and we have*

$$w(A/K) = (-1)^{\frac{a(A/K)}{2}+\frac{g(q_K+1)}{e}}.$$

THEOREM 0.3 (Prop. 2.6 and Cor. 5.4). *Let A/K be an abelian variety with real multiplcation. We suppose that $p \neq 2$ and that A/K does not have potentially good reduction. Then A/K has potentially totally toric reduction and*

$$w(A/K) = \begin{cases} (-1)^g & \text{if the reduction (over } K\text{) is split multiplicative;} \\ 1 & \text{if the reduction is non-split multiplicative;} \\ (-1)^{g\frac{q_K-1}{2}} & \text{if the reduction is additive.} \end{cases}$$

In addition, the three possibilities in the above formula are the only ones.

THEOREM 0.4 (Prop. 3.12, Cor. 5.4). *If A/K is an abelian variety of even dimension with real multiplication , then $w(A/K) = 1$.*

COROLLARY 0.5. *Let $\mathcal{K}$ be a number field. If $A/\mathcal{K}$ is an abelian variety with real multiplication and $\dim A$ is even, then $w(A/\mathcal{K}) = 1$.*

PROOF. The local root number at each finite place of $\mathcal{K}$ is 1 by Thm 0.4. At infinite places they are also 1 by [Sab07, Lemma 2.1]. □

0.6. The structure of the chapter. In Section 1 we recall the general theory of local Weil–Deligne representations and root numbers associated to abelian varieties. In Section 2 we present some properties of $\rho_\ell(A/K)$ implied by the structure of $\mathrm{End}_K(A/K)$ for a general field K; we prove some geometric restrictions in the RM case over a p-adic field. These results are probably known to specialists but are somewhat difficult to find in the existing literature, so we include the details for the sake of completeness. In Section 3 we continue the study by assuming potentially good reduction. The results of Sections 2 and 3 are then used in Section 4 to prove Thm. 0.2 and in Section 5 to prove Thm. 0.3.

0.7. Notation and conventions. Given a field K, we fix a separable closure $\overline{K}$ and denote the absolute Galois group by $\Gamma_K := \mathrm{Gal}(\overline{K}/K)$, equipped with the Krull topology. We will suppose implicitly that every separable extension of K mentioned in the text lies inside $\overline{K}$. Note that if K is perfect, then $\overline{K}$ is an algebraic closure of K. For a topological ring R, we denote by $\mathrm{Rep}_R(\Gamma_K)$ the category of continuous R-linear finite-rank representations of Γ_K.

Let K be a field equipped with a valuation v_K. We write $\mathcal{O}_K$, $\mathfrak{m}_K$, and k_K for, respectively, the ring of integers associated to v_K, the maximal ideal of $\mathcal{O}_K$, and the residue field $\mathcal{O}_K/\mathfrak{m}_K$. Whenever v_K is discrete, we suppose that v_K is normalized, i.e., that $v_K(K^\times) = \mathbb{Z}$. An element ϖ_K of valuation one is called a uniformizer of K.

If K is a local field, then, in particular, k_K is a finite field of some order q_K. In this case we have a canonical topological generator $\mathrm{Frob}_{k_K} : x \mapsto x^{q_K}$ of Γ_{k_K}, called the arithmetic Frobenius element. Let $\pi\colon \Gamma_K \twoheadrightarrow \Gamma_{k_K}$ be the surjection induced by an isomorphism $\mathcal{O}_{\overline{K}}/\mathfrak{m}_{\overline{K}} \simeq \overline{k}_K$, and denote by φ_K a geometric Frobenius lift, i.e., an element in Γ_K which is sent to $\mathrm{Frob}_{k_K}^{-1}$ via π.

For an abelian variety A/K defined over a field K, let $A^\vee/K$ be its dual variety, and let $\mathrm{End}_K^0(A) := \mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}$. When K is the fraction field of a Dedekind domain $\mathcal{D}$, we denote by $\mathcal{A}$ the corresponding Néron model over $\mathcal{D}$, by $\mathcal{A}_k$ the special fiber over a residue field k, and by $\mathcal{A}_k^0$ the identity component of that special fiber.

1. From Galois representations to root numbers

Let p be any prime number and let $K/\mathbb{Q}_p$ be a finite extension. We give a brief summary of the general theory of local root numbers, which we will define via Weil–Deligne representations.

1.1. Structure of the absolute Galois group. The elements of Γ_K that induce the trivial automorphism of $k_{\overline{K}}$ define a normal closed subgroup I_K, the inertia subgroup of Γ_K, which cuts out the maximal unramified extension $K^{\mathrm{ur}} := \overline{K}^{I_K}$ of K. The quotient $\Gamma_K/I_K \cong \Gamma_{k_K}$ is the profinite completion $\widehat{\langle \mathrm{Frob}_{k_K} \rangle}$ of the infinite cyclic group generated by the Frobenius element. Let $\varphi_K \in \Gamma_K$ be a lift of the geometric Frobenius. The closure of the subgroup generated by φ_K is the subgroup $\widehat{\langle \varphi_K \rangle} \subset \Gamma_K$ isomorphic to Γ_{k_K}. Thus, we have a splitting $\Gamma_K = I_K \rtimes \widehat{\langle \varphi_K \rangle}$.

On the other hand, the elements acting trivially on $\overline{K}^\times/(1+\mathfrak{m}_{\overline{K}})$ define a normal pro-p subgroup I_K^{w} of Γ_K, called the wild inertia subgroup, which cuts out the maximal tamely ramified extension K^{t}/K. The tame inertia group is the quotient $I_K^{\mathrm{t}} := I_K/I_K^{\mathrm{w}}$, which is isomorphic to the pro-p-complementary completion $\prod_{p' \neq p} \mathbb{Z}_{p'}$ of $\mathbb{Z}$. For every $j \in I_K$ we have $\varphi_K^{-1} j \varphi_K \equiv j^{q_K} \bmod I_K^{\mathrm{w}}$. An application of the profinite version of the Schur–Zassenhaus theorem (see, e.g., [RZ10, Thm. 2.3.15]) shows that I_K^{t} lifts to a profinite subgroup of I_K, thus giving a semidirect product structure on I_K. Each lift of the tame inertia is determined by a choice of a topological generator $\tau_K \in I_K$. As a consequence of the above discussion, we have

$$\Gamma_K = \left(I_K^{\mathrm{w}} \rtimes \widehat{\langle \tau_K \rangle}' \right) \rtimes \widehat{\langle \varphi_K \rangle}, \tag{1.1.1}$$

where $\widehat{\cdot}'$ denotes the pro-p-complementary completion. We will need the following more refined result.

Theorem 1.2 (Iwasawa). *For every lift $\tau_K \in I_K$ of a topological generator of I_K^{t} we can choose φ_K so that we have*

$$\Gamma_K = I_K^{\mathrm{w}} \rtimes \left(\widehat{\langle \tau_K \rangle}' \rtimes \widehat{\langle \varphi_K \rangle} \right),$$

and $\varphi_K^{-1}\tau_K\varphi_K = \tau_K^{q_K}$.

PROOF. This is essentially [Iwa55, Thm. 2]. We first choose any lifts $\varphi_K \in \Gamma_K$ and $\tau_K \in I_K$, for which (1.1.1) holds. Following [Iwa55, Lemma 4], we can modify φ_K so that $\varphi_K^{-1} \cdot \widehat{\langle\tau_K\rangle}' \cdot \varphi_K = \widehat{\langle\tau_K\rangle}'$. Then, $\varphi_K^{-1}\tau_K\varphi_K$ is in $(\tau_K^{q_K} I_K^{\mathrm{w}}) \cap \widehat{\langle\tau_K\rangle}' = \{\tau_K^{q_K}\}$. The closed subgroup $H := \widehat{\langle\tau_K\rangle}' \cdot \widehat{\langle\varphi_K\rangle} \subset \Gamma_K$ has the desired semi-direct product structure. Also, we have $I_K^{\mathrm{w}} H = \Gamma_K$, and $H \cap I_K^{\mathrm{w}}$ is trivial, thus proving the theorem. □

1.3. Weil groups and representations. Let K'/K be a Galois extension such that $K^{\mathrm{ur}} \subseteq K'$. We have an isomorphism $k_{K'} \simeq \overline{k}_K$. The arguments used to obtain (1.1.1) apply similarly to show that the exact sequence

$$0 \to I(K'/K) \to \mathrm{Gal}(K'/K) \xrightarrow{\pi} \Gamma_{k_K} \to 0$$

splits, giving a semidirect product structure

$$\mathrm{Gal}(K'/K) = I(K'/K) \rtimes \widehat{\langle\varphi_K\rangle} \tag{1.3.1}$$

where $I(K'/K) := I_K/I_{K'} \subset \mathrm{Gal}(K'/K)$ is the inertia subgroup. The Weil group of K'/K is defined as

$$W(K'/K) := \pi^{-1}(\langle \mathrm{Frob}_{k_K} \rangle).$$

In other words, $W(K'/K)$ consists of the elements of $\mathrm{Gal}(K'/K)$ that π sends to $\mathrm{Frob}_{k_K}^n$ for some $n \in \mathbb{Z}$. We note that

$$W(K'/K) = I(K'/K) \rtimes \langle\varphi_K\rangle. \tag{1.3.2}$$

We equip $W(K'/K)$ with the topology generated by the open subgroups of $I(K'/K)$ and their translates. We denote $W_K := W(\overline{K}/K)$.

Let F be a field of characteristic zero. An F-linear Weil representation is defined as a continuous representation $\rho\colon W_K \to \mathrm{GL}(V)$ where V is a finite-dimensional F-vector space, and $\mathrm{GL}(V)$ is equipped with the discrete topology. Continuity is equivalent to $\rho(I_K)$ being a finite group. Let us note that if $F = \mathbb{C}$, then we get an equivalent definition if we equip $\mathrm{GL}(V)$ with the standard topology (see [Roh94, §2]). The category of F-linear Weil representations over K will be denoted by $\mathrm{Rep}_F(W_K)$. Every $f \in \mathrm{End}(V)$ gives the transpose endomorphism $f^{\mathsf{T}} \in \mathrm{End}(V^*)$ on the dual vector space. The dual representation of $\rho \in \mathrm{Rep}_F(W_K)$ is given by $\rho^*(g) := \rho(g^{-1})^{\mathsf{T}}$ for every $g \in W_K$.

1.4. Unramified Weil characters. Let R be a ring in which p is invertible. We define the cyclotomic character $\omega_K\colon W_K \to R^\times$ to be the unramified character such that $\omega_K(\varphi_K) = q_K^{-1}$. When $R = \mathbb{C}$, for any $z \in \mathbb{C}$, we define the unramified complex Weil character ω_K^z by taking $b = -\ln(q_K)$ and then setting $\omega_K^z(\varphi_K) = \exp(zb)$. We note that any unramified complex Weil character is of the form ω_K^z for some $z \in \mathbb{C}$. For a complex Weil representation ρ

on V, we define the Tate twist $\rho(z) := \rho \otimes \omega_K^z$ for any $z \in \mathbb{C}$ and denote the underlying vector space by $V(z)$.

1.5. Weil–Deligne representations. Let F be a field of characteristic zero. An F-linear Weil–Deligne (WD for short) representation is a pair (ρ, N) where ρ is an F-linear Weil representation on V and N is a nilpotent F-endomorphism of V, called the monodromy operator, satisfying $\rho N \rho^{-1} = \omega_K N$. The F-linear WD-representations form a category $\mathrm{Rep}_F(W'_K)$ where the morphisms between two WD-representations are the morphisms between their respective Weil representations that commute with the monodromy operators. Trivially, there is an equivalence between the category $\mathrm{Rep}_F(W_K)$ and the full subcategory of F-linear WD-representations with trivial monodromy. If $\rho' = (\rho, N)$ and $\sigma' = (\sigma, P)$ are two WD-representations, then we define their direct sum as $\rho' \oplus \sigma' = (\rho \oplus \sigma, N \oplus P)$, their tensor product as $\rho' \otimes \sigma' = (\rho \otimes \sigma, N \otimes \mathrm{id} + \mathrm{id} \otimes P)$, and the dual representation of ρ' as $(\rho')^* = (\rho^*, -N^{\mathsf{T}})$.

Remark 1.6. As in [Del73, 8.3.6], one may define the Weil–Deligne group W'_K as a group scheme over $\mathbb{Q}$ that is the semidirect product of W_K by $\mathbb{G}_a$ where for every $\mathbb{Q}$-algebra R, every $x \in \mathbb{G}_a(R)$, and every $\sigma \in W_K$ we have $\sigma x \sigma^{-1} = \omega_K(\sigma)x$. A representation of the group scheme W'_K over a field of characteristic 0 may be shown to correspond to a pair (ρ, N) as above.

1.7. ℓ-adic monodromy. Let $\ell \neq p$ be a prime number, φ_K a geometric Frobenius lift, and $t_\ell \colon I_K \to \mathbb{Q}_\ell$ a nontrivial continuous homomorphism. Grothendieck's ℓ-adic monodromy theorem (see [Del73, 8.4.2]) provides a fully faithful functor

$$\begin{aligned} \mathrm{WD} \colon \mathrm{Rep}_{\mathbb{Q}_\ell}(\Gamma_K) &\to \mathrm{Rep}_{\mathbb{Q}_\ell}(W'_K) \\ \rho_\ell &\mapsto (\mathrm{W}(\rho_\ell), N_{\rho_\ell}). \end{aligned}$$

The construction of $\mathrm{W}(\rho_\ell)$ depends on the choice of φ_K, and N_{ρ_ℓ} is the unique nilpotent endomorphism such that $\rho_\ell(j) = \exp(t_\ell(j) N_{\rho_\ell})$ for every j in a sufficiently small open subgroup of I_K. In particular, if $\rho_\ell(I_K)$ is finite, then $N_{\rho_\ell} = 0$. By [Del73, 8.4.3], the isomorphism class of $\mathrm{WD}(\rho_\ell)$ is independent of the choices of t_ℓ and φ_K.

1.8. Complex WD-representations. Let $\rho_\ell \in \mathrm{Rep}_{\mathbb{Q}_\ell}(\Gamma_K)$. We fix an embedding $i \colon \mathbb{Q}_\ell \to \mathbb{C}$ for the rest of the text. By extending the scalars of $\mathrm{WD}(\rho_\ell)$ to $\mathbb{C}$ via i we obtain a complex WD-representation $\mathrm{WD}_i(\rho_\ell) = (\mathrm{W}_i(\rho_\ell), N_{i,\rho_\ell})$. As the notation indicates, the isomorphism class of $\mathrm{WD}_i(\rho_\ell)$ generally depends on i.

1.9. Geometric ℓ-adic representations. Let K be any field with a separable closure $\overline{K}$, and let $\ell \neq \mathrm{char}(K)$ be a prime. If X/K is a smooth and proper variety, then we have a natural ℓ-adic Galois representation on the (m-th) ℓ-adic

cohomology group $H^m_{\text{ét}}(X_{\overline{K}}, \mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ for each $m \geqslant 0$. For a commutative algebraic group G over K, one defines its ℓ-adic Tate module as the projective limit of $\overline{K}$-valued ℓ^n-torsion points

$$T_\ell G = \varprojlim_n G(\overline{K})[\ell^n]$$

equipped with the ℓ-adic topology. The natural Γ_K-action on $T_\ell G$ is continuous and defines a $\mathbb{Q}_\ell$-linear representation on $V_\ell G := T_\ell G \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. For an abelian variety A/K of dimension g, the $\mathbb{Z}_\ell$-module $T_\ell A$ is free of rank $2g$, and its dual $(T_\ell A)^*$ is canonically isomorphic to $H^1_{\text{ét}}(A_{\overline{K}}, \mathbb{Z}_\ell)$ in $\mathrm{Rep}_{\mathbb{Z}_\ell}(\Gamma_K)$. We will denote the corresponding ℓ-adic Galois representation on $(V_\ell A)^*$ by $\rho_\ell(A/K)$ or simply by ρ_ℓ when the context is clear.

The multiplicative group $\mathbb{G}_m/K$ induces a $\mathbb{Z}_\ell$-linear Galois representation on $T_\ell \mathbb{G}_m$ of dimension one, which corresponds to a character $\omega_K \colon \Gamma_K \to \mathbb{Z}_\ell^\times$. For every $n \in \mathbb{Z}$ and every ℓ-adic representation ρ on V, we define the Tate twist by $\rho(n) := \rho \otimes \omega_K^n$ and denote its underlying space by $V(n)$.

For the rest of Section 1 we return to the case where K is a finite extension of $\mathbb{Q}_p$ and $\ell \neq p$. Restricting the Γ_K-action on $T_\ell \mathbb{G}_m$ to W_K we obtain exactly the unramified character $\omega_K \colon W_K \to \mathbb{Z}_\ell^\times$ of 1.4.

1.10. Reduction of abelian varieties. Let $K/\mathbb{Q}_p$ be a finite extension. An abelian variety A/K is said to have good (resp. semistable, synonymous with semi-abelian) reduction if the identity component $\mathcal{A}^0_{k_K}$ of the special fiber of the Néron model is an abelian variety (resp. a semi-abelian variety). More generally, the reduction is potentially good (resp. potentially semistable) if there exists a finite extension L/K such that A/L has good (resp. semistable) reduction. We will say that A/K has bad reduction if it does not have good reduction. Recall the following well-known results.

THEOREM 1.11. *An abelian variety A/K:*

(1) *has good reduction if and only if ρ_ℓ is unramified, i.e., if and only if I_K acts trivially on $V_\ell A$ (Néron–Ogg–Shafarevich criterion);*
(2) *has semistable reduction if and only if $\rho_\ell|_{I_K}$ is unipotent (Grothendieck's inertial criterion);*
(3) *always has potentially semistable reduction (Grothendieck's semistable reduction theorem).*

PROOF. For (1) see [ST68, Thm. 1]; for (2) see [SGA 7.I, p. 350, Prop. 3.5]; for (3) see [SGA 7.I, p. 21, Thm. 6.1]. □

DEFINITION 1.12. Given an abelian variety A/K with potentially good reduction, an extension L'/K will be called *inertially minimal (IM) for A/K* if $L'K^{\mathrm{ur}} = M$ where M/K^{ur} is the extension cut out by $\ker \rho_\ell|_{I_K}$.

LEMMA 1.13. *Let A/K be an abelian variety with potentially good reduction. Let M/K be as in Def. 1.12. Then*

(1) *An extension L'/K is IM for A/K if and only if $I_{L'} = \ker \rho_\ell|_{I_K} = I_M$. This is also equivalent to the condition that A has good reduction over L' and has bad reduction over any smaller extension L''/K such that L'/L'' is ramified.*
(2) *The extension M/K is Galois;*
(3) *For any choice of a Frobenius lift φ_K, there exists a finite totally ramified extension L'/K which is fixed by φ_K and is IM for A/K;*
(4) *Let L'/K be an IM-extension for A/K and let L/K be its Galois closure in $\overline{K}$. Then L/K is also IM for A/K. In particular, L/L' is unramified.*

Proof. The first equivalence of (1) follows from Galois theory, and the second is a reformulation of the Néron–Ogg–Shafarevich criterion. For (2) we observe that $\ker \rho_\ell|_{I_K} = I_K \cap \ker \rho_\ell$, which is normal in Γ_K. For any φ_K, the subgroup $I_M \cdot \widehat{\langle \varphi_K \rangle} \subseteq \Gamma_K$ (cf. (1.1.1)) is closed (as a product of two compact subgroups) and has finite index, thus is open. It cuts out a finite totally ramified extension L'/K with $I_{L'} = I_M$, so (3) follows. The part (4) follows from the observation that $L \subset M$ (since M/K is Galois), which implies that $I_{L'} = I_M \subseteq I_L \subseteq I_{L'}$. □

1.14. p-adic uniformization. Let A/K be an abelian variety of dimension g. As stated in [Cha00, Prop. 3.1], there exists a semi-abelian variety E/K of dimension g, defined by a Raynaud extension $0 \to T \to E \to B \to 0$ where

(i) T is a torus over K,
(ii) B is an abelian variety over K with potentially good reduction,
(iii) the rigid analytification of A/K is the rigid analytic quotient of the analytification of E/K by a free Galois sub-$\mathbb{Z}$-module $M \subset E(\overline{K})$ of rank $r = \dim T$.

We denote $(\kappa, 0) = \mathrm{WD}_i(\rho_\ell(B/K))$, note that the monodromy is trivial by Thm. 1.11.(1) and 1.7. Let $X(T) := \mathrm{Hom}_{\overline{K}}(T, \mathbb{G}_m)$, and let $\eta\colon W_K \to \mathrm{GL}(X(T)_{\mathbb{Q}})$ be the representation given by the Galois action on $X(T)_{\mathbb{Q}} := X(T) \otimes_{\mathbb{Z}} \mathbb{Q}$, which has finite image.

Proposition 1.15 ([Sab07, Prop. 1.10]). *There is an isomorphism of WD-representations*

$$\mathrm{WD}_i(\rho_\ell(A/K)) \cong (\kappa, 0) \oplus (\eta(-1) \otimes \mathrm{sp}(2)),$$

where $\mathrm{sp}(2) = (\mathbb{1} \oplus \omega_K, \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right))$ *is the so-called special WD-representation. The representations* $\mathrm{W}_i(\rho_\ell(B/K))$ *and* $\mathrm{W}_i(\rho_\ell(A/K))$ *are semisimple, and the isomorphism classes of* $\mathrm{WD}_i(\rho_\ell(B/K))$ *and* $\mathrm{WD}_i(\rho_\ell(A/K))$ *are independent of ℓ and i.*

Remark 1.16.
(1) The Galois modules $X(T)_{\mathbb{Q}}$ and $M \otimes \mathbb{Q}$ are isomorphic, see [Sab07, Lemma 1.11].

(2) Let us recall a few ideas behind the construction of T in order to give a direct description of η. By Thm. 1.11.(3), there exists a finite Galois extension L/K such that the identity component $\mathscr{A}^{\circ}_{k_L}$ of the special fiber of the Néron model of A/L is a semi-abelian variety. By replacing L with a larger extension, we may suppose that the maximal subtorus $\widetilde{T}$ of $\mathscr{A}^{0}_{k_L}$ is split. By the universal property of the Néron model, the k_L-scheme $\widetilde{T}$ is equipped with a k_L-semilinear $\mathrm{Gal}(L/K)$-action. The resulting Γ_K-representation on $X(\widetilde{T})_{\mathbb{Q}} = \mathrm{Hom}_{k_L}(\widetilde{T}, \mathbb{G}_m) \otimes_{\mathbb{Z}} \mathbb{Q}$ is isomorphic to η.

1.17. Local reciprocity. Local class field theory provides a reciprocity isomorphism for any finite Galois extension L/K of local fields:

$$\theta_{L/K} : K^{\times}\Big/\mathcal{N}_{L/K}(L^{\times}) \xrightarrow{\sim} \mathrm{Gal}(L/K)^{\mathrm{ab}}.$$

There exist exactly two canonical choices for $\theta_{L/K}$, and they are inverses of each other. Following Deligne, we normalise $\theta_{L/K}$ by supposing that it sends the class of a uniformizer of K to the class of a geometric Frobenius lift. Using the projective limit of these reciprocity maps as well as the Existence Theorem we obtain (see, e.g., [Kna97, Cor. 2.5]) an isomorphism

$$\theta_K : K^{\times} \xrightarrow{\sim} W_K^{\mathrm{ab}}.$$

1.18. The epsilon factor. We fix a nontrivial locally constant additive character $\psi_K\colon K \to \mathbb{C}^{\times}$ and a Haar measure $\mathrm{d}x_K$ on K. We let $n(\psi_K) := \max\{n \in \mathbb{Z} \,|\, \psi_K(\mathfrak{m}_K^{-n}) = 1\}$. For a complex WD-representation $\rho' = (\rho, N)$ with underlying vector space V, we define the ϵ-factor of ρ' as the product

$$\epsilon(\rho', \psi_K, \mathrm{d}x_K) := \epsilon(\rho, \psi_K, \mathrm{d}x_K)\delta(\rho'),$$

where

$$\delta(\rho') := \det\left(-\rho(\varphi_K)\Big| V^{I_K}\Big/(\ker N)^{I_K}\right)$$

and $\epsilon(\cdot, \psi_K, \mathrm{d}x_K)$ is the unique function satisfying the following axioms (see [Del73, Théorème 4.1]):

(i) The map $\epsilon(\cdot, \psi_K, \mathrm{d}x_K)\colon \mathrm{Rep}_{\mathbb{C}}(W_K) \to \mathbb{C}^{\times}$ is multiplicative in short exact sequences of Weil representations, i.e., it induces a group homomorphism from the Grothendieck group of virtual complex Weil representations to $\mathbb{C}^{\times}$.

(ii) For any finite extension L/K, any $\mathrm{d}x_L$, and any $\rho \in \mathrm{Rep}_{\mathbb{C}}(W_L)$ we have

$$\epsilon(\mathrm{Ind}_{W_L}^{W_K}\rho, \psi_K, \mathrm{d}x_K) = \epsilon(\rho, \psi_K \circ \mathrm{Tr}_{L/K}, \mathrm{d}x_L)\left(\frac{\epsilon(\mathrm{Ind}_{W_L}^{W_K}\mathbb{1}_{W_L}, \psi_K, \mathrm{d}x_K)}{\epsilon(\mathbb{1}_{W_L}, \psi_K \circ \mathrm{Tr}_{L/K}, \mathrm{d}x_L)}\right)^{\dim\rho}.$$

(iii) For any finite extension L/K, any ψ_L, any $\mathrm{d}x_L$, and any one-dimensional $\xi \in \mathrm{Rep}_{\mathbb{C}}(W_L)$ with Artin conductor $a(\xi)$ we have

$$\epsilon(\xi, \psi_L, \mathrm{d}x_L) = \begin{cases} \int_{c^{-1}\mathfrak{O}_L^\times} \xi^{-1}(\theta_L(x))\psi_L(x)\,\mathrm{d}x_L & \text{if } \xi \text{ is ramified,} \\ (\xi\omega_L^{-1})(\theta_L(c)) \int_{\mathfrak{O}_L} \mathrm{d}x_L & \text{if } \xi \text{ is unramified,} \end{cases}$$

where $c \in L$ is any element of valuation $n(\psi_L) + a(\xi)$.

The condition (iii) expresses the fact that the ϵ-factor is the coefficient in Tate's local functional equation of the L-function of ξ, as described in [Tat79, §3].

1.19. The root number. Given a $\rho' = (\rho, N) \in \mathrm{Rep}_{\mathbb{C}}(W'_K)$, we define its root number as

$$w(\rho', \psi_K) := \frac{\epsilon(\rho', \psi_K, \mathrm{d}x_K)}{|\epsilon(\rho', \psi_K, \mathrm{d}x_K)|}.$$

It follows from basic properties of ϵ-factors (see [Roh94, §11, Prop.]) that the root number $w(\rho', \psi_K)$ is independent of the choice of $\mathrm{d}x_K$, and that it is also independent of ψ_K if $\det \rho$ is real positive, which is always the case for a WD-representation obtained from an abelian variety.

1.20. Some custom conventions. The dependence of ϵ-factors on ψ_K and $\mathrm{d}x_K$ will not be important in what follows, so we make some particular choices for the rest of the chapter. We denote by μ_{p^∞} the group of all complex roots of unity of orders that are powers of p, and we fix an isomorphism $\mathbb{Q}_p/\mathbb{Z}_p \simeq \mu_{p^\infty}$. For a finite extension $K/\mathbb{Q}_p$ we define ψ_K as the composition

$$\psi_K \colon K \xrightarrow{\mathrm{Tr}} \mathbb{Q}_p \to \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{\sim} \mu_{p^\infty} \subseteq \mathbb{C}^\times.$$

We note that $n(\psi_K)$ is the valuation of any generator of the different ideal $\mathfrak{D}_{K/\mathbb{Q}_p} \subseteq \mathfrak{O}_K$. We normalize $\mathrm{d}x_K$ by demanding that $\mathrm{d}x(\mathfrak{O}_K) = 1$.

Proposition 1.21. *Let $\rho' = (\rho, N) \in \mathrm{Rep}_{\mathbb{C}}(W'_K)$, then*

(1) *For any unramified character χ, we have*

$$\epsilon(\rho' \otimes \chi, \psi_K, \mathrm{d}x_K) = \epsilon(\rho', \psi_K, \mathrm{d}x_K) \cdot \chi(\varphi_K)^{n(\psi_K)\cdot \dim \rho' + a(\rho')};$$

In particular, for any $s \in \mathbb{R}$, we have $w(\rho'(s), \psi_K) = w(\rho', \psi_K)$;

(2) *We have $w(\rho', \psi_K)w((\rho')^*, \psi_K) = \det(\rho(\theta_K(-1)))$;*

(3) *If ρ has a finite image and is self-dual, then*

$$w(\rho \otimes \mathrm{sp}(2), \psi_K) = \det(\rho(\theta_K(-1))) \cdot (-1)^{\langle \rho | \mathbb{1} \rangle},$$

where $\langle \cdot | \cdot \rangle$ denotes the usual inner product on characters of finite groups.

Proof. These properties can be deduced from [Roh94, §11, Prop.(iii)], [Roh94, §12, Lemma.(iii)], and [Roh96, p. 327, Prop. 6], respectively. □

2. Abelian varieties with an action by a number field

Let A/K be an abelian variety of dimension g over some field K. We suppose that there exists an inclusion of unitary rings $F \hookrightarrow \mathrm{End}_K^0(A)$ where F is a number field of some degree n. We fix a prime number $\ell \neq \mathrm{char}(K)$. Let us recall that ρ_ℓ is the $\mathbb{Q}_\ell$-linear representation of Γ_K given by the Galois action on $(V_\ell A)^*$.

2.1. The F-action on $(V_\ell A)^*$. Since the $\mathbb{Q}_\ell$-linear Galois representation ρ_ℓ commutes with the action of the semisimple $\mathbb{Q}_\ell$-algebra $F_\ell := F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ on $(V_\ell A)^*$, we may interpret ρ_ℓ as an F_ℓ-linear representation. It is well known (see [ST61, p. 39, Prop. 2]) that $n|2g$, and we denote $h := 2g/n$. We have a decomposition

$$F_\ell = \prod_\lambda F_\lambda \tag{2.1.1}$$

where λ runs through all finite places of F above ℓ, and where F_λ is the corresponding completion of F. Consequently, we may decompose

$$(V_\ell A)^* = \prod_\lambda V_\lambda \tag{2.1.2}$$

where $V_\lambda = (V_\ell A)^* \otimes_{F_\ell} F_\lambda$ is an F_λ-vector space of some dimension h_λ. By F_ℓ-linearity of ρ_ℓ, the decomposition (2.1.2) is Γ_K-equivariant, so we obtain a family of Galois representations $\rho_\lambda \colon \Gamma_K \to \mathrm{Aut}_{F_\lambda}(V_\lambda)$.

Theorem 2.2 ([Rib76, Thm. 2.1.1]). *In the notation above, $h_\lambda = h$ for all λ, so $V_\ell(A)^*$ is a free F_ℓ-module of rank h.*

2.3. The F_ℓ-bilinear Weil pairing. Let $P_{\mathbb{Q}_\ell} \colon V_\ell A \times V_\ell(A^\vee) \to \mathbb{Q}_\ell(1)$ be the Γ_K-equivariant perfect $\mathbb{Q}_\ell$-bilinear Weil pairing. Each $f \in \mathrm{End}_K^0(A)$ acts on $V_\ell(A^\vee)$ via its dual $f^\vee \in \mathrm{End}_K^0(A^\vee)$ and satisfies $P_{\mathbb{Q}_\ell}(f(x), y) = P_{\mathbb{Q}_\ell}(x, f^\vee(y))$ for all $(x, y) \in V_\ell A \times V_\ell(A^\vee)$. Then, the pairing induces an isomorphism

$$P'_{\mathbb{Q}_\ell} \colon \mathrm{Hom}_{\mathbb{Q}_\ell}(V_\ell A, \mathbb{Q}_\ell) \cong V_\ell(A^\vee)(-1)$$

in $\mathrm{Rep}_{\mathbb{Q}_\ell}(\Gamma_K)$, which is $\mathrm{End}_K^0(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$-linear and, in particular, F_ℓ-linear.

We claim that the map

$$t \colon \mathrm{Hom}_{F_\ell}(V_\ell A, F_\ell) \to \mathrm{Hom}_{\mathbb{Q}_\ell}(V_\ell A, \mathbb{Q}_\ell)$$

given by $f \mapsto \mathrm{Tr}_{F_\ell/\mathbb{Q}_\ell} \circ f$ is an isomorphism in $\mathrm{Rep}_{F_\ell}(\Gamma_K)$. Indeed, it is straightforward to verify that t defines a morphism in $\mathrm{Rep}_{F_\ell}(\Gamma_K)$ and that the $\mathbb{Q}_\ell$-dimensions of the source and the target agree. We are left to verify the injectivity. Let $f \in \mathrm{Hom}_{F_\ell}(V_\ell A, F_\ell)$ be non-zero, and let $x \in \mathrm{Im}(f) \setminus \{0\}$. By F_ℓ-linearity, we may suppose that x is the image of $1 \in F_\lambda$ via $F_\lambda \hookrightarrow F_\ell$ for some λ. Then $\mathrm{Tr}_{F_\ell/\mathbb{Q}_\ell}(x) = [F_\lambda : \mathbb{Q}_\ell] \neq 0$, so $\mathrm{Tr}_{F_\ell/\mathbb{Q}_\ell} \circ f \neq 0$.

Composing $P'_{\mathbb{Q}_\ell}$ with t gives an isomorphism $P'_{F_\ell}\colon \mathrm{Hom}_{F_\ell}(V_\ell A, F_\ell) \to V_\ell(A^\vee)(-1)$ in $\mathrm{Rep}_{F_\ell}(\Gamma_K)$, which translates back to a Γ_K-equivariant perfect F_ℓ-bilinear pairing

$$P_{F_\ell}\colon V_\ell A \times V_\ell(A^\vee) \to F_\ell(1).$$

Given a polarization $\lambda\colon A \to A^\vee$ defined over K, let $\cdot^\dagger\colon \mathrm{End}^0_K(A) \to \mathrm{End}^0_K(A)$ be the corresponding Rosati involution. By composing the second argument of P_{F_ℓ} with λ, we obtain a map

$$P^\lambda_{F_\ell}\colon V_\ell A \times V_\ell A \to F_\ell(1).$$

Proposition 2.4. *Let A/K be an abelian variety with a polarization λ such that $\mathrm{End}^0_K(A)$ contains a totally real field F fixed by the Rosati involution $\cdot^\dagger$. The pairing $P^\lambda_{F_\ell}$ is alternating, F_ℓ-bilinear, Γ_K-equivariant, and perfect. Consequently, $h := \frac{2\dim A}{[F:\mathbb{Q}]}$ is an even integer, $\rho_\ell^* \cong \rho_\ell(1)$ in $\mathrm{Rep}_{F_\ell}(\Gamma_K)$, and $\det_{F_\ell}\rho_\ell = \omega_K^{-h/2}$.*

Proof. By construction, the map $P^\lambda_{F_\ell}$ is Γ_K-equivariant, $\mathbb{Q}_\ell$-bilinear, non-degenerate, and F_ℓ-linear in the first variable. As it is standard, for any $f \in \mathrm{End}_K(A)\otimes_{\mathbb{Z}}\mathbb{Q}_\ell$ and $a, b \in V_\ell A$ we have $P_{\mathbb{Q}_\ell}(a, \lambda(a)) = 0$ and $P_{\mathbb{Q}_\ell}(f(a), \lambda(b)) = P_{\mathbb{Q}_\ell}(a, \lambda(f^\dagger(b)))$. Using the isomorphism t we see that the same statements are true when we replace $P_{\mathbb{Q}_\ell}$ by P_{F_ℓ}. Since $\cdot^\dagger$ acts trivially on F_ℓ, the pairing $P^\lambda_{F_\ell}$ is F_ℓ-bilinear and perfect.

From classical bilinear algebra, the existence of an alternating and perfect F_ℓ-bilinear pairing on $V_\ell A$ implies that h is even. The Γ_K-equivariance and non-degeneracy of $P^\lambda_{F_\ell}$ gives $(V_\ell A)^* \cong (V_\ell A)(-1)$ in $\mathrm{Rep}_{F_\ell}(\Gamma_K)$. Taking the dual objects we obtain $\rho_\ell^* \cong \rho_\ell(1)$. It remains to compute the determinant.

For any $n \geqslant 1$, the F_ℓ-module $(\wedge^n(V_\ell A))^*$ of F_ℓ-multilinear alternating n-forms on $V_\ell A$ is free of rank $\binom{h}{n}$. It is equipped with a natural F_ℓ-linear Galois action given by $\sigma P = P \circ \wedge^n \rho_\ell^*(\sigma^{-1})$ for every $P \in (\wedge^n(V_\ell A))^*$ and every $\sigma \in \Gamma_K$ (note that we need to put σ^{-1} in order to have $(\tau\sigma)P = \tau(\sigma P)$). Then, the pairing $P^\lambda_{F_\ell} \in (\wedge^2(V_\ell A))^*$ satisfies $\sigma P^\lambda_{F_\ell} = \omega_K(\sigma^{-1})P^\lambda_{F_\ell}$. Using the notion of alternating product of multilinear forms, see [Bou70, A III.142, Exemple 3)], we consider the $h/2$-fold product $\phi = \left(P^\lambda_{F_\ell}\right)^{\wedge h/2} \in (\wedge^h(V_\ell A))^*$, on which σ acts as multiplication by $\omega_K(\sigma)^{-h/2}$. Since Γ_K acts on the F_ℓ-module $(\wedge^h(V_\ell A))^* = (\det_{F_\ell} V_\ell A)^*$ as $(\det_{F_\ell}\rho_\ell^*)^* \cong \det_{F_\ell}\rho_\ell$, we are left to check that $\phi \neq 0$. There is a suitable F_ℓ-basis $e_1, \ldots, e_h$ of $V_\ell A$ such that the matrix of $P^\lambda_{F_\ell}$ in this basis is diagonal by blocks $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. If we denote by $e'_1, \ldots, e'_h$ the corresponding dual basis of $(V_\ell A)^*$, then $P^\lambda_{F_\ell} = \sum_{i=1}^{h/2} e'_{2i-1} \wedge e'_{2i}$. It is straightforward to verify that $\phi = (h/2)!\, e'_1 \wedge \ldots \wedge e'_h$, and the latter is clearly non-zero. □

2.5. A geometric trichotomy. Let $K/\mathbb{Q}_p$ be a finite extension, $\ell \neq p$ a prime, and A/K an abelian variety. We consider the identity component $\mathscr{A}^0_{k_K}$ of the special fiber of the Néron model of A/K. By Barsotti–Chevalley theorem

(see, e.g., [Mil17, Thm. 8.27 and Prop. 16.15]), there exist a unipotent group U/k_K, a torus T'/k_K, and an abelian variety B'/k_K that fit an exact sequence

$$0 \to T' \times U \to \mathscr{A}^0_{k_K} \to B' \to 0. \tag{2.5.1}$$

The functoriality of the Néron model, along with the well-known facts that $\mathrm{Hom}_{k_K}(T', B') = 0$, $\mathrm{Hom}_{k_K}(T', U) = 0$, and $\mathrm{Hom}_{k_K}(U, B') = 0$, implies that we have a morphism of unitary $\mathbb{Q}$-algebras

$$\mathrm{End}^0_K(A) \to \mathrm{End}^0_{k_K}(T') \times \mathrm{End}^0_{k_K}(B'). \tag{2.5.2}$$

The following proposition is a slightly sharper version of [Rib76, Prop. 3.6.1].

Proposition 2.6. *We suppose that A/K has real multiplication by F. Then, exactly one of the algebraic groups T', U, and B' is nontrivial.*

Proof. Let us suppose that T' is nontrivial. From (2.5.2) we get an inclusion $F \hookrightarrow \mathrm{End}^0_{k_K}(T')$. It follows that $X(T') \otimes_{\mathbb{Z}} \mathbb{Q}$ is a nontrivial F-vector space. Then, $\dim T' \geqslant [F : \mathbb{Q}] = \dim A = \dim \mathscr{A}^0_{k_K}$, so U and B' are trivial.

It remains to prove that if B' is nontrivial, then $\dim B' = \dim A$. We see from (2.5.2) that $\mathrm{End}^0_{k_K}(B')$ contains F as a subfield. Using Poincaré's complete reducibility theorem we may assume that B' is some n-th power of a simple abelian variety S'. Then, using Albert's classification of endomorphism algebras of simple abelian varieties one can show that $[F : \mathbb{Q}] \leqslant n \dim S' = \dim B'$, this is done in [Cha95, Lemma 6]. □

3. Rationality of representations on Tate modules

3.1. The setup. We fix a prime number p, a finite extension $K/\mathbb{Q}_p$, and an abelian variety A/K having potentially good reduction. Let us suppose that A/K has real multiplication (RM), i.e., that the $\mathbb{Q}$-algebra $\mathrm{End}^0_K(A)$ contains a totally real number field F of degree $g = \dim A$ as a subalgebra. We recall the decomposition $F_\ell = F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = \prod_\lambda F_\lambda$. In addition, we have

$$F_{\mathbb{C}} := F \otimes_{\mathbb{Q}} \mathbb{C} = \prod_{\iota\colon F \hookrightarrow \mathbb{C}} \mathbb{C}. \tag{3.1.1}$$

Let ρ_ℓ be the Galois representation as in 1.9 for some $\ell \neq p$. It is also F_ℓ-linear. As in 1.8, let us fix an embedding $i : \mathbb{Q}_\ell \hookrightarrow \mathbb{C}$, then the associated complex Weil–Deligne representation is given by the pair $(W_i(\rho_\ell), 0)$ where $W_i(\rho_\ell)$ denotes the $F_{\mathbb{C}}$-linear Weil representation obtained by restricting $\rho_\ell \otimes_{i,\mathbb{Q}_\ell} \mathbb{C}$ to W_K.

Proposition 3.2. *The representation ρ_ℓ on $(V_\ell A)^*$ is semisimple in* $\mathrm{Rep}_{F_\ell}(W_K)$.

Proof. It suffices to prove semisimplicity of the restriction to a subgroup $W_L \subseteq W_K$ of finite index (after applying the argument of [BH06, §2.7 Lemma]). Therefore, we may suppose that the reduction is already good over K. In this case, the inertia acts trivially and the action of the arithmetic

Frobenius φ_K^{-1} on $V_\ell A \cong V_\ell \mathscr{A}_{k_K}$ is induced by the Frobenius endomorphism ϕ of the reduced abelian variety $\mathscr{A}_{k_K}/k_K$. It is well known that $\mathbb{Q}[\phi]$ is a semisimple $\mathbb{Q}$-subalgebra of $\mathrm{End}^0_{k_K}(\mathscr{A}_{k_K})$. It follows that $F_\ell \otimes_{\mathbb{Q}} \mathbb{Q}[\phi]$ is a semisimple $\mathbb{Q}_\ell$-algebra, and we conclude that ρ_ℓ is semisimple. □

PROPOSITION 3.3. *For any $\sigma \in W_K$, let $P_{\ell,\sigma} \in F_\ell[T]$ be the F_ℓ-characteristic polynomial[1] of $\rho_\ell(\sigma)$. Then, $P_{\ell,\sigma}$ has coefficients in F and each F_λ-characteristic polynomial $P_{\lambda,\sigma}$ of $\rho_\lambda(\sigma)$ is the image of $P_{\ell,\sigma}$ via the inclusion $F[T] \hookrightarrow F_\lambda[T]$.*

PROOF. We will prove that $V_\ell(A)^*$ is an $F_\ell[\sigma]$-module that can be realized over F, i.e., there exists an $F[\sigma]$-module W such that $W \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \simeq V_\ell(A)^*$.

The F_ℓ-linear representation ρ_ℓ induces a morphism of F_ℓ-algebras

$$\nu\colon F_\ell[\sigma] \to \mathrm{End}_{F_\ell}(V_\ell(A)^*).$$

As explained by [ST68, p. 499, Corollary] and its proof, for every $\alpha \in F[\sigma]$ there exists an integer n and finite extension L/K over which A has good reduction and such that the action of $n\alpha$ is induced by an endomorphism of the reduced abelian variety $\mathscr{A}_{k_L}$. Then, by a classical argument due to Weil (see [Mum70, p. 181]), the $\mathbb{Q}_\ell$-characteristic polynomial of $\nu(\alpha)$ has rational coefficients.

The semisimplicity of ρ_ℓ implies that $F[\nu(\sigma)]$ is a semisimple $\mathbb{Q}$-algebra. Since $F[\nu(\sigma)]$ is also commutative and finite over $\mathbb{Q}$, we may write $F[\nu(\sigma)] = \prod_i \mathbb{Q}(\alpha_i)$ as a finite product of number fields and, accordingly, $(V_\ell A)^* = \prod_i V_i$. Each V_i is the underlying space of a semisimple $\mathbb{Q}_\ell$-linear representation $\nu_i\colon \mathbb{Q}(\alpha_i) \to \mathrm{End}_{\mathbb{Q}_\ell}(V_i)$. By the above paragraph, for every $\alpha \in \mathbb{Q}(\alpha_i)$, the $\mathbb{Q}_\ell$-characteristic polynomial of $\nu_i(\alpha)$ has rational coefficients. Therefore, [ST61, p. 38, Lemma 1] applies and gives an isomorphism $V_i \simeq \mathbb{Q}(\alpha_i)^{d_i} \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ of semisimple $\mathbb{Q}_\ell(\alpha_i)$-modules for some positive integer d_i.

Let us define the $F[\sigma]$-module $W := \prod_i \mathbb{Q}(\alpha_i)^{d_i}$, so that, by construction, $W \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \simeq V_\ell(A)^*$ as semisimple $F_\ell[\sigma]$-modules. Let $Q \in F[T]$ be the F-characteristic polynomial of σ acting on W. Then, $P_{\ell,\sigma} = Q$. On the other hand, $P_{\ell,\sigma}$ can be calculated locally at each λ and can be seen as a family of polynomials $(P_{\lambda,\sigma})_\lambda$ in $\prod_\lambda F_\lambda[T]$. Since $P_{\ell,\sigma}$ has coefficients in F, the family is constant. □

PROPOSITION 3.4. *Let A/K be an abelian variety with RM by F and with potentially good reduction. Then we have the following decomposition of the complex Weil representation:*

$$\mathrm{W}_i(\rho_\ell) = \prod_{\iota\colon F \hookrightarrow \mathbb{C}} \rho_\iota, \tag{3.4.1}$$

where each ρ_ι is a semisimple Weil representation on a complex 2-dimensional vector space V_ι. Furthermore:

[1] It is well-defined because of Thm. 2.2.

(1) *The representations ρ_ι are $\mathrm{Aut}(\mathbb{C})$-conjugate; i.e., for every pair of embeddings $\iota, \iota' \colon F \hookrightarrow \mathbb{C}$ there exists an automorphism $u \in \mathrm{Aut}(\mathbb{C})$ such that $\rho_{\iota'} \cong \rho_\iota \otimes_u \mathbb{C}$.*
(2) *Let M/K be as in Def. 1.12. The restrictions $\rho_\iota|_{I_K}$ have a common kernel I_M. Each ρ_ι thus induces a faithful 2-dimensional representation of the finite group $I(M/K)$.*
(3) *Each representation ρ_ι is essentially symplectic of weight 1, i.e., $\rho_\iota(\frac{1}{2})$ is symplectic. In particular, $\rho_\iota^* \cong \rho_\iota(1)$ and $\det \rho_\iota = \omega_K^{-1}$.*
(4) *The root number $w(\rho_\iota, \psi_K)$ is 1 or -1.*

Proof. By $F_{\mathbb{C}}$-linearity, the decomposition (3.1.1) implies (3.4.1), and we have $V_\iota \cong V_\ell(A)^* \otimes_{F_{\ell,\iota}} \mathbb{C}$ where the tensor product is taken over the unique extension $F_\ell \to \mathbb{C}$ of ι (having fixed $i \colon \mathbb{Q}_\ell \hookrightarrow \mathbb{C}$, see 1.8). Recall that $V_\ell(A)^*$ is a free F_ℓ-module of dimension 2 (Thm. 2.2), so V_ι is a complex Weil representation of dimension 2.

(1) From Prop. 3.3 we conclude that the $\mathbb{C}$-characteristic polynomial of $\sigma \in W_K$ acting on V_ι is the image via ι of a polynomial $P_\sigma \in F[T]$ that is independent of ι. We recall that for any two embeddings $\iota, \iota' \colon F \hookrightarrow \mathbb{C}$, there exists a $u \in \mathrm{Aut}(\mathbb{C})$ such that $\iota' = u \circ \iota$. The characteristic polynomials of $\rho_\iota(\sigma) \otimes_u \mathbb{C}$ and $\rho_{\iota'}(\sigma)$ are equal, so, by semisimplicity, $\rho_\iota \otimes_u \mathbb{C} \simeq \rho_{\iota'}$.
(2) Part (1) shows that all the ρ_ι have the same kernel, which must be the kernel of ρ_ℓ. In particular, $\ker \rho_\iota|_{I_K} = \ker \rho_\ell \cap I_K = I_M$.
(3) Applying the functor $- \otimes_{F_{\ell,\iota}} \mathbb{C}$ to the objects of Prop. 2.4 gives the result.
(4) We use (3) together with Prop. 1.21.(1),(2) to get

$$\begin{aligned} w(\rho_\iota, \psi_K)^2 &= w(\rho_\iota, \psi_K) w(\rho_\iota(1), \psi_K) \\ &= w(\rho_\iota, \psi_K) w(\rho_\iota^*, \psi_K) \\ &= \det(\rho_\iota(\theta_K(-1))). \end{aligned}$$

We know that $\det \rho_\iota = \omega_K^{-1}$ is unramified, so $w(\rho_\iota, \psi_K)^2 = 1$. □

Remark 3.5. Prop. 3.4 shows that $(\rho_\iota)_\iota$ is a family of $\mathrm{Aut}(\mathbb{C})$-conjugate representations of even dimensions that are essentially symplectic of odd weight. Then, [Roh11, Thm. 1] shows that $w(\rho_\iota, \psi_K)$ is independent of ι. Let us fix some ι. It follows from (3.4.1) and multiplicativity of root numbers that

$$w(A/K) = w(W_i(\rho_\ell), \psi_K) = w(\rho_\iota, \psi_K)^g. \tag{3.5.1}$$

Proposition 3.6. *We keep the hypotheses and notation of Prop. 3.4. Let us fix an embedding $\iota \colon F \hookrightarrow \mathbb{C}$ and regard ρ_ι as a representation of the group $G := W(M/K) = I(M/K) \cdot \langle \varphi_K \rangle$. Exactly one of the following is true:*

(a) *M/K is abelian. In this case $\rho_\iota = \chi_\iota \oplus \chi_\iota^{-1}\omega_K^{-1}$ for a character $\chi_\iota\colon G \to \mathbb{C}^\times$, which is faithful on $I(M/K)$, and there exists a finite totally ramified cyclic extension L/K which is IM (see Def. 1.12) for A/K;*
(b) *M/K is non-abelian. In this case ρ_ι is irreducible. If $p \neq 2$, then $\rho_\iota = \mathrm{Ind}_H^G \chi_\iota$ where χ_ι is a character of a normal subgroup $H \subset G$ of index 2. Furthermore, every such H is an abelian group containing $I^{\mathrm{w}}(M/K)$ such that $H \cap I(M/K)$ is cyclic.*

Before proving the proposition we establish a few lemmas.

LEMMA 3.7. *The representation ρ_ι is faithful on G.*

PROOF. The eigenvalues of ρ_ι on $I(M/K)$ are roots of unity and the eigenvalues of φ_K have absolute values $\sqrt{q_K}$. Since ρ_ι is faithful on $I(M/K)$, we infer that ρ_ι is faithful on G. □

LEMMA 3.8. *The following statements are equivalent:*

(1) *Every IM-extension L'/K for A/K is abelian;*
(2) *M/K is abelian;*
(3) *$\rho_\ell(\Gamma_K)$ is abelian;*
(4) *$\rho_\ell(W_K)$ is abelian;*
(5) *$\rho_\iota(W_K)$ is abelian;*
(6) *$\rho_\iota\colon W_K \to \mathrm{GL}_2(\mathbb{C})$ is reducible;*
(7) *ρ_ι is a direct sum of two characters of W_K;*
(8) *G is abelian.*

PROOF. The lemma is a slight generalisation of [Roh93, Prop. 2.(ii)]. (1) implies that $M = L'K^{\mathrm{ur}}$ is abelian over K as the compositum of two abelian extensions in $\overline{K}$, so we have (2). We have (2) $\Rightarrow$ (3) since ρ_ℓ factors through the quotient $\mathrm{Gal}(M/K)$ of Γ_K. Restricting ρ_ℓ to W_K gives (3) $\Rightarrow$ (4). The implication (4) $\Rightarrow$ (5) follows from the natural projection $\mathrm{W}_i(\rho_\ell) \to \rho_\iota$ (see (3.4.1)). Schur's lemma gives (5) $\Rightarrow$ (6), and (6) $\Rightarrow$ (7) follows by semisimplicity of ρ_ι. The statement (7) implies that $\rho_\iota(G)$ is abelian, and thus G is abelian by Lemma 3.7, thus giving (8). We prove (8) $\Rightarrow$ (2) by recalling that $G = W(M/K)$ is a dense subgroup of $\mathrm{Gal}(M/K)$, so commutativity of the former implies comutativity of the latter. We are left to establish (2) $\Rightarrow$ (1), which follows by recalling that every IM-extension for A/K is a subextension of M/K. □

PROOF OF PROP. 3.6. If M/K is abelian, then ρ_ι decomposes into a sum of two characters (Lemma 3.8) whose product is $\det \rho_\iota = \omega_K^{-1}$ (see Prop. 3.4,(3)), so we may write $\rho_\iota = \chi_\iota \oplus \chi_\iota^{-1}\omega_K^{-1}$. Since ω_K is unramified, the character χ_ι sends $I(M/K)$ injectively to a finite subgroup of $\mathbb{C}^\times$, which must be cyclic. Let us fix a Frobenius lift φ_K, and let $L = L'$ be the extension given

by Lemma 1.13.(3), which is abelian by Lemma 3.8. We see that $\mathrm{Gal}(L/K) = I(L/K) \simeq I(M/K)$ is cyclic.

Let us suppose that M/K is non-abelian. Lemma 3.8 shows that ρ_ι is irreducible. If $p \neq 2$, then applying [Tat79, (2.2.5.3)] shows that there exist a subgroup $H \subset G$ of index 2 and a character χ_ι of H such that $\rho_\iota = \mathrm{Ind}_H^G \chi_\iota$.

By adjunction, the restriction $\rho_\iota|_H$ contains χ_ι as a subrepresentation, so $\rho_\iota|_H = \chi_\iota \oplus \chi_\iota^{-1}\omega_K^{-1}$, and thus $\rho_\iota|_H$ has abelian image. By faithfulness, H is abelian, and χ_ι identifies the finite group $I(M/K) \cap H$ with its cyclic image in $\mathbb{C}^\times$.

If H does not contain $I^{\mathrm{w}}(M/K)$, then $H \cdot I^{\mathrm{w}}(M/K) = G$ and

$$2 = |G/H| = \left| I^{\mathrm{w}}(M/K) \Big/ I^{\mathrm{w}}(M/K) \cap H \right|.$$

Therefore, 2 must be a power of p, which is impossible if $p \neq 2$. □

Corollary 3.9. *The group $I^{\mathrm{w}}(M/K)$ is cyclic if M/K is abelian or if $p \neq 2$.*

Proof. If M/K is abelian, then every subgroup of $I(M/K)$ is cyclic by Prop. 3.6.(a). If M/K is non-abelian and $p \neq 2$, then $I^{\mathrm{w}}(M/K)$ is contained in the cyclic group $H \cap I(M/K)$. □

Remark 3.10. We note that the subgroup H in the case (b) is not unique for ι. We will show how to make a more precise choice of H in Lemma 4.5.

Other restrictions.

Lemma 3.11. *Let A/K be an abelian variety of dimension g with RM and potentially good reduction. Let $\sigma \in \rho_\ell(I_K)$ be an element of order d. Denote by φ Euler's totient function. Then $\varphi(d)$ divides $2g$.*

Proof. Recall from Prop. 3.3 that the F_ℓ-characteristic polynomial P_σ of σ is of degree 2 and has coefficients in F. Since $\sigma^d = \mathrm{id}$, the complex roots of P_σ are among the roots of $X^d - 1$. Since $\det \sigma = 1$ (by Prop. 3.4.(3)), the two roots of P_σ are roots of unity ζ and ζ^{-1} of some order $d'|d$. Then $\sigma^{d'} = \mathrm{id}$, which implies that $d' = d$. On the other hand, $\alpha := \mathrm{Tr}(\sigma) = \zeta + \zeta^{-1} \in F$. Since α has degree $\max\{1, \frac{\varphi(d)}{2}\}$ over $\mathbb{Q}$, we conclude that $\varphi(d)|2g$. □

As we have seen in Prop. 3.4.(2), the representations $\rho_\iota|_{I_K}$ induce faithful $\mathrm{Aut}(\mathbb{C})$-conjugate representations of a finite group $I(M/K)$. Let $p^r e = |I(M/K)|$ with e prime to p. If $p \neq 2$, then Cor. 3.9 shows that $I^{\mathrm{w}}(M/K)$ is cyclic.

Proposition 3.12. *For A/K as in Lemma 3.11, the following statements hold:*

(1) *If g is even, then $w(A/K) = 1$;*
(2) *If $r \geqslant 1$ and $p \neq 2$, then $p^{r-1}(p-1)|2g$; in particular, if g is odd, then $p \equiv 3 \bmod 4$;*

(3) *If g is odd, then e can only be s^m, $2s^m$, or 4, where $m \geqslant 0$ and $s \equiv 3 \bmod 4$ is a prime different from p.*

PROOF. (1) follows from Prop. 3.4.(4) and (3.5.1). Applying Lemma 3.11 to a generator of $I^{\mathrm{w}}(M/K)$ and using $\varphi(p^r) = p^{r-1}(p-1)$ we obtain (2). Suppose now that g is odd. If $\varphi(e)$ is odd, then e is 1 or 2. If $\varphi(e)$ is even, then applying Lemma 3.11 to a generator of $I^{\mathrm{t}}(M/K)$ gives $\varphi(e) \equiv 2 \bmod 4$. Now (3) follows from the usual formulas of $\varphi(e)$. □

4. The case of abelian inertia

We continue to work in the setting of 3.1 and suppose that $p \neq 2$. We adopt the notation of Prop. 3.4 and regard each ρ_ι as a faithful representation of $G = W(M/K)$ (see Lemma 3.7). Let us write $|I(M/K)| = p^r e$ with $e = |I^{\mathrm{t}}(M/K)|$, so that $p \nmid e$. Applying (3.5.1), it suffices to determine the root number $w(\rho_\iota, \psi_K)$ for a fixed embedding $\iota\colon F \hookrightarrow \mathbb{C}$.

THEOREM 4.1. *If $\rho_\ell(\Gamma_K)$ is abelian, then $e \mid (q_K - 1)$ and*

$$w(\rho_\iota, \psi_K) = (-1)^{\frac{q_K - 1}{e}}.$$

PROOF. The image $\rho_\ell(\Gamma_K)$ is abelian if and only if M/K is abelian by Lemma 3.8, so we are in the case (a) of Prop. 3.6. Then, we have a decomposition $\rho_\iota = \chi_\iota \oplus \chi_\iota^{-1}\omega_K^{-1}$. Using multiplicativity of the root number and Prop. 1.21.(1),(2) we obtain

$$w(\rho_\iota, \psi_K) = \chi_\iota(\theta_K(-1)) \in \{\pm 1\}.$$

By Lemma 1.13, there exists a finite IM-extension L/K for A/K. By Lemma 3.8, L/K is abelian. We identify $I(L/K) \simeq I(M/K)$. Then the composition $(\chi_\iota \circ \theta_K)|_{\mathcal{O}_K^\times}$ can be seen as the following sequence of group homomorphisms:

(4.1.1)
$$\mathcal{O}_K^\times \twoheadrightarrow \mathcal{O}_K^\times \Big/ \mathcal{N}_{L/K}(\mathcal{O}_L^\times) \xrightarrow{\theta_{L/K}}_{\sim} I^{\mathrm{w}}(L/K) \times I^{\mathrm{t}}(L/K) \xhookrightarrow{\chi_\iota} \mathbb{C}^\times.$$

Let us recall the identification $\mathcal{O}_K^\times \cong k_K^\times \times (1 + \mathfrak{m}_K)$. The image of $k_K^\times$ is trivial in $I^{\mathrm{w}}(L/K)$, so $\theta_{L/K}$ induces a homomorphism $\theta_{k_K}\colon k_K^\times \to I^{\mathrm{t}}(L/K)$. On the other hand, the image of the pro-p group $1 + \mathfrak{m}_K$ is trivial in $I^{\mathrm{t}}(L/K)$, so θ_{k_K} must be surjective. In particular, $e \mid (q_K - 1)$. Since $p \neq 2$, the class of -1 in $k_K^\times$ is nontrivial, so $\chi_\iota(\theta_K(-1)) = \chi_\iota(\theta_{k_K}(-1)) = 1$ if and only if -1 belongs to the unique subgroup of index e in $k_K^\times$, which can be characterized by $\{x \in k_K^\times : x^{\frac{q_K-1}{e}} = 1\}$. □

4.2. Representation having non-abelian image. It remains to study the case where $\rho_\ell(\Gamma_K)$ is non-abelian, which is the case (b) of Prop. 3.6 (see Lemma 3.8), when M/K is non-abelian. In this case, ρ_ι is induced by a character χ_ι of an abelian normal subgroup $H \subset G = W(M/K)$ of index 2, which contains $I^{\mathrm{w}}(M/K)$.

LEMMA 4.3. *We can choose a geometric Frobenius lift φ_K so that φ_K^2 is contained in the center of G.*

PROOF. Let τ_K and φ_K be as in Thm. 1.2. Since H is commutative of index 2 in G and contains $I^{\mathrm{w}}(M/K)$, the element φ_K^2 is in H and commutes with every element of $I^{\mathrm{w}}(M/K)$. We are left to prove that $\varphi_K^{-2}\tau_K\varphi_K^2 = \tau_K$, which is equivalent to e dividing $q_K^2 - 1$ by the aforementioned theorem. If $\tau_K \in H$, there is nothing to prove since H is abelian, so we may suppose that $\tau_K \notin H$. Then, $\tau_K^2 \in H$ and $e = |I^{\mathrm{t}}(M/K)|$ is even.

If $\varphi_K \in H$, then $\tau_K^{2q_K} = \varphi_K^{-1}\tau_K^2\varphi_K = \tau_K^2$, so $e|2q_K - 2$, which implies that $e|q_K^2 - 1$.

If $\varphi_K \notin H$, then $\varphi_K\tau_K \in H$ commutes with φ_K^2, so $\tau_K = \varphi_K^{-3}(\varphi_K\tau_K)\varphi_K^2$, and we are done. □

HYPOTHESIS 4.4. *The image of the inertia subgroup I_K via the representation ρ_ℓ is commutative.*

The hypothesis is verified in the following cases:

(1) $\rho_\ell|_{I_K}$ factors through the tame inertia group I_K^{t}, or, equivalently, A/K attains good reduction over a finite (at most) tamely ramified extension L'/K, the explicit formulas for root numbers are given by [Bis19, Thm. 1.4];
(2) A/K is an elliptic curve with discriminant of even valuation, this case is settled in [Kob02, 5.2. b)];
(3) A/K has complex multiplication, see [ST68, p. 502, Cor. 2].

By Prop. 3.4.(1), the group $\rho_\ell(I_K)$ is commutative if and only if $\rho_\iota(I_K)$ is commutative for any ι.

LEMMA 4.5. *If Hypothesis 4.4 is satisfied, then we can choose H so that, independently of ι, the representation ρ_ι is induced by a character of H and that the extension $M^{\overline{H}}/K$ is unramified (here $\overline{H} \subset \mathrm{Gal}(M/K)$ denotes the closure of H).*

PROOF. Let us set $H := I(M/K) \times \langle\varphi_K^2\rangle$ for a lift φ_K as in Lemma 4.3, so that H identifies with a commutative subgroup of G of index 2, independent of ι. By semisimplicity, the restriction $\rho_\iota|_H$ decomposes to a sum of two characters

$$\rho_\iota|_H = \chi_\iota \oplus \chi_\iota^{-1}\omega_K^{-1}$$

and then by the adjunction property we have a nontrivial morphism of complex G-representations

$$\mathrm{Ind}_H^G \chi_\iota \to \rho_\iota,$$

which is surjective as ρ_ι is irreducible (by Lemma 3.8) and therefore an isomorphism since the dimensions agree. On the other hand, if L_u/K is the unramified quadratic extension, then $W(M/L_u)$ is a subgroup of G of index 2 and contains $I(M/K)$. The element φ_K^2 is a lift of $\mathrm{Frob}_{k_{L_u}}^{-1}$ in Γ_{L_u}, so $\varphi_K^2 \in W(M/L_u)$. Therefore, $H \subseteq W(M/L_u)$. The latter inequality is an equality because both subgroups have index 2 in G, thus $\overline{H} = \mathrm{Gal}(M/L_u)$. □

THEOREM 4.6. *We suppose that $\rho_\ell(\Gamma_K)$ is non-abelian and that $\rho_\ell(I_K)$ is abelian. For the subgroup $H \subset G$ from Lemma 4.5, we have $\rho_\iota = \mathrm{Ind}_H^G \chi_\iota$. Then:*

(1) *$a(\rho_\iota) = 2 \cdot a(\chi_\iota)$, where $a(\cdot)$ denote the Artin conductor,*
(2) *e divides $q_K + 1$, and*
(3) $w(\rho_\iota, \psi_K) = (-1)^{\frac{a(\rho_\iota)}{2} + \frac{q_K+1}{e}}$.

PROOF. Let us denote $L_u := M^{\overline{H}}$, which is quadratic and unramified over K by Lemma 4.5 and its proof. (1) follows from the general formulas of Artin conductors (see, e.g., [Roh94, §10]).

The formula 1.18.(ii) for the ϵ-factor of an induced representation gives

$$w(\rho_\iota, \psi_K) = w(\chi_\iota, \psi_{L_u})\, w\big(\mathrm{Ind}_H^G \mathbb{1}_H, \psi_K\big), \tag{4.6.1}$$

since $w(\mathbb{1}_H, \psi_{L_u})^{-1} = 1$ (from 1.18.(iii)).

Let χ_0 be the unramified quadratic character of G given by the composition $G \to \mathrm{Gal}(L_u/K) \cong \{-1, 1\}$. Then $\mathrm{Ind}_H^G \mathbb{1}_H \cong \mathbb{1}_G \oplus \chi_0$. Using 1.18.(i),(iii) we have:

$$w(\mathrm{Ind}_H^G \mathbb{1}_H, \psi_K) = w(\mathbb{1}_G, \psi_K) w(\chi_0, \psi_K) = \chi_0(\theta_K(c)) = (-1)^{n(\psi_K)}, \tag{4.6.2}$$

where $c \in K^\times$ has valuation $n(\psi_K)$.

We prove (2) and compute $w(\chi_\iota, \psi_{L_u})$ in the following lemma.

LEMMA 4.7. *We have $e \mid (q_K + 1)$ and*

$$w(\chi_\iota, \psi_{L_u}) = (-1)^{n(\psi_K) + a(\chi_\iota) + \frac{q_k+1}{e}}. \tag{4.7.1}$$

PROOF. Let χ_0 be the character corresponding to L_u/K as before, and let $t\colon G^{\mathrm{ab}} \to H^{\mathrm{ab}} = H$ be the transfer homomorphism, which corresponds to the inclusion $K^\times \hookrightarrow L_u^\times$ via the reciprocity maps. The twisted representation $\rho_\iota(\frac{1}{2})$ has trivial determinant (see Prop. 3.4.(3)), so Deligne's determinant formula from [Del73, p. 508] gives

$$1 = \det\left(\mathrm{Ind}_H^G \chi_\iota(\tfrac{1}{2})\right)(g) = \chi_0(g)\chi_\iota(\tfrac{1}{2})(t(g)) \tag{4.7.2}$$

for every $g \in G$. Therefore, for every $x \in K^\times$,

$$(\chi_\iota(\tfrac{1}{2}) \circ \theta_{L_u})(x) = \chi_0^{-1}\left(\theta_K(x)\right) = (-1)^{v_K(x)}. \tag{4.7.3}$$

Let χ_1 be the nontrivial quadratic unramified character of H, so that for all $x \in L_u$ we have $\chi_1 \circ \theta_{L_u}(x) = (-1)^{v_{L_u}(x)}$. Since the valuations v_K and v_{L_u} agree on $K^\times$, the character $\left(\chi_\iota(\frac{1}{2}) \cdot \chi_1\right) \circ \theta_{L_u}$ is trivial on $K^\times$. The extension

L_u/K is unramified and $[L_u : K] = 2$, so $L_u = K(\zeta_{2q_K-2})$ where ζ_{2q_K-2} is a primitive root of unity of order $2q_K - 2$. We have $\zeta_{2q_K-2}^2 \in K^\times$, so applying [FQ73, Thm. 3] gives

$$\begin{aligned} w(\chi_\iota(\tfrac{1}{2}) \cdot \chi_1, \psi_{L_u}) &= \chi_\iota(\tfrac{1}{2})\left(\theta_{L_u}(\zeta_{2q_K-2})\right) \cdot \chi_1\left(\theta_{L_u}(\zeta_{2q_K-2})\right) \\ &= \chi_\iota\left(\theta_{L_u}(\zeta_{2q_K-2})\right), \end{aligned} \tag{4.7.4}$$

the last equality holds because χ_1 and $\omega_K^{1/2}$ are unramified. On the other hand, applying Prop. 1.21,(1) gives

$$w(\chi_\iota(\tfrac{1}{2}) \cdot \chi_1, \psi_{L_u}) = w(\chi_\iota, \psi_{L_u}) \cdot (-1)^{n(\psi_{L_u})+a(\chi_\iota)}. \tag{4.7.5}$$

Combining (4.7.4), (4.7.5), and the observation that $n(\psi_K) = n(\psi_{L_u})$, we obtain

$$w(\chi_\iota, \psi_{L_u}) = (-1)^{n(\psi_K)+a(\chi_\iota)}\chi_\iota(\theta_{L_u}(\zeta_{2q_K-2})). \tag{4.7.6}$$

Let L/K be a finite, Galois, and IM extension for A/K (see Lemma 1.13). Then L_uL/K is also a Galois and IM extension, so we identify $I(M/K) \simeq I(L/K) \simeq I(L_uL/L_u)$. As in the proof of Thm. 4.1, we use the decomposition $\mathfrak{O}_{L_u}^\times \cong k_{L_u}^\times \times (1 + \mathfrak{m}_{L_u})$ to obtain a surjective homomorphism $\theta_{k_{L_u}} : k_{L_u}^\times \twoheadrightarrow I^{\mathrm{t}}(L_uL/L_u)$ induced by θ_{L_u}. We see from (4.7.3) that $\chi_\iota \circ \theta_{L_u}$ is trivial on $\mathfrak{O}_K^\times$. It follows that the subgroup $\ker(\chi_\iota \circ \theta_{L_u}|_{k_{L_u}^\times}) = \ker(\theta_{k_{L_u}})$ contains $k_K^\times$. This implies that $e = |I^{\mathrm{t}}(L_uL/L_u)|$ divides $[k_{L_u}^\times : k_K^\times] = q_K + 1$.

The subgroup $\ker(\chi_\iota \circ \theta_{L_u}|_{k_{L_u}^\times})$ of index e in $k_{L_u}^\times$ contains ζ_{2q_K-2} if and only if $1 = \zeta_{2q_K-2}^{(q_K^2-1)/e} = (-1)^{\frac{q_K+1}{e}}$. Since $(\chi(\frac{1}{2}) \cdot \chi_1) \circ \theta_{L_u}|_{K^\times}$ is trivial, (4.7.6) gives $\chi(\theta_{L_u}(\zeta_{2q_K-2}))^2 = 1$, and thus (4.7.1) follows. □

Plugging (4.6.2) and (4.7.1) into (4.6.1), as well as using (1), we obtain (3). □

Corollary 4.8. *Let A/K be as in 3.1, let denote by $a(A/K)$ its Artin conductor, and let e be the largest prime-to-p divisor of the order of $\rho_\ell(I_K)$.*

(1) *If $\rho_\ell(\Gamma_K)$ is commutative, then $w(A/K) = (-1)^{\frac{g(q_K-1)}{e}}$;*
(2) *If $\rho_\ell(\Gamma_K)$ is non-commutative and $\rho_\ell(I_K)$ is commutative, then*

$$w(A/K) = (-1)^{\frac{a(A/K)}{2}+\frac{g(q_K+1)}{e}}.$$

Proof. Let us recall formula (3.5.1). Then, (1) follows from Thm. 4.1; the part (2) follows from Thm. 4.6,(3) and multiplicativity of Artin conductor. □

Remark 4.9. If $\rho_\ell(I_K^{\mathrm{w}})$ is trivial, then Corollary 4.8 allows us to compute the root number $w(A/K)$. In this case, if A/K has bad potentially good reduction, then we always have $a(A/K) = 2g$. The obtained formulas are special cases of the results of [Bis19, Thm. 1.4], as it can be verified by a calculation using Prop. 3.12.

5. Potentially totally toric reduction

Let A/K be an abelian variety of dimension g with RM by F, and recall the notation and results of 1.14. We suppose that A/K does not have potentially good reduction. Then it must have potentially totally toric reduction by Prop. 2.6, so $B = 0$. The analytification A/K is a quotient of the analytification of a torus T/K, which gives rise to a $\mathbb{Q}$-linear Weil representation

$$\eta\colon W_K \to \mathrm{GL}_{\mathbb{Q}}(X(T) \otimes_{\mathbb{Z}} \mathbb{Q})$$

with finite image. Prop. 1.15 then gives

$$\mathrm{WD}_i(\rho_\ell) \cong \eta(-1) \otimes \mathrm{sp}(2). \tag{5.0.1}$$

Let us fix a basis $v_1, \dots, v_g$ of the underlying vector space of η and let e_0, e_1 be the standard basis of $\mathrm{sp}(2) = (\mathbb{1} \oplus \omega_K, \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right))$. Then, in the basis

$$\mathbb{B} := (v_1 \otimes e_0, \dots, v_g \otimes e_0, v_1 \otimes e_1, \dots, v_g \otimes e_1),$$

the WD-representation $\mathrm{WD}_i(\rho_\ell)$ is given as

$$\mathrm{WD}_i(\rho_\ell) \simeq \left(\eta(-1) \oplus \eta, \left(\begin{array}{c|c} 0_g & 0_g \\ \hline I_g & 0_g \end{array}\right)\right). \tag{5.0.2}$$

From (5.0.2) one can recover the isomorphism class of the representation ρ_ℓ by a procedure inverse to the one in 1.7. Let us choose a continuous nontrivial homomorphism $t_\ell\colon I_K \to \mathbb{Q}_\ell$. Then, in the same basis $\mathbb{B}$, for every $j \in I_K$,

$$\rho_\ell(j) = \left(\begin{array}{c|c} \eta(j) & 0_g \\ \hline 0_g & \eta(j) \end{array}\right) \cdot \exp\left(\begin{array}{c|c} 0_g & 0_g \\ \hline t_\ell(j) I_g & 0_g \end{array}\right) = \left(\begin{array}{c|c} \eta(j) & 0_g \\ \hline t_\ell(j)\eta(j) & \eta(j) \end{array}\right), \tag{5.0.3}$$

and

$$\rho_\ell(\varphi_K) = \left(\begin{array}{c|c} q_K \eta(\varphi_K) & 0_g \\ \hline 0_g & \eta(\varphi_K) \end{array}\right). \tag{5.0.4}$$

Proposition 5.1. *An abelian variety A/K with RM which does not have potentially good reduction must have one of the following reduction types:*

(a) *$\mathscr{A}^0_{k_K}$ is a split torus, or, equivalently, η is the trivial representation (split multiplicative reduction);*
(b) *$\mathscr{A}^0_{k_K}$ is a non-split torus, or, equivalently, η is unramified and nontrivial (non-split multiplicative reduction);*
(c) *$\mathscr{A}^0_{k_K}$ is unipotent, but A/L has completely toric reduction for some finite L/K, or, equivalently, η is ramified (additive potentially multiplicative reduction).*

Proof. Let us suppose that η is unramified. Then $\rho_\ell|_{I_K}$ is unipotent, as it can be seen from (5.0.3), so A/K has semistable reduction by Thm. 1.11.(2),

and thus $\mathscr{A}^0_{k_K}$ must be a torus T' (see Prop. 2.6). After writing the matrices of the dual representation ρ_ℓ^* in the dual basis of $\mathbb{B}$, we see that

$$(V_\ell A)^{I_K} = \mathrm{Vect}(v_1^* \otimes e_0^*, \dots, v_g^* \otimes e_0^*),$$

on which φ_K acts as $q_K^{-1}\eta^*(\varphi_K) = \eta^*(1)(\varphi_K)$. On the other hand, we have isomorphisms of ℓ-adic Γ_{k_K}-representations $(V_\ell A)^{I_K} \cong V_\ell \mathscr{A}_{k_K}$ (see [ST68, Lemma 2]), $V_\ell \mathscr{A}_{k_K} \cong V_\ell T'$ (since $\mathscr{A}_{k_K}/\mathscr{A}^0_{k_K}$ is finite), and, formally, $V_\ell T' \cong \mathrm{Hom}(X(T') \otimes_{\mathbb{Z}} \mathbb{Q}_\ell, \mathbb{Q}_\ell)(1)$. Therefore, the Γ_{k_K}-action on $X(T')$ is trivial if and only if η^* is trivial. Since η is $\mathbb{Q}$-linear, we have $\eta \simeq \eta^*$. Therefore, we conclude that η is trivial if and only if T' is split.

Suppose that η is ramified. The image of $\eta|_{I_K}$ is finite, so $\eta|_{I_K}$ and, subsequently, $\rho_\ell|_{I_K}$ cannot be unipotent. Thm. 1.11.(2) implies that A/K does not have semistable reduction, so $\mathscr{A}^0_{k_K}$ is not a torus and we may conclude via Prop. 2.6. □

5.2. F-rationality again. Recalling the description of η given by Remark 1.16.(2) and using (2.5.2) we see that η is F-linear of dimension one. We may then regard η as a homomorphism $\eta_F \colon W_K \to F^\times$. We have a decomposition $F \otimes_{\mathbb{Q}} \mathbb{C} \cong \prod_{\iota \colon F \to \mathbb{C}} \mathbb{C}$, so

$$\eta \otimes_{\mathbb{Q}} \mathbb{C} \cong \prod_{\iota \colon F \to \mathbb{C}} \eta_\iota, \tag{5.2.1}$$

with $\eta_\iota := \eta_F \otimes_{F,\iota} \mathbb{C}$, where the structural morphism is given by ι. Consequently, defining $\rho'_\iota := \eta_\iota(-1) \otimes \mathrm{sp}(2)$, the isomorphism (5.0.1) gives

$$\mathrm{WD}_i(\rho_\ell) \cong \prod_\iota \rho'_\iota. \tag{5.2.2}$$

We note that $\eta_\iota = \iota \circ \eta_F$, which implies that the η_ι's are $\mathrm{Aut}(\mathbb{C})$-conjugate, and thus the ρ'_ι's are also $\mathrm{Aut}(\mathbb{C})$-conjugate. As in Rem. 3.5, we may apply [Roh11, Thm. 1] to see that $w(\rho'_\iota, \psi_K)$ is independent of ι.

THEOREM 5.3. *Let us fix some $\iota \colon F \hookrightarrow \mathbb{C}$. In the ongoing notation,*

$$w(\rho'_\iota, \psi_K) = \begin{cases} -1 & \text{if } A/K \text{ has split multiplicative reduction;} \\ 1 & \text{if } A/K \text{ has non-split multiplicative reduction;} \\ (-1)^{\frac{q_K-1}{2}} & \text{if } A/K \text{ has additive potentially multiplicative} \\ & \text{reduction and } p \neq 2. \end{cases}$$

PROOF. We observe that, since F is totally real, η_F and η_ι are quadratic. Applying Prop. 1.21.(1),(3) gives

$$w(\rho'_\iota, \psi_K) = \eta_\iota\left(\theta_K(-1)\right) \cdot (-1)^{\langle \eta_\iota | \mathbb{1} \rangle}.$$

Since η_ι's are $\mathrm{Aut}(\mathbb{C})$-conjugate, we may replace η with any η_ι in Prop. 5.1.

Let us suppose that η_ι is unramified. Then $\eta_\iota(\theta_K(-1)) = 1$. Depending on whether $\langle \eta_\iota | \mathbb{1} \rangle$ is 1 or 0, the reduction is split or non-split multiplicative, respectively, since $\langle \eta_\iota | \mathbb{1} \rangle = 1$ if and only if η_ι is trivial.

It remains to treat the case when η_ι is ramified. In particular, η_ι is non-trivial, so $\langle \eta_\iota | \mathbb{1} \rangle = 0$. More precisely, η_ι is of exact order 2, so it factors through a quotient $\mathrm{Gal}(L/K)$ of order 2. If $p \neq 2$, then L/K is totally tamely ramified. In that case, $\eta_\iota(\theta_K(-1)) = 1$ if and only if -1 is a norm for L/K. The latter is equivalent to -1 being a square in k_K, which happens exactly when $q_K \equiv 1 \bmod 4$. □

Corollary 5.4. *For A/K given at the begining of Section 5 and for $p \neq 2$,*

$$w(A/K) = \begin{cases} (-1)^g & \text{if the reduction (over } K\text{) is split multiplicative;} \\ 1 & \text{if the reduction is non-split multiplicative;} \\ (-1)^{g\frac{q_K-1}{2}} & \text{if the reduction is additive.} \end{cases}$$

Proof. The formulas follow from (5.2.2), multiplicativity of root numbers, and Thm 5.3. □

Remark 5.5. Let $\mathcal{K}$ be a number field and let $A/\mathcal{K}$ be an abelian variety with real multiplication by F. For each finite place v of $\mathcal{K}$, we have a decomposition of associated complex WD-representations $\mathrm{WD}_i(\rho_\ell(A_v/\mathcal{K}_v)) = \prod_{\iota\colon F\hookrightarrow\mathbb{C}} \rho'_{v,\iota}$, where each family $(\rho'_{v,\iota})_\iota$ is composed of $\mathrm{Aut}(\mathbb{C})$-conjugate representations (we established this for the potentially good reduction case in Prop. 3.4.(1) and for the remaining cases in 5.2). The root numbers $w(\rho'_{v,\iota}, \psi_{\mathcal{K}_v})$ are independent of ι by [Roh11, Thm. 1]. We choose some ι, fix any place v of $\mathcal{K}$, and define

$$w(\iota A_v/\mathcal{K}_v) := \begin{cases} w(\rho'_{v,\iota}, \psi_{\mathcal{K}_v}) & \text{if } v \text{ is finite,} \\ -1 & \text{if } v \text{ is infinite.} \end{cases}$$

Furthermore, let us define

$$w(\iota A/\mathcal{K}) := \prod_v w(\iota A_v/\mathcal{K}_v).$$

We have $w(A/\mathcal{K}) = w(\iota A/\mathcal{K})^{\dim A}$. The number $w(\iota A/\mathcal{K})$ appears, for example, in the functional equation of a certain L-function (see [Nek15, (0.1) and §4.9]) and, consequently, in a certain version of the p-Parity Conjecture (now a theorem by Nekovář [Nek18, Thm. D]).

CHAPTER II

ROOT NUMBERS OF CURVES OF GENUS 1 AND 2 HAVING MAXIMAL RAMIFICATION

ABSTRACT. We consider a curve of genus 2 defined over a 5-adic field such that the inertia acts on the first ℓ-adic cohomology group through the largest possible finite quotient, isomorphic to $C_5 \rtimes C_8$. We give a few criteria to identify such curves and prove a formula for their local root numbers in terms of other invariants.

Our result is analogous to the formulas for the root numbers of elliptic curves, due to Kobayashi. We also present a geometric interpretation of Kobayashi's result which eliminates explicit dependency on a particular Weierstrass equation of a given elliptic curve.

Introduction

Given an abelian variety A defined over a number field $\mathcal{K}$, its global root number $w(A/\mathcal{K})$ is the sign appearing in the conjectural functional equation of its completed L-function. Granting the general Birch–Swinnerton-Dyer conjecture, $w(A/\mathcal{K}) = -1$ exactly when the Mordel–Weil rank is odd. Due to Deligne [Del73], we can define $w(A/\mathcal{K})$ unconditionally by computing the local root numbers $w(A_v/\mathcal{K}_v)$ of the localized abelian variety at each place v of $\mathcal{K}$.

For each infinite place we have $w(A_v/\mathcal{K}_v) = (-1)^{\dim A}$. For a finite place v of $\mathcal{K}$ we follow the general procedure valid over any local field which we will describe in the next paragraph. In this case the local root number is closely related to the reduction type of $A_v/\mathcal{K}_v$. If the reduction is good at v, then $w(A_v/\mathcal{K}_v) = 1$, which allows us to compute

$$w(A/\mathcal{K}) = \prod_v w(A_v/\mathcal{K}_v),$$

the product being taken over all places of $\mathcal{K}$.

Let p be a prime number, let $K/\mathbb{Q}_p$ be a finite extension with an algebraic closure $\overline{K}$, and let A/K be an abelian variety. We choose another prime number $\ell \neq p$ and consider the ℓ-adic Galois representation ρ_ℓ on the étale cohomology group $H^1_{\text{ét}}(A_{\overline{K}}, \mathbb{Q}_\ell)$. Applying Grothendieck's monodromy construction we obtain a complex Weil–Deligne representation $\mathrm{WD}(\rho_\ell)$, whose isomorphism class does not depend on ℓ (see, e.g., [Sab07, Cor. 1.15]). Next, following Langlands and Deligne, after choosing an additive character ψ on K

and a Haar measure $\mathrm{d}x$ on K, we consider the ϵ-factor $\epsilon(\mathrm{WD}(\rho_\ell), \psi, \mathrm{d}x) \in \mathbb{C}^\times$. The local root number is then defined as

$$w(A/K) := \frac{\epsilon(\mathrm{WD}(\rho_\ell), \psi, \mathrm{d}x)}{|\epsilon(\mathrm{WD}(\rho_\ell), \psi, \mathrm{d}x)|}.$$

We note that $w(A/K)$ is independent on the choices of ℓ, ψ, or $\mathrm{d}x$, see, e.g., [Roh94, §11, §12]

It follows (see, e.g., [Cha00, Prop. 3.1]) from the semi-stable reduction theorems and the theory of p-adic uniformization that there exist an abelian variety B/K with potentially good reduction and an extension S of B by a torus T such that the rigid analytification of A is a quotient of the analytification of S by a lattice. Then, it follows from the result of Sabitova [Sab07, Prop. 1.10] that $w(A/K)$ can be determined by computing $w(B/K)$ and the Galois action on T. In this chapter we treat the case when A/K itself has potentially good reduction. This condition is equivalent to $T = 0$ and, by the criterion of Néron–Ogg–Shafarevich, to the condition that the image of inertia via ρ_ℓ is finite. By Serre–Tate [ST68, p. 497, Cor. 2] the representation ρ_ℓ is always at most tamely ramified when $p > 2\dim(A) + 1$.

If A/K is an elliptic curve with potentially good reduction, formulas for root numbers have been given by Rohrlich [Roh96] when $p \geqslant 5$, by Kobayashi [Kob02] when $p = 3$, and by the Dokchitsers [DD08] when $p = 2$. For general abelian varieties, the case when ρ_ℓ is tamely ramified has been studied by Bisatt [Bis19].

0.1. The main setup and results. We consider a curve C of genus 2 defined over a 5-adic field K. Let $J(C)/K$ be its Jacobian surface. Our aim is to produce a formula for $w(C/K) := w(J(C)/K)$ in terms of other invariants of C/K. We suppose that $J(C)/K$ has potentially good reduction and that the associated Galois representation ρ_ℓ is wildly ramified. We suppose further that ρ_ℓ has the maximal possible inertia image, isomorphic to the semi-direct product $C_5 \rtimes C_8$ where C_8 acts on C_5 via $C_8 \twoheadrightarrow C_4 \simeq \mathrm{Aut}(C_5)$. By choosing a Weierstrass equation we define a discriminant $\Delta \in K^\times$, whose class in $K^\times/(K^\times)^2$ does not depend on the choice of the equation, see 2.2. Let $m(C/K)$ denote the number of irreducible components of the geometric special fiber of the minimal regular model of C/K.

Let k_K be the residue field of K. We denote by $(\frac{\cdot}{k_K})$ the Legendre symbol on $k_K^\times$ and by $(\cdot,\cdot)_K$ the quadratic Hilbert symbol on $K^\times \times K^\times$. We consider the normalized valuation v_K of K such that $v_K(K^\times) = \mathbb{Z}$. Let F_5 denote the Frobenius group on 5 elements, defined as the semi-direct product $F_5 = C_5 \rtimes C_4$ where C_4 acts faithfully on C_5.

Theorem 0.2 (Prop. 3.17, Prop. 5.1, Thm. 6.1). *Let C/K be a smooth projective curve of genus 2 defined over a 5-adic field K. Suppose that ρ_ℓ has finite inertia image of order divisible by 5. There exists an equation $Y^2 = P(X)$ defining C/K with*

unitary, irreducible $P \in K[X]$ of degree 5 having integral coefficients and a constant term a_6 of valuation prime to 5.

The image of inertia of ρ_ℓ is the maximal possible, i.e., isomorphic to $C_5 \rtimes C_8$, if and only if any of the following equivalent conditions is verified :

(1) *For any discriminant Δ of C/K the valuation $v_K(\Delta)$ is odd;*
(2) *The $\mathbb{F}_2$-linear Galois representation on the 2-torsion points $J(C)[2]$ has inertia image isomorphic to the Frobenius group F_5;*
(3) *The Artin conductor $a(C/K)$ of ρ_ℓ is odd.*

In this case, the root number is given by

$$w(C/K) = (-1)^{[k_K:\mathbb{F}_5]+1} \cdot \left(\frac{m(C/K)+3}{k_K}\right) \cdot (\Delta, a_6)_K.$$

REMARK 0.3. The setting of Thm. 0.2 is a particular case of the study by Coppola [Cop20], where a description of ρ_ℓ is given. Very recently, building on Coppola's results, Bisatt [Bis21, Thm. 2.1] produced similar formulas of root numbers of hyperelliptic curves. The results of Thm. 0.2 have been obtained independently of [Bis21].

0.4. Kobayashi's formula for elliptic curves revisited. Thm. 0.2 is an analogue of [Kob02, Thm. 5.9]. These results rely on particular Weierstrass equations. For an elliptic curve E/K over a 3-adic field K we find that the factor $(\Delta, a_6)_K$ appearing in Kobayashi's formula can be replaced by a sign depending only on the Tamagawa number of E over $H = K(\sqrt{\Delta})$. Since the extension H/K does not depend on the choice of Δ, we obtain a formula for the root number without terms referring to a Weierstrass equation. Recall that the Tamagawa number of E/H, denoted $c(E/H)$, is defined as the number of rational points $|\Phi(k_H)|$ where Φ is the algebraic group of the connected components of the special fiber of the Néron model of E/H.

Let $\lfloor\cdot\rfloor$ denote the floor function of real numbers, and let v_3 denote the normalized 3-adic valuation on $\mathbb{Q}$.

THEOREM 0.5 (Prop. 8.7, Thm. 8.10). *Let E/K be an elliptic curve defined over a 3-adic field K. Suppose that E/K has potentially good reduction and that the associated Galois representation ρ_ℓ is wildly ramified. The image of inertia of ρ_ℓ is the maximal possible, i.e., isomorphic to $C_3 \rtimes C_4$, if and only if the following equivalent conditions are verified:*

(1) *Any discriminant $\Delta \in K$ of E/K has odd valuation $v_K(\Delta)$;*
(2) *The $\mathbb{F}_2$-linear Galois representation on the 2-torsion points $E[2]$ has inertia image isomorphic to the symmetric group S_3;*
(3) *The Artin conductor $a(E/K)$ of ρ_ℓ is odd.*

In this case, let $H := K(\sqrt{\Delta})$. Then the local root number is given by

$$w(E/K) = (-1)^{v_3(c(E/H))} \cdot \left(\frac{-1}{k_K}\right)^{\frac{a(E/K)+m(E/K)}{2}+\lfloor\frac{m(E/K)+1}{6}\rfloor}. \tag{0.5.1}$$

REMARK 0.6. In the setting of Thm. 0.5:

1. The Kodaira symbol (see [Sil94, IV.8.2]) of E/K can only be II, II^*, IV, or IV^*, and thus $m(E/K)$ is 1, 9, 3, or 7, respectively. The particular form of (0.5.1) was chosen because, for general elliptic curves with potentially good reduction, the star "*" appears in the Kodaira symbol if and only if $\lfloor \frac{m(E/K)+1}{6} \rfloor = 1$, otherwise $\lfloor \frac{m(E/K)+1}{6} \rfloor = 0$. Another explanation can be derived from (8.14.3).
2. The Kodaira symbol of E/H is always IV of IV^*, so $c(E/H) \in \{1, 3\}$. In contrast, the Tamagawa number $c(E/K)$ over the base field K appears to have no direct influence on the root number. Indeed, the root number depends only on the isogeny class of E/K, while $c(E/K)$, in general, varies in this class.

0.7. Structure of the chapter. In Section 1 we recall the theory of ϵ-factors for characters and give formulas of root numbers for some wildly ramified characters by using explicit local class field theory. In Section 2 we recall some results from the classical theory of hyperelliptic curves and their conductors. In Section 3 we specialize to genus 2: we prove the first part of Thm. 0.2 and show connections among some invariants of C/K. In Section 4 we employ the theory of Artin–Schreier curves in order to study ρ_ℓ via the automorphisms of curves over finite fields. In Section 5 we prove a few characterizations of the maximal ramification case and exploit some of its implications. Section 6 is dedicated to proving the formula of Thm. 0.2, where we connect the results of Section 1 to a particular Weierstrass equation. In Section 7 we exhibit some possible applications of Thm. 0.2. In Section 8 we turn our attention to the case of elliptic curves and give two proofs of (0.5.1).

Notation and conventions

Let p be a prime number, and let $K/\mathbb{Q}_p$ be a finite extension. We fix the notation of Table 1. We adopt the convention that every algebraic extension of K used in this text is a subfield of $\overline{K}$.

By a *Weil representation* on a complex vector space V we mean a group homomorphism $\rho\colon W_K \to \mathrm{GL}(V)$ such that $\rho(I_K)$ is finite. For any $s \in \mathbb{C}^\times$, its Tate twist is $\rho(s) := \rho \otimes \chi_{\mathrm{ur}}^s$.

Let $\theta_K\colon K^\times \cong W_K^{\mathrm{ab}}$ be Artin's reciprocity map normalized to send a uniformiser to the class of a geometric Frobenius lift. It follows that $||\cdot||_K := \chi_{\mathrm{ur}} \circ \theta_K$ is the non-Archimedean norm on K induced by v_K. For every finite Galois extension L/K, the map θ_K induces an isomorphism $\theta_{L/K}\colon K^\times/\mathcal{N}_{L/K}(L^\times) \cong \mathrm{Gal}(L/K)^{\mathrm{ab}}$, where $\mathcal{N}_{L/K}\colon L^\times \to K^\times$ is the norm map. Abusively, we will make no notational difference between a one-dimensional Weil representation of W_K and the induced quasi-character of $K^\times$.

TABLE 1. Notation for a p-adic field K

v_K	the valuation of K normalized by $v_K(K^\times)=\mathbb{Z}$;
$\mathcal{O}_K$	the ring of integers;
$\mathfrak{m}_K$	the maximal ideal;
ϖ_K	a uniformizer;
k_K	the residue field;
q_K	the order $\lvert k_K\rvert$;
$\mathfrak{m}_K^n$	the subgroup $\varpi_K^n\mathcal{O}_K \subset K$ for any $n\in\mathbb{Z}$;
U_K^n	$1+\mathfrak{m}_K^n$ for $n\geqslant 1$, and $U_K^0=\mathcal{O}_K^\times$;
$\left(\frac{\cdot}{k_K}\right)$	the Legendre symbol on $k_K^\times$;
$(\cdot,\cdot)_K$	the quadratic Hilbert symbol on $K^\times\times K^\times$;
$\overline{K}$	an algebraic closure of K;
$\overline{k}_K$	the residue field of $\overline{K}$;
Γ_K	the group $\mathrm{Gal}(\overline{K}/K)$;
W_K	the Weil subgroup of Γ_K;
I_K	the inertia subgroup;
I_K^{w}	the wild inertia subgroup;
φ_K	a lift in W_K of the geometric Frobenius;
χ_{ur}	the unramified (cyclotomic) character $W_{\mathbb{Q}_p}\to\mathbb{C}^\times$ such that $\chi_{\mathrm{ur}}(\varphi_K)=q_K^{-1}$ for every finite $K/\mathbb{Q}_p$.

Given schemes X, S, S' as well as morphisms $X\to S$ and $S'\to S$, we will write $X_{S'}:=X\times_S S'$, and also $X_{R'}:=X\times_R R':=X_{S'}$ if $S'=\operatorname{Spec}R'$ and $S=\operatorname{Spec}R$ are affine.

1. Root numbers and explicit class field theory

Let $p>2$ be a prime number and let $K/\mathbb{Q}_p$ be a finite extension.

1.1. Additive characters. Let $\mathbb{S}^1$ denote the subgroup of complex numbers of absolute value 1. By an *additive character* we will mean a locally constant group homomorphism $\psi\colon K\to\mathbb{S}^1\subset\mathbb{C}^\times$. Let $n(\psi)$ denote the largest integer n such that ψ is trivial on $\mathfrak{m}_K^{-n}$. The group of additive characters will be denoted by $\mathrm{Hom}(K,\mathbb{C}^\times)$. The Pontryagin duality implies, in particular, that there exists a nontrivial additive character ψ. Due to Tate [Tat67, Lemma 2.2.1], the map $\Psi: x\mapsto\psi(x\,\cdot)$ defines an isomorphism $\Psi\colon K\cong\mathrm{Hom}(K,\mathbb{C}^\times)$ of topological K-vector spaces. We note that $n(\Psi(x))=n(\psi)+v_K(x)$. For every $m\in\mathbb{Z}$, the map Ψ induces an isomorphism

$$\Psi|_{\mathfrak{m}_K^m}\colon \mathfrak{m}_K^m\cong\mathrm{Hom}(K/\mathfrak{m}_K^{-m-n(\psi)},\mathbb{C}^\times). \tag{1.1.1}$$

For every integer $n\leqslant -m-n(\psi)$, since $\mathbb{C}^\times$ is divisible, the restriction map

$$\mathrm{res}_{n,m}\colon \mathrm{Hom}(K/\mathfrak{m}_K^{-m-n(\psi)},\mathbb{C}^\times)\twoheadrightarrow\mathrm{Hom}(\mathfrak{m}_K^n/\mathfrak{m}_K^{-m-n(\psi)},\mathbb{C}^\times)$$

is surjective. Composing $\Psi|_{\mathfrak{m}_K^m}$ with $\mathrm{res}_{n,m}$ induces an isomorphism (see, e.g., [Mar08, 2.9])

$$\Psi_{n,m}\colon \mathfrak{m}_K^m/\mathfrak{m}_K^{-n-n(\psi)}\cong\mathrm{Hom}(\mathfrak{m}_K^n/\mathfrak{m}_K^{-m-n(\psi)},\mathbb{C}^\times). \tag{1.1.2}$$

1.2. In order to simplify the computations of the root number we fix a particular additive character. We define ψ_k on $\mathcal{O}_K$ as the composition

$$\psi_k \colon \mathcal{O}_K \twoheadrightarrow k \xrightarrow{\mathrm{tr}_{k/\mathbb{F}_p}} \mathbb{Z}/p\mathbb{Z} \xhookrightarrow{\exp\left(\frac{2\pi i}{p}\cdot\right)} \mathbb{C}^\times.$$

We see that ψ_k is trivial on $\mathfrak{m}_K$. Since $\mathrm{tr}_{k/\mathbb{F}_p}$ is nontrivial, ψ_k is nontrivial. Using $\mathrm{res}_{0,-n(\psi)-1}$ we can non-uniquely extend ψ_k to an additive character of K, which we again denote by ψ_k. Independently on the choice of this extension we have $n(\psi_k) = -1$.

1.3. ψ-gauges of Weil characters. Let $\psi \colon K \to \mathbb{C}^\times$ be a fixed nontrivial additive character. Let $\chi \colon W_K \to \mathbb{C}^\times$ be a one-dimensional and ramified Weil representation, and let $a(\chi)$ denote its Artin conductor. Recall that χ induces a character of $K^\times$ via θ_K, and that $a(\chi)$ is the smallest integer a such that χ is trivial on U_K^a. Let

$$n := \left\lfloor \frac{a(\chi)+1}{2} \right\rfloor.$$

For $x \in \mathfrak{m}_K^n$, the map $x \mapsto \chi(1+x)$ is additive and is trivial on $\mathfrak{m}_K^{a(\chi)}$. We let

$$m := -a(\chi) - n(\psi).$$

The isomorphism $\Psi_{n,m}$ of (1.1.2) shows that there exists an element $c_\chi \in K$, called a *ψ-gauge of χ*, of exact valuation m, unique modulo $\mathfrak{m}_K^{-n-n(\psi)}$, such that for all $x \in \mathfrak{m}_K^n$,

$$\chi(1+x) = \psi(c_\chi x). \tag{1.3.1}$$

1.4. Epsilon factors of characters. In addition to the setting of 1.3, we fix a Haar mesure $\mathrm{d}x$ on K. We recall that the *ϵ-factor* of χ is defined as the integral

$$\epsilon(\chi, \psi, \mathrm{d}x) := \int_{\varpi_K^m \mathcal{O}_K^\times} \chi^{-1}(x)\psi(x)\,\mathrm{d}x. \tag{1.4.1}$$

We will be mainly interested in the *root number*

$$w(\chi, \psi) := \frac{\epsilon(\chi, \psi, \mathrm{d}x)}{|\epsilon(\chi, \psi, \mathrm{d}x)|},$$

which does not depend on $\mathrm{d}x$. For $a, b \in \mathbb{C}^\times$ we will write $a \approx b$ whenever ab^{-1} is contained in the multiplicative subgroup generated by strictly positive real numbers and the complex roots of unity of p-power orders. We note that if $p \neq 2$ and $a, b \in \{-1, 1\}$ are such that $a \approx b$, then $a = b$.

1.5. The group $\chi(I_K)$ is finite and cyclic, we denote its order by ep^r with e prime to p. We view the restriction $\chi|_{I_K}$ as a character of the group $\mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{ur}})$. The group $\ker(\chi|_{I_K})$ cuts out an abelian extension L'/K containing K^{ur}. The closure of the subgroup generated by φ_K in $\mathrm{Gal}(L'/K)$ cuts out a totally ramified abelian extension L/K, such that $L' = LK^{\mathrm{ur}}$. We then have canonical isomorphisms

$$\mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{ur}})\Big/_{\ker(\chi|_{I_K})} \cong \mathrm{Gal}(L'/K^{\mathrm{ur}}) \cong \mathrm{Gal}(L/K).$$

The restriction $\chi|_{I_K}$ induces a faithful complex character of the finite group $\mathrm{Gal}(L/K)$, and thus $\mathrm{Gal}(L/K)$ must be cyclic. Let M/K be the unique subextension of L/K of degree p^r. Then $\chi^e|_{I_K}$ has order p^r and induces a faithful character of the cyclic group $\mathrm{Gal}(M/K)$.

The following theorem is an amalgamation of some of the results of [Kob02] and [AS10].

THEOREM 1.6. *Let ψ_k be as in 1.2. Let $\chi\colon W_K \to \mathbb{C}^\times$ be a Weil character such that $|\chi(I_K^{\mathrm{w}})| = p$. Let $ep = |\chi(I_K)|$ with e prime to p. Let M/K be as in 1.5. We denote by $\sigma \in \mathrm{Gal}(M/K)$ the generator that is sent to $\exp(\frac{2\pi i}{p})$ via χ. Let ϖ_M be a uniformizer of M, and let $\delta_\chi := \mathcal{N}_{M/K}(1 - \frac{\sigma(\varpi_M)}{\varpi_M})$. Let us write $\delta_\chi = u\varpi_K^{v_K(\delta_\chi)}$ with $u \in \mathcal{O}_K^\times$, whose class in $k_K^\times$ we denote by $\overline{u}$.*

(1) *If $a(\chi)$ is even, then $\epsilon(\chi, \psi_k, \mathrm{d}x) \approx \chi(\delta_\chi)$;*
(2) *If $a(\chi)$ is odd, and $p \equiv 1 \bmod 4$, then*

$$\epsilon(\chi, \psi_k, \mathrm{d}x) \approx -\chi(\delta_\chi) \cdot \left(\frac{2\overline{u}}{k_K}\right) \cdot (-1)^{[k_K:\mathbb{F}_p]}.$$

LEMMA 1.7. *We have $v_K(\delta_\chi) = a(\chi) - 1$ and $c_\chi\delta_\chi \in U_K^1$. In particular, $\chi^{-1}(c_\chi) \approx \chi(\delta_\chi)$.*

PROOF. The lemma is essentially proved in [Kob02, p. 618]. We repeat Kobayashi's argument in our setting.

Let t be the largest integer such that the t-th ramification subgroup G_t of $\mathrm{Gal}(M/K)$ is nontrivial. We then have $G^t = G_t = \mathrm{Gal}(M/K)$ and $G^{t'} = \{1\}$ for $t' > t$, see [Ser79, V.§3]. The reciprocity map (see [Ser79, XV.§2]) and χ induce a commutative diagram

$$\begin{array}{ccccc} U_K^t\Big/U_K^{t+1}\mathcal{N}_{M/K}(U_M^t) & \xrightarrow{\sim} & G^t = \mathrm{Gal}(M/K) & \xrightarrow{\chi^e|_{I_K}} & \mathbb{C}^\times \\ \uparrow & & \uparrow & & \uparrow{\scriptstyle z\mapsto z^e} \\ U_K^t & \hookrightarrow & \mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{ur}}) & \xrightarrow{\chi|_{I_K}} & \mathbb{C}^\times. \end{array} \tag{1.7.1}$$

As e is prime to p we observe that $a(\chi) = a(\chi^e)$ and that $a(\chi^e) = t + 1$ by the diagram. Since $\sigma \in G_t \setminus G_{t+1}$, by using [Ser79, IV.Prop. 5] we obtain

$$v_K(\delta_\chi) = v_M\left(1 - \frac{\sigma(\varpi_M)}{\varpi_M}\right) = t = a(\chi) - 1. \tag{1.7.2}$$

Applying [Ser79, XV.§3, Exercise 1] shows that for all $v \in U_K^{a(\chi)-1}$,

$$\theta_{M/K}(v) = \sigma^{\mathrm{tr}_{k_K/\mathbb{F}_p}((v-1)/\delta_\chi \bmod \mathfrak{m}_K)}. \tag{1.7.3}$$

For every $x \in \mathfrak{m}_K^{a(\chi)-1} \subseteq \mathfrak{m}_K^n$, taking the image of (1.7.3) by χ^e, we obtain $\chi^e(1+x) = \psi_k(e\delta_\chi^{-1}x)$. Taking the e-th power of (1.3.1) gives $\chi^e(1+x) = \psi_k(ec_\chi x)$. We note that $e\delta_\chi^{-1}\mathfrak{m}_K^{a(\chi)-1} = \mathfrak{O}_K$, and therefore,

$$\psi_k((1-\delta_\chi c_\chi)\mathfrak{O}_K) = \psi_k((e\delta_\chi^{-1} - ec_\chi)\mathfrak{m}_K^{a(\chi)-1}) = 1.$$

Since $n(\psi_k) = -1$, we must have $1 - \delta_\chi c_\chi \in \mathfrak{m}_K$. The last part of the lemma follows from the fact that $\chi(U_K^1)$ is a finite p-group. □

Proof of Theorem 1.6. We wish to apply [AS10, Prop. 8.7, (ii)] which allows to express the epsilon factor using a refined ψ_k-gauge c of χ. Abbes–Saito proves that there exists an element $c \in K$, unique modulo $\mathfrak{m}_K^{-n+1}$, such that for every $x \in \mathfrak{m}_K^{a(\chi)-n}$ we have

$$\chi\left(1 + x + \tfrac{x^2}{2}\right) = \psi_k(cx).$$

Let $\tau\colon k_K \to K$ be the Teichmüler lift. We consider the quadratic Gauss sum

$$G_{\psi_k} := \sum_{x \in k_K} \psi_k(\tau(x)^2).$$

The formulas $G_{\psi_k} = \sum_{x \in k_K^\times} \left(\frac{x}{k_K}\right)\psi_k(\tau(x))$ and $G_{\psi_k}^2 = \left(\frac{-1}{k_K}\right)q_K$ are well-known (see, e.g., [BEW98, §1.1]). The Abbes–Saito formula [AS10, (8.7.3)] can be rewritten as

$$\epsilon(\chi, \psi_k, \mathrm{d}x) \approx \chi^{-1}(c)\psi_k(c)\left(\frac{-1}{k_K}\right)^{\binom{a(\chi)}{2}} G_{\psi_k}^{-a(\chi)} \times \begin{cases} 1 & \text{if } a(\chi) \text{ is even,} \\ (-2c, \varpi_K)_K & \text{if } a(\chi) \text{ is odd.} \end{cases} \tag{1.7.4}$$

Since c is also a ψ_k-gauge of χ, we have $\chi^{-1}(c) \approx \chi(\delta_\chi)$ by Lemma 1.7. For $r \in \mathbb{Z}$ large enough, $\psi_k(p^r c) = 1$, so $\psi_k(c) \approx 1$. If $a(\chi)$ is even, then it is straightforward to verify that $\epsilon(\chi, \psi_k, \mathrm{d}x) \approx \chi(\delta_\chi)$, thus (1) holds.

We assume the hypotheses of (2). Then $\left(\frac{-1}{k_K}\right) = 1$, and $G_{\psi_k} \approx -(-1)^{[k_K:\mathbb{F}_p]}$, see [BEW98, Thm. 11.5.4]. We also have $(-2, \varpi_K)_K = \left(\frac{2}{k_K}\right)$. Taking into account Lemma 1.7 and making the relevant substitutions into (1.7.4) we are left to prove that $(c, \varpi_K)_K = \left(\frac{\overline{u}}{k_K}\right)$. Lemma 1.7 also shows that $c \in u^{-1}\varpi_K^{-a(\chi)+1}U_K^1$. Since $a(\chi)$ is odd and U_K^1 is pro-p, the Hilbert symbol is trivial on $\varpi_K^{-a(\chi)+1}U_K^1$, thus

$$(c, \varpi_K)_K = (u, \varpi_K)_K = \left(\frac{\overline{u}}{k_K}\right).$$ □

Proposition 1.8. *We continue in the situation of Theorem 1.6. Let $\alpha \in \mathfrak{O}_M$ be such that $p \nmid v_M(\alpha)$, and let $D_\alpha := \mathcal{N}_{M/K}\left(1 - \frac{\sigma(\alpha)}{\alpha}\right)$. Then*

$$D_\alpha \equiv v_M(\alpha)\delta_\chi \bmod U_K^1.$$

PROOF. Kobayashi [Kob02, p. 614] gave a proof in the case $p = 3$, which can be generalized for a general $p > 2$ without significant modifications as follows. We write $\alpha = \varpi_M^{v_M(\alpha)} x$ for some $x \in \mathcal{O}_M^\times$. By definition of the group G_t, we have $\frac{\sigma(x)}{x} \in U_M^{t+1}$. It follows from (1.7.2) that there exists a $y \in \mathcal{O}_M^\times$ such that $\frac{\sigma(\varpi_M)}{\varpi_M} = 1 + \varpi_M^t y$. Taking the latter to the power $v_K(\alpha)$ gives

$$\Big(\frac{\sigma(\varpi_M)}{\varpi_M}\Big)^{v_M(\alpha)} \equiv 1 + v_M(\alpha)\varpi_M^t y \bmod \mathfrak{m}_M^{t+1},$$

and then after multiplying by $\frac{\sigma(x)}{x}$ we obtain

$$\frac{\sigma(\alpha)}{\alpha} \equiv 1 + v_M(\alpha)\varpi_M^t y \bmod \mathfrak{m}_M^{t+1}. \tag{1.8.1}$$

By using that $v_M(\alpha)y \in \mathcal{O}_M^\times$ we rewrite (1.8.1) multiplicatively as

$$1 - \frac{\sigma(\alpha)}{\alpha} \equiv v_M(\alpha)\Big(1 - \frac{\sigma(\varpi_M)}{\varpi_M}\Big) \bmod U_M^1.$$

Taking the norm of the latter we obtain $D_\alpha \equiv v_M(\alpha)^p \delta_\chi \bmod U_K^1$. We finish the proof by noting that $v_M(\alpha)^{p-1} \in 1 + p\mathcal{O}_K \subset U_K^1$. □

COROLLARY 1.9. *If $a(\chi)$ is even and $\alpha \in \mathcal{O}_M$ is such that $p \nmid v_M(\alpha)$, then*

$$\epsilon(\chi, \psi_k, \mathrm{d}x) \approx \chi\left(\frac{D_\alpha}{v_M(\alpha)}\right).$$

PROOF. Follows from Thm. 1.6.(1) and Prop. 1.8. □

2. Conductors and discriminants of curves of genus 2

2.1. The base setting. Let K be a p-adic local field with $p \neq 2$, and let C/K be a smooth, projective, and geometrically connected curve of genus 2 defined over K.

2.2. Generalities. Since the curve C/K is hyperelliptic (see [Liu02, 7. Prop. 4.9]), there exists a non-empty open affine K-subscheme C_{aff} of C which is defined by a single Weierstrass equation

$$Y^2 = P(X), \tag{2.2.1}$$

where $P \in K[X]$ has simple roots and $\deg P$ is 5 or 6.

The differentials $w_0 = \frac{\mathrm{d}X}{2Y}$, $w_1 = \frac{X\,\mathrm{d}X}{2Y} \in H^0(C_{\mathrm{aff}}, \Omega^1_{C/K})$ extend to C and define a K-basis of $H^0(C, \Omega^1_{C/K})$.

We define the *discriminant* of an equation (2.2.1) in terms of the discriminant of the polynomial P : let a_0 be the leading coefficient of $4P$, then (following [Liu96, §2])

$$\Delta(P) := \begin{cases} 2^{-12}\operatorname{disc}(4P) & \text{if } \deg P = 6, \\ 2^{-12}a_0^2 \operatorname{disc}(4P) & \text{if } \deg P = 5. \end{cases} \tag{2.2.2}$$

In particular, if $P(X) = (X-\alpha_1)(X-\alpha_2)(X-\alpha_3)(X-\alpha_4)(X-\alpha_5)$, then

$$\Delta(P) = 2^8 \prod_{1\leqslant i<j\leqslant 5} (\alpha_i - \alpha_j)^2. \tag{2.2.3}$$

We note that since C is non-singular, $\Delta(P) \neq 0$.

The equation (2.2.1) is unique up to a change of variables

$$X' = \frac{aX+b}{cX+d}, \qquad Y' = \frac{eY}{(cX+d)^3} \tag{2.2.4}$$

where $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(K)$ and $e \in K^\times$.

If $Y'^2 = P'(X')$ is the equation obtained from (2.2.1) via (2.2.4), then the new differentials w_0' and w_1' satisfy

$$\begin{pmatrix} w_0' \\ w_1' \end{pmatrix} = e^{-1} \begin{vmatrix} a & b \\ c & d \end{vmatrix} \begin{pmatrix} d & c \\ b & a \end{pmatrix} \begin{pmatrix} w_0 \\ w_1 \end{pmatrix},$$

and the new discriminant is

$$\Delta(P') = e^{20} \begin{vmatrix} a & b \\ c & d \end{vmatrix}^{-30} \Delta(P)\,. \tag{2.2.5}$$

As an immediate consequence, the class of a discriminant in $K^\times/(K^\times)^2$ does not depend on the choice of Weiserstrass equation.

2.3. Minimal equation. Let $\mathscr{C}/\mathfrak{O}_K$ be the minimal regular (integral, proper, and flat) model of C/K. In fact, $\mathscr{C}$ is a projective $\mathfrak{O}_K$-scheme (see [Stacks, Tag 0C5P]). It follows that the dualizing sheaf $\omega_{\mathscr{C}/\mathfrak{O}_K}$ is isomorphic to the canonical sheaf of $\mathscr{C}/\mathfrak{O}_K$ (see [Liu02, 6. Thm. 4.32]) and, in particular, is invertible. Since C/K is smooth we have $\omega_{\mathscr{C}/\mathfrak{O}_K}|_C \cong \Omega^1_{C/K}$. Since $\mathscr{C}$ is integral and $\omega_{\mathscr{C}/\mathfrak{O}_K}$ is torsion-free, restricting sections induces an injection

$$H^0(\mathscr{C}, \omega_{\mathscr{C}/\mathfrak{O}_K}) \hookrightarrow H^0(C, \Omega^1_{C/K}).$$

We note that $H^0(C, \Omega^1_{C/K})$ is a K-vector space of dimension two and that $H^0(\mathscr{C}, \omega_{\mathscr{C}/\mathfrak{O}_K})$ is a free $\mathfrak{O}_K$-module of rank two.

A hyperelliptic equation (2.2.1) will be called *minimal* if the associated differential forms w_0, w_1 extend to $\mathscr{C}$ and define an $\mathfrak{O}_K$-basis of $H^0(\mathscr{C}, \omega_{\mathscr{C}/\mathfrak{O}_K})$. The resulting discriminant $\Delta_{\min}$ will be called minimal. It is proven in [Liu94a, Prop. 2] that a minimal equation exists and is unique up to a transformation given by (2.2.4) with $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathfrak{O}_K)$ and $e \in \mathfrak{O}_K^\times$. We note that although $\Delta_{\min}$ depends on the choice the minimal equation, its valuation $v_K(\Delta_{\min})$ does not.

REMARK 2.4. A minimal equation need not have coefficients in $\mathcal{O}_K$ and, contrary to the case of elliptic curves, there might not exist a minimal equation with integral coefficients.

2.5. Conductors. Let C/K be a smooth, projective, and geometrically connected curve of some genus $g \geqslant 1$ and let $\mathscr{C}/\mathcal{O}_K$ be its minimal regular model. In this section χ will denote the Euler-Poincaré characteristic relative to ℓ-adic cohomology. Let $\mathrm{sw}(\rho_\ell)$ (resp. $a(\rho_\ell)$) denote the Swan (resp. Artin) conductor of the ℓ-adic Γ_K-representation ρ_ℓ on $H^1(C_{\overline{K}}, \mathbb{Q}_\ell)$. We define

$$\mathrm{Art}(\mathscr{C}/\mathcal{O}_K) := \chi(C_{\overline{K}}) - \chi(\mathscr{C}_{\overline{k}_K}) - \mathrm{sw}(\rho_\ell).$$

If $m(C/K)$ denotes the number of irreducible components of $\mathscr{C}_{\overline{k}_K}$, then by [Liu94a, Prop. 1] we have

$$-\mathrm{Art}(\mathscr{C}/\mathcal{O}_K) = a(\rho_\ell) + m(C/K) - 1. \tag{2.5.1}$$

There exists a different notion of the conductor. Let $h\colon \mathscr{C} \to \operatorname{Spec} \mathcal{O}_K$ denote the structural morphism. Given an invertible sheaf $\mathscr{F}$ on $\mathscr{C}$ we will use the construction $\det(Rh_*\mathscr{F})$, which produces an invertible sheaf on $\operatorname{Spec} \mathcal{O}_K$, see [KM76, p. 46] for details. The $\mathcal{O}_K$-modules of global sections

$$M := H^0\big(\det(Rh_*(\omega_{\mathscr{C}/\mathcal{O}_K}^{\otimes 2}))\big) \quad \text{and} \quad N := H^0\big((\det(Rh_*(\omega_{\mathscr{C}/\mathcal{O}_K})))^{\otimes 13}\big)$$

are free of rank 1. Since h is smooth on C over K, due to Deligne [Del85], there exists a canonical isomorphism

$$\det(Rh_*(\omega_{C/K}^{\otimes 2})) \cong (\det(Rh_*(\omega_{C/K})))^{\otimes 13}. \tag{2.5.2}$$

The construction $\det(Rh_*)$ commutes with flat base change by [Har77, III.9.3], so (2.5.2) induces a canonical K-linear isomorphism $i\colon M \otimes_{\mathcal{O}_K} K \cong N \otimes_{\mathcal{O}_K} K$. It follows that there exists an integer $\operatorname{ord} \Delta_{\mathscr{C}/\mathcal{O}_K} := n$ such that $i(M) = \varpi_K^n N$.

Saito [Sai88] has proved that, in fact,

$$-\mathrm{Art}(\mathscr{C}/\mathcal{O}_K) = \operatorname{ord} \Delta_{\mathscr{C}/\mathcal{O}_K}, \tag{2.5.3}$$

which generalizes Ogg's formula for elliptic curves (see also [Liu98]).

2.6. Difference between the minimal discriminant and the conductor. Let C/K be a hyperelliptic curve. A natural question is how the invariants of (2.5.3) compare to $v_K(\Delta_{\min})$ from 2.3. Their difference was described in purely geometric terms by Liu [Liu94a] as follows. Let $\mathscr{C}_{k_K}$ denote the special fiber of $\mathscr{C}$, and let $\pi\colon \mathscr{C} \to \mathscr{Y}$ be the contraction of those irreducible components D of $\mathscr{C}_{k_K}$ which satisfy $\deg(\omega_{\mathscr{C}/\mathcal{O}_K}|_D) = 0$. Liu shows that $\mathscr{Y}/\mathcal{O}_K$ is a projective normal model of C/K. The hyperelliptic involution of C/K extends to $\mathscr{C}/\mathcal{O}_K$ and induces an involution j on $\mathscr{Y}/\mathcal{O}_K$. The quotient scheme $\mathscr{P} := \mathscr{Y}/\langle j \rangle$ is a normal proper model of $\mathbb{P}^1_K$, we let $\widetilde{\mathscr{P}} \to \mathscr{P}$ be its minimal

desingularization. Let d denote the number of irreducible components of the geometric fiber $\widetilde{\mathcal{P}}_{\overline{k}_K}$. Then [Liu94a, Thm. 1] affirms that d is odd and that

$$v(\Delta_{\min}) = -\operatorname{Art}(\mathscr{C}/\mathfrak{O}_K) + \frac{d-1}{2}. \tag{2.6.1}$$

3. Wild ramification for Jacobian surfaces

Let C/K be as in 2.1. We denote by $J(C)/K$ the associated Jacobian variety of dimension 2. Let $\mathscr{J}(C/K)/\mathfrak{O}_K$ denote its Néron model, and let $\mathscr{J}(C/K)^\circ$ be the indentity component of $\mathscr{J}(C/K)$. Let $\ell \neq p$ be a prime number. We have an isomorphism of ℓ-adic Γ_K-representations

$$H^1_{\text{ét}}(C_{\overline{K}}, \mathbb{Q}_\ell) \cong H^1_{\text{ét}}(J(C)_{\overline{K}}, \mathbb{Q}_\ell),$$

we denote either of them by ρ_ℓ. The main aim of this chapter is to produce a formula for the root number $w(C/K) := w(\rho_\ell)$, which is defined via the the complex Weil–Deligne representation associated to ρ_ℓ (see, e.g., [Roh94]).

Let $ab(C/K)$, $t(C/K)$, and $u(C/K)$ denote the abelian, toric, and unipotent ranks of the special fiber $\mathscr{J}(C/K)^\circ_{k_K}$, respectively. We have

$$ab(C/K) + t(C/K) + u(C/K) = 2.$$

3.1. Stable reduction. In order to compare the reduction of a curve and of its Jacobian we recall some results of [DM69, §2]. Every smooth projective geometrically connected curve C/K of genus $g \geqslant 2$ has potentially semi-stable reduction, i.e., there exists a finite extension L/K such that one of the following equivalent conditions holds:

(1) the minimal regular model $\mathscr{C}'/\mathfrak{O}_L$ of C_L/L has semi-stable geometric special fiber—the curve $\mathscr{C}'_{\overline{k}_L}$ is reduced and its singular points are ordinary double points;
(2) the canonical model $\mathscr{C}'_{\text{can}}/\mathfrak{O}_L$ of C_L/L (which is obtained by contracting the "(-2)-curves" of $\mathscr{C}'/\mathfrak{O}_L$) has stable geometric special fiber—the curve $(\mathscr{C}'_{\text{can}})_{\overline{k}_L}$ is semi-stable and its components isomorphic to $\mathbb{P}^1$ each intersect other irreducible components at at least 3 points;
(3) $u(C_L/L) = 0$;
(4) the representation $\rho_\ell|_{I_L}$ is unipotent.

If C_L/L has semi-stable reduction, then the $\mathfrak{O}_L$-scheme $\mathscr{J}(C_L/L)^\circ$ represents the relative Picard functor $\operatorname{Pic}^0_{\mathscr{C}'/\mathfrak{O}_L}$ (see [BLR90, Cor. 2, p. 287]).

3.2. Potentially good wild reduction hypothesis. Sabitova's decomposition [Sab07, Prop. 1.10] allows to separate the contributions to $w(C/K)$ coming from the abelian and toric parts of $\mathscr{J}(C_L/L)^\circ_{k_L}$. We suppose that $ab(C_L/L) = 2$, or, in other words, that $J(C)/K$ has potentially good reduction. This happens exactly when $\rho_\ell(I_K)$ is finite. In this case we write $|\rho_\ell(I_K)| = ep^r$ with e coprime to p. We further suppose that $r \geqslant 1$, i.e., ρ_ℓ is wildly ramified. Due to Serre–Tate [ST68, p. 497, Cor. 2], necessarily $p \leqslant 5$.

3.3. Inertially minimal extensions. It follows from the Néron–Ogg–Shafarevich criterion that $J(C)$ attains good reduction over $L' := \overline{K}^{\ker \rho_\ell|_{I_K}}$ and that L'/K^{ur} is the minimal such extension. We call an algebraic extension L/K *inertially minimal (IM) for* $J(C)/K$ if $I_L = \ker \rho_\ell|_{I_K}$. In other words, L/K is IM if and only if $J(C)$ has good reduction over L and has bad reduction over every proper subextension of $K^{\mathrm{ur}}L/K^{\mathrm{ur}}$.

3.4. Good reduction and torsion. For $m \geqslant 1$ we denote by $J(C)[m]$ the subgroup of m-torsion points of $J(C)(\overline{K})$ and by $K(J(C)[m])$ the smallest extension of K over which all the points of $J(C)[m]$ are rational. For $m \geqslant 3$ coprime to p, it follows from Serre–Tate [ST68, Cor. 3, p. 498] that the extension $K(J(C)[m])/K$ is IM for $J(C)/K$. Similarly, for $p \neq 2$, Serre [Ser61] shows that $|\rho_\ell(I_{K(J(C)[2])})| \leqslant 2$. Thus, if $K(J(C)[2])/K$ is not an IM extension, then there is a totally ramified quadratic extension $L/K(J(C)[2])$ such that L/K is IM for $J(C)/K$. Therefore, if $p \neq 2$, then the groups $\rho_\ell(I_K^{\mathrm{w}})$ and $I^{\mathrm{w}}(K(J(C)[2])/K)$ are isomorphic.

3.5. Possible inertia actions. It follows from the Silverberg–Zarhin classification [SZ05, Thm. 1.7] that if $J(C)/K$ has potentially good reduction and if ρ_ℓ is wildly ramified, then $\rho_\ell(I_K)$ is isomorphic to a group (in the notation of [GN]) from the following lists.

a) If $p = 3$, the list is $\{C_3, C_6, C_{12}, C_3 \times C_3, C_3 \times C_6, S_3, C_3 \times S_3, \mathrm{Dic}_3, C_3 \times \mathrm{Dic}_3, C_3 \rtimes C_8, C_3^2 \rtimes C_4, C_3^2 \rtimes_2 C_8\}$.
b) If $p = 5$, the list is $\{C_5, C_{10}, \mathrm{Dic}_5, C_5 \rtimes C_8\}$.

For $p = 5$ each possible group has the form $C_5 \rtimes C_{2^i}$ where C_{2^i} is a subgroup of C_8 acting on C_5 with kernel $C_2 \cap C_{2^i} \subset C_8$. We note that $C_5 \subset C_{10} \subset \mathrm{Dic}_5 \subset C_5 \rtimes C_8$ and that each inclusion is strict and unique.

Recall that the Frobenius group is $F_5 = C_5 \rtimes C_4$ where C_4 acts faithfully on C_5. In particular, F_5 and Dic_5 are not isomorphic.

3.6. We suppose from now that K is 5-adic. It follows immediately from 3.5 that $\rho_\ell(I_K^{\mathrm{w}})$ is cyclic of order 5.

Proposition 3.7. *Let L/K be a finite extension. Under the hypotheses of 3.2 and 3.6, if $J(C)$ has semi-abelian reduction over L, i.e., $u(C_L/L) = 0$, then C has good reduction over L, i.e., the minimal regular model $\mathscr{C}'/\mathcal{O}_L$ is smooth.*

Proof. From 3.1 we see that $(\mathscr{C}'_{\mathrm{can}})_{\overline{k}_L}$ is a stable curve. The ring $R := \mathcal{O}_{K^{\mathrm{ur}}L}$ is strictly Henselian and the canonical model of $C_{K^{\mathrm{ur}}L}/K^{\mathrm{ur}}L$ is canonically isomorphic to $(\mathscr{C}'_{\mathrm{can}})_R$. Wild ramification of ρ_ℓ implies that 5 divides $[K^{\mathrm{ur}}L : K^{\mathrm{ur}}]$. By studying the possible orders of automorphisms of stable curves Liu [Liu93, Cor. 4.1.(4)] shows that $(\mathscr{C}'_{\mathrm{can}})_{\overline{k}_L}/\overline{k}_L$ must be smooth. It follows that $(\mathscr{C}'_{\mathrm{can}})_R/R$ and hence $\mathscr{C}'_{\mathrm{can}}/\mathcal{O}_L$ are smooth. We may use [Liu02, 10. Prop. 1.21] to conclude that $\mathscr{C}'/\mathcal{O}_L$ is smooth. □

REMARK 3.8. The hypotheses that ρ_ℓ is wildly ramified and that K is 5-adic are essential. The curve C_L/L might have bad reduction even if $J(C)$ has good reduction over L. On the other hand, [BLR90, Example 8, p. 246] shows that the non-rational irreducible components of $\mathscr{C}'_{\overline{k}_L}$ correspond to non-trivial abelian varieties as quotients of $\mathscr{J}(C_L/L)^\circ_{\overline{k}_L}$. Using this it can be shown in general that if $\mathscr{J}(C_L/L)^\circ_{\overline{k}_L}$ is a simple abelian variety, then C_L/L has good reduction.

3.9. An explicit IM extension. Let $Y^2 = P(X)$ be a hyperelliptic equation defining C/K. Generalizing the results of Kraus [Kra90], Liu [Liu94b, §5.1] provides an explicit description in terms of invariants of P of the tame part of the minimal extension L'/K^{ur} over which C has stable reduction. By Prop. 3.7, this extension is precisely the IM extension for $J(C)/K$ defined in 3.3. The discriminant $\Delta(P)$ (as defined by (2.2.2)) is equal to the Igusa invariant J_{10}. Let A_5 denote one the so-called affine invariants (see [Liu94b, §2.1] for the definition) of P. After Prop. 3.17 we will always have $A_5 = 1$. We fix an 8th root of

$$\beta := -A_5^{-6}\Delta(P)$$

in $\overline{K}$, which we denote by $\beta^{1/8}$. Let $L'_{\mathrm{t}}/K^{\mathrm{ur}}$ be the maximal tamely ramified subextension of L'/K^{ur}, then L'/L'_{t} is totally wildly ramified of degree 5. Liu proves that

$$L'_{\mathrm{t}} = K^{\mathrm{ur}}(\beta^{1/8}).$$

Let $\nu := v_K(\beta)$, $M := K(J(C)[2])$, $N := K\left(\beta^{1/8}\right)$, $H := K\left(\beta^{1/4}\right)$, and $L := MN$. We fix a primitive 8th root of unity $\zeta_8 \in \overline{K}$.

Let us recall from [Mum84, 3.39, Cor. 2.11] that M is the splitting field of P. The extension M/K is finite Galois, while L/K is finite but not necessarily Galois.

LEMMA 3.10. *The extension L/H is Galois.*

PROOF. The compositum of N/H and HM/H is L/H. Since $[N : H] \leqslant 2$, the extension N/H is Galois. Since M/K is Galois, so is HM/H. □

PROPOSITION 3.11. *The extension L/K is inertially minimal for $J(C)/K$. The extension $L(\zeta_8)/K$ is Galois. In particular, L/K is a Galois extension if the residual degree $f(K/\mathbb{Q}_5)$ is even.*

PROOF. Combining 3.4 with 3.9 shows that L' contains LK^{ur}. Also, from 3.4 we have $|\rho_\ell(I_M)| \leqslant 2$, so $\rho_\ell|_{\Gamma_M}$ is at most tamely ramified. It now follows from 3.9 that $J(C)$ has good reduction over LK^{ur}. We conclude that $LK^{\mathrm{ur}} = L'$, and thus L/K is IM.

The Galois closure of N/K is $N(\zeta_8)$. It follows that $L(\zeta_8)/K$ is Galois. The field $\mathbb{Q}_5$ already contains all the 4th roots of unity, so its quadratic unramified extension is $\mathbb{Q}_5(\zeta_8)$. If $f(K/\mathbb{Q}_5)$ is even, then K contains ζ_8, so $L = L(\zeta_8)$ is Galois over K. □

PROPOSITION 3.12. *The group* $\mathrm{Gal}(M/K)$ *is isomorphic to a subgroup of* F_5 *(as in 3.5). As a consequence, the polynomial* P *has an irreducible factor over* K *of degree 5.*

PROOF. We recall that $\deg P = 5$ or 6, so we may view $\mathrm{Gal}(M/K) = \mathrm{Gal}(P)$ as a subgroup of S_5 or S_6, respectively. Since the wild inertia subgroup of $\mathrm{Gal}(P)$ is normal of order 5, the group $\mathrm{Gal}(P)$ must be a subgroup of a normalizer subgroup G of a 5-cycle in S_5 or S_6. We naturally have $F_5 \subseteq G$ and, in fact, an equality holds because for $n = 5, 6$ we have

$$|G| = \frac{|S_n|}{\#\{\text{5-Sylow's in } S_n\}} = \frac{n!}{\frac{n!}{4\cdot 5\cdot (n-5)!}} = 20.$$

If P was irreducible over K and had degree 6, then $\mathrm{Gal}(P)$ would have a subgroup of index 6, which is impossible. On the other hand, since $\mathrm{Gal}(P)$ contains a 5-cycle, P must have an irreducible factor of degree at least 5. □

PROPOSITION 3.13. *The group* $\rho_\ell(I_K)$ *is isomorphic to* $C_5 \rtimes C_8$, Dic_5, C_{10}, *or* C_5 *if and only if* $\nu \equiv 1 \bmod 2$, $\nu \equiv 2 \bmod 4$, $\nu \equiv 4 \bmod 8$, *or* $\nu \equiv 0 \bmod 8$, *respectively. In particular, if* $e(L/K)$ *denotes the ramification index of* L/K, *then* $40 \mid e(L/K)\cdot\nu$.

PROOF. By 3.9 and Prop. 3.11, the tame ramification index of L/K is determined by the residue $\nu \bmod 8$ and is exactly the maximal prime-to-5 divisor of $|\rho_\ell(I_K)|$. The group $\rho_\ell(I_K)$ can then be identified from the list 3.5.b). □

LEMMA 3.14. *Every extension* F/K *of ramification index* 2 *is abelian.*

PROOF. For any uniformiser $\varpi_K \in K$ we have $F \subset K^{\mathrm{ur}}(\sqrt{\varpi_K})$. The extension $K^{\mathrm{ur}}(\sqrt{\varpi_K})/K$ is abelian as a compositum of two abelian extensions $K(\sqrt{\varpi_K})/K$ and K^{ur}/K. Thus, F/K is also abelian. □

PROPOSITION 3.15. *Let* $\sigma \in I_K^{\mathrm{w}}$ *and let* $\tau \in \Gamma_K$ *denote a lift of a topological generator of the tame inertia group* I_K^{t}. *Let* $\varphi_L \in \Gamma_L$ *and* $\varphi_{L(\zeta_8)} \in \Gamma_{L(\zeta_8)}$ *be lifts of the geometric Frobenii. Then:*

(1) *The images* $\rho_\ell(\sigma)$, $\rho_\ell(\tau^4)$, *and* $\rho_\ell(\varphi_L)$ *commute;*
(2) *The images* $\rho_\ell(\tau)$ *and* $\rho_\ell(\varphi_{L(\zeta_8)})$ *commute.*

In particular, $\rho_\ell(\varphi_{L(\zeta_8)})$ *is central in* $\mathrm{Im}(\rho_\ell)$.

PROOF. Recall from Prop. 3.11 that $\rho|_{I_L}$ is trivial and $L' = LK^{\mathrm{ur}}$. Thus, for (1) we only need to show that the classes σI_L, $\tau^4 I_L$, and $\varphi_L I_L$ in $\mathrm{Gal}(L'/K) = \Gamma_K/I_L$ commute. From 3.5 we have $\sigma^5 \in I_L$ and $\tau^8 \in I_L$. We note that the subfield of L' fixed by $\varphi_L I_L$ is L.

Let F/K be the subextension of M/K fixed by the unique 5-Sylow subgroup of $\mathrm{Gal}(M/K)$. By Prop. 3.12, $[F : K]$ divides 4. We claim that L/F is abelian. We observe that L/F is the compositum of the cyclic extension M/F and the maximal at most tamely ramified subextension L_t/F of L/F. By 3.4,

the ramification index of L_t/F is at most 2, and therefore L_t/F is abelian by Lemma 3.14. It follows that L/F is abelian. The extension L'/F is abelian as the compositum of L/F and $K^{\mathrm{ur}}F/F$.

We observe that the closure of the subgroup generated by $\tau^4 I_K^{\mathrm{w}}$ in I_K cuts out the unique extension of K^{ur} of degree 4, which contains F. Thus, the class $\tau^4 I_L$ is in $\mathrm{Gal}(L'/F)$. On the other hand, σI_L and $\varphi_L I_L$ are also in $\mathrm{Gal}(L'/F)$, so they all commute.

For (2) we first note that, for $\gamma \in I_K$, we have $\eta := \gamma\varphi_{L(\zeta_8)}\gamma^{-1}\varphi_{L(\zeta_8)}^{-1} \in I_K$. Since $L(\zeta_8)/K$ is Galois by Prop. 3.11, we have $\gamma\varphi_{L(\zeta_8)}\gamma^{-1} \in \Gamma_{L(\zeta_8)}$, and thus $\eta \in \Gamma_{L(\zeta_8)} \cap I_K = I_L$. Then $\rho_\ell(\eta)$ is trivial, hence (2) holds. □

3.16. Particular form of hyperelliptic equation. If $\deg P = 6$, then Prop. 3.12 shows that P has a root in K. By applying a change of variables (2.2.4) that sends this root to the point at infinity, we may assume that the curve C/K is defined by a Weierstrass equation $Y^2 = P(X)$ with P irreducible of degree 5. By applying another change of variables, we obtain the following result, which is a slight reformulation of [Liu94b, Prop. 5.1].

Proposition 3.17 (Liu). *There exists an equation*

$$Y^2 = P(X) = X^5 + a_2X^4 + \ldots + a_6,$$

which defines C/K with $a_2, \ldots, a_6 \in \mathcal{O}_K$ such that $v_K(a_6) \in \{1, 2, 3, 4, 6, 7, 8, 9\}$. The integer $v_K(a_6)$ determines the Namikawa–Ueno (NU) type of the minimal regular model $\mathscr{C}/\mathcal{O}_K$ (see [NU73]) as in Table 2. With respect to this equation, $A_5 = 1$.

Proof. We start with an equation $Y^2 = P(X)$ with $P \in K[X]$ of degree 5 as in 3.16. The output of [Liu94b, Algorithme, p. 150] is an equation $Y^2 = P_1(X)$ from which the NU type can be determined by manually computing the blow-ups and normalizations needed to produce the minimal regular model of C/K (a more systematic approach will be described in III.2). The NU type is completely described by the integer $v_K(P_1(0))$. The equation $Y^2 = P_1(X)$ satisfies all the conditions demanded in our proposition except the leading coefficient $a_1 \in \mathcal{O}_K^\times$ of P_1 is not necessarily 1. This can be dealt with by applying another change of variables $X = a_1X'$, $Y = a_1^3Y'$, which does not change the valuations of the coefficients of the equation. The invariant A_5 can be determined via [Liu94b, (5), p. 139]. □

3.18. Ogg and Namikawa–Ueno types. Each possible value of $v_K(a_6)$ from Prop. 3.17 corresponds to a row in Table 2. We convert the Namikawa–Ueno [NU73] notation to the one used in [Ogg66] and then apply the results from [Liu94a, §5.2] to complete every column of Table 2 except the last one (see 2.5 and 2.6 for the notation).

TABLE 2. Geometric reduction types

$v_K(a_6)$	NU type	Ogg type	$m(C/K)$	$\mathscr{P}_{\overline{k}_K}$	d	$v_K(\Delta_{\min}) - a(\rho_\ell)$
1	[VIII-1]	[0]	1	$\mathbb{P}^1$	1	0
3	[VIII-2]	[7]	9	$\mathbb{P}^1$	1	8
7	[VIII-3]	[16]	4	$2\mathbb{P}^1$	3	4
9	[VIII-4]	[20]	13	$\mathbb{P}^1$	1	12
2	[IX-1]	[8]	5	$\mathbb{P}^1$	1	4
4	[IX-2]	[36]	3	$\mathbb{P}^1$	1	2
6	[IX-3]	[21]	11	$\mathbb{P}^1$	1	10
8	[IX-4]	[44]	9	$\mathbb{P}^1$	1	8

COROLLARY 3.19. *We have*

$$v_K(\Delta_{\min}) - a(\rho_\ell) = m(C/K) + \frac{d-3}{2}.$$

In particular, $v_K(\Delta_{\min}) - a(\rho_\ell)$ is positive and even.

PROOF. The formula is obtained by combining (2.5.1) and (2.6.1). The quantities on the right-hand side of the equation can be read from Table 2. □

REMARK 3.20. The corollary above generalizes Ogg's formula for elliptic curves $v_K(\Delta_{\min}) - a(\rho_\ell) = m(C/K) - 1$.

COROLLARY 3.21. *For a_6 as in Prop. 3.17 we have*

(1) $v_K(a_6) \equiv 1 + a(\rho_\ell) - v_K(\Delta_{\min}) \equiv 2d - m(C/K) \bmod 5$;
(2) $v_K(a_6) \equiv m(C/K) + 3 \bmod (\mathbb{F}_5^\times)^2$.

PROOF. Both claims are straightforward to verify using Table 2. □

4. Galois action on the special fiber

Let k be a finite field of some characteristic $p > 2$.

4.1. Artin–Schreier curves. We briefly recall some basic Artin–Schreier theory. Let F be the map on the field of rational functions $k(y)$ in one variable given by $g \mapsto g^p$. If $f \in k(y)$ is not in the image of the map $F - \mathrm{Id}$, then the equation $x^p - x = f$ defines a smooth projective curve C_f over k together with a finite morphism $\pi\colon C_f \to \mathbb{P}^1_k$ of degree p. In other words, the function field $k(C_f) = k(x, y)$ is a cyclic extension of $k(y)$ of degree p. Inversely, every cyclic extension of $k(y)$ of order p is of this form. For $P \in \mathbb{P}^1_k$ and $P' \in C_f$ we denote their associated normalized valuations on $k(y)$ and $k(x, y)$ by v_P and $v_{P'}$, respectively.

4.2. Standard form. We may assume that f is in *standard form*, i.e., each pole of f is of order prime to p. Indeed, there exists $g \in k(y)$ such that $f - (g^p - g)$ is in standard form—this can be done by decomposing $f(y)$ into partial fractions and writing the numerators as p-th powers modulo the maximal ideals, see [Has35, §2]. A change of variables $x \to x - g$ now transforms f into standard form. We claim that such f has poles at exactly the branch points of π. Let $P \in \mathbb{P}^1_k$ and let $P' \in C_f$ be a point above it, with some branching index $e \leqslant p$, so $v_{P'}(f) = e v_P(f)$. If f has a pole at P, then $v_P(f) < 0$ is prime to p, and x has a pole at P'. Thus, $v_{P'}(f) = v_{P'}(x^p - x) = p v_{P'}(x)$. It follows that $e = p$. Inversely, if $v_P(f) \geqslant 0$, then x is integral over the valuation ring $\mathcal{O}_P$ and its minimal polynomial is $h(x) = x^p - x - f$, whose derivative is $h' = -1$. The different ideal of the extension $\mathcal{O}_{P'}/\mathcal{O}_P$ contains $h'(x)$, which is of valuation 0, so P' must be unramified over P by the Dedekind criterion.

In particular, if π has a unique branch point $P \in \mathbb{P}^1_k(k)$ which is a pole of y, and f is in standard form, then P is the unique pole of f, so f is a polynomial in y. If this is the case, then the genus of C_f is given by $g(C_f) = \frac{(\deg f - 1)(p-1)}{2}$, see, e.g., [Sti09, 3.7.8.(d)].

For every $a \in k^\times$ and $c \in k$ we denote by $C_{a,c}$ the Artin–Schreier curve given by the equation $x^p - x - c = ay^2$.

LEMMA 4.3. *Let $p \equiv 1 \bmod 4$. On the curve $C_{1,0}/\mathbb{F}_p$ we have the automorphisms $\sigma_1 : (x, y) \mapsto (x + 1, y)$, $\iota : (x, y) \mapsto (x, -y)$, and the endomorphism $F : (x, y) \mapsto (x^p, y^p)$. They commute pairwise and, for all $n, r, f \in \mathbb{Z}$, the trace of the pullback $(\iota^n \circ \sigma_1^r \circ F^f)^*$ on $H^1_{\text{ét}}((C_{1,0})_{\overline{\mathbb{F}}_p}, \mathbb{Q}_\ell)$ is given by*

$$\operatorname{Tr}\left((\iota^n \circ \sigma_1^r \circ F^f)^*\right) = \begin{cases} (-1)^{n+1} p^{f/2} & \text{if } f \text{ is even and } p \nmid r, \\ (-1)^n p^{f/2}(p-1) & \text{if } f \text{ is even and } p \mid r, \\ (-1)^{n+1}\left(\frac{r}{\mathbb{F}_p}\right) p^{\frac{f+1}{2}} & \text{if } f \text{ is odd.} \end{cases}$$

PROOF. It is straightforward to verify that σ_1, F, and ι commute. The hyperelliptic involution ι acts as multiplication by -1 on the Jacobian variety, so $(\iota^n)^* = (-\operatorname{Id})^n$.

The curve $C_{1,0}$ has genus $\frac{p-1}{2}$, and $\dim H^1_{\text{ét}}((C_{1,0})_{\overline{\mathbb{F}}_p}, \mathbb{Q}_\ell) = p - 1$. Let $C_{\text{aff}} \subset C_{1,0}$ be the affine open subscheme isomorphic to $V(x^5 - x - y^2) \subset \mathbb{A}^2_{\mathbb{F}_p}$. The set $C_{1,0} \setminus C_{\text{aff}}$ contains a single point, which is $\mathbb{F}_p$-rational. We recall from the classical theory that the action of F^* is semisimple and its eigenvalues have absolute value $\sqrt{p}$. We claim that $(F^2)^*$ acts as mulplication by p. For this we only need to show that $\operatorname{Tr}\left((F^2)^*\right) = p(p-1)$. The Lefschetz trace formula

$$\operatorname{Tr}\left((F^2)^*\right) = 1 + p^2 - |C_{1,0}(\mathbb{F}_{p^2})|$$

leaves us to prove that $|C_{1,0}(\mathbb{F}_{p^2})| = p + 1$. For every $x \in \mathbb{F}_{p^2}$ we have $\operatorname{Tr}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(x^p) = \operatorname{Tr}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(x)$. It follows that every $(x, y) \in C_{\text{aff}}(\mathbb{F}_{p^2})$ must be such that $\operatorname{Tr}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(y^2) = 0$, which is equivalent to $y^2 + y^{2p} = 0$. The non-zero

solutions of the latter satisfy $y^{2(p-1)} = -1$, raising this to the odd power $\frac{p+1}{2}$ leads to a contradiction. We conclude that $C_{\mathrm{aff}}(\mathbb{F}_{p^2})$ consists of the points $(x, 0)$ with $x \in \mathbb{F}_p$, and thus the claim holds.

The polynomial $X^2 - p$ is irreducible over $\mathbb{Z}$. Since the characteristic polynomial of F^* is in $\mathbb{Z}[X]$, it must be $(X^2 - p)^{\frac{p-1}{2}}$.

We have $0 = (\sigma_1^p)^* - \mathrm{Id} = (\sigma_1^* - \mathrm{Id})\Phi_p(\sigma_1^*)$ where $\Phi_p \in \mathbb{Z}[X]$ is the p-th cyclotomic polynomial. The characteristic polynomial P_{σ_1} of σ_1^* is in $\mathbb{Z}[X]$, so its irreducible divisors can only be $X-1$ and Φ_p. Since $\deg P_{\sigma_1} = p-1$, we must have $P_{\sigma_1}(X) = (X-1)^{p-1}$ or $P_{\sigma_1} = \Phi_p$. The first case is impossible since σ_1^* in nontrivial. Thus, $\mathrm{Tr}\left((\sigma_1^r)^*\right) = -1$ if r is prime to p, and $\mathrm{Tr}\left((\sigma_1^r)^*\right) = p - 1$ otherwise. The formulas for the case when f is even hence follow.

If f is odd, then

$$\mathrm{Tr}\left((\iota^n \circ \sigma_1^r \circ F^f)^*\right) = (-1)^n p^{\frac{f-1}{2}} \mathrm{Tr}\left((\sigma_1^r \circ F)^*\right). \tag{4.3.1}$$

We use the Lefchetz formula

$$\mathrm{Tr}\left((\sigma_1^r \circ F)^*\right) = 1 + p - \left|\mathrm{Fix}(\sigma_1^r \circ F)\right|.$$

The points $(x, y) \in C_{\mathrm{aff}}(\overline{\mathbb{F}}_p)$ fixed by $\sigma_1^r \circ F$ satisfy $x = x^p + r$ and $y = y^p$, so $y \in \mathbb{F}_p$ and $-r = x^p - x = y^2$. The latter equation has exactly $\left(\frac{-r}{\mathbb{F}_p}\right) + 1 = \left(\frac{r}{\mathbb{F}_p}\right) + 1$ solutions in y for each $r \in \mathbb{F}_p$. Each solution y gives exactly p solutions for $x^p - x = y^2$. We have therefore proved that $\sigma_1^r \circ F$ has exactly $p\left(\left(\frac{r}{\mathbb{F}_p}\right) + 1\right) + 1$ fixed points, so

$$\mathrm{Tr}\left((\sigma_1^r \circ F)^*\right) = -\left(\frac{r}{\mathbb{F}_p}\right) p. \tag{4.3.2}$$

Substituting (4.3.2) into (4.3.1) finishes the proof. □

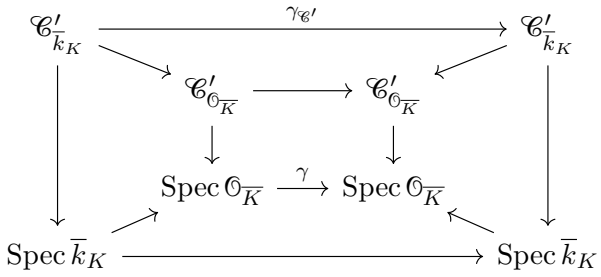
Remark 4.4. If $p \equiv 3 \bmod 4$, then, using similar methods, one can show that $|C_{1,0}(\mathbb{F}_{p^2})| = p(2p-1) + 1$ and $(F^*)^2 + p = 0$. Then, analogous formulas for the traces can be given.

4.5. We now continue in the setting where K is a 5-adic field and C/K is a curve of genus 2 whose ℓ-adic representation has cyclic wild inertia image $\rho_\ell(I_K^{\mathrm{w}})$ of order 5. Recall the notation of 3.9.

4.6. Galois action on the minimal smooth model. Prop. 3.11 tells us that $\ker \rho_\ell|_{I_K} = I_L$. By the Néron–Ogg–Shafarevich criterion and Prop. 3.7, the curve C_L/L has good reduction, so its minimal regular model $\mathscr{C}'/\mathcal{O}_L$ is smooth. For every finite Galois extension K'/K containing L, the minimal regular model of $C_{K'}/K'$ is given by the base change $\mathscr{C}'_{\mathcal{O}_{K'}} := \mathscr{C}' \times_{\mathcal{O}_L} \mathcal{O}_{K'}$. Every element of $\mathrm{Gal}(K'/K)$ gives an K'-semilinear automorphism $C_{K'} \xrightarrow{\sim} C_{K'}$, which extends uniquely to an $\mathcal{O}_{K'}$-semilinear automorphism $\mathscr{C}'_{\mathcal{O}_{K'}} \xrightarrow{\sim} \mathscr{C}'_{\mathcal{O}_{K'}}$ (see, e.g., [LT16, Corollary 1.2]). Passing to the projective limit shows that

each $\gamma \in \Gamma_K$ induces an $\mathcal{O}_{\overline{K}}$-semilinear automorphism $\mathscr{C}'_{\mathcal{O}_{\overline{K}}} \xrightarrow{\sim} \mathscr{C}'_{\mathcal{O}_{\overline{K}}}$. The morphism preserves the special fiber, so we obtain a commutative diagram

(4.6.1)



By functoriality, Γ_K acts on $H^1_{\text{ét}}(\mathscr{C}'_{\overline{k}_K}, \mathbb{Q}_\ell)$, and, for every $n \in \mathbb{Z}$ prime to p, the smooth base change theorem provides an isomorphism of Γ_K-modules

$$H^1_{\text{ét}}(C_{\overline{K}}, \mathbb{Z}/n\mathbb{Z}) \cong H^1_{\text{ét}}(\mathscr{C}'_{\overline{k}_K}, \mathbb{Z}/n\mathbb{Z}). \tag{4.6.2}$$

We note that every element $\gamma \in \Gamma_L$ acts on $\mathscr{C}'_{\mathcal{O}_{\overline{K}}} = \mathscr{C}' \times_{\mathcal{O}_L} \mathcal{O}_{\overline{K}}$ as $\mathrm{id} \times \gamma$. Since I_K acts trivially on $\overline{k}_K$, the group I_L acts trivially on $\mathscr{C}'_{\overline{k}_K}$, thus inducing an action of I_K/I_L on $\mathscr{C}'_{\overline{k}_K}$ by $\overline{k}_K$-automorphisms. We obtain a chain of group homomorphisms

$$I_K/I_L \hookrightarrow \operatorname{Aut}(\mathscr{C}'_{\overline{k}_K}) \to \operatorname{Aut}\Big(H^1_{\text{ét}}(\mathscr{C}'_{\overline{k}_K}, \mathbb{Q}_\ell)\Big) \xrightarrow{\sim} \operatorname{Aut}\big(H^1_{\text{ét}}(C_{\overline{K}}, \mathbb{Q}_\ell)\big)\,. \tag{4.6.3}$$

Proposition 4.7. *Let $\sigma \in I_K^{\mathrm{w}}$. The induced automorphism $\sigma_{\mathscr{C}'}$ on $\mathscr{C}'_{\overline{k}_K}$ descends to k_L, and $\mathscr{C}'_{k_L}$ is k_L-isomorphic to $C_{a,0}$ for some $a \in k_L^\times$. The automorphism of $C_{a,0}$ induced by $\sigma_{\mathscr{C}'}$ is given by $\sigma_a^r : (x, y) \mapsto (x + r, y)$ with some $r \in \mathbb{F}_5$. The image $\rho_\ell(\sigma)$ is nontrivial if and only if $r \neq 0$.*

Proof. If $\rho_\ell(\sigma) = \mathrm{Id}$, then $\sigma \in I_L$, so $\sigma_{\mathscr{C}'}$ is the identity on $\mathscr{C}'_{\overline{k}_K}$ by (4.6.3). In the same way, if $\rho_\ell(\sigma)$ is nontrivial, then the class of σ in I_K/I_L has order 5, so it induces an automorphism on $\mathscr{C}'_{\overline{k}_K}$ of order 5.

We have seen in Prop. 3.15 that the classes of σ and φ_L commute in Γ_K/I_L. It follows that they commute as scheme-automorphisms of $\mathscr{C}'_{\overline{k}_L}$, which means that $\sigma_{\mathscr{C}'}$ descends to a k_L-automorphism of $\mathscr{C}'_{k_L}$.

The main arguments for the remainder are given in [Roq70] and [Hom81], which we specialize to our situation. Let $\Gamma \simeq C_5$ be the image of I_K^{w} in $\operatorname{Aut}(\mathscr{C}'_{k_L})$, and let $\pi\colon \mathscr{C}'_{k_L} \to \mathscr{C}'_{k_L}/\Gamma$ be the quotient map, which is defined over k_L. As a consequence of the Hurwitz formula, [Hom81, Remark 1.2.(A).(b)] shows that Γ fixes a unique closed point P in $\mathscr{C}'_{k_L}$ and that $\mathscr{C}'_{k_L}/\Gamma$ has genus zero. Since Γ commutes with $(\varphi_L)_{\mathscr{C}'}$, the point $(\varphi_L)_{\mathscr{C}'}(P)$ is also fixed by Γ, so $(\varphi_L)_{\mathscr{C}'}(P) = P$, meaning that P is a k_L-rational point. Then $\pi(P)$ is k_L-rational, so π is in indeed a finite k_L-morphism $\mathscr{C}'_{k_L} \to \mathbb{P}^1_{k_L}$. Let $k_L(\mathscr{C}'_{k_L})$ denote the function field of $\mathscr{C}'_{k_L}$, then $k_L(\mathscr{C}'_{k_L})^\Gamma$ is a rational function field over k_L, and we fix a generator y which has a (unique) pole at P.

Since $k_L(\mathscr{C}'_{k_L})/k_L(y)$ is cyclic of order 5, by applying Artin–Schreier theory we have $k_L(\mathscr{C}'_{k_L}) = k_L(x,y)$ for some x satisfying an equation $x^5 - x = f$ with $f \in k_L(y)$. It follows from 4.2 that we may assume that $f \in k_L[y]$. Since $\mathscr{C}'_{k_L}$ has genus 2, we must have $\deg f = 2$. We may further suppose that $f(y) = ay^2 + c$ with $a, c \in k_L$, $a \neq 0$, thus we have a k_L-isomorphism $\mathscr{C}'_{k_L} \simeq C_{a,c}$.

With our particular choice of L/K in 3.9, the points of $J(C)[2]$ are rational over L. The isomorphism (4.6.2) implies that the points of $J(C_{a,c})[2]$ are k_L-rational, which means that the polynomial $x^5 - x - c$ splits completely over k_L. By translating x with one of the roots we find that $\mathscr{C}'_{k_L} \simeq C_{a,0}$ as k_L-schemes.

Lastly, every $\gamma \in \Gamma$ fixes y, so $x - \gamma(x)$ is a root of $X^5 - X = 0$, thus giving $\gamma = \sigma_a^r$ for some $r \in \mathbb{F}_5$, which is zero if and only if γ is trivial. □

Proposition 4.8. *We fix $\sigma \in I_K^{\mathrm{w}}$. Let $a \in k_L^\times$ and $r \in \mathbb{F}_5$ be as in Prop. 4.7. For every $m, n \in \mathbb{Z}$ we have*

$$\operatorname{Tr} \rho_\ell(\sigma^m \varphi_L^n) = \begin{cases} -\left(\frac{a}{k_L}\right)^n 5^{\frac{n[k_L:\mathbb{F}_5]}{2}} & \text{if } n[k_L:\mathbb{F}_5] \text{ is even and } 5 \nmid m, \\ \left(\frac{a}{k_L}\right)^n 4 \cdot 5^{\frac{n[k_L:\mathbb{F}_5]}{2}} & \text{if } n[k_L:\mathbb{F}_5] \text{ is even and } 5 \mid m, \\ -\left(\frac{a}{k_L}\right)^n \left(\frac{rm}{\mathbb{F}_5}\right) 5^{\frac{n[k_L:\mathbb{F}_5]+1}{2}} & \text{if } n[k_L:\mathbb{F}_5] \text{ is odd.} \end{cases}$$

Proof. From the classical theory of the Frobenius actions on the étale cohomology group we know that the morphism $F_q : (x,y) \mapsto (x^{q_L}, y^{q_L})$ of $C_{a,0}$ induces the action of φ_L on $H^1_{\text{ét}}(\mathscr{C}'_{\overline{k}_K}, \mathbb{Q}_\ell)$.

We fix a square root $\sqrt{a} \in \overline{k}_K$. Then there is a $\overline{k}_K$-isomorphism $C_{1,0} \to C_{a,0}$ given by $(x,y) \mapsto (x, \frac{y}{\sqrt{a}})$. Using this isomorphism we compute that the $\overline{k}_K$-automorphism on $C_{1,0}$ induced by σ_a^r descends to $\mathbb{F}_5$ and is exactly σ_1^r. Similarly, F_q induces $F^{[k_L:\mathbb{F}_5]} \circ \iota$ on $C_{1,0}$ if $\left(\frac{a}{k_L}\right) = -1$ or $F^{[k_L:\mathbb{F}_5]}$ if $\left(\frac{a}{k_L}\right) = 1$.

Therefore,

$$\operatorname{Tr} \rho_\ell(\sigma^m \varphi_L^n) = \left(\frac{a}{k_L}\right)^n \cdot \operatorname{Tr}\left(\left(\sigma_1^{rm} \circ F^{n[k_L:\mathbb{F}_5]}\right)^* \right).$$

The desired formulas now follow from Lemma 4.3. □

4.9. Square classes of differences of Weierstrass roots. Let $Y^2 = P(X)$ be a Weierstrass equation defining C/K with $P \in K[X]$ unitary of degree 5 as in Prop. 3.17. In particular, $A_5 = 1$. Any element $\sigma \in I_K^{\mathrm{w}}$ for which $\rho_\ell(\sigma)$ is nontrivial acts transitively on the roots of P. We fix a root $\alpha_1 \in M$ of P, then the other roots are $\alpha_i := \sigma^{i-1}(\alpha_1)$. Following Prop. 4.7, there exists an $a \in k_L^\times$ such that $\mathscr{C}_{k_L} \simeq C_{a,0}$ over k_L, and σ induces $\sigma_a^r \in \operatorname{Aut}(C_{a,0})$ for some $r \in \mathbb{F}_p^\times$. We note that the curve $C_{a,0}$ is k_L-isomorphic to the curve defined by the equation $y'^2 = x'^5 - a^4 x'$, where $y' = a^3 y$ and $x' = ax$. We have $\sigma_a^r : (x', y') \mapsto (x' + ar, y')$.

Proposition 4.10. *The following properties hold :*

(1) *The valuation of $\alpha_i - \alpha_j$ is the same for every $i \neq j$;*
(2) *Assume that $[k_L : \mathbb{F}_5]$ is odd. There exists a $\sigma \in I_K^w$ such that $\left(\frac{ar}{k_L}\right) = 1$. In this case, $\alpha_1 - \sigma(\alpha_1) \in (L^\times)^2$.*

Proof. (1) Since C_L/L has good reduction by Prop. 3.7, there exists an affine variable change over L which transforms $Y^2 = P(X)$ into an equation $Y'^2 = P'(X')$ with coefficients in $\mathcal{O}_L$ and an invertible discriminant (we can use [Liu96, Lemme 3] and the fact that translating Y by a polynomial in X does not change the discriminant). An affine transformation modifies all $v_L(\alpha_i - \alpha_j)$ by adding the same constant v. The new discriminant has valuation zero, so we must have $v_L(\alpha_i - \alpha_j) + v = 0$ for all $i \neq j$.

(2) The existence of σ such that $\left(\frac{ar}{k_L}\right) = 1$ follows from $\left(\frac{r}{k_L}\right) = \left(\frac{r}{\mathbb{F}_5}\right)$.

The extension H/K from 3.9 is at most tamely ramified, so σ acts trivially on it. Thus, by Lemma 3.10, the restriction of σ to L gives an automorphism of L. Then, σ induces an L-semilinear automorphism of C_L/L.

The action of σ on the function field $K(X,Y)$ with $Y^2 = P(X) \in K[X]$ is trivial. Applying the change of variables $X = X' + \alpha_1$ gives the equation

$$Y^2 = P'(X') := X'(X' - \alpha_2 + \alpha_1)\dots(X' - \alpha_5 + \alpha_1) \in M[X'].$$

The σ-action extends M-semilinearly to $M(X,Y) = M(X',Y)$ and

$$\sigma(X') = X' - \alpha_2 + \alpha_1.$$

Since P is as in Prop. 3.17, we have $40 \mid e(L/K)v_K(\Delta(P))$ by Prop. 3.13. Let ϖ_L be any uniformizer of L and $\delta := \varpi_L^{\frac{e(L/K)v_K(\Delta(P))}{40}}$. After applying another change of variables $Y = \delta^5 Y''$, $X' = \delta^2 X''$ we obtain

$$Y''^2 = P''(X'') := X''\left(X'' - \frac{\alpha_2 - \alpha_1}{\delta^2}\right)\dots\left(X'' - \frac{\alpha_5 - \alpha_1}{\delta^2}\right),$$

and $\sigma(X'') = X'' - \frac{\alpha_2 - \alpha_1}{\delta^2}$. The formula (2.2.5) gives

$$v_L\left(\Delta(P'')\right) = v_L\left(\delta^{-100} \cdot \delta^{60}\Delta(P)\right) = e(L/K)v_K\left(\Delta(P)\right) - 40v_L(\delta) = 0.$$

For all $i \neq j$, applying part (1) gives

$$v_L\left(\frac{\alpha_i - \alpha_j}{\delta^2}\right) = \frac{1}{20}v_L(\Delta(P)) - 2v_L(\delta) = 0.$$

It follows that $Y''^2 = P''(X'')$ defines a smooth model $\mathcal{W}/\mathcal{O}_L$ of C_L/L, which is unique up to isomorphism. Its reduction $\mathcal{W}_{k_L}/k_L$ must be k_L-isomorphic to the curve $C_{a,0}/k_L$, defined by $y'^2 = x'^5 - a^4x'$. Let x'' and y'' denote the classes of X'' and Y'', respectively, in the function field of $\mathcal{W}_{k_L}$. By construction, the points at infinity of both of these models are fixed by the k_L-linear automorphisms induced by σ. Since on each curve there is a unique such fixed point (proven in [Hom81]), there must be an affine variable change $y'' = ay'$, $x'' = bx' + c$ for some $a, b, c \in k_L$. Then $b^5 = a^2$, so b is a square in k_L.

On one hand, as pointed out in 4.9, we have

$$\sigma(x'') = b\sigma(x') + c = bx' + bar + c,$$

and on the other hand, from the construction of P'', we have

$$\sigma(x'') = bx' + c + \left(\frac{\alpha_1 - \alpha_2}{\delta^2} \bmod \mathfrak{m}_L\right).$$

Thus, the class of $\frac{\alpha_1-\alpha_2}{\delta^2}$ in k_L is bar, which is a square, so $\alpha_1 - \alpha_2 \in (L^\times)^2$. □

Proposition 4.11.

(1) *We have $H \subset M$.*
(2) *For all $k \neq l$, the element $\alpha_k - \alpha_l$ is a square in $L(\zeta_8)$.*

Proof. For (2), by replacing σ with some power, without loss of generality we may assume that $k = 1$, $l = 2$. Applying (2.2.3) gives

$$-\beta = \Delta(P) = 2^8 \prod_{i<j}(\alpha_i - \alpha_j)^2 = 2^8(\alpha_1 - \alpha_2)^{20} \prod_{i<j}\left(\frac{\alpha_i - \alpha_j}{\alpha_1 - \alpha_2}\right)^2. \tag{4.11.1}$$

The wild ramification subgroup $I^{\mathrm{w}}(M/K)$ acts trivially on $M^\times/U_M^1$, so

$$\frac{\alpha_i - \alpha_1}{\alpha_2 - \alpha_1} = \sum_{k=0}^{i-2} \frac{\sigma^k(\alpha_2 - \alpha_1)}{\alpha_2 - \alpha_1} \equiv i - 1 \bmod \mathfrak{m}_M.$$

Then

$$\prod_{i<j}\left(\frac{\alpha_i - \alpha_j}{\alpha_1 - \alpha_2}\right)^2 \equiv \prod_{i<j}(j-i)^2 \equiv (288)^2 \equiv -1 \bmod \mathfrak{m}_M.$$

Since U_M^1 is 8-divisible, it follows that $\beta \in (M^\times)^4$, thus giving (1). Recall that $\beta \in (L^\times)^8$, thus $(\alpha_1 - \alpha_2)^4 \in (L^\times)^8$. It follows that $\alpha_1 - \alpha_2$ is a square in $L(\zeta_8)^\times$, thus proving (2). □

Remark 4.12. Prop. 4.11.(2) should be contracted with Prop. 4.10.(2). Unless $L = L(\zeta_8)$, only half of the differences $\alpha_i - \alpha_j$ are squares in L. Indeed, suppose that $\zeta_8 \notin L$. Then $[k_L : \mathbb{F}_5]$ is odd. For every $\sigma \in I_K^{\mathrm{w}}$ such that the induced $r \in \mathbb{F}_5^\times$ satisfies $\left(\frac{ar}{k_L}\right) = -1$, the proof of Prop. 4.10.(2) shows that $\alpha_1 - \sigma(\alpha_1)$ is not a square in L.

5. Maximal inertia action over 5-adic fields

We continue to work in the setting of 4.5. We will use the notation of [GN] to describe finite groups.

Proposition 5.1. *The following are equivalent :*

(1) *$v_K(\Delta)$ is odd for any discriminant Δ of C/K;*
(2) *The extension M/K is totally ramified and $\mathrm{Gal}(M/K) \simeq F_5$;*
(3) *$a(C/K) := a(\rho_\ell)$ is odd;*
(4) *$\rho_\ell(I_K) \simeq C_5 \rtimes C_8$.*

PROOF. (1) and (4) are equivalent by Prop. 3.13, (1) and (3) are equivalent by Cor. 3.19 and (2.2.5). Prop. 3.11 shows that $\rho_\ell(I_K)$ has a quotient isomorphic to the inertia subgroup of $\mathrm{Gal}(M/K)$. Then 3.5 shows that (2) implies (4). Suppose (4), then L/K has ramification index 40. By 3.4, the ramification index of M/K is at least 20. Statement (2) now follows from Prop. 3.12. □

5.2. The maximal ramification hypothesis. From now on we suppose that

$$\rho_\ell(I_K) \simeq C_5 \rtimes C_8.$$

The associated complex Weil–Deligne representation is given by the Weil representation $\rho := \rho_\ell|_{W_K} \otimes_{\mathbf{Q}_\ell} \mathbb{C}$ and the trivial monodromy operator.

PROPOSITION 5.3. *The extension L/K is totally ramified, and $[L : M] = 2$, $[M : H] = 5$, $[H : K] = 4$.*

PROOF. We have $[N : H] \leqslant 2$. It follows from Prop. 4.11.(1) that $H \subset N \cap M$, and thus $[N \cap M : H] \leqslant 2$. By Prop. 5.1, $v_K(\Delta)$ is odd, so N/K and H/K are totally ramified of degrees 8 and 4, respectively. Also by Prop. 5.1 we have $20 = [M : K] = 4[N \cap M : H][M : N \cap M]$, thus $N \cap M = H$. It follows that $[L : K] = [N : K][M : H] = 40$. Prop. 5.1 and Prop. 3.11 give $I(L/K) = 40$, so L/K is totally ramified. □

PROPOSITION 5.4. *We have*

$$\mathrm{Gal}(L(\zeta_8)/K) \simeq \begin{cases} C_5 \rtimes C_8 & \text{if } [k_K : \mathbb{F}_5] \text{ is even,} \\ C_2^2.F_5 & \text{if } [k_K : \mathbb{F}_5] \text{ is odd.} \end{cases}$$

PROOF. The inertia subgroup $I(L(\zeta_8)/K) \subset \mathrm{Gal}(L(\zeta_8)/K)$ is isomorphic to $C_5 \rtimes C_8$ and has index at most 2 (from Prop. 3.11 and Prop. 5.3).

It remains to show that if $L(\zeta_8)/L$ is nontrivial, then $\mathrm{Gal}(L(\zeta_8)/K) \simeq C_2^2.F_5$. In this case we have $\mathrm{Gal}(L(\zeta_8)/M) \simeq C_2^2$ since L/M is totally ramified of degree 2. It follows from Prop. 5.1 that $\mathrm{Gal}(L(\zeta_8)/K)$ is an extension G of F_5 by C_2^2. The extension cannot be split, because otherwise $\mathrm{Gal}(L(\zeta_8)/K)$ would have $C_2^2 \rtimes C_4$ as a 2-Sylow subgroup, which has exponent 4 and therefore has no element of order 8. In order to identify $\mathrm{Gal}(L(\zeta_8)/K)$ as $C_2^2.F_5$ by using [GN] we are left to show that the extension G is non-central, i.e., that the subgroup $C_2^2 \subset G$ which is identified with $\mathrm{Gal}(L(\zeta_8)/M) \subset \mathrm{Gal}(L(\zeta_8)/K)$ is non-central. Indeed, $\mathrm{Gal}(L(\zeta_8)/M)$ cannot be central because $\mathrm{Gal}(L/K)$ is non-Galois (otherwise the Galois closure of N is contained in L, which implies that $\zeta_8 \in L$). □

PROPOSITION 5.5. *Under the hypothesis of 5.2 the following statements hold :*

(1) *The representation ρ is irreducible;*
(2) *There exist characters χ and χ' of W_H such that*

$$\rho|_{W_H} \simeq \chi \oplus \chi^{-1}(-1) \oplus \chi' \oplus \chi'^{-1}(-1); \tag{5.5.1}$$

(3) *If χ is any of the four characters appearing as direct factors in (5.5.1), then*

$$\rho \simeq \mathrm{Ind}_{W_H}^{W_K} \chi.$$

Proof. We observe that every irreducible representation of $C_5 \rtimes C_8$ necessarily has dimension 1 or 4 (see, e.g., [GN]). It follows that $\rho|_{I_K}$ is irreducible since it cannot be a direct sum of 1-dimensional representations. Thus, (1) holds.

The extension L/H is the compositum of the C_5-extension M/H and the quadratic extension N/H, so $\mathrm{Gal}(L/H) \simeq C_{10}$. It follows that LK^{ur}/H is abelian. Therefore, $\rho|_{W_H}$ has abelian image and splits into 1-dimensional factors

$$\rho|_{W_H} \simeq \chi_1 \oplus \chi_2 \oplus \chi_3 \oplus \chi_4. \tag{5.5.2}$$

Frobenius reciprocity gives a nontrivial morphism of representations

$$\mathrm{Ind}_{W_H}^{W_K} \chi_1 \to \rho.$$

Since ρ is irreducible, the morphism is surjective and, in fact, is an isomorphism because $\dim(\mathrm{Ind}_{W_H}^{W_K} \chi_1) = 4 = \dim \rho$. Thus, (3) holds.

Furthermore, since H/K is tamely ramified, $I_H^{\mathrm{w}} = I_K^{\mathrm{w}}$ is normal in W_K. If $\chi_1(I_H^{\mathrm{w}})$ is trivial, then using an explicit construction of the induced representation we obtain that $\rho(I_H^{\mathrm{w}})$ is trivial, which is impossible. It follows that χ_1 is wildly ramified.

The twisted representation $\rho(\frac{1}{2})$ is symplectic with respect to the Weil pairing on $H^1_{\text{ét}}(J(C)_{\overline{K}}, \mathbb{Q}_\ell)$, so, in particular, the dual of ρ is $\rho^* \cong \rho(1)$ and $\det \rho = \chi_{\mathrm{ur}}^{-2}$. Then (5.5.2) gives

$$\rho|_{W_H} \simeq (\rho|_{W_H})^*(-1) \simeq \chi_1^{-1}(-1) \oplus \chi_2^{-1}(-1) \oplus \chi_3^{-1}(-1) \oplus \chi_4^{-1}(-1).$$

Since χ_1 is wildly ramified, we cannot have $\chi_1 \simeq \chi_1^{-1}(-1)$, so we may suppose that $\chi_2 \simeq \chi_1^{-1}(-1)$. We then have $\chi_4 \simeq \chi_3^{-1}(-1)$. Posing $\chi = \chi_1$ and $\chi' = \chi_3$ gives (2). □

Proposition 5.6. *If χ is as in Prop. 5.5 (3), then its Artin conductor $a(\chi)$ is even.*

Proof. Since H/K is totally tamely ramified of degree 4, we have $a(\rho_\ell) = a(\rho) = a(\chi) + 3$ from [Roh94, §10.(a2)], and $a(\rho_\ell)$ is odd by Prop. 5.1. □

5.7. Study of the 4-torsion. Let $Y^2 = P(X)$ be as in Prop. 3.17. If $\alpha_1, \ldots, \alpha_5 \in \overline{K}$ are the roots of P, then $M = K(\alpha_1, \ldots, \alpha_5)$.

Proposition 5.8. *Each point of $J(C)[4]$ is rational over $L(\zeta_8)$.*

Proof. Let $\widetilde{M} := \mathbb{Q}(\sqrt{-1}, \alpha_1, \ldots, \alpha_5) \subset M$. Then the curve C and its Jacobian are defined over $\widetilde{M}$, and it follows from [Yel15, Remark 4.2] that

$$\widetilde{M}(J(C)[4]) = \widetilde{M}\left(\left(\sqrt{\alpha_i - \alpha_j}\right)_{i<j}\right).$$

The proposition now follows from Prop. 4.11.(2). □

COROLLARY 5.9. *The map $\rho(\varphi_{L(\zeta_8)})$ is given as multiplication by the scalar $\sqrt{q_{L(\zeta_8)}}$. As an immediate consequence, the twisted representation $\rho(\frac{1}{2})$ is trivial on $W_{L(\zeta_8)}$.*

PROOF. Since $\rho(\varphi_{L(\zeta_8)})$ is central in $\mathrm{Im}(\rho)$ by Prop. 3.15, it acts as multiplication by a scalar $z \in \mathbb{C}^\times$ by Schur's lemma. From (5.5.1) we see that $z = z^{-1}q_{L(\zeta_8)}$, so $z = \pm\sqrt{q_{L(\zeta_8)}}$. We note that $\sqrt{q_{L(\zeta_8)}}$ is always an integral power of 5, thus, in particular, $z \equiv \pm 1 \bmod 4$. On the other hand, Prop. 5.8 implies that $\rho_2(\varphi_{L(\zeta_8)}) \in \mathrm{Aut}_{\mathbb{Z}_2}\left(H^1_{\text{ét}}(C_{\overline{K}}, \mathbb{Z}_2)\right)$ satisfies $\rho_2(\varphi_{L(\zeta_8)}) \equiv \mathrm{Id} \bmod 4$. We therefore conclude that $z = \sqrt{q_{L(\zeta_8)}}$. □

6. Computation of root numbers

We will work under the hypotheses of 5.2 and prove our main result.

THEOREM 6.1. *Let a_6 be as in Prop. 3.17, and let Δ be any discriminant associated to any Weierstrass equation defining C/K. The root number of C/K is given by*

$$w(C/K) = (-1)^{[k_K:\mathbb{F}_5]+1} \cdot \left(\frac{m(C/K)+3}{k_K}\right) \cdot (\Delta, a_6)_K.$$

Let $\psi_k \colon K \to \mathbb{C}^\times$ be the additive character from 1.2. For the basic general theory and the formulas of root numbers the reader may refer to [Roh94].

6.2. Root number of an induced representation. We have $\rho = \mathrm{Ind}_{W_H}^{W_K} \chi$ from Prop. 5.5, so the formula of root numbers of induced representations (see I.1.18) gives

$$w(C/K) = w(\chi, \psi_k \circ \mathrm{Tr}_{K/H}) \cdot w(\mathrm{Ind}_{W_H}^{W_K} \mathbb{1}, \psi_k). \tag{6.2.1}$$

LEMMA 6.3. *We have $w(\mathrm{Ind}_{W_H}^{W_K} \mathbb{1}, \psi_k) = -1$.*

PROOF. The representation $\mathrm{Ind}_{W_H}^{W_K} \mathbb{1}$ is isomorphic to the regular representation of $\mathrm{Gal}(H/K) \simeq C_4$. Let $\chi_4 \colon W_K \to \mathbb{C}^\times$ denote a totally ramified character of order 4 such that $\ker \chi_4 = W_H$. We then have a decomposition

$$\mathrm{Ind}_{W_H}^{W_K} \mathbb{1} \simeq \mathbb{1} \oplus \chi_4^2 \oplus \chi_4 \oplus \chi_4^{-1}, \tag{6.3.1}$$

and thus multiplicativity of root numbers gives

$$w(\mathrm{Ind}_{W_H}^{W_K} \mathbb{1}, \psi_k) = w(\chi_4^2, \psi_k) \cdot w(\chi_4 \oplus \chi_4^{-1}, \psi_k).$$

The general properties of root numbers (see Prop. I.1.21,(2)) give

$$w(\chi_4 \oplus \chi_4^{-1}, \psi_k) = \chi_4(\theta_K(-1)),$$

where θ_K is Artin's reciprocity map. We have $\chi_4(\theta_K(-1)) = 1$ exactly when -1 is a 4th power in $K^\times$, so

$$w(\chi_4 \oplus \chi_4^{-1}, \psi_k) = (-1)^{[k_K:\mathbb{F}_5]}.$$

In order to compute $w(\chi_4^2, \psi_k)$ we apply the formula [AS10, (8.7.1)] with $\beta = 1$ there and $\tau(\chi_4^2, \psi_k) = -G_{[k_K:\mathbb{F}_5]}(\chi_4^2) = (-\sqrt{p})^{[k_K:\mathbb{F}_5]}$ (we use [BEW98, Thm. 11.5.2]), which gives

$$w(\chi_4^2, \psi_k) = (-1)^{[k_K:\mathbb{F}_5]+1},$$

thus the lemma follows. □

6.4. Connection with a Weierstrass equation. Let $Y^2 = P(X)$ be the Weierstrass equation defining C/K from Prop. 3.17. We fix a root α_1 of the irreducible polynomial P. Let χ be as in Prop. 5.5, and let $\sigma \in I_H$ be an element such that

$$\chi(\sigma) = \exp\left(\frac{2\pi i}{5}\right). \tag{6.4.1}$$

It follows that σ restricts to a generator of $\mathrm{Gal}(M/H) \simeq C_5$. We recall that M is the splitting field of P and note that $M = H(\alpha_1)$. Having fixed σ and α_1, the roots of P are $\alpha_j = \sigma^{j-1}(\alpha_1)$. We have

$$\mathcal{N}_{M/H}(\alpha_1) = -a_6 \tag{6.4.2}$$

and

$$v_M(\alpha_1) = v_H(\mathcal{N}_{M/H}(\alpha_1)) = v_H(a_6) = 4v_K(a_6). \tag{6.4.3}$$

Let

$$d_{\alpha_1} := \mathcal{N}_{M/H}(\alpha_1 - \alpha_2) = \mathcal{N}_{M/H}(\alpha_1)\mathcal{N}_{M/H}\Big(1 - \frac{\sigma(\alpha_1)}{\alpha_1}\Big).$$

Since $a(\chi)$ is even by Prop. 5.6, we may apply Cor. 1.9 (with $K = H$ there) and find (recall the notation $\approx$ from 1.4)

$$\begin{aligned} w(\chi, \psi_k \circ \mathrm{Tr}_{H/K}) &\approx \chi \circ \theta_H \left(v_M(\alpha_1) \cdot \mathcal{N}_{M/H}(\alpha_1)\right)^{-1} \cdot \chi \circ \theta_H(d_{\alpha_1}) \\ &\approx \chi \circ \theta_H(-4v_K(a_6)a_6)^{-1} \cdot \chi \circ \theta_H(d_{\alpha_1}). \end{aligned} \tag{6.4.4}$$

Recall that $\det \rho = \chi_{\mathrm{ur}}^{-2}$. Let $t\colon W_K^{\mathrm{ab}} \to W_H^{\mathrm{ab}}$ be the transfer map. Deligne's determinant formula [Del73, p. 508] gives

$$\chi_{\mathrm{ur}}^{-2} = \det\big(\mathrm{Ind}_{W_H}^{W_K} \chi\big) = \det\big(\mathrm{Ind}_{W_H}^{W_K} \mathbb{1}\big) \cdot \chi \circ t.$$

Composing with θ_K and taking into account the decomposition (6.3.1) gives

$$||\cdot||_K^{-2} = \chi_4^2 \circ \theta_K \cdot (\chi \circ \theta_H)|_{K^\times}.$$

Since $-4v_K(a_6)a_6 \in K^\times$ and $||\cdot||_K \approx 1$, the above gives

$$\chi \circ \theta_H(-4v_K(a_6)a_6) \approx \chi_4^2 \circ \theta_K(-4v_K(a_6)a_6). \tag{6.4.5}$$

We note that $-\beta \in \mathcal{N}_{K(\sqrt{\beta})/K}(K(\sqrt{\beta})^\times)$, so $\chi_4^2 \circ \theta_K(-\beta) = 1$. Therefore, $\chi_4^2 \circ \theta_K$ is equal to the Hilbert symbol $(\beta, \cdot)_K$, since both are quadratic ramified characters trivial on $-\beta$. Since β differs from any discriminant Δ of C/K by

a square in $K^\times$, we have $(\beta,\cdot)_K = (\Delta,\cdot)_K$. Applying this to (6.4.5) together with the formula [Neu99, V.(3.4)] gives

$$\chi\circ\theta_H(-4v_K(a_6)a_6) \approx \left(\frac{v_K(a_6)}{k_K}\right)\cdot(\Delta,a_6)_K. \tag{6.4.6}$$

Plugging (6.4.6) into (6.4.4) and applying Cor. 3.21.(2) we obtain

$$w(\chi,\psi_k\circ\mathrm{Tr}_{H/K}) \approx \left(\frac{m(C/K)+3}{k_K}\right)\cdot(\Delta,a_6)_K\cdot\chi\circ\theta_H(d_{\alpha_1}). \tag{6.4.7}$$

6.5. The twisted representation $\rho(\frac{1}{2})$ is trivial on $W_{L(\zeta_8)}$ by Cor. 5.9. Since $\rho(\frac{1}{2}) = \mathrm{Ind}_{W_H}^{W_K}(\chi(\frac{1}{2}))$, the character $\chi(\frac{1}{2})$ is trivial on $W_{L(\zeta_8)}$ and therefore $\chi(\frac{1}{2})\circ\theta_H$ is trivial on $\mathcal{N}_{L(\zeta_8)/H}(L(\zeta_8)^\times)$. We note also that

$$\chi\circ\theta_H(d_{\alpha_1}) = \chi\circ\theta_M(\alpha_1-\alpha_2). \tag{6.5.1}$$

Lemma 6.6. *If $[k_K:\mathbb{F}_5]$ is even, then $\chi\circ\theta_H(d_{\alpha_1})\approx 1$.*

Proof. Here we have $L(\zeta_8)=L$. Then Prop. 4.11.(2) implies that

$$\alpha_1-\alpha_2 \in \mathcal{N}_{L(\zeta_8)/M}(L(\zeta_8)^\times),$$

thus d_{α_1} is a norm from $L(\zeta_8)^\times$. Using 6.5 we have

$$\chi\circ\theta_H(d_{\alpha_1}) = ||d_{\alpha_1}||_H^{-\frac{1}{2}}\cdot\left(\chi(\tfrac{1}{2})\circ\theta_H\right)(d_{\alpha_1}) = ||d_{\alpha_1}||_H^{-\frac{1}{2}} \approx 1. \tag{6.6.1}$$ □

Lemma 6.7. *Let $[k_K:\mathbb{F}_5]$ be odd. Let $a\in k_L$ and $r\in\mathbb{F}_5$ be associated to σ as in Prop. 4.7. Then for every geometric Frobenius lift $\varphi_L\in W_L$, we have*

$$\chi(\varphi_L) = -\left(\frac{ar}{k_L}\right)\sqrt{q_K}.$$

Proof. Recall from Prop. 5.3 that L/K is totally ramified, thus $k_L=k_K$. Since $[k_K:\mathbb{F}_5]$ is odd, $q_K=q_L=\sqrt{q_{L(\zeta_8)}}$, and $(\frac{\cdot}{\mathbb{F}_5})$ is the restriction of $(\frac{\cdot}{k_L})$ to $\mathbb{F}_5$.

Let χ' be the other character appearing in Prop. 5.5. From Prop. 4.8 we have $\mathrm{Tr}\,\rho(\sigma)=-1$, which, together with (6.4.1), forces

$$\chi'(\sigma)\in\left\{\exp\left(\tfrac{2\pi i}{5}\right)^2,\exp\left(\tfrac{2\pi i}{5}\right)^3\right\}. \tag{6.7.1}$$

Cor. 5.9 implies that the eigenvalues of $\rho(\varphi_L)$ are $\pm\sqrt{q_L}$. From Prop. 4.8 we have $\mathrm{Tr}\,\rho(\varphi_L)=0$, so there exists some $w=\pm1$ such that

$$\chi(\varphi_L)=w\sqrt{q_L} \quad\text{and}\quad \chi'(\varphi_L)=-w\sqrt{q_L}. \tag{6.7.2}$$

Using (6.4.1), (6.7.1), and (6.7.2) together with a formula for Gauss sums (see, e.g., [BEW98, §1.1]) gives

$$\begin{aligned}\mathrm{Tr}\,\rho(\sigma\varphi_L) &= w\sqrt{q_L}\left(\exp\left(\tfrac{2\pi i}{5}\right)+\exp\left(\tfrac{2\pi i}{5}\right)^4-\exp\left(\tfrac{2\pi i}{5}\right)^2-\exp\left(\tfrac{2\pi i}{5}\right)^3\right)\\ &= w\sqrt{5q_L}.\end{aligned}$$

It now follows from Prop. 4.8 that $w=-(\frac{ar}{k_L})$. □

6.8. Choosing χ. We assume that $[k_K : \mathbb{F}_5]$ is odd. Then $[k_L : \mathbb{F}_5]$ is also odd. Although the root number $w(\chi, \psi_k \circ \mathrm{Tr}_{H/K})$ does not depend on the choice of the character χ in Prop. 5.5.(3), in order to carry out a detailed computation we will need to fix a particular χ. Depending on whether or not a is a square in $k_L^\times$, we may choose σ and, consequently, χ so that $\left(\frac{ar}{k_L}\right) = 1$ and that we still have (6.4.1).

LEMMA 6.9. *If $[k_K : \mathbb{F}_5]$ is odd and χ is as in 6.8, then $\chi \circ \theta_H(d_{\alpha_1}) \approx -1$.*

PROOF. Applying Lemma 6.7 for the chosen χ gives

$$\chi(\varphi_L) = -\sqrt{q_K}.$$

On the other hand, we are also set to apply Prop. 4.10.(2), which tells us that $\alpha_1 - \alpha_2$ is a square in L. Since -1 is a square in K, it follows that there exists some $b \in L$ such that $\alpha_1 - \alpha_2 = \mathcal{N}_{L/M}(b)$. Recall from Prop. 5.3 that L/K and, thus, all its intermediate extensions are totally ramified. Together with Prop. 4.10.(1) we then obtain

$$v_L(b) = v_M(\alpha_1 - \alpha_2) = \frac{1}{20} v_M(\Delta) = v_K(\Delta).$$

By using Prop. 5.1 we then have

$$v_L(b) \equiv 1 \bmod 2.$$

The restriction $\chi|_{W_L}$ is unramified, so the above discussion shows that

$$\chi \circ \theta_H(d_{\alpha_1}) = \chi \circ \theta_L(b) = \chi(\varphi_L)^{v_L(b)} = (-\sqrt{q_K})^{v_L(b)} \approx -1. \qquad \square$$

PROOF OF THEOREM 6.1. When $[k_K : \mathbb{F}_5]$ is even we use Lemma 6.6, and when $[k_K : \mathbb{F}_5]$ is odd we choose χ as in 6.8 and use Lemma 6.9 to obtain $\chi \circ \theta_H(d_{\alpha_1}) \approx (-1)^{[k_K:\mathbb{F}_5]}$. Plugging this into (6.4.7) then gives

$$w(\chi, \psi_k \circ \mathrm{Tr}_{H/K}) \approx (-1)^{[k_K:\mathbb{F}_5]} \cdot \left(\frac{m(C/K)+3}{k_K}\right) \cdot (\Delta, a_6)_K. \tag{6.9.1}$$

Combining (6.9.1) and Lemma 6.3 into (6.2.1) proves the relation $\approx$ between the two sides of the formula in Thm. 6.1. Since both sides take values in $\{1, -1\}$, the theorem follows (see 1.4). $\square$

7. Examples of curves of genus 2 with maximal ramification

In this section we give some explicit examples of computations of root numbers. All our examples are curves defined over $\mathbb{Q}$. We will use the labels of [LMFDB] to indentify the curves that appear in the database.

For any prime number $\ell \neq 5$, let ρ_ℓ be the ℓ-adic $\Gamma_{\mathbb{Q}_5}$-representation associated to the curve obtained by extending the coefficients to $\mathbb{Q}_5$. We recall that the Hilbert symbol satisfies $(5,5)_{\mathbb{Q}_5} = \left(\frac{-1}{\mathbb{F}_5}\right) = 1$ and $(5, 2\cdot 5)_{\mathbb{Q}_5} = -\left(\frac{-1}{\mathbb{F}_5}\right) = -1$.

EXAMPLE 7.1 (Genus 2 curve 3125.a.3125.1). Let $C/\mathbb{Q}$ be the hyperelliptic curve defined by

$$Y^2 = X^5 + \frac{1}{4}.$$

Its discriminant is $\Delta = 5^5$. It follows that the curve has good reduction at every prime p except 5 and, possibly, 2. Actually, the reduction is good at 2, and the smooth model is given by $Y^2 + Y = X^5$.

Recall that $\mathbb{Q}_5(J(C)[2])/\mathbb{Q}_5$ is the splitting field of $X^5 + \frac{1}{4}$. Note that $(X'+1)^5 + \frac{1}{4}$ is an Eisenstein polynomial over $\mathbb{Z}_5$. Thus, $\mathbb{Q}_5(J(C)[2])/\mathbb{Q}_5$ is wildly ramified. Then ρ_ℓ must also be wildly ramified. By Prop. 3.7, $C/\mathbb{Q}_5$ has potentially good reduction.

We observe also that $Y^2 = (X'+1)^5 + \frac{1}{4}$ satisfies the conditions of Prop. 3.17 with $a_6 = \frac{5}{4}$. Then $m(C/\mathbb{Q}_5) = 1$ from Table 2. Since Δ has odd valuation, Thm. 6.1 gives

$$w(C/\mathbb{Q}_5) = \left(5^5, \frac{5}{4}\right)_{\mathbb{Q}_5} = 1.$$

The global root number is then $w(C/\mathbb{Q}) = 1$, which is compatible with the Hasse–Weil and the BSD conjectures since both analytic and Mordeil–Weil ranks of $J(C)/K$ are 0 (see [LMFDB]).

EXAMPLE 7.2 (Genus 2 curve 12500.a.12500.1). Let $C/\mathbb{Q}$ be the hyperelliptic curve defined by

$$Y^2 = 5X^6 + 10X^3 - 4X + 1.$$

First, we make the change of variables $X' = \frac{-1}{X+1}$, $Y' = \frac{Y}{2(X+1)^3}$ in order to send the rational point $X = -1$, $Y = 0$ to infinity and to make the polynomial on the right-hand side unitary. The resulting equation is

$$Y'^2 = P(X') := X'^5 + \frac{45}{4}X'^4 + \frac{90}{4}X'^3 + \frac{75}{4}X'^2 + \frac{30}{4}X' + \frac{5}{4}$$

and has discriminant $\Delta = 2^2 \cdot 5^5$. The polynomial $P \in \mathbb{Z}_5[X']$ is Eisenstein of degree 5, so its splitting field extension $\mathbb{Q}_5(J(C)[2])/\mathbb{Q}_5$ is wildly ramified. It follows that ρ_ℓ is wildly ramified. By Prop. 3.7, $C/\mathbb{Q}_5$ has potentially good reduction. The polynomial P satisfies the conditions of Prop. 3.17 with $a_6 = \frac{5}{4}$. Then, $m(C/K) = 1$, and Thm. 6.1 gives

$$w(C/\mathbb{Q}_5) = \left(2^2 \cdot 5^5, \frac{5}{4}\right)_{\mathbb{Q}_5} = 1.$$

EXAMPLE 7.3 (Genus 2 curve 703125.a.703125.1). Let $C/\mathbb{Q}$ be the hyperelliptic curve defined by

$$Y^2 = X^5 - 5X^3 + 5X - \frac{7}{4}.$$

Its discriminant is $\Delta = 3^2 \cdot 5^7$. We make a change of variable $X' = X - 3$, then the equation becomes

$$Y^2 = P(X') := X'^5 + 15X'^4 + 85X'^3 + 225X'^2 + 275X' + \frac{485}{4}.$$

We see again that P is Eisenstein with $a_6 = \frac{485}{4}$. Then, Thm. 6.1 gives

$$w(C/\mathbb{Q}_5) = \left(3^2 \cdot 5^7, \frac{485}{4}\right)_{\mathbb{Q}_5} = -1.$$

EXAMPLE 7.4. Let $C/\mathbb{Q}$ be the curve defined by

$$Y^2 = X^5 - 5^3,$$

its discriminant is $\Delta = 2^8 \cdot 5^{17}$. The fact that $X^5 - 5^3$ is irreducible over $\mathbb{Q}_5$ can be established by looking at its Newton polygon, which contains a unique segment of slope $\frac{3}{5}$. Furthermore, its splitting field is wildly ramified over $\mathbb{Q}_5$, thus ρ_ℓ is wildly ramified. We see that $a_6 = -5^3$, so $m(C/\mathbb{Q}_5) = 9$. Then, Thm. 6.1 gives

$$w(C/\mathbb{Q}_5) = \left(\frac{12}{\mathbb{F}_5}\right) \cdot (2^8 \cdot 5^{17}, -5^3)_{\mathbb{Q}_5} = -1.$$

8. Elliptic curves over 3-adic fields

Let $p > 2$ be a prime number. Throughout this section E/K will be an elliptic curve over a finite extension $K/\mathbb{Q}_p$ having potentially good reduction. Eventually, we will take p equal to 3. It is a classical fact that E/K has potentially good reduction if and only if the invariant $j(E)$ has non-negative valuation. Root numbers of such elliptic curves have been thoroughly studied by Rohrlich [Roh93; Roh96] for $p \geqslant 5$ and, more generally, by Kobayashi [Kob02, Thm. 1.1] in terms of Weierstrass models. The aim of this section is to prove a reformulation of Kobayashi's formula which does not refer to a particular Weierstrass equation.

If $\rho_\ell(I_K)$ is abelian, such formulas can be given by [Kob02, Thm. 1.1] or Thm. I.0.2. The case where $\rho_\ell(I_K)$ is non abelian can only happen in particular setting, see [Kra90] for a classification of possible inertia images.

LEMMA 8.1. *If $p > 2$ and $\rho_\ell(I_K)$ in non abelian, then $p = 3$ and $\rho_\ell(I_K)$ is isomorphic to the dicyclic group* $\mathrm{Dic}_3 = C_3 \rtimes C_4$.

PROOF. The ramification of ρ_ℓ cannot be tame. In particular, this rules out $p \geqslant 5$ by Serre–Tate. Therefore, $p = 3$ and $3 \mid |\rho_\ell(I_K)|$. Similarly as in (4.6.3), the group $\rho_\ell(I_K)$ injects into the automorphism group $\mathrm{Aut}(\widetilde{E})$ of an elliptic curve $\widetilde{E}$ defined over a finite field of characteristic 3. It it well known (see, e.g., [Hus87, 3.(5.2)]) that $\mathrm{Aut}(\widetilde{E})$ injects into Dic_3. We conclude by noting that Dic_3 has no proper non abelian subgroups. □

8.2. Weierstrass models. The reader may refer to [Sil94, IV.§9] for the standard formulas for Weierstrass equations. We will be working over 3-adic fields and their residue fields, so we may assume that E/K is defined by a Weierstrass equation

$$Y^2 = X^3 + a_2X^2 + a_4X + a_6$$

with $a_2, a_4, a_6 \in K$. An elliptic curve is non-singular, i.e., the discriminant Δ of an associated Weierstrass equation is nonzero. We define the associated *invariant differential* as $w = \frac{\mathrm{d}X}{2Y}$.

For any $u \in K^\times$ we may substitute

$$\begin{matrix} X = u^2X', \\ Y = u^3Y', \end{matrix} \quad \text{that give new} \quad \begin{matrix} a_2' = u^{-2}a_2, \\ a_4' = u^{-4}a_4, \\ a_6' = u^{-6}a_6, \end{matrix} \quad \text{and} \quad \begin{matrix} \Delta' = u^{-12}\Delta, \\ w' = u \cdot w. \end{matrix} \tag{8.2.1}$$

It is clear that applying a change of variables as above we can obtain an *integral* Weierstrass equation, i.e., one in which $a_2, a_4, a_6 \in \mathcal{O}_K$. Homogenizing an integral Weierstrass equation and applying the Proj construction produces a projective model of E/K, called a *Weierstrass model*.

Among the integral Weierstrass equations there are some that minimize the integer $v_K(\Delta) \geqslant 0$. Such an equation gives rise to a *minimal* Weierstrass model, denoted by $\mathscr{W}/\mathcal{O}_K$, a *minimal discriminant* Δ_K, and a *minimal differential* w_K, which extends to $\mathscr{W}$. Since $\Omega^1_{E/K}$ is of dimension 1 over K, any other given differential w differs from w_K by some scalar in K, which we denote by $\frac{w}{w_K}$.

8.3. Regular models. The elliptic curve E/K admits a minimal regular (proper) model $\mathscr{C}/\mathcal{O}_K$ and a (smooth) Néron model $\mathscr{C}/\mathcal{O}_K$. Both are unique up to an isomorphism. Given a Weierstrass equation, Tate's algorithm (see [Sil94, IV.§9]) provides a way to construct a minimal regular model. In addition, $\mathscr{C}/\mathcal{O}_K$ can be taken to be the maximal smooth open subscheme of $\mathscr{C}/\mathcal{O}_K$.

8.4. Classical invariants. We denote by $m(E/K)$ the number of irreducible components of $\mathscr{C}_{\overline{k}_K}$ and by $a(E/K)$ the Artin conductor of ρ_ℓ. We recall Ogg's formula [Sil94, IV.§11], which relates the aforementioned invariants:

$$a(E/K) = v_K(\Delta_K) + 1 - m(E/K). \tag{8.4.1}$$

The group of components $\Phi := \mathscr{C}_{k_K}\big/\mathscr{C}^\circ_{k_K}$ of the special fiber of the Néron model is finite. The *Tamagawa number* of E/K is defined as $c(E/K) := |\Phi(k_K)|$.

8.5. Kodaira types. Let E/K be an elliptic curve with bad but potentially good reduction. In order to indicate the different reduction types over K we will use Kodaira symbols II, III, IV, I_0^*, IV^*, III^*, II^*, which correspond to $m(E/K) + 1 = 2, 3, 4, 6, 8, 9, 10$, respectively (see [Sil94, p. 365,

Table 4.1]). We observe that the star "*" appears in the Kodaira symbol if and only if $\lfloor \frac{m(E/K)+1}{6} \rfloor = 1$, otherwise $\lfloor \frac{m(E/K)+1}{6} \rfloor = 0$.

8.6. The setting. We suppose from now on that $p = 3$. We also suppose that $\rho_\ell(I_K) \simeq \mathrm{Dic}_3$, except in Prop. 8.7. This corresponds to the case *vi)* of [Kob02, Thm. 3.1]. Let Δ be any discriminant of E/K. As shown in [Kra90, p. 362, Corollaire], the extension $K^{\mathrm{ur}}(E[2], \Delta^{1/4})/K^{\mathrm{ur}}$ is the minimal extension of K^{ur} over which E attains good reduction, and its Galois group is isomorphic to Dic_3.

Let $H = K(\sqrt{\Delta})$, $M = K(E[2])$, $L = K(E[2], \Delta^{1/4})$, and $F = K(\alpha)$ for some fixed $\alpha \in E[2] \setminus \{0\}$. We list some general facts and consequences in the present situation.

(1) The splitting field of a Weierstrass polynomial is M. The extension M/K is Galois. In particular, $\mathrm{Gal}(M/K)$ is isomorphic to a subgroup of the symmetric group S_3, and M contains H, which is the subfield fixed by the unique 3-Sylow subgroup of $\mathrm{Gal}(M/K)$.

(2) Let $e(\cdot/\cdot)$ denote the ramification index. We have

$$2 \cdot 3 \cdot 2 \geqslant e(H/K)e(M/H)e(L/M) = e(L/K) = [LK^{\mathrm{ur}} : K^{\mathrm{ur}}] = 12,$$

so the extensions H/K, M/H, L/M, and L/K are totally ramified of degrees 2, 3, 2, and 12, respectively. In particular, $v_K(\Delta)$ is odd.

(3) We see from (1) and (2) that, in fact, $\mathrm{Gal}(M/K) \simeq S_3$. It follows that M/H is cyclic of order 3.

(4) By the Néron–Ogg–Shafarevich criterion, E has good reduction over L but not over any proper subextension of L/K. However, L/K is not necessarily Galois.

(5) The Weil–Deligne representation (ρ, N) associated to ρ_ℓ with some $\ell \neq 3$ is given by $\rho = \rho_\ell|_{W_K} \otimes_{\mathbb{Q}_\ell} \mathbb{C}$ and $N = 0$. The Weil representation ρ is irreducible and is induced by a wildly ramified character χ of W_H (see [Kob02, Prop. 3.3]).

(6) Because ρ_ℓ is wildly ramified, $a(E/K) \geqslant 3$, and the Kodaira symbol of E/K can only be II, II^*, IV, or IV^* (see [Kob02, Thm. 3.1]), thus $m(E/K) = 1$, 9, 3, or 7, respectively. Since the minimal $v_K(\Delta_K)$ is odd by (2), the formula (8.4.1) shows that $m(E/K) + a(E/K)$ is even, and thus that $a(E/K)$ is odd.

(7) After applying, possibly multiple times, the changes of variables in Steps 2, 8, and 11 of Tate's algorithm as in [Sil94, IV.§9], we may suppose that the Weierstrass coefficient a_6 has valuation $\frac{m(E/K)+1}{2}$, which is coprime to 3 by (6).

PROPOSITION 8.7. *Let $p = 3$ and let ρ_ℓ be wildly ramified. Then the following are equivalent :*

(1) *$v_K(\Delta)$ is odd for any discriminant Δ of E/K;*

(2) *The inertia subgroup of M/K is isomorphic to S_3;*
(3) *$a(E/K)$ is odd;*
(4) $\rho_\ell(I_K) \simeq \mathrm{Dic}_3$.

Proof. We have seen in 8.6 that (4) implies all the other conditions. Suppose (1), then $e(M/K) \geqslant 6$, thus necessarily $\mathrm{Gal}(M/K) \simeq I(M/K) \simeq S_3$. Suppose (2), then $\rho_\ell(I_K)$ is non-abelian, so, by [Kob02, Thm. 3.1], we have (4). Suppose (3). Since ρ_ℓ is wildly ramified, the Kodaira symbol of E/K is II, II^*, IV, or IV^*, thus $m(E/K)$ is odd. Then, by (8.4.1), $v_K(\Delta_K)$ is odd, thus (1) holds. □

We recall Kobayashi's formula in the present setting:

Theorem 8.8. *[Kob02, Theorem 5.9] Under the hypotheses of 8.6 and with a_6 as in 8.6(7), the root number of E/K is given by*

$$w(E/K) = -(\Delta_K, a_6 v_K(a_6))_K \cdot \left(\frac{-1}{k_K}\right)^{\frac{v_K(\Delta_K)-1}{2}}.$$

Remark 8.9. We can replace the minimal discriminant Δ_K in the above formula with any discriminant of a defining Weierstrass equation over K, since they all define the same class in $K^\times/(K^\times)^4$.

The following is the main result of this section for which we will give two proofs.

Theorem 8.10. *Let E/K be an elliptic curve as in 8.6. Let $\lfloor\cdot\rfloor$ denote the floor function of real numbers. Then, the root number is given by*

$$w(E/K) = (-1)^{v_3(c(E/H))} \cdot \left(\frac{-1}{k_K}\right)^{\frac{a(E/K)+m(E/K)}{2} + \lfloor \frac{m(E/K)+1}{6} \rfloor}.$$

Remark 8.11. Since every exponent in the formula above can by replaced by any integer of the same parity, one may find many equivalent variants of this. The above form of the formula was deliberately chosen to pertain to the geometric interpretation described by 8.5. One might want to eliminate the slightly awkward double appearance of the invariant $m(E/K)$ or the floor function. For example, since $m(E/K) = 1, 3, 7$, or 9 it can be checked that the formula of Thm. 8.10 is equivalent to

$$w(E/K) = (-1)^{v_3(c(E/H))} \cdot \left(\frac{-1}{k_K}\right)^{\frac{a(E/K)-1}{2}} \cdot \left(\frac{m(E/K)+1}{k_K}\right).$$

Proof of Thm. 8.10 via Weierstrass coefficients. From the formula of tame Hilbert symbols (see [Neu99, V.(3.4)]), for any $\alpha, \beta \in K^\times$ of K-valuations a, b, respectively, we have

$$(\alpha, \beta)_K = \left(\frac{-1}{k_K}\right)^{ab} \cdot \left(\frac{\frac{\alpha^b}{\beta^a} \bmod \mathfrak{m}_K}{k_K}\right).$$

Since $v_K(\Delta_K) \equiv 1 \bmod 2$ (by 8.6.(2)) and $3 \nmid v_K(a_6)$ (by 8.6.(7)), the above formula gives

$$(\Delta_K, v_K(a_6))_K = \left(\frac{v_K(a_6)}{k_K}\right). \tag{8.11.1}$$

We fix a uniformizer $\varpi_H \in \mathfrak{m}_H$ and denote $\widetilde{a_6} := \frac{a_6}{\varpi_H^{v_H(a_6)}} \in \mathcal{O}_H^\times$. Then, Δ_K is a square in H, and

$$\frac{a_6^{v_K(\Delta_K)}}{\Delta_K^{v_K(a_6)}} \equiv \widetilde{a_6} \bmod (\mathcal{O}_H^\times)^2,$$

so

$$(\Delta_K, a_6)_K = \left(\frac{-1}{k_K}\right)^{v_K(a_6)} \cdot \left(\frac{\widetilde{a_6} \bmod \mathfrak{m}_H}{k_H}\right). \tag{8.11.2}$$

A straightforward verification in each case of $v_K(a_6) = \frac{m(E/K)+1}{2} = 1, 2, 4, 5$ proves that

$$\left(\frac{-1}{k_K}\right)^{v_K(a_6)} \cdot \left(\frac{v_K(a_6)}{k_K}\right) = \left(\frac{-1}{k_K}\right)^{1+\lfloor \frac{m(E/K)+1}{6} \rfloor}. \tag{8.11.3}$$

Multiplying (8.11.1) with (8.11.2) and then using (8.11.3) produces

$$(\Delta_K, a_6 v_K(a_6))_K = \left(\frac{-1}{k_K}\right)^{1+\lfloor \frac{m(E/K)+1}{6} \rfloor} \cdot \left(\frac{\widetilde{a_6} \bmod \mathfrak{m}_H}{k_H}\right). \tag{8.11.4}$$

Ogg's formula (8.4.1) gives

$$\left(\frac{-1}{k_K}\right)^{\frac{v_K(\Delta_K)-1}{2}} = \left(\frac{-1}{k_K}\right)^{\frac{a(E/K)+m(E/K)-2}{2}}. \tag{8.11.5}$$

LEMMA 8.12. *Let E/K be as in 8.6. Independently on the choice of the uniformiser ϖ_H in the definition of $\widetilde{a_6}$, we have*

$$-\left(\frac{\widetilde{a_6} \bmod \mathfrak{m}_H}{k_H}\right) = (-1)^{v_3(c(E/H))}.$$

PROOF. We apply Tate's algorithm by following the steps in [Sil94, IV.§9] over K and over H for each of the Kodaira types over K. We note that $a_1 = a_3 = 0$. Also, we cannot have Kodaira types other than II, II^*, IV, or IV^* over H by 8.6.(6).

II : We have $v_K(a_6) = 1$, so $v_H(a_6) = 2$, and E_H/H has Kodaira symbol IV. We find that $c(E/H) = 3$ if $\frac{a_6}{\varpi_H^2}$ is a square in $H^\times$ and $c(E/H) = 1$ otherwise.

II^* : We have $v_K(a_6) = 5$, so $v_H(a_6) = 10$, and we apply a change of variables over H like in (8.2.1) with $u = \varpi_H$ in order to minimize the Weierstrass equation over H. The new coefficient will be $a_6' = \frac{a_6}{\varpi_H^6}$. We find that E_H/H has Kodaira symbol IV^* and that $c(E/H) = 3$ if $\frac{a_6'}{\varpi_H^4} = \frac{a_6}{\varpi_H^{10}}$ is a square in $H^\times$ and $c(E/H) = 1$ otherwise.

IV : We have $v_K(a_6) = 2$, so $v_H(a_6) = 4$, and E_H/H has Kodaira symbol IV^*. We find that $c(E/H) = 3$ if $\frac{a_6}{\varpi_H^4}$ is a square in $H^\times$ and $c(E/H) = 1$ otherwise.

IV^* : We have $v_K(a_6) = 4$, so $v_H(a_6) = 8$, and we apply a change of variables like in (8.2.1) with $u = \varpi_H$ in order to minimize the Weierstrass equation over H. The new coefficient will be $a_6' = \frac{a_6}{\varpi_H^6}$. We find that E_H/H has Kodaira symbol IV and that $c(E/H) = 3$ if $\frac{a_6'}{\varpi_H^2} = \frac{a_6}{\varpi_H^8}$ is a square in $H^\times$ and $c(E/H) = 1$ otherwise. □

Plugging (8.11.4) and (8.11.5) into the formula of Thm. 8.8 and using Lemma 8.12 concludes the proof of Thm. 8.10. □

Another proof is based on the following result, whose original proof depends on a certain version of the global 3-parity conjecture (now a theorem by the same authors).

THEOREM 8.13. *[DD11, Theorem 6.3] Let M/K be a Galois extension of group S_3 and let H/K (resp. F/K) be a subextension of degree 2 (resp. 3). We denote $f_H = [k_H : \mathbb{F}_3]$ and $f_M = [k_M : \mathbb{F}_3]$. For an elliptic curve E/K we have*

$$w(E/K)w(E/H)w(E/F) = (-1)^{v_3\left(\frac{c(E/M)}{c(E/H)}\right)+f_M\cdot v_M\left(\frac{w_M}{w_K}\right)+f_H\cdot v_H\left(\frac{w_H}{w_K}\right)}.$$

REMARK 8.14. We note that in order to determine $w(E/K)$, the only root numbers that have to compute are associated to elliptic curves whose Galois representations have non-maximal, thus abelian, inertia image.

PROOF OF THM. 8.10 VIA MINIMAL DIFFERENTIALS. We apply Thm. 8.13 in the setting 8.6. We compute all the involved terms except $w(E/K)$ and $c(E/H)$.

Consider the elliptic curve E/F. It attains good reduction over L and L/F is a minimal such extension. Since L/F is totally ramified of degree 4, from [Kob02, Thm. 3.1] we see that the Kodaira type of E/F is III or III^*. Applying [Kob02, Thm. 1.1] gives

$$w(E/F) = \left(\frac{-2}{k_F}\right) = 1. \tag{8.14.1}$$

The extension L/H is abelian and totally ramified of degree 6, so from Thm. I.0.2,(1)we have

$$w(E/H) = (-1)^{\frac{q_H-1}{2}} = \left(\frac{-1}{k_H}\right) = \left(\frac{-1}{k_K}\right). \tag{8.14.2}$$

As we have seen in the proof of Lemma 8.12, E/H has type IV or IV^*, and in order to minimize the Weierstrass equation over H we had to make a change of variables (8.2.1) with $u = \varpi_H$ exactly in the case where E/K was of type

II^* or IV^*. We have noted in 8.5 that the types II^* and IV^* appear exactly when $\lfloor \frac{m(E/K)+1}{6} \rfloor = 1$, so

$$(-1)^{f_H \cdot v_H\left(\frac{w_H}{w_K}\right)} = \left(\frac{-1}{k_H}\right)^{\lfloor \frac{m(E/K)+1}{6} \rfloor} = \left(\frac{-1}{k_K}\right)^{\lfloor \frac{m(E/K)+1}{6} \rfloor}. \tag{8.14.3}$$

The Kodaira type of E/M is I_0^*. From Tate's algorithm $c(E/M) = 1$, 2, or 4, so

$$v_3(c(E/M)) = 0. \tag{8.14.4}$$

Since $\rho_\ell|_{G_M}$ has tame and finite ramification, the Weierstrass equation over M is minimal if and only if the M-valuation of its discriminant is < 12. Indeed, the "if" part is general and follows from the equations (8.2.1); the "only if" part can be deduced from Ogg's formula (8.4.1) over M as $a(E/M) = 2$ and $m(E/M) < 10$. We have $v_M(\Delta_K) = 6 \cdot v_K(\Delta_K)$, so in order to minimise the equation over M we will need to apply a change of variables (8.2.1) with $u \in M$ such that

$$v_M(u) = \lfloor \frac{v_K(\Delta_K)}{2} \rfloor = \frac{v_K(\Delta_K) - 1}{2}.$$

We have $u = \frac{w_M}{w_K}$ and, hence, by applying Ogg's formula,

$$(-1)^{f_M \cdot v_M\left(\frac{w_M}{w_K}\right)} = \left(\frac{-1}{k_K}\right)^{\frac{a(E/K)+m(E/K)-2}{2}}. \tag{8.14.5}$$

Plugging (8.14.1), (8.14.2), (8.14.3), (8.14.4), and (8.14.5) into the formula of Thm. 8.13 terminates the proof of Thm. 8.10. □

Chapter III

On local Tamagawa numbers of hyperelliptic curves

Abstract. For an odd prime number p, let J be the Jacobian of a hyperelliptic curve of genus $\frac{p-1}{2}$ defined over a p-adic field. We suppose that the attached ℓ-adic Galois representation is wildly ramified and give a formula for the number of rational points of the component group of the Néron model. As an application in the case where $p = 5$ and the curve has a discriminant of odd valuation, we give a formula for the local root number which no longer requires a Weierstrass equation, building on Thm. II.0.2.

The setting and main results

Let $p > 2$ be a prime number. We fix a finite extension $K/\mathbb{Q}_p$ and its algebraic closure $\overline{K}$. We adopt the convention that every algebraic extension of K considered in this text is contained in $\overline{K}$. By Γ_K, I_K, and I_K^{w} we denote the absolute Galois group, the inertia subgroup, and the wild inertia subgroup, respectively. Let v_K be the valuation of K normalized so that $v_K(K^\times) = \mathbb{Z}$. By $\mathcal{O}_K$, $\mathfrak{m}_K$, and k_K we denote the ring of integers, the maximal ideal, and the residue field of K, respectively. Let $\varpi_K \in \mathfrak{m}_K$ be a uniformizer of K. There exists a unique maximal unramified extension K^{ur}/K, its residue field $\overline{k}_K$ is an algebraic closure of k_K. We let $\Gamma_{k_K} := \mathrm{Gal}(\overline{k}_K/k_K)$.

0.1. The hypotheses. Throughout the chapter we fix the following setting. Let C/K be a hyperelliptic curve of genus $g = \frac{p-1}{2}$. Let J/K be its Jacobian, and let ρ_ℓ be the ℓ-adic Galois representation on $H^1_{\text{ét}}(C_{\overline{K}}, \mathbb{Q}_\ell) \cong H^1_{\text{ét}}(J_{\overline{K}}, \mathbb{Q}_\ell)$ for some prime number $\ell \neq p$. We suppose that ρ_ℓ is wildly ramified, i.e., that $\rho_\ell(I_K^{\mathrm{w}})$ is nontrivial.

0.2. Néron models. Let L/K be an algebraic extension. We form the Néron model $\mathcal{J}/\mathcal{O}_L$ of the abelian L-variety $J_L := J \times_K L$. Let $\mathcal{J}_{k_L}/k_L$ denote its special fiber. The identity component $\mathcal{J}^\circ_{k_L}$ of $\mathcal{J}_{k_L}$ is an extension of an abelian variety B by a product of a torus T and a unipotent group U. We denote the abelian, toric, and unipotent ranks of J_L/L by $a_L := \dim B$, $t_L := \dim T$, and $u_L := \dim U$, respectively. We have $a_L + t_L + u_L = g$.

The algebraic group $\Phi_L := \mathcal{J}_{k_L}/\mathcal{J}^\circ_{k_L}$ is finite. We define the local Tamagawa number of J (or C) over L as $c(C/L) := c(J/L) := |\Phi_L(k_L)|$. Under

the hypotheses given in 0.1, it follows from [Lor10, Prop. 2.1.(4)] that $c(C/L)$ divides p.

The main results of this chapter are the following.

THEOREM 0.3 (Prop. 1.2, Thm. 3.1). *Let C/K be as in 0.1. There exists a Weierstrass equation $Y^2 = P(X)$ defining C/K with $P \in \mathcal{O}_K[X]$ unitary and irreducible of degree p with constant coefficient a_0 of prime-to-p valuation $v < 2p$. Then the Tamagawa number is given by*

$$c(C/K) = \begin{cases} p & \text{if } a_0 \in (K^\times)^2, \\ 1 & \text{otherwise.} \end{cases}$$

Our proof of Thm. 0.3 relies on Dokchitser's algorithm [Dok18] which constructs an explicit regular model of C/K. We will also use the results of Bosch–Liu [BL99] that will allow to compute the Tamagawa number by using the geometry of this regular model.

As an application of Thm. 0.3, using our previous Thm. II.0.2 we derive another formula for the local root number (see I.1.19) in the case where $p = 5$ and C/K has a discriminant of odd valuation. Equivalently, this is the case where ρ_ℓ has the maximal possible inertia action. The new formula no longer refers to a particular Weierstrass equation.

THEOREM 0.4 (Cor. 4.3). *Let $p = 5$ and let C/K be as in 0.1. Let Δ be any discriminant of C/K, and let $H = K(\sqrt{\Delta})$. Let $m(C/K)$ denote the number of irreducible components of the special geometric fiber of the minimal regular model of C/K. Let $\left(\frac{\cdot}{k_K}\right)$ be the Legendre symbol on k_K, and let v_5 be the normalized 5-adic valuation on $\mathbb{Q}$. If H/K is ramified, then the root number is given by*

$$w(C/K) = (-1)^{[k_K:\mathbb{F}_5]} \cdot \left(\frac{m(C/K)+3}{k_K}\right) \cdot (-1)^{v_5(c(C/H))}.$$

1. A particular Weierstrass model

PROPOSITION 1.1. *Under the hypotheses 0.1, the Jacobian J/K has potentially good reduction, i.e., there exists a finite extension L/K for which we have $u_L = t_L = 0$. Also, $\rho_\ell(I_K^{\mathrm{w}})$ is cyclic of order p.*

PROOF. Following Grothendieck's semistable reduction theorem [SGA 7.I, p. 21, Thm. 6.1], there exists a Galois extension L'/K containing K^{ur} over which C attains semistable reduction, i.e., $u_{L'} = 0$. Equivalently, $\rho_\ell|_{I_{L'}}$ is unipotent and, in particular, torsion-free. On the other hand, since the pro-p and the ℓ-adic topologies are incompatible, $\rho(I_K^{\mathrm{w}})$ is finite. Therefore, L'/K^{ur} must wildly ramified, and let $p^r > 1$ be its wild ramification index. It follows from a result by Lorenzini [Lor90, Prop. 3.1] that

$$p^{r-1}(p-1) \leqslant 2u_{K^{\mathrm{ur}}} + t_{K^{\mathrm{ur}}} - t_{L'}.$$

Since the formation of the Néron model commutes with étale base change, we have

$$2u_{K^{\mathrm{ur}}} + t_{K^{\mathrm{ur}}} = 2u_K + t_K \leqslant 2g = p - 1.$$

The two inequalities above imply that $t_{L'} = 0$ and also that $r = 1$. Therefore, J/L' has good reduction. The subfield of L' fixed by a Frobenius lift in Γ_K defines a finite extension of K over which J has good reduction (see [ST68, p. 498]). □

We propose a slight generalization of Liu's results [Liu94b, §5.1].

PROPOSITION 1.2. *If C/K is as in 0.1, then it is defined by an equation $Y^2 = P(X)$, where $P \in K[X]$ is irreducible of degree p. Furthermore, P can be chosen of the form*

$$P(X) = X^p + a_{p-1}X^{p-1} + \ldots + a_0 \in \mathfrak{O}_K[X]$$

with $a_{p-1}, \ldots, a_0 \in \mathfrak{O}_K$ such that for all $1 \leqslant i \leqslant p-1$ we have

$$v_K(a_i) > v_K(a_0) \cdot \frac{p-i}{p}, \tag{1.2.1}$$

and $1 \leqslant v_K(a_0) \leqslant 2p-1$, $v_K(a_0) \neq p$.

PROOF. We know from the classical theory of hyperelliptic curves (see, e.g., [Liu02, 7. Prop. 4.24]) that C/K is defined by an equation $Y^2 = P(X)$ with $P \in K[X]$ of degree d equal to p or $p+1$. Let $M := K(J[2])$ be the finite Galois extension of K cut out by the kernel of the Γ_K-action on the 2-torsion points $J[2]$. By Prop. 1.1, the Jacobian J/K has potentially good reduction. It follows from [Ser61] that J_M/M attains good reduction over an extension of M of degree at most 2. Applying the Néron–Ogg–Shafarevich criterion shows that the finite p-groups $I^{\mathrm{w}}(M/K)$ and $\rho_\ell(I_K^{\mathrm{w}})$ are isomorphic.

Since M is the splitting field of P (see, e.g., [Mum84, 3.39, Cor. 2.11]), the group $\mathrm{Gal}(M/K)$ can be regarded as a subgroup G of the symmetric group S_d. The wild inertia subgroup $I^{\mathrm{w}}(M/K)$ is cyclic of order p and is normal in $\mathrm{Gal}(M/K)$, so G must be contained in the normalizer subgroup N of a p-cycle in S_d. The group N contains the Frobenius group $F_p = C_p \rtimes C_{p-1}$ where C_{p-1} acts faithfully on C_p. Using the conjugation action of S_d on its p-Sylow subgroups, we compute

$$|N| = \frac{|S_d|}{|\{p\text{-Sylow's of } S_d\}|} = \frac{d!}{\frac{d!}{(d-p)!\cdot p(p-1)}} = p(p-1).$$

We have thus proved that $N = F_p$ holds and that $\mathrm{Gal}(M/K)$ is isomorphic to a subgroup of F_p. If P is irreducible of degree $p+1$, then F_p must have a quotient of order $p+1$, which is impossible. On the other hand, if P has only irreducible factors of degrees $< p$, then $\mathrm{Gal}(M/K)$ injects into S_{p-1}^r for some $r \in \mathbb{N}$. However, this is impossible since $\mathrm{Gal}(M/K)$ has an element of order p because ρ_ℓ is wildly ramified. In any case, we proved that P has an irreducible

factor of degree p. If $\deg P = p+1$, the remaining linear factor gives a K-point on C which can be sent to infinity by a change of variables. We may now assume that $\deg P = p$.

In order to complete the proof we extend the arguments of [Liu94b, (5.1)]. We note that the above paragraph shows also that P is irreducible over K^{ur}. After making a change of variables, we may further assume that P is unitary with integral coefficients (see also Step 1 below). The Newton polygon of P must have a unique slope, so we obtain (1.2.1) with non-strict inequalities. Suppose that there is an equality for some $1 \leqslant i_0 \leqslant p-1$. Then, p divides $v_K(a_0)$. The polynomial

$$\widetilde{P}(X) := \varpi_K^{-v_K(a_0)} P\left(\varpi_K^{\frac{v_K(a_0)}{p}} X\right) \in \mathcal{O}_K[X]$$

is unitary and has coefficients $\widetilde{a}_0$ and $\widetilde{a}_{i_0}$ in $\mathcal{O}_K^\times$. Then, the derivative of the class $\overline{P}$ of $\widetilde{P}$ in $k_K[X]$ is not identically 0. Therefore, $\overline{P}$ splits into at least two coprime factors in $\overline{k}_K[X]$. By Hensel's lemma, this factorization lifts to $K^{\mathrm{ur}}[X]$, which is impossible. Therefore, the inequalities in (1.2.1) must be strict.

The last part of the proof is done algorithmically.

Step 1. Performing a change of variables $X \mapsto a^2X$, $Y \mapsto a^pY$ with $a \in K^\times$ and dividing by a^{2p} replaces a_0 by a_0a^{-2p}. With a suitable choice of a we obtain P such that $0 \leqslant v_K(a_0) \leqslant 2p-1$. The inequalities (1.2.1) are needed to ensure that the coefficients of P stay in $\mathcal{O}_K$.

Step 2. If $v_K(a_0) = v$ with $v = 0$ or p, then (since k_K is prefect) we may choose $b \in \mathcal{O}_K$ such that $b^p \equiv -a_0\varpi_K^{-v} \bmod \mathfrak{m}_K$. Performing the change $X \mapsto X + b\varpi_K^{v/p}$ produces P for which $v_K(a_0) > v$ (here we again need (1.2.1)). If $v_K(a_0) > 2p-1$, then we return to Step 1.

The algorithm ends eventually since Step 1 decreases the valuation of the discriminant of P and Step 2 does not change it (see [Liu96, §2]). □

2. A regular model having normal crossings

We shall construct a regular $\mathcal{O}_K$-model of C/K having normal crossings by following Dokchitser [Dok18]. We will recall the definitions needed to describe the model and gradually apply them for the polynomial $Y^2 - P(X)$ provided by Prop. 1.2.

2.1. Some elements of affine geometry. Let $n \in \mathbb{N}$. By an *affine subspace* A of $\mathbb{R}^n$ we mean a subset $A \subseteq \mathbb{R}^n$ such that for every $a \in A$, the set $V_A := \{v - a \mid v \in A\} \subseteq \mathbb{R}^n$ is an $\mathbb{R}$-vector subspace. The space V_A is independent of the choice of a. A map $h\colon A \to B$ between affine subspaces $A \subset \mathbb{R}^n$ and $B \subset \mathbb{R}^m$ is called an *affine map* if there exists a linear map $\widetilde{h}\colon \mathbb{R}^n \to \mathbb{R}^m$ and a $t \in \mathbb{R}^m$ such that for all $a \in A$ we have $h(a) = \widetilde{h}(a) + t$. If $a_1, \ldots, a_k \in A$ and $\mu_1, \ldots, u_k \in \mathbb{R}$ are such that $\sum_{i=1}^k \mu_i = 1$, then $\sum_{i=1}^k \mu_i a_i \in A$ and for every

affine map $h\colon A \to B$ we have $h(\sum_{i=1}^k \mu_i a_i) = \sum_{i=1}^k \mu_i h(a_i)$. By $\mathrm{Conv}(S)$ we denote the convex hull of a subset $S \subset \mathbb{R}^n$.

Similarly, a subset $\Lambda \subseteq \mathbb{Z}^n$ is called an *affine lattice* if for every $l \in \Lambda$, the subset $\Lambda - l \subseteq \mathbb{Z}^n$ is a free $\mathbb{Z}$-submodule. A map $h\colon \Lambda \to \Lambda'$ between affine sublattices $\Lambda \subset \mathbb{Z}^n$ and $\Lambda' \subset \mathbb{Z}^m$ is called *affine* if there exists a $\mathbb{Z}$-linear map $\widetilde{h}\colon \mathbb{Z}^n \to \mathbb{Z}^m$ and a $t \in \mathbb{Z}^m$ such that for all $l \in La$ we have $h(l) = \widetilde{h}(l) + t$. We will view $\mathbb{Z}^n$ as the canonical lattice in $\mathbb{R}^n$.

2.2. The Newton polytope. Let

$$Q(X,Y) = \sum_{(i,j)\in\mathbb{Z}^2} a_{ij} X^i Y^j \in K[X,Y]$$

be a polynomial in two variables. The *Newton polygon of* Q is

$$D := \mathrm{Conv}\big(\{(i,j) \in \mathbb{Z}^2 \mid a_{ij} \neq 0\}\big) \subset \mathbb{R}^2.$$

Let

$$\widetilde{D}_v := \mathrm{Conv}\left(\{(i,j,v_K(a_{ij})) \in \mathbb{R}^3 \mid a_{ij} \neq 0\}\right) \subset \mathbb{R}^3,$$

then the *Newton polytope of* Q is defined as the lower convex hull of $\widetilde{D}_v$, i.e.,

$$D_v := \{s \in \widetilde{D}_v \mid \forall \epsilon > 0,\ s - (0,0,\epsilon) \notin \widetilde{D}_v\} \subset \mathbb{R}^3.$$

The surface D_v is piecewise affine and can be homeomorphically transformed into the polygon D by setting the third coordinate (height) to zero. For each $(i,j) \in D$ let $h(i,j) \in \mathbb{R}$ denote its height defined so that $(i,j,h(i,j)) \in D_v$. The polyhedron D_v breaks into a collection of *closed two-dimensional faces* and *closed one-dimensional edges*. We identify each of these components with its projection in D. Let E_1 be the set of edges in D, let E_2 be the set of faces in D, and let $E_{1,2} = E_1 \cup E_2$.

2.3. Multiplicities. We note that every face of D_v is a convex polygon whose vertices have integral coordinates. More generally, for every $(i,j) \in D \cap \mathbb{Z}^2$ we have $h(i,j) \in \mathbb{Q}$. For every $\lambda \in E_{1,2}$ we define its *multiplicity* by

$$\delta_\lambda := \min\{n \in \mathbb{N}^* \mid \forall (i,j) \in \mathbb{Z}^2 \cap \lambda,\ n \cdot h(i,j) \in \mathbb{Z}\}.$$

2.4. Let P be a polynomial provided by Prop. 1.2, we describe the Newton polytope of $Y^2 - P(X)$. Let $a_0 = u\varpi_K^v$ with $u \in \mathcal{O}_K^\times$, $v \in \mathbb{Z}$. Let $\bar{u} \in k_K^\times$ be the class of u. In this case, the produced D and D_v are both triangles by (1.2.1), so there is only one face and three edges in D_v. The heights are given by (cf. 2.14)

$$h(i,j) = \begin{cases} \frac{v(p-i)}{p} & \text{if } j = 0 \text{ and } 0 \leqslant i \leqslant p, \\ \frac{v(p-i)}{p} - v/2 & \text{if } j = 1 \text{ and } 0 \leqslant i \leqslant \frac{p-1}{2}, \\ 0 & \text{if } (i,j) = (0,2). \end{cases} \tag{2.4.1}$$

We represent the polytope D_v in Figure 1 by drawing D and writing the corresponding heights of D_v for each point of $D \cap \mathbb{Z}^2$.

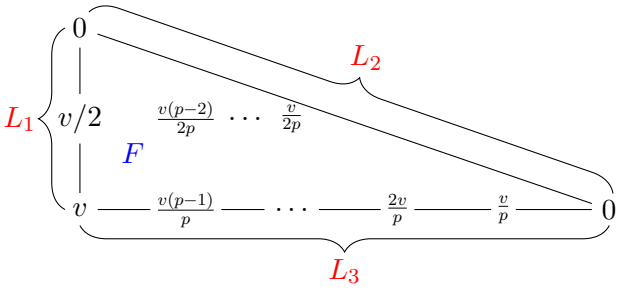


FIGURE 1. The Newton polytope of $Y^2 - P(X)$

If v is odd, then the only points of $D \cap \mathbb{Z}^2$ with integer heights are $(0,0)$, $(0,2)$, and $(p,0)$. If v is even, then one has to add $(0,1)$ to this list.

Let $F = D$ be the projection of the face of D_v. It is delimited by three edges: L_1 is the segment joining $(0,0)$ and $(0,2)$, L_2 is the segment joining $(0,2)$ and $(p,0)$, and L_3 is the segment joining $(0,0)$ and $(p,0)$. The multiplicities are given in Table 1.

TABLE 1. The multiplicities δ_λ associated to $Y^2 - P(X)$

λ	v even	v odd
F	p	$2p$
L_1	1	2
L_2	1	1
L_3	p	p

2.5. Restriction. We return to the general case 2.2. Let $\lambda \in E_{1,2}$ be any face or edge in D associated to $Q(X,Y)$. The points $P \in \lambda \cap \mathbb{Z}^2$ such that $h(P) \in \mathbb{Z}$ form a set S_λ and generate an affine sublattice $\Lambda_\lambda \subset \mathbb{Z}^2$ of rank $n \leqslant 2$. We note that $n = 1$ if λ is an edge, and $n = 2$ if λ is a face. We choose an affine isomorphism $\psi\colon \Lambda_\lambda \to \mathbb{Z}^n$. We denote $\mathbf{T}^{(i_1,i_2)} := T_1^{i_1} T_2^{i_2}$ and $\mathbf{T}^i := T_1^i$. The *restriction of Q to λ* is defined as

$$Q|_\lambda := \sum_{s \in S_\lambda} a_s \mathbf{T}^{\psi(s)} \in K[(T_i)_{1 \leqslant i \leqslant n}].$$

2.6. Reduction. We suppose that after performing a change of variables of the form $T_1 \to \varpi_K^i T_1$, $T_2 \to \varpi_K^j T_2$ for $Q|_\lambda$ we obtain a polynomial $\varpi_K^k \widetilde{Q|_\lambda}$ where $\widetilde{Q|_\lambda}$ has the coefficients in $\mathfrak{O}_K$. If the Newton polygons (as defined in 2.2) of $Q|_\lambda$ and

$$\overline{Q|_\lambda} := \widetilde{Q|_\lambda} \bmod \mathfrak{m}_K \in k_K[(T_i)_{1 \leqslant i \leqslant n}]$$

are equal, then the polynomial $\overline{Q|_\lambda}$ is called a *reduction of Q at λ*. In this case, we consider the k_K-subscheme $X_\lambda \subset \mathbb{G}_m^n \subset \mathbb{A}^n$ defined by the equation $\overline{Q|_\lambda} = 0$.

2.7. We continue where we left off with 2.4 and determine restrictions and reductions associated to each of the components F, L_1, L_2, and L_3, see Figure 1. We denote

$$v[2] := \begin{cases} 0 & \text{if } v \text{ is even,} \\ 1 & \text{if } v \text{ is odd.} \end{cases}$$

F : The set

$$S_F = \begin{cases} \{(0,0),(0,2),(0,1),(p,0)\} & \text{if } v \text{ is even,} \\ \{(0,0),(0,2),(p,0)\} & \text{if } v \text{ is odd,} \end{cases}$$

generates the lattice $\Lambda_F = \langle (p,0),(0,1+v[2])\rangle_{\mathbb{Z}}$. Let $\psi\colon \Lambda_F \to \mathbb{Z}^2$ be the affine isomorphism given by $\psi(0,0) = (0,0)$, $\psi(p,0) = (1,0)$ and $\psi(0,1+v[2]) = (0,1)$. The restriction of Q to F is then calculated as

$$Q|_F = \begin{cases} T_2^2 - T_1 - a_0 & \text{if } v \text{ is even,} \\ T_2 - T_1 - a_0 & \text{if } v \text{ is odd.} \end{cases}$$

A reduction of Q at F can be computed in a straightforward manner:

$$\overline{Q|_F} = \begin{cases} T_2^2 - T_1 - \bar{u} & \text{if } v \text{ is even,} \\ T_2 - T_1 - \bar{u} & \text{if } v \text{ is odd.} \end{cases}$$

The affine k_K-scheme $X_F \subset \mathbb{G}_m^2$ cut out by $\overline{Q|_F} = 0$ is smooth.

L_1 : The set $S_{L_1} = \{(0,0),(0,2),(0,1+v[2])\}$ generates a lattice of rank one, which we normalize by letting $\psi(0,1+v[2]) = 1$ and $\psi(0,0) = 0$. Then, the restriction of Q to L_1 is computed as

$$Q|_{L_1} = \begin{cases} T_1^2 - a_0 & \text{if } v \text{ is even,} \\ T_1 - a_0 & \text{if } v \text{ is odd.} \end{cases}$$

The reduction is given by

$$\overline{Q|_{L_1}} = \begin{cases} T_1^2 - \bar{u} & \text{if } v \text{ is even,} \\ T_1 - \bar{u} & \text{if } v \text{ is odd.} \end{cases}$$

If v is even, then $\overline{Q|_{L_1}} = 0$ cuts out our scheme $X_{L_1} \subset \mathbb{G}_m$, which has exactly two $\overline{k}_K$-points, and Γ_{k_K} permutes the two points nontrivially if and only if u is not a square in $K^\times$. If v is odd, then X_{L_1} has a single point, which is rational.

L_2 : The set $S_{L_2} = \{(0,2),(p,0)\}$ generates the affine lattice $\mathbb{Z}(p,-2) + (0,2)$. After normalizing it with $\psi(p,0) = 1$ and $\psi(0,2) = 0$, we obtain the restriction $Q|_{L_2} = 1 - T_1$. The reduction $\overline{Q|_{L_2}} = 1 - T_1 \in k_K[T_1]$ cuts out the scheme X_{L_2}, which has a single $\overline{k}_K$-point.

L_3 : The set $S_{L_3} = \{(0,0),(p,0)\}$ generates a lattice of rank one, which we normalize by letting $\psi(p,0) = 1$ and $\psi(0,0) = 0$. We obtain the restriction $Q|_{L_3} = -T_1 - a_0$. The reduction $\overline{Q|_{L_3}} = -T_1 - \bar{u}$ cuts out the scheme X_{L_3}, which has a single $\overline{k}_K$-point.

2.8. Slopes. We return to the general case 2.2. For each edge $\lambda \in E_1$ Dokchitser [Dok18, §3.12] defines a slope, denoted by $[s_1^\lambda, s_2^\lambda]$. In our applications, every edge will be "outer", i.e., one that bounds only one face.

Let $F \in E_2$ be a face bounded by λ (in other words, $\lambda \subset \partial F$). Let $h^F\colon \mathbb{R}^2 \to \mathbb{R}$ be the unique affine extension of the restriction of the height function $h|_F$ introduced in 2.2. On the other hand, there exists a unique surjective affine map $\lambda_F^*\colon \mathbb{Z}^2 \twoheadrightarrow \mathbb{Z}$ such that $\lambda_F^*|_{\lambda\cap\mathbb{Z}^2} = 0$ and $\lambda_F^*|_{F\cap\mathbb{Z}^2} \geqslant 0$. Next, we choose points $x_0, x_1 \in \mathbb{Z}^2$ such that $\lambda_F^*(x_0) = 0$ and $\lambda_F^*(x_1) = 1$. Let $\lfloor\cdot\rfloor$ be the floor function on $\mathbb{R}$. A *slope of an outer edge λ at F* is defined by the rational numbers

$$s_1^\lambda := \delta_\lambda \cdot (h^F(x_1) - h^F(x_0)) \quad \text{and} \quad s_2^\lambda := \lfloor s_1^\lambda - 1 \rfloor.$$

The numbers s_1^λ and s_2^λ depend on the choices of x_0 and x_1, however we will see that this dependency can be ignored for our purposes.

Remark 2.9. In practice, we can choose x_0 and x_1 as follows. For x_0 we take any point in the affine lattice L_λ generated by $\lambda \cap \mathbb{Z}^2$. The affine line $\mathrm{Conv}(L_\lambda) = \mathrm{Conv}(\Lambda_\lambda)$ divides $\mathbb{R}^2$ into two closed half-planes, and one of them, call it H, contains F. Then, we take $x_1 \in (H \cap \mathbb{Z}^2) \setminus L_\lambda$ to be any point with the minimal distance to the affine line $\mathrm{Conv}(L_\lambda)$.

Lemma 2.10. *The classes of s_1^λ and s_2^λ in $\mathbb{Q}/\mathbb{Z}$ and the number $s_1^\lambda - s_2^\lambda \in \mathbb{Q}$ do not depend on the choices of x_0 and x_1.*

Proof. We have $s_2^\lambda = \lfloor s_1^\lambda \rfloor - 1$, so it is enough to prove the claim for s_1^λ. The set $\lambda \cap \mathbb{Z}^2$ generates an affine sublattice $L_\lambda \subset \mathbb{Z}^2$ of rank one, which is the kernel of λ_F^*. We may choose $x_0', x_0'' \in \lambda \cap \mathbb{Z}^2$ such that $L_\lambda = x_0' + \mathbb{Z}(x_0'' - x_0')$.

Let $x_0 \in \mathbb{Z}^2$ be such that $\lambda_F^*(x_0) = 0$. It means that $x_0 \in L_\lambda$, so there exists $n \in \mathbb{Z}$ such that $x_0 = x_0' + n(x_0'' - x_0') = (1-n)x_0' + nx_0''$. Then, by recalling the properties of affine maps given in 2.1, we have

$$h^F(x_0) = (1-n) \cdot h^F(x_0') + n \cdot h^F(x_0'').$$

If then follows from the definition 2.3 of δ_λ that $\delta_\lambda \cdot h^F(x_0) \in \mathbb{Z}$.

Let x_1 and x_1' be points in $\mathbb{Z}^2$ such that $\lambda_F^*(x_1) = \lambda_F^*(x_1') = 1$. Then, $\lambda_F^*(x_0' + x_1 - x_1') = 0$. Applying the above paragraph we obtain

$$\delta_\lambda \cdot (h^F(x_1) - h^F(x_1')) = \delta_\lambda \cdot h^F(x_0' + x_1 - x_1') - \delta_\lambda \cdot h^F(x_0) \in \mathbb{Z}. \qquad \square$$

Remark 2.11. If λ is inner, i.e., if λ bounds two faces F_1 and F_2, then a slope is given by $s_1^\lambda := \delta_\lambda \cdot (h^{F_1}(x_1) - h^{F_1}(x_0))$ and $s_2^\lambda := \delta_\lambda \cdot (h^{F_2}(x_1) - h^{F_2}(x_0))$. Lemma 2.10 also holds for inner edges. In this case, our proof can be adapted

to show that s_2^λ is invariant in $\mathbb{Q}/\mathbb{Z}$. We observe that $h^{F_1}|_{L_\lambda} = h^{F_2}|_{L_\lambda}$, which immediately shows that $s_1^\lambda - s_2^\lambda$ is independent of the choice of x_0. Having fixed some point $x_0 \in L_\lambda$, for any $x_1, x_1' \in (\lambda_F^*)^{-1}(1)$ we have $x_0 + x_1 - x_1' \in L_\lambda$. For $i = 1, 2$ we obtain that

$$\delta_\lambda \cdot (h^{F_i}(x_1) - h^{F_i}(x_1')) = \delta_\lambda \cdot (h^{F_i}(x_0 + x_1 - x_1') - h^{F_i}(x_0))$$

is an integer independent from i.

2.12. Farey–Haros sequences. For every slope given by s_1^λ and s_2^λ we will need a sequence of rational numbers

(2.12.1)
$$s_1^\lambda = \frac{m_0}{d_0} > \frac{m_1}{d_1} > \ldots > \frac{m_{r+1}}{d_{r+1}} = s_2^\lambda \quad \text{such that} \quad \forall i,\ \det\begin{pmatrix} m_i & m_{i+1} \\ d_i & d_{i+1} \end{pmatrix} = 1.$$

Such sequences always exist as subsequences of the Farey–Haros sequences (see, e.g., [NZM91, §6.1]) translated by integers and can be chosen to be minimal. In our case of an outer edge λ, the fractions in (2.12.1) can be produced as follows. We note that the open interval $(s_2^\lambda, s_1^\lambda)$ contains at most one integer, which is $\lfloor s_1^\lambda \rfloor$. Let $\frac{m_i}{d_i}$ be a rational number with m_i and $d_i > 1$ coprime. Let $d_{i+1} \in \mathbb{Z}$ be such that $0 < d_{i+1} < d_i$ and its class in $(\mathbb{Z}/d_i\mathbb{Z})^\times$ is the multiplicative inverse of the class of m_i. Then there exists a unique $m_{i+1} \in \mathbb{Z}$ such that $m_i d_{i+1} - m_{i+1} d_i = 1$. Applying this construction recursively we will eventually be left with $d_r = 1$. Then $m_{r+1} = m_r - 1$ and $d_{r+1} = 1$. We note that if $d_0 \geqslant 2$, then $r \geqslant 1$, and for every $i \leqslant r-1$ we have $d_i \geqslant 2$ and $\lfloor \frac{m_i}{d_i} \rfloor = \lfloor \frac{m_{i+1} d_i + 1}{d_{i+1} d_i} \rfloor = \lfloor \frac{m_{i+1}}{d_{i+1}} \rfloor$.

By Lemma 2.10, changing the choices of x_0 and x_1 in the definition of a slope translates s_1^λ and s_2^λ by some common integer. We note that translating each member of a sequence (2.12.1) by some common integer produces a sequence which also satisfies the determinant requirement. It follows that the sequence of denominators $d_0 > d_1 > \ldots > d_r = d_{r+1} = 1$ constructed above does not depend on the choices of x_0 and x_1.

Remark 2.13. A sequence (2.12.1) can be also produced as follows. Every rational number can be written in a unique way as a continued fraction

$$s_1^\lambda = c_0 + \cfrac{1}{c_1 - \cfrac{1}{c_2 - \cfrac{1}{\ddots - \cfrac{1}{c_r}}}} = c_0 + \frac{1|}{|c_1} - \frac{1|}{|c_2} - \ldots - \frac{1|}{|c_r}$$

with $r \in \mathbb{N}$, $c_0 \in \mathbb{Z}$, and $c_1, \ldots c_r \in \mathbb{N}_{\geqslant 2}$. Let q_j denote the convergent $c_0 + \frac{1|}{|c_1} - \frac{1|}{|c_2} - \ldots - \frac{1|}{|c_j}$. Writing q_j in the lowest terms gives $\frac{m_i}{d_i} = q_{r-i}$ for

$0 \leqslant i \leqslant r$, and $m_{r+1} = c_0 - 1$, $d_{r+1} = 1$. See [Dok18, Remark 3.15] for more details and references.

2.14. We will now compute the slopes for every $\lambda \in \{L_1, L_2, L_3\}$, see Figure 1, associated to $Y^2 - P(X)$ as in 2.4. Recall that the multiplicities δ_λ are given in Table 1. For the unique face F, the function h^F is given by

$$h^F(i,j) = -\frac{vi}{p} - \frac{vj}{2} + v.$$

L_1: We choose $x_0 = (0,2)$ and $x_1 = (1,1)$. Then the slope is given by $s_1^{L_1} = \delta_{L_1} \cdot \frac{v(p-2)}{2p}$ and $s_2^{L_1} = \lfloor s_1^{L_1} - 1 \rfloor$.

L_2: We choose $x_0 = (0,2)$ and $x_1 = (\frac{p-1}{2}, 1)$. Then the slope is given by $s_1^{L_2} = \frac{v}{2p}$ and $s_2^{L_2} = \lfloor s_1^{L_2} - 1 \rfloor$.

L_3: We choose $x_0 = (p,0)$ and $x_1 = (0,1)$. Then the slope is given by $s_1^{L_3} = \frac{pv}{2}$ and $s_2^{L_3} = \lfloor s_1^{L_3} - 1 \rfloor$.

2.15. Description of a regular model. As we have seen in 2.7, the scheme X_λ / k_K is smooth for each $\lambda \in \{F, L_1, L_2, L_3\}$. Then, C/K satisfies the hypotheses of [Dok18, Thm. 3.13], which produces a regular model $\mathscr{C}/\mathcal{O}_K$. Moreover, the model $\mathscr{C}/\mathcal{O}_K$ has normal crossings, i.e., the special fiber $\mathscr{C}_{k_K}$ defines an effective divisor on $\mathscr{C}$ which has normal crossings, see [Liu02, 9. Def. 1.6]. The special geometric fiber $\mathscr{C}_{\overline{k}_K}/\overline{k}_K$ is described by the contributions of the X_λ's as follows.

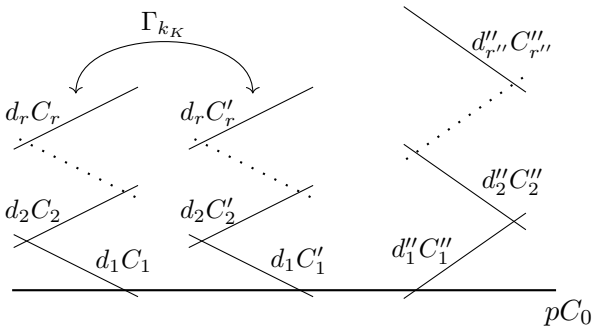


FIGURE 2. The structure of $\mathscr{C}_{\overline{k}_K}$ when v is even. The Γ_{k_K}-action is trivial if and only if $a_0 \in (K^\times)^2$.

F : The smooth compactification of X_F is $\overline{X}_F \simeq \mathbb{P}^1$. It appears as an irreducible component of the special fiber with multiplicity δ_F. This component will be denoted by C_0.

L_1 : Each point of $X_{L_1}(\overline{k}_K)$ corresponds to a chain of transversally intersecting $\mathbb{P}^1$'s starting at C_0. The multiplicities of the components of the chain are given by the sequence $\delta_{L_1} d_1 > \delta_{L_1} d_2 > \ldots > \delta_{L_1} d_r$ with d_i's as in (2.12.1) for $s_1^{L_1}$ and $s_2^{L_1}$. The Galois action on the set of

chains is given by the Galois action on $X_{L_1}(\overline{k}_K)$. It is nontrivial if and only if v is even and $a_0 \notin (K^\times)^2$.

If v is even, then we have two chains. Their components are denoted by $C_1, \dots, C_r$ and $C'_1, \dots, C'_r$.

If v is odd, then we have a single chain $C_1, \dots, C_r$.

L_2 : The set $X_{L_2}(\overline{k}_K)$ is a singleton. This gives a single chain of $\mathbb{P}^1$'s starting at C_0, and the multiplicities of the components are given by the sequence $d''_1 > d''_2 > \dots > d''_{r''}$ as in (2.12.1) for $s_1^{L_2}$ and $s_2^{L_2}$. The components of the chain will be denoted by $C''_1, \dots, C''_{r''}$.

L_3 : The set $X_{L_3}(\overline{k}_K)$ is a singleton. This produces a single chain of $\mathbb{P}^1$'s starting at C_0.

If v is even, then $s_1^{L_3} = \frac{pv}{2} \in \mathbb{Z}$, so we find that $r = 0$ in (2.12.1). This means that L_3 does not contribute to the special fiber.

If v is odd, then $s_1^{L_3} = \frac{pv}{2} > \lfloor \frac{pv}{2} \rfloor > s_2^{L_3}$, so $r = 1$. We have a single chain consisting of only one component C''_0 of multiplicity p.

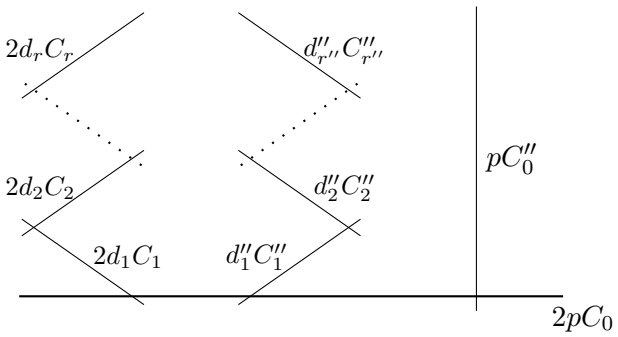


FIGURE 3. The structure of $\mathscr{C}_{\overline{k}_K}$ when v is odd. The Γ_{k_K}-action is trivial.

COROLLARY 2.16. *We have $d_r = d''_{r''} = 1$. Moreover, if v is odd (resp. even), then $\mathscr{C}_{\overline{k}_K}$ has exactly 1 (resp. 3) irreducible component(s) of multiplicity 1.*

PROOF. For each $\lambda \in \{L_1, L_2\}$, the number s_1^λ is not an integer, so $r \geqslant 1$ and $r'' \geqslant 1$. Also, the only trivial denominators in (2.12.1) are $d_r = d_{r+1} = d''_{r''} = d''_{r''+1} = 1$. The corollary can now be deduced from Figures 2 and 3. □

REMARK 2.17. If we take the minimal sequence in (2.12.1), then the regular model $\mathscr{C}/\mathcal{O}_K$ produced above is minimal as a regular model having normal crossings (see [Dok18, §5]), but, in general, it is not minimal as just a regular model. The minimal regular model can be obtained from $\mathscr{C}/\mathcal{O}_K$ by sequentially contracting the $\mathbb{P}^1$'s that appear in the special fiber with self-intersection number -1. Doing this, however, does not preserve the property of having normal crossings.

3. Tamagawa numbers via intersection theory

This section is devoted to proving the following.

THEOREM 3.1. *Let C/K be as in 0.1. If P is given by Prop. 1.2, then*

$$c(C/K) = \begin{cases} p & \text{if } a_0 \in (K^\times)^2, \\ 1 & \text{otherwise.} \end{cases}$$

Let $\mathscr{C}/\mathcal{O}_K$ be the regular model having normal crossings whose special geometric fiber was described in 2.15.

3.2. Intersection matrices. Let $\overline{I}$ denote the set of all irreducible components of $\mathscr{C}_{\overline{k}_K}$. Let $\mathbb{Z}^{\overline{I}}$ denote the free $\mathbb{Z}$-module on $\overline{I}$. Then

$$\operatorname{rk}\left(\mathbb{Z}^{\overline{I}}\right) = |\overline{I}| = \begin{cases} 1 + 2r + r'' & \text{if } v \text{ is even,} \\ 2 + r + r'' & \text{if } v \text{ is odd.} \end{cases}$$

The group Γ_{k_K} acts $\mathbb{Z}$-linearly on $\mathbb{Z}^{\overline{I}}$. As seen in 2.15, the action is trivial if $a_0 \in (K^\times)^2$ or if v is odd. Otherwise, the Frobenius element in Γ_{k_K} fixes $C_0, C_1'', \ldots, C_{r''}''$ and exchanges each C_i with C_i' for $1 \leqslant i \leqslant r$.

Viewing any two components $C, C' \in \overline{I}$ as Weil divisors on $\mathscr{C}_{\mathcal{O}_{K^{\mathrm{ur}}}}$, we denote by $\langle C, C' \rangle$ their intersection number. Since the Jacobian J/K has potentially good reduction (by 1.1), we see from [BLR90, 9.6, Remark 8] that the configuration of the components of $\mathscr{C}_{\overline{k}_K}$ is "tree-like", and thus, in particular, $\langle C, C' \rangle = 1$ whenever $C \neq C'$ and $C \cap C' \neq \varnothing$. More directly, we can obtain the same conclusion by using the fact that $\mathscr{C}_{\mathcal{O}_{K^{\mathrm{ur}}}}$ has normal crossings together with the description of the special fiber as in Figures 2 and 3.

Let $\overline{\alpha}\colon \mathbb{Z}^{\overline{I}} \to \mathbb{Z}^{\overline{I}}$ be the $\mathbb{Z}$-linear and Γ_{k_K}-equivariant map such that for all $C \in \overline{I}$ we have

$$\overline{\alpha}(C) = \sum_{C' \in \overline{I}} \langle C, C' \rangle C'.$$

Let $\overline{\beta}\colon \mathbb{Z}^{\overline{I}} \to \mathbb{Z}$ be the $\mathbb{Z}$-linear and Γ_{k_K}-equivariant map which sends each element $C \in \overline{I}$ to its multiplicity d_C in $\mathscr{C}_{\overline{k}_K}$, and let

$$\overline{\beta}^\top := \sum_{C \in \overline{I}} d_C C \in \mathbb{Z}^{\overline{I}}.$$

Let $\iota_i := \langle C_i, C_i \rangle$ and $\iota_i'' := \langle C_i'', C_i'' \rangle$ denote the indicated self-intersection numbers. We define the tridiagonal matrices

$$B := \begin{pmatrix} \iota_1 & 1 & & 0 \\ 1 & \iota_2 & \ddots & \\ & \ddots & \ddots & 1 \\ 0 & & 1 & \iota_r \end{pmatrix} \quad \text{and} \quad B'' := \begin{pmatrix} \iota_1'' & 1 & & 0 \\ 1 & \iota_2'' & \ddots & \\ & \ddots & \ddots & 1 \\ 0 & & 1 & \iota_{r''}'' \end{pmatrix}.$$

PROPOSITION 3.3. *The map $\overline{\alpha}$ has rank $|\overline{I}|-1$, and $\ker\overline{\alpha}$ is generated by $\overline{\beta}^\top$. We have $|\det B| = p$ and $|\det B''| = \delta_F$.*

(1) *If v is even, then the matrix $\overline{M}$ of $\overline{\alpha}$ in the basis*

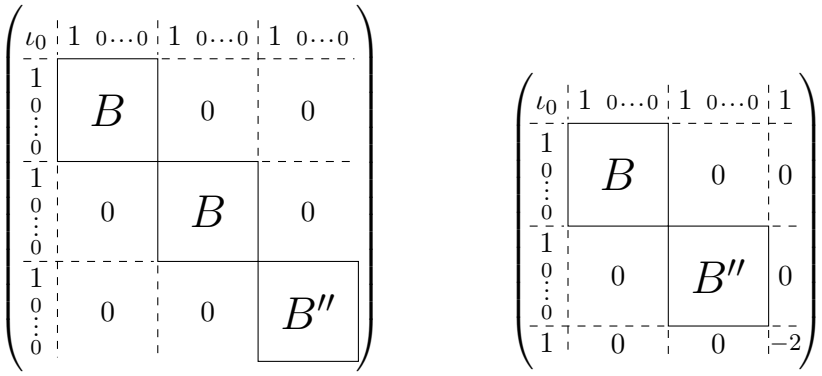
$$(C_0, C_1, \dots, C_r, C_1', \dots, C_r', C_1'', \dots, C_{r''}'')$$

is given in Figure 4a.

(2) *If v is odd, then the matrix $\overline{M}$ of $\overline{\alpha}$ in the basis*

$$(C_0, C_1, \dots, C_r, C_1'', \dots, C_{r''}'', C_0'')$$

is given in Figure 4b.



(A) even v (B) odd v

FIGURE 4. The matrix $\overline{M}$ of $\overline{\alpha}$

PROOF. The divisor given by $\mathscr{C}_{\overline{k}_K}$ on $\mathscr{C}_{\mathfrak{O}_{K^{\mathrm{ur}}}}$ is principal, thus for every $C \in \overline{I}$ we have $\overline{\beta}\circ\overline{\alpha}(C) = \langle C, \mathscr{C}_{\overline{k}_K}\rangle = 0$. Since the bilinear form $\langle\cdot,\cdot\rangle$ is symmetric, we also have $\overline{\beta}^\top \in \ker\overline{\alpha}$. Furthermore, if we regard $\langle\cdot,\cdot\rangle$ as a real quadratic form, then [Liu02, 9. Thm. 1.23] shows that its isotropic cone is generated by $\overline{\beta}^\top$. Therefore, $\overline{\alpha}$ has rank $|\overline{I}|-1$ and $(\ker\overline{\alpha})\otimes_{\mathbb{Z}}\mathbb{R} = \mathbb{R}\cdot\overline{\beta}^\top$. By Cor. 2.16, $\overline{\beta}^\top$ has some coordinates equal to 1, so we must have $\ker\overline{\alpha} = \mathbb{Z}\cdot\overline{\beta}^\top$.

In both (1) and (2), the desired form of $\overline{M}$ follows from the discussion in 2.15. The families $\mathbb{B} := (C_1, \dots, C_r)$ and $\mathbb{B}'' := (C_1'', \dots, C_{r''}'')$ are free in $\mathbb{Z}^{\overline{I}}$ and generate free $\mathbb{Z}$-submodules, denoted by $\langle\mathbb{B}\rangle$ and $\langle\mathbb{B}''\rangle$, respectively. The structure of the isotropic cone of $\langle\cdot,\cdot\rangle$ implies that the restrictions of $\langle\cdot,\cdot\rangle$ to $\langle\mathbb{B}\rangle$ and $\langle\mathbb{B}''\rangle$ are nondegenerate as real bilinear forms. This implies that B and B'' are invertible as matrices with real coefficients. Rewriting $\overline{\alpha}(\overline{\beta}^\top) = 0$ in terms of the matrices from Figure 4 and looking at the components in $\langle\mathbb{B}\rangle$ and $\langle\mathbb{B}''\rangle$

gives respectively

$$B\begin{pmatrix}\delta_{L_1}d_1\\ \vdots\\ \delta_{L_1}d_r\end{pmatrix}=\begin{pmatrix}-\delta_F\\ 0\\ \vdots\\ 0\end{pmatrix}\quad\text{and}\quad B''\begin{pmatrix}d''_1\\ \vdots\\ d''_{r''}\end{pmatrix}=\begin{pmatrix}-\delta_F\\ 0\\ \vdots\\ 0\end{pmatrix}. \tag{3.3.1}$$

We multiply the equalities of (3.3.1) on the left by the adjugate matrices of B and B'', respectively, and then compare the bottom coefficients in order to obtain $|\det B|=\frac{\delta_F}{\delta_{L_1}d_r}=p$ and $|\det B''|=\frac{\delta_F}{d''_{r''}}=\delta_F$. □

3.4. Computation of Tamagawa numbers. By the Γ_{k_K}-equivariant version of Raynaud's theorem given in [BL99, Thm. 1.1], we have a short exact sequence of Γ_{k_K}-modules

$$0\to\operatorname{Im}\overline{\alpha}\to\operatorname{Ker}\overline{\beta}\to\Phi_K(\overline{k}_K)\to 0. \tag{3.4.1}$$

We denote $\mathbb{Z}^I:=\left(\mathbb{Z}^{\overline{I}}\right)^{\Gamma_{k_K}}$. Let $\alpha\colon\mathbb{Z}^I\to\mathbb{Z}^I$ and $\beta\colon\mathbb{Z}^I\to\mathbb{Z}$ be the respective restrictions of $\overline{\alpha}$ and $\overline{\beta}$ to $\mathbb{Z}^I$. The set of Γ_{k_K}-orbits in $\overline{I}$ induces a canonical basis of $\mathbb{Z}^I$, denoted by I. Since the Γ_{k_K}-orbit of C_0 is trivial, we take the first element of I to be C_0. We will write I explicitly when necessary.

It follows from Prop. 1.2 that C has a K-point, and thus Bosch–Liu [BL99, Cor. 1.12] shows that (3.4.1) induces a short exact sequence

$$0\to\operatorname{Im}\alpha\to\operatorname{Ker}\beta\to\Phi_K(k_K)\to 0. \tag{3.4.2}$$

Proof of Thm. 3.1. Following (3.4.2) we only need to compute the order of the quotient $\operatorname{Ker}\beta\big/\operatorname{Im}\alpha$. To do this we shall apply Lorenzini's formula [BL99, Remark 1.16] for the matrix M associated to α in the basis I and its $(1,1)$-minor, denoted by $m^*_{1,1}$. We note that in this formula we have $r_1=1$ since the Γ_{k_K}-orbit of C_0 is trivial, $e_1=1$ since k_K is perfect, and $d=\delta'=1$ by Cor. 2.16. In our setting, Lorenzini's formula is

$$\left|\ker\beta\big/\operatorname{Im}\alpha\right|=|m^*_{1,1}|\cdot\beta(C_0)^{-2}=|m^*_{1,1}|\cdot\delta_F^{-2}. \tag{3.4.3}$$

If $a_0\in(K^\times)^2$, then v must be even, and the discussion in 2.15 shows that Γ_{k_K} acts trivially on $\mathbb{Z}^{\overline{I}}$, so $\alpha=\overline{\alpha}$, $\beta=\overline{\beta}$, and $M=\overline{M}$. It now follows from (3.4.3) and Prop. 3.3 that

$$c(C/K)=\left|\ker\beta\big/\operatorname{Im}\alpha\right|=|\det B|^2\cdot|\det B''|\cdot p^{-2}=p.$$

We now suppose that $a_0\notin(K^\times)^2$. If v is even, then

$$I=(C_0,C_1+C'_1,\dots,C_r+C'_r,C''_1,\dots,C''_{r''})$$

is a $\mathbb{Z}$-basis of $\mathbb{Z}^I$, in which the matrix of α is given by

$$M = \begin{pmatrix} \iota_0 & 2 & 0\cdots 0 & 1 & 0\cdots 0 \\ 1 & & & & \\ 0 & & B & & 0 \\ \vdots & & & & \\ 0 & & & & \\ 1 & & & & \\ 0 & & & & \\ \vdots & & 0 & & B'' \\ 0 & & & & \end{pmatrix}.$$

Now (3.4.3) and Prop. 3.3 give

$$c(C/K) = \left| \ker \beta \Big/ \operatorname{Im} \alpha \right| = |\det B| \cdot |\det B''| \cdot p^{-2} = 1.$$

If v is odd, then $\alpha = \overline{\alpha}$ and $M = \overline{M}$ always, so (3.4.3) and Prop. 3.3 give

$$c(C/K) = \left| \ker \beta \Big/ \operatorname{Im} \alpha \right| = |\det B| \cdot |\det B''| \cdot 2 \cdot (2p)^{-2} = 1. \qquad \square$$

4. Applications to local root numbers

We continue in the setting fixed in 0.1. Let $w(C/K)$ denote the root number associated to ρ_ℓ (see, e.g., I.1.19 or [Roh94, §12]). Let v_p denote the normalized p-adic valuation on $\mathbb{Q}$, let $(\cdot,\cdot)_K$ denote the quadratic Hilbert symbol on $K^\times$, and let $\left(\frac{\cdot}{k_K}\right)$ denote the Legendre symbol on $k_K^\times$.

Proposition 4.1. *Let C/K be as in 0.1, and let P and a_0 be provided by Prop. 1.2. We suppose that some discriminant $\Delta \in K$ of C/K has odd valuation and let $H = K(\sqrt{\Delta})$. Then*

$$(\Delta, a_0)_K \cdot \left(\frac{-1}{k_K}\right)^{v_K(a_0)} = -(-1)^{v_p(c(C/H))}.$$

Proof. We observe that H/K is a ramified extension of degree 2. Let $\epsilon = 1$ if $a_0 \in (H^\times)^2$ and $\epsilon = -1$ otherwise. Similarly as we did earlier to prove (II.8.11.2), by applying [Neu99, V.(3.4)] we obtain

$$(\Delta, a_0)_K = \epsilon \cdot \left(\frac{-1}{k_K}\right)^{v_K(a_0)}.$$

We note that C/H also satisfies the hypotheses of Prop. 1.2 and thus, as in its proof, P is irreducible over H. The integer $v_H(a_0) = 2v_K(a_0)$ is even and prime to p. If necessary, we make a change of variables like in the proof of Prop. 1.2, Step 1, in order to obtain an irreducible polynomial $P' \in \mathfrak{O}_H[X]$ with constant coefficient a_0' having prime-to-p valuation $v_H(a_0') < 2p$. We note that $a_0' \equiv a_0 \bmod (H^\times)^2$ and, in particular, $v_H(a_0')$ is even. It follows from Thm. 3.1 that $a_0' \in (H^\times)^2$ if and only if $c(C/H) = p$. Thus $\epsilon = -(-1)^{v_p(c(C/H))}$. $\square$

Remark 4.2. The choice of Δ in Prop. 4.1 is irrelevant since all discriminants define the same class in $K^\times/(K^\times)^2$.

COROLLARY 4.3. *Let $p = 5$ and let C/K be of genus $g = 2$ as in 0.1. We suppose that some discriminant Δ of C/K has odd valuation and let $H = K(\sqrt{\Delta})$. Let $m(C/K)$ denote the number of irreducible components of the special geometric fiber of the minimal regular model of C/K. The root number is given by*

$$w(C/K) = (-1)^{[k_K:\mathbb{F}_5]} \cdot \left(\frac{m(C/K)+3}{k_K}\right) \cdot (-1)^{v_5(c(C/H))}.$$

PROOF. Follows from Thm. II.0.2, Prop. 4.1, and $\left(\frac{-1}{k_K}\right) = 1$. □

REMARK 4.4. Prop. 4.1 may be used with Bisatt's result [Bis21, Thm. 2.1] in order to obtain another formula of the root number for hyperelliptic curves of higher genus. It would be interesting to replace the integer $v_K(a_0)$ by an invariant of C/K that does not depend on a Weierstrass equation. The formulae from Thm. II.0.5 and Cor. 4.3 suggest that the invariant $m(C/K)$ might be suitable for this purpose. Under the hypotheses of 0.1 the integer $v_K(a_0)$ determines $m(C/K)$ completely (see Remark 2.17), however the converse in not true, see Table II.2.

Bibliography

[AS10] A. Abbes and T. Saito, "Local Fourier transform and epsilon factors", *Compos. Math.*, vol. 146, no. 6, pp. 1507–1551, 2010. DOI: 10.1112/S0010437X09004631.

[BEW98] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi sums*, ser. Canadian Mathematical Society Series of Monographs and Advanced Texts. John Wiley & Sons, Inc., New York, 1998, pp. xii+583.

[BH06] C. J. Bushnell and G. Henniart, *The local Langlands conjecture for* GL(2), ser. Grundlehren Math. Wiss. Springer-Verlag, Berlin, 2006, vol. 335, pp. xii+347. DOI: 10.1007/3-540-31511-X.

[Bis19] M. Bisatt, "Explicit root numbers of abelian varieties", *Trans. Amer. Math. Soc.*, vol. 372, no. 11, pp. 7889–7920, 2019. DOI: 10.1090/tran/7926.

[Bis21] ——, *Root number of the jacobian of* $y^2 = x^p + a$, 2021. arXiv: 2102.05720 [math.NT].

[BKS18] A. Brumer, K. Kramer, and M. Sabitova, "Explicit determination of root numbers of abelian varieties", *Trans. Amer. Math. Soc.*, vol. 370, no. 4, pp. 2589–2604, 2018. DOI: 10.1090/tran/7116.

[BL99] S. Bosch and Q. Liu, "Rational points of the group of components of a Néron model", *Manuscripta Math.*, vol. 98, no. 3, pp. 275–293, 1999. DOI: 10.1007/s002290050140.

[BLR90] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, ser. Ergeb. Math. Grenzgeb. (3). Springer-Verlag, Berlin, 1990, vol. 21, pp. x+325. DOI: 10.1007/978-3-642-51438-8.

[Bou70] N. Bourbaki, *Éléments de mathématique. Algèbre. Chapitres 1 à 3*. Hermann, Paris, 1970, pp. xiii+635 (not consecutively paged).

[Čes18] K. Česnavičius, "The ℓ-parity conjecture over the constant quadratic extension", *Math. Proc. Cambridge Philos. Soc.*, vol. 165, no. 3, pp. 385–409, 2018. DOI: 10.1017/S030500411700055X.

[CFKS10] J. Coates, T. Fukaya, K. Kato, and R. Sujatha, "Root numbers, Selmer groups, and non-commutative Iwasawa theory", *J. Algebraic Geom.*, vol. 19, no. 1, pp. 19–97, 2010.

[Cha95] C.-L. Chai, "Every ordinary symplectic isogeny class in positive characteristic is dense in the moduli", *Invent. Math.*, vol. 121, no. 3, pp. 439–479, 1995. DOI: 10.1007/BF01884309.

[Cha00] ——, "Néron models for semiabelian varieties: congruence and change of base field", *Asian J. Math.*, vol. 4, no. 4, pp. 715–736, 2000. DOI: 10.4310/AJM.2000.v4.n4.a1.

[Con94] I. Connell, "Calculating root numbers of elliptic curves over Q", *Manuscripta Math.*, vol. 82, no. 1, pp. 93–104, 1994. DOI: 10.1007/BF02567689.

[Cop20] N. Coppola, *Wild galois representations: a family of hyperelliptic curves with large inertia image*, 2020. arXiv: 2001.08287 [math.NT].

[DD08] T. Dokchitser and V. Dokchitser, "Root numbers of elliptic curves in residue characteristic 2", *Bull. Lond. Math. Soc.*, vol. 40, no. 3, pp. 516–524, 2008. DOI: 10.1112/blms/bdn034.

[DD10] ——, "On the Birch-Swinnerton-Dyer quotients modulo squares", *Ann. of Math. (2)*, vol. 172, no. 1, pp. 567–596, 2010. DOI: 10.4007/annals.2010.172.567.

[DD11] ——, "Root numbers and parity of ranks of elliptic curves", *J. reine angew. Math.*, vol. 658, pp. 39–64, 2011.

[Del73] P. Deligne, "Les constantes des équations fonctionnelles des fonctions L", in *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, ser. Lecture Notes in Math. Vol. 349, Springer, Berlin, 1973, pp. 501–597.

[Del85] ——, *Le discriminant d'une courbe*, Lettre à Quillen, Appendice 3, 1985.

[DM69] P. Deligne and D. Mumford, "The irreducibility of the space of curves of given genus", *Inst. Hautes Études Sci. Publ. Math.*, no. 36, pp. 75–109, 1969.

[Dok13] T. Dokchitser, "Notes on the parity conjecture", in *Elliptic curves, Hilbert modular forms and Galois deformations*, ser. Adv. Courses Math. CRM Barcelona, Birkhäuser/ Springer, Basel, 2013, pp. 201–249.

[Dok18] ——, *Models of curves over dvrs*, 2018. arXiv: 1807.00025 [math.NT].

[Dwo56] B. Dwork, "On the Artin root number", *Amer. J. Math.*, vol. 78, pp. 444–472, 1956. DOI: 10.2307/2372524.

[FQ73] A. Fröhlich and J. Queyrut, "On the functional equation of the Artin L-function for characters of real representations", *Invent. Math.*, vol. 20, pp. 125–138, 1973. DOI: 10.1007/BF01404061.

[GN] T. Dokchitser. "*GroupNames*". (Feb. 2020), [Online]. Available: http://groupnames.org.

[Hal98] E. Halberstadt, "Signes locaux des courbes elliptiques en 2 et 3", *C. R. Acad. Sci. Paris Sér. I Math.*, vol. 326, no. 9, pp. 1047–1052, 1998. DOI: 10.1016/S0764-4442(98)80060-8.

[Har77] R. Hartshorne, *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977, pp. xvi+496.

[Has35] H. Hasse, "Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper", *J. Reine Angew. Math.*, vol. 172, pp. 37–54, 1935. DOI: 10.1515/crll.1935.172.37.

[Hom81] M. Homma, "Automorphisms of prime order of curves", *Manuscripta Math.*, vol. 33, no. 1, pp. 99–109, 1980/81. DOI: 10.1007/BF01298341.

[Hus87] D. Husemoller, *Elliptic curves*, ser. Graduate Texts in Mathematics. Springer-Verlag, New York, 1987, vol. 111, pp. xvi+350. DOI: 10.1007/978-1-4757-5119-2.

[Iwa55] K. Iwasawa, "On Galois groups of local fields", *Trans. Amer. Math. Soc.*, vol. 80, pp. 448–469, 1955. DOI: 10.2307/1992998.

[KM76] F. F. Knudsen and D. Mumford, "The projectivity of the moduli space of stable curves. I. Preliminaries on "det" and "Div"", *Math. Scand.*, vol. 39, no. 1, pp. 19–55, 1976. DOI: 10.7146/math.scand.a-11642.

[Kna97] A. W. Knapp, "Introduction to the Langlands program", in *Representation theory and automorphic forms (Edinburgh, 1996)*, ser. Proc. Sympos. Pure Math. Vol. 61, Amer. Math. Soc., Providence, RI, 1997, pp. 245–302.

[Kob02] S. Kobayashi, "The local root number of elliptic curves with wild ramification", *Math. Ann.*, vol. 323, no. 3, pp. 609–623, 2002. DOI: 10.1007/s002080200318.

[Kra90] A. Kraus, "Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive", *Manuscripta Math.*, vol. 69, no. 4, pp. 353–385, 1990. DOI: 10.1007/BF02567933.

[Lan70] R. P. Langlands, *On the functional equation of the Artin L-functions*, unpublished notes, available at https://publications.ias.edu/sites/default/files/a-ps.pdf, 1970.

[Liu93] Q. Liu, "Courbes stables de genre 2 et leur schéma de modules", *Math. Ann.*, vol. 295, no. 2, pp. 201–222, 1993. DOI: 10.1007/BF01444884.

[Liu94a] ——, "Conducteur et discriminant minimal de courbes de genre 2", *Compos. Math.*, vol. 94, no. 1, pp. 51–79, 1994.

[Liu94b] ——, "Modèles minimaux des courbes de genre deux", *J. Reine Angew. Math.*, vol. 453, pp. 137–164, 1994. DOI: 10.1515/crll.1994.453.137.

[Liu96] ——, "Modèles entiers des courbes hyperelliptiques sur un corps de valuation discrète", *Trans. Amer. Math. Soc.*, vol. 348, no. 11, pp. 4577–4610, 1996. DOI: 10.1090/S0002-9947-96-01684-4.

[Liu98] ——, "Formule d'Ogg d'après Saito", unpublished note, available at https://www.math.u-bordeaux.fr/~qliu/Notes/Ogg-Saito.pdf, 1998.

[Liu02] ——, *Algebraic geometry and arithmetic curves*, ser. Oxford Graduate Texts in Mathematics. Oxford University Press, Oxford, 2002, vol. 6, pp. xvi+576.

[LMFDB] The LMFDB Collaboration, *The L-functions and modular forms database*, http://www.lmfdb.org, 2021.

[Lor90] D. J. Lorenzini, "Groups of components of Néron models of Jacobians", *Compositio Math.*, vol. 73, no. 2, pp. 145–160, 1990.

[Lor10] ——, "Models of curves and wild ramification", *Pure Appl. Math. Q.*, vol. 6, no. 1, Special Issue: In honor of John Tate. Part 2, pp. 41–82, 2010. DOI: 10.4310/PAMQ.2010.v6.n1.a3.

[LT16] Q. Liu and J. Tong, "Néron models of algebraic curves", *Trans. Amer. Math. Soc.*, vol. 368, no. 10, pp. 7019–7043, 2016. DOI: 10.1090/tran/6642.

[Mar08] A. Marmora, "Facteurs epsilon p-adiques", *Compos. Math.*, vol. 144, no. 2, pp. 439–483, 2008. DOI: 10.1112/S0010437X07002990.

[Mel19] L. Melninkas, *On the root numbers of abelian varieties with real multiplication*, 2019. arXiv: 1912.10263 [math.NT].

[Mel21] ——, *Root numbers of curves of genus 1 and 2 having maximal ramification*, 2021. arXiv: 2102.07745 [math.NT].

[Mil17] J. S. Milne, *Algebraic groups*, ser. Cambridge Stud. Adv. Math. Cambridge Univ. Press, Cambridge, 2017, vol. 170, pp. xvi+644. DOI: 10.1017/9781316711736.

[Mum70] D. Mumford, *Abelian varieties*, ser. Tata Inst. Fund. Res. Stud. on Math. and Phys., No. 5. Published for the Tata Institute of Fundamental Research, Bombay; Oxford University Press, London, 1970, pp. viii+242.

[Mum84] ——, *Tata lectures on theta. II*, ser. Progress in Mathematics. Birkhäuser Boston, Inc., Boston, MA, 1984, vol. 43, pp. xiv+272. DOI: 10.1007/978-0-8176-4578-6.

[Nek15] J. Nekovář, "Compatibility of arithmetic and algebraic local constants (the case $\ell \neq p$)", *Compos. Math.*, vol. 151, no. 9, pp. 1626–1646, 2015. DOI: 10.1112/S0010437X14008069.

[Nek18] ——, "Compatibility of arithmetic and algebraic local constants, II: the tame abelian potentially Barsotti-Tate case", *Proc. Lond. Math. Soc. (3)*, vol. 116, no. 2, pp. 378–427, 2018. DOI: 10.1112/plms.12085.

[Neu99] J. Neukirch, *Algebraic number theory*, ser. Grundlehren Math. Wiss. Springer-Verlag, Berlin, 1999, vol. 322, pp. xviii+571. DOI: 10.1007/978-3-662-03983-0.

[NU73] Y. Namikawa and K. Ueno, "The complete classification of fibres in pencils of curves of genus two", *Manuscripta Math.*, vol. 9, pp. 143–186, 1973. DOI: 10.1007/BF01297652.

[NZM91] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An introduction to the theory of numbers*, Fifth. John Wiley & Sons, Inc., New York, 1991, pp. xiv+529.

[Ogg66] A. P. Ogg, "On pencils of curves of genus two", *Topology*, vol. 5, pp. 355–362, 1966. DOI: 10.1016/0040-9383(66)90027-9.

[Rib76] K. A. Ribet, "Galois action on division points of Abelian varieties with real multiplications", *Amer. J. Math.*, vol. 98, no. 3, pp. 751–804, 1976. DOI: 10.2307/2373815.

[Roh93] D. E. Rohrlich, "Variation of the root number in families of elliptic curves", *Compositio Math.*, vol. 87, no. 2, pp. 119–151, 1993.

[Roh94] ——, "Elliptic curves and the Weil-Deligne group", in *Elliptic curves and related topics*, ser. CRM Proc. Lecture Notes, vol. 4, Amer. Math. Soc., Providence, RI, 1994, pp. 125–157.

[Roh96] ——, "Galois theory, elliptic curves, and root numbers", *Compositio Math.*, vol. 100, no. 3, pp. 311–349, 1996.

[Roh11] ——, "Galois invariance of local root numbers", *Math. Ann.*, vol. 351, no. 4, pp. 979–1003, 2011. DOI: 10.1007/s00208-010-0626-z.

[Roq70] P. Roquette, "Abschätzung der Automorphismenanzahl von Funktionenkörpern bei Primzahlcharakteristik", *Math. Z.*, vol. 117, pp. 157–163, 1970. DOI: 10.1007/BF01109838.

[RZ10] L. Ribes and P. Zalesskii, *Profinite groups*, Second, ser. Ergeb. Math. Grenzgeb. (3). Springer-Verlag, Berlin, 2010, vol. 40, pp. xvi+464. DOI: 10.1007/978-3-642-01642-4.

[Sab07] M. Sabitova, "Root numbers of abelian varieties", *Trans. Amer. Math. Soc.*, vol. 359, no. 9, pp. 4259–4284, 2007. DOI: 10.1090/S0002-9947-07-04148-7.

[Sab14] ——, "Change of root numbers of elliptic curves under extension of scalars", *J. Number Theory*, vol. 134, pp. 293–319, 2014. DOI: 10.1016/j.jnt.2013.07.004.

[Sai88] T. Saito, "Conductor, discriminant, and the Noether formula of arithmetic surfaces", *Duke Math. J.*, vol. 57, no. 1, pp. 151–173, 1988. DOI: 10.1215/S0012-7094-88-05706-7.

[Ser61] J.-P. Serre, *Rigidité du foncteur de jacobi d'échelon $n \geqslant 3$*, Appendix to A. Grothendieck, Techniques de construction en géométrie analytique, X. Construction de l'espace de Teichmüller, Séminaire Henri Cartan, 1960/61, no. 17.

[Ser70] ——, "Facteurs locaux des fonctions zêta des varietés algébriques (définitions et conjectures)", in *Séminaire Delange-Pisot-Poitou. 11e année: 1969/70. Théorie des nombres. Fasc. 1: Exposés 1 à 15; Fasc. 2: Exposés 16 à 24*, Secrétariat Math., Paris, 1970, p. 15.

[Ser79] ——, *Local fields*, ser. Graduate Texts in Mathematics. Springer-Verlag, New York-Berlin, 1979, vol. 67, pp. viii+241.

[SGA 7.I] *Groupes de monodromie en géométrie algébrique. I*, ser. Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I), Dirigé par A. Grothendieck. Avec la collaboration de M. Raynaud et D. S. Rim. Lecture Notes in Mathematics, Vol. 288. Springer-Verlag, Berlin-New York, 1972, pp. viii+523.

[Sil94] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, ser. Grad. Texts in Math. Springer-Verlag, New York, 1994, vol. 151.

[ST61] G. Shimura and Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, ser. Publ. Math. Soc. Japan. The Mathematical Society of Japan, Tokyo, 1961, vol. 6, pp. xi+159.

[ST68] J.-P. Serre and J. Tate, "Good reduction of abelian varieties", *Ann. of Math. (2)*, vol. 88, pp. 492–517, 1968.

[Stacks] The Stacks Project Authors, *Stacks Project*, https://stacks.math.columbia.edu, 2020.

[Sti09] H. Stichtenoth, *Algebraic function fields and codes*, Second, ser. Graduate Texts in Mathematics. Springer-Verlag, Berlin, 2009, vol. 254, pp. xiv+355.

[SZ05] A. Silverberg and Y. G. Zarhin, "Inertia groups and abelian surfaces", *J. Number Theory*, vol. 110, no. 1, pp. 178–198, 2005. DOI: 10.1016/j.jnt.2004.05.015.

[Tat67] J. T. Tate, "Fourier analysis in number fields, and Hecke's zeta-functions", in *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, Thompson, Washington, D.C., 1967, pp. 305–347.

[Tat79] ——, “Number theoretic background”, in *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2*, ser. Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I., 1979, pp. 3–26.

[Yel15] J. Yelton, “Images of 2-adic representations associated to hyperelliptic Jacobians”, *J. Number Theory*, vol. 151, pp. 7–17, 2015. DOI: 10.1016/j.jnt.2014.10.020.

Étant donné une variété abélienne définie sur un corps de nombres $\mathcal{K}$ on peut considérer sa fonction L complétée. Il est conjecturé que cette fonction satisfait une équation fonctionnelle sur $\mathbb{C}$. Le coefficient qui apparaît dans l'équation est appelé le signe global, il vaut 1 ou -1. Grâce à Langlands et Deligne on peut exprimer inconditionnellement ce signe global comme un produit eulérien de signes locaux de variétés localisées, indexé par les places de $\mathcal{K}$.

Le signe local est un invariant associé à une variété abélienne A définie sur un corps p-adique K. Il est défini en utilisant la représentation galoisienne ℓ-adique ρ_ℓ sur le module de Tate pour un nombre premier $\ell \neq p$. Dans cette thèse on cherche à exprimer le signe local en termes d'autres invariants. Parmi les invariants utilisés il y a l'ordre du corps résiduel de K, le conducteur d'Artin de ρ_ℓ, le type du modèle de Néron, les nombres de Tamagawa. Si A est une jacobienne d'une courbe C, on peut aussi utiliser les invariants associés à C.

Dans le cas des courbes elliptiques les formules pour les signes locaux sont connues. En s'inspirant de ces résultats on démontre des formules de signes locaux pour des variétés abéliennes avec multiplication réelle. Ensuite, on travaille avec des surfaces jacobiennes telles que ρ_ℓ est sauvagement ramifiée. D'après Serre–Tate, ceci ne peut se produire que pour $p \leq 5$. On obtient des formules dans le cas où $p = 5$ et ρ_ℓ est de ramification maximale. La dernière partie de la thèse est consacrée à l'étude des nombres de Tamagawa associés à des courbes hyperelliptiques en utilisant la construction explicite de modèles réguliers due à T. Dokchitser et la théorie d'intersection.

INSTITUT DE RECHERCHE MATHÉMATIQUE AVANCÉE
UMR 7501
Université de Strasbourg
CNRS
IRMA, UMR 7501
7 rue René Descartes
F-67000 STRASBOURG
Tél. 03 68 85 01 29
irma.math.unistra.fr
irma@math.unistra.fr
IRMA 2021/003
http://tel.archives-ouvertes.fr/tel-03258699