TWISTS WITH FEW CONGRUENCES

Prerequisites. Valuations on $\bar{\mathbb{Q}}_\ell$ [Ne, Ch. II]; roots of unity of prime power order [Wa, Ch. 1–2]; inertia groups and tame inertia at a finite place. Chapter 68, *Roots of unity for many polynomials*: Theorem 68.2.1 and Problems 68.2.7 and 68.2.5. Chapter 65, *Denominators of projections to lifts*: Section 65.4 with its definitions (coefficient rings and normalized lengths, auxiliary twists, main-summand-like representations, Selmer bounds, the numbers tw_ℓ and cl_ℓ) and Theorem 65.4.1. The data of Chapter 33; twists and critical pairs (Chapter 34, Section 34.6 and Definition 34.10.1); heights of families (Section 5.3) and the twist at each prime of Chapter 6; regular families (Definitions 64.2.2 and 64.2.3). As background: Stickelberger elements (Chapter 26) and Selmer groups (Chapter 30).

Chapter 65 bounds the denominator of a projection to lifts through the Selmer groups of twisted Galois representations, and the cost of comparing a lift at two twists involves ratios of Hecke L-values (Chapter 60). For each prime ℓ and each $\iota \mid \ell$, can one twist bound the Selmer lengths for a prescribed finite family satisfying the hypotheses of Theorem 67.1.2 and the valuations of the ratios for every ramified critical pair and both signs? The proof reduces both to values of polynomials at points $(\zeta_w - 1)_w$, with ζ_w roots of unity of ℓ-power order. The lemma that chooses the roots of unity is proved in Chapter 68; Section 67.1 states the polynomial input, deduces the existence of small twists (Theorem 67.1.1) and states the twisting theorem; Section 67.2 provides the regular families used in Chapters 60 and 54.

Throughout, ℓ is a prime and val is the valuation of $\bar{\mathbb{Q}}_\ell$ with $\mathrm{val}(\ell) = 1$ and $\mathrm{val}(0) = \infty$, as in Chapter 68; $\mathrm{val}_+ := \max(\mathrm{val}, 0)$, and val_ℓ is the ℓ-adic valuation of integers. Coefficient rings $\mathcal{O}$ and normalized lengths are those of Section 65.4.

67.1. The twisting theorem

Fix a CM field $E \subseteq \bar{\mathbb{Q}}$, with $G_E := \mathrm{Gal}(\bar{\mathbb{Q}}/E)$ and $g^c := cgc$ for the complex conjugation c of Section 65.4, a finite set Σ_0 of finite places of E containing those above ℓ, and an element g_0 of inertia at a place of Σ_0 prime to ℓ. Fix finitely many Selmer data and finitely many Stickelberger systems for (Σ_0, g_0), defined in the next paragraphs. Chapter 30 gives examples of Selmer classes arising from congruences, and Chapter 26 treats the classical cyclotomic Stickelberger element.

The Selmer data T_{Sel} have a common coefficient ring $\mathcal{O}$. A *Selmer datum* for (Σ_0, g_0) is a free $\mathcal{O}$-module T_{Sel} of finite rank $\mathrm{rk}\, T_{\mathrm{Sel}} \geq 1$ with a continuous $\mathcal{O}$-linear action of G_E, unramified outside a set $\Sigma(T_{\mathrm{Sel}}) \subseteq \Sigma_0$ containing the places above ℓ; write $T_{\mathrm{Sel}}(g)$ for the action of g. The endomorphisms $T_{\mathrm{Sel}}(g)$, $g \in G_E$, span $\mathrm{End}_{\mathcal{O}}(T_{\mathrm{Sel}})$ over $\mathcal{O}$. For each finite place w of E fix a place of $\bar{\mathbb{Q}}$ above w, and write G_w for its decomposition group. For each $w \mid \ell$ the datum supplies a finitely generated $\mathcal{O}$-module Z_w of cocycles $G_w \to T_{\mathrm{Sel}}$ containing the coboundaries, with $\sum_{w|\ell}(\mathrm{rk}\, Z_w - \mathrm{rk}\, T_{\mathrm{Sel}}) \leq f_E\, \mathrm{rk}\, T_{\mathrm{Sel}}$, where f_E is the number of infinite places of E. The *local relations* at w are the relations $\sum_j a_j z(g_j) = 0$, with finitely many $g_j \in G_w$ and $a_j \in \mathrm{End}_{\mathcal{O}}(T_{\mathrm{Sel}})$, satisfied by all $z \in Z_w$. The datum also supplies an

Date: November 26, 2026.

element $\gamma(T_{\mathrm{Sel}})$ of inertia at a place of $\Sigma(T_{\mathrm{Sel}})$ prime to ℓ and a scalar $\lambda \in \mathcal{O}$ with $\lambda^2 - 1 \in \mathcal{O}^\times$; both $\gamma(T_{\mathrm{Sel}})$ and $(\gamma(T_{\mathrm{Sel}})^c)^{-1}$ act on T_{Sel} by λ.

A datum has three terms, in the nonnegative extended integers. For $0 \neq a \in \mathcal{O}$ write $\bar{T}_a := T_{\mathrm{Sel}}/aT_{\mathrm{Sel}}$, and $\bar{T}_a^{*c}$ for the additive dual $\mathrm{Hom}_{\mathbb{Z}}(\bar{T}_a, \mathbb{Q}/\mathbb{Z})$, on which $\mathcal{O}$ acts by precomposition and $g \in G_E$ acts by $y \mapsto y \circ \big(\chi_{\mathrm{cyc}}(g^c)\, T_{\mathrm{Sel}}((g^c)^{-1})\big)$, with χ_{cyc} the ℓ-adic cyclotomic character. The global term $\mathrm{glob}(T_{\mathrm{Sel}})$ is the supremum, over $0 \neq a \in \mathcal{O}$, of the $\mathcal{O}$-length of the module of $\mathcal{O}$-linear G_E-equivariant maps $\bar{T}_a \to \bar{T}_a^{*c}$. At a place $v \in \Sigma(T_{\mathrm{Sel}})$ prime to ℓ, the local term is the supremum over the same a of the excess, taken to be 0 if negative, of the length of the module of restrictions to G_v of the locally constant cocycles $G_E \to \bar{T}_a$ over the length of $\bar{T}_a$; $\mathrm{plc}(T_{\mathrm{Sel}})$ is the sum of these local terms over the places $v \in \Sigma(T_{\mathrm{Sel}})$ prime to ℓ. The third term is $\mathrm{inr}(T_{\mathrm{Sel}}) := \sum_g \mathrm{ord}_{\mathcal{O}} \det(T_{\mathrm{Sel}}(g) - 1)$, the sum over $g = g_0$ and $g = (g_0^c)^{-1}$, where $\mathrm{ord}_{\mathcal{O}}$ gives a uniformizer the value 1. For a datum, $\mathrm{glob}(T_{\mathrm{Sel}})$ and $\mathrm{plc}(T_{\mathrm{Sel}}) + \mathrm{inr}(T_{\mathrm{Sel}})$ are finite. Write $\mathrm{bd}(T_{\mathrm{Sel}}) := (\mathrm{glob}(T_{\mathrm{Sel}}) + \mathrm{plc}(T_{\mathrm{Sel}}) + \mathrm{inr}(T_{\mathrm{Sel}}))/e_{\mathcal{O}}$, with $e_{\mathcal{O}} := \mathrm{ord}_{\mathcal{O}}(\ell)$.

For a finite set Q of finite places and a character $\chi\colon G_E \to \bar{\mathbb{Q}}_\ell^\times$, a bound $\mathrm{len}\,\mathrm{Sel}_Q(T_{\mathrm{Sel}}\chi) \leq d$ means that for every sufficiently large coefficient ring $\mathcal{O}' \supseteq \mathcal{O}$ there is an $\mathcal{O}'$-valued model of χ for which the following module has normalized length at most d: the locally constant cocycles with coefficients in the extended twisted lattice tensored over $\mathcal{O}'$ with $\mathrm{Frac}(\mathcal{O}')/\mathcal{O}'$ that are unramified outside $\Sigma(T_{\mathrm{Sel}}) \cup Q \cup \bar{Q}$, satisfy the local relations with coefficients extended to $\mathcal{O}'$, and vanish at $\gamma(T_{\mathrm{Sel}})$.

A finite set Q of finite places is *auxiliary* for Σ_0 if its places have prime norm, and Q, its conjugate $\bar{Q}$ and Σ_0 are pairwise disjoint. For a finite set Q of finite places, write Cl_Q for the group of finite ideles u of E with $u\bar{u} = 1$, modulo the subgroup generated by those that are principal and those that are units at every place and congruent to 1 at every place of Q. Every class of Cl_Q is represented by $y/\bar{y}$ for a finite idele y. Let $\chi\colon G_E \to \bar{\mathbb{Q}}_\ell^\times$ be a locally constant character coming by $y \mapsto y/\bar{y}$ from a finite idele class character of tame level Q trivial above ℓ. Its value at the class of $y/\bar{y}$ is $\chi(\mathrm{Art}\, y)$, where Art is the Artin map; it depends only on the class. Extend this evaluation linearly to $\bar{\mathbb{Z}}_\ell[\mathrm{Cl}_Q]$.

A *Stickelberger system* St for (Σ_0, g_0) comprises a continuous character $\alpha\colon G_E \to \bar{\mathbb{Q}}_\ell^\times$ unramified outside Σ_0 with $\alpha(g_0) \neq 1$, a finite list L of integer exponents, and an element $\mathrm{St}_Q \in \bar{\mathbb{Z}}_\ell[\mathrm{Cl}_Q]$ for each finite set Q of finite places, such that $1(\mathrm{St}_\varnothing) \neq 0$, where 1 denotes the trivial character. If $v \notin Q$ and $Q \cup \{v\}$ is auxiliary for Σ_0, then

$$\chi(\mathrm{St}_{Q\cup\{v\}}) = \chi(\mathrm{St}_Q) \prod_{e\in L} \prod_{\epsilon=\pm 1} \big(1 - (\alpha(\mathrm{Fr}_v)\chi(\mathrm{Fr}_v))^\epsilon\, (\#k_v)^{-e}\big)$$

for every locally constant χ coming by $y \mapsto y/\bar{y}$ from a finite idele class character of tame level Q trivial above ℓ, and every arithmetic Frobenius element Fr_v at any place of $\bar{\mathbb{Q}}$ above v; here k_v is the residue field at v, and the product over L counts entries with multiplicity. The finite number attached to the system is

$$\mathrm{bd}(\mathrm{St}) := \mathrm{val}\big(1(\mathrm{St}_\varnothing)\big) + 2\,\#L\ \mathrm{val}\big(\alpha(g_0) - 1\big),$$

where $\#L$ counts entries with multiplicity.

The polynomial input below is read from the proof; it follows by descent, which we do not treat. It holds for any finite Σ_0 with g_0 inertial at a place of Σ_0 prime to ℓ, subject to the hypotheses on the data, systems and c_{tor} below. We use it with Σ_0 containing the places above ℓ. Fix a natural number c_{tor}, a *torsion level*: for

every datum, $\mathrm{bd}(T_{\mathrm{Sel}}) + 1 < c_{\mathrm{tor}}$ and $2 \operatorname{rk} T_{\mathrm{Sel}} \operatorname{ord}_{\mathcal{O}}(\ell^{c_{\mathrm{tor}}}) + 1 < \#k_{\mathcal{O}}$, where $k_{\mathcal{O}}$ is the residue field and $\operatorname{ord}_{\mathcal{O}}$ gives a uniformizer the value 1. There is an integer $s_0 \geq 1$ such that for every rational $\rho > 0$ with $s_0\rho < 1$ and every sufficiently large h_1 there are:

(1) an auxiliary set Q of at most $s_0/2$ places, and for each $w \in Q$ a locally constant homomorphism $\lg_w \colon G_E \to \mathbb{Z}/\ell^{h_1}$, onto on inertia at w, coming by $y \mapsto y/\bar{y}$ from a finite idele class character of tame level $\{w\}$ trivial above ℓ; thus it is anticyclotomic, unramified outside w and $\bar{w}$, and trivial on the decomposition groups above ℓ;
(2) for each datum and each system a polynomial F over $\bar{\mathbb{Z}}_\ell$ in variables X_w, $w \in Q$, and a point with coordinates of valuation at least ρ at which $\mathrm{val}(F) \leq \mathrm{bd} + s_0\rho$, where bd is $\mathrm{bd}(T_{\mathrm{Sel}})$ or $\mathrm{bd}(\mathrm{St})$;
(3) for ℓ^{h_1}-th roots of unity ζ_w, with $\chi_\zeta := \prod_{w\in Q} \zeta_w^{\lg_w}$ and $x := (\zeta_w - 1)_w$: for a system, $F(x) = \chi_\zeta(\mathrm{St}_Q)$; for a datum with $\mathrm{val}(F(x)) < \mathrm{bd}(T_{\mathrm{Sel}}) + 1$, $\operatorname{len} \mathrm{Sel}_Q(T_{\mathrm{Sel}}\chi_\zeta) \leq \mathrm{val}(F(x))$.

Problem 67.1.1. For $\chi_\zeta = \prod_w \zeta_w^{\lg_w}$ and $n \geq 1$, $\chi_\zeta^n = \prod_w (\zeta_w^n)^{\lg_w}$, and $\chi_\zeta^{\ell^{h_1}} = 1$. For $w \in Q$ some g in an inertia group at w has $\chi_\zeta(g) = \zeta_w$.

Problem 67.1.2. Let $0 < \rho < 1$ and $m \geq 1$, and let the ζ_w, $w \in Q$, be ℓ^{h_1}-th roots of unity with $\mathrm{val}(\zeta_w - 1) \leq \rho/m$. Then $\mathrm{val}\big(\chi_\zeta^n(s_{w'}) - 1\big) \leq \rho$ for every $1 \leq n \leq m$, every $w' \in Q \cup \bar{Q}$ and every generator $s_{w'}$ of tame inertia at a place of $\bar{\mathbb{Q}}$ above w'. Hence $\sum_{w'\in Q\cup\bar{Q}} \mathrm{val}\big(\chi_\zeta^n(s_{w'}) - 1\big) \leq 2\,\#Q\,\rho$.

Problem 67.1.3. Let $0 < \varepsilon < 1$ and $m \geq 1$. There are auxiliary data as in the input and a character $\chi_\zeta = \prod_w \zeta_w^{\lg_w}$ such that, for all $1 \leq n \leq m$, $\operatorname{len} \mathrm{Sel}_Q(T_{\mathrm{Sel}}\chi_\zeta^n) \leq \mathrm{bd}(T_{\mathrm{Sel}}) + \varepsilon$ for every datum, $\mathrm{val}(\chi_\zeta^n(\mathrm{St}_Q)) \leq \mathrm{bd}(\mathrm{St}) + \varepsilon$ for every system, χ_ζ^n is ramified at every place of Q, and $\sum_{w'\in Q\cup\bar{Q}} \mathrm{val}\big(\chi_\zeta^n(s_{w'}) - 1\big) \leq \varepsilon$ for any generators $s_{w'}$ of tame inertia.

Theorem 67.1.1 (small twists)**.** *Let Σ_0, g_0, finitely many Selmer data over one coefficient ring $\mathcal{O}$, finitely many Stickelberger systems and a torsion level c_{tor} be as above, and let $m \geq 1$ be an integer and $\varepsilon > 0$ real. There are a finite set Q of places, auxiliary for Σ_0, and a character $\chi \colon G_E \to \bar{\mathbb{Q}}_\ell^\times$ such that for every $1 \leq n \leq m$:*

(1) *χ^n is locally constant, of ℓ-power order, comes by $y \mapsto y/\bar{y}$ from a finite idele class character of tame level Q trivial above ℓ, and is ramified at every place of Q;*
(2) *$\operatorname{len} \mathrm{Sel}_Q(T_{\mathrm{Sel}}\chi^n) \leq \mathrm{bd}(T_{\mathrm{Sel}}) + \varepsilon$ for every datum, and $\mathrm{val}(\chi^n(\mathrm{St}_Q)) \leq \mathrm{bd}(\mathrm{St}) + \varepsilon$ for every system;*
(3) *$\sum_{w'\in Q\cup\bar{Q}} \mathrm{val}\big(\chi^n(s_{w'}) - 1\big) \leq \varepsilon$ for any generators $s_{w'}$ of tame inertia at any places of $\bar{\mathbb{Q}}$ above the w'.*

Problems 67.1.1–67.1.3 give Theorem 67.1.1 for $0 < \varepsilon < 1$. The proof uses the same reduction to the polynomial input.

For the data of Chapter 33 the proof applies Theorem 67.1.1, with $\varepsilon = 2^{-\ell}$, to Selmer data on lattices in given representations and to one Stickelberger system for each ramified critical pair and sign. We use the notation of Chapters 33 and 34 (f, r, t, m, b, p_0, p_1, $M = p_0p_1$, N, the chosen places $\mathcal{M}$, the integer $\mathcal{N}$, m-fold twists ϑ with their sets Q_ϑ), the critical pairs $P = (\nu, z)$, their ratios $R_P(\vartheta, \epsilon)$, $\epsilon = \pm 1$,

and ramified pairs of Definition 34.10.1, and the number of Definition 65.4.1,

$$\mathrm{tw}_\ell := (4f+3)\, r\ \mathrm{val}_\ell(\mathcal{N}) + 2^{-\ell}.$$

For a twist ϑ and $\iota\colon \mathbb{C} \simeq \bar{\mathbb{Q}}_\ell$, $\hat{\vartheta}$ is the inverse avatar of Definition 65.4.5.

Theorem 67.1.2 (twisting theorem)**.** *Let $\iota\colon \mathbb{C} \simeq \bar{\mathbb{Q}}_\ell$, and let $R_1, \dots, R_n$ ($n \geq 0$) be ℓ-adic representations of G_E such that each R_i is main-summand-like for (t_i', HT_i), for some integer $t_i' \geq 0$ and some family HT_i (Definition 65.4.7). There is an m-fold twist ϑ such that for every $1 \leq j \leq m$:*

1. *the twist ϑ^j is auxiliary with ramification at most tw_ℓ (Definition 65.4.5);*
2. *for each i, the twist $\widehat{\vartheta^j} R_i$ has Selmer bound tw_ℓ (Definition 65.4.9);*
3. *for each ramified critical pair P and each sign ϵ, $\mathrm{val}_+\big(\iota(R_P(\vartheta^j, \epsilon))\big) \leq \mathrm{tw}_\ell$.*

Status: read from the proof [GL]; not proved here. The proof applies Theorem 67.1.1 with Σ_0 the places dividing ℓMN. The hypothesis on the R_i (Definition 65.4.7) imposes, at each place of $\bar{\mathbb{Q}}$ above a chosen place away from ℓ, the determinant bounds for the distinguished tame generator; it does not include the trace identity of Definition 65.4.8. The orders of finite general linear groups enter tw_ℓ through $\mathcal{N}$. The next problem uses the same group-order formula in a numerical example.

Problem 67.1.4. $\#\mathrm{GL}_3(\mathbb{F}_7) = 33784128 = 2^6 \cdot 3^4 \cdot 7^3 \cdot 19$, and $\mathrm{val}_3(7^e - 1) = 1, 1, 2$ for $e = 1, 2, 3$, with sum $4 = \mathrm{val}_3(\#\mathrm{GL}_3(\mathbb{F}_7))$.

Problem 67.1.5. For an integer $n \geq 1$ and a finite set P_0 of primes, $\sum_{\ell \in P_0} \mathrm{val}_\ell(n) \log \ell \leq \log n$. Moreover $\sum_\ell 2^{-\ell} \log \ell = 0.3776\ldots$, the sum over all primes. Hence $\sum_{\ell \in P_0} \mathrm{tw}_\ell \log \ell \leq (4f+3)\, r \log \mathcal{N} + 1$.

67.2. Regular families

As in Chapter 6, the twist may depend on the prime: it is chosen for every $\iota \mid \ell$, and families $y = (y_\iota)$ are measured by their heights (Section 5.3). Regular families and small ratios are those of Definitions 64.2.3 and 64.2.2; the denominators are measured against the budget $B = U/(mk)$, $U = fa \log^3 b$.

Problem 67.2.1. Let $e_\ell \geq 0$ be reals with $\sum_{\ell \in P_0} e_\ell \log \ell \leq c$ for every finite set P_0 of primes. If $\|\iota(y_\iota)\| \leq \ell^{e_\ell}$ for every $\iota \mid \ell$, then y has height at most c.

Problem 67.2.2. If $y \in \mathbb{C}$ and $\mathrm{val}_+(\iota(y)) \leq c$ for a real $c \geq 0$, then $y \neq 0$ and $\|\iota(y^{-1})\| \leq \ell^c$.

Problem 67.2.3. If Q is auxiliary for a set Σ_0 containing the places above ℓ, then ℓ does not divide the product of the norms of the places of Q.

The clearing bound cl_ℓ of Definition 65.4.1 contains the local loss $\mathrm{loc}_\ell = 4f\, \mathrm{defect}_\ell$ of Definition 66.1.1, in which Int_b is the product of the positive integers in $(b - 30(\Delta/2)^3, b + 30(\Delta/2)^3]$ and $\Delta/2 = r^8$. For the data, $m \geq 1$, $k \geq 1$ and $b > 1$.

Problem 67.2.4. For every finite set P_0 of primes, $\sum_{\ell \in P_0} \mathrm{defect}_\ell \log \ell \leq 10^6 \frac{m}{k} \big(b \log M + \log\big((2b)!\, (b + 30(\Delta/2)^3)^{60(\Delta/2)^6}\big)\big)$.

By Theorem 66.4.1, $\sum_{\ell \in P_0} \mathrm{loc}_\ell \log \ell \leq 4 \cdot 10^6 e^{180} f \frac{m}{k}\, b \log b$ for every finite set P_0 of primes.

Problem 67.2.5. $4 \cdot 10^6 e^{180} f \frac{m}{k}\, b \log b \le B$ if and only if $4 \cdot 10^6 e^{180}\, m^2 \le x \log^2 b$. In particular this holds if $m^2 \le 4x$ and $\log^2 b \ge 16 \cdot 10^6 e^{180}$.

Problem 67.2.5 compares the upper bound for the sum of the local losses with the budget. The data have $x \le m^2 \le 4x$, by Definition 33.3.1. Problem 65.4.4 bounds $\sum_{\ell \in P_0} (\mathrm{cl}_\ell + \mathrm{val}_\ell(C_1)) \log \ell$ by B for every finite set P_0 of primes, with C_1 the number of $U(1)$ double cosets at the chosen level.

Theorem 67.2.1. *For all data D there is a regular family $\theta = (\theta_\iota)$ of m-fold twists.*

Status: read from the proof [GL]. The next two problems give the clause on small ratios and one step of the clause on denominators. For the hypothesis of the first: the comparison of sizes displayed before Problem 65.4.4 gives $(4f+3)\, r \log \mathcal{N} + 2 \le x^{999}$, and $x^{999} \le x_1$ by Definition 33.3.1, so by Problem 67.1.5 the sum of $\mathrm{tw}_\ell \log \ell$ over every finite set of primes is at most x_1.

Problem 67.2.6. Assume $\sum_{\ell \in P_0} \mathrm{tw}_\ell \log \ell \le x_1$ for every finite set P_0 of primes. If each θ_ι satisfies the conclusions of Theorem 67.1.2 at ι, then θ has small ratios.

Problem 67.2.7. Let $C_1 \ge 1$ be an integer, $y \in \mathbb{C}$ and c real. If $\|\iota(C_1 y)\| \le e^c$, then $\|\iota(y)\| \le e^{c + \mathrm{val}_\ell(C_1) \log \ell}$.

For the denominator clause of regularity, the proof uses the ramification and Selmer bounds of Theorem 67.1.2. It takes one main summand for each lift index and each eigensystem occurring on the good forms of W_m, and one rank-one main summand for the untwisted lift from $U(1)$ for each main pair and its lift index. At $\vartheta = \theta_\iota^j$ it applies Theorem 65.4.1 to the image of the good-form lift from W_j and to the line of the twisted lift of the constant function for each main pair for j. The $U(1)$ stabilizers at the chosen level are trivial. The logarithmic allowance for the pairing of the projections of two test forms onto that line is $(\mathrm{cl}_\ell + \mathrm{val}_\ell(C_1)) \log \ell$; the class number enters as in Problem 67.2.7. This allowance also suffices for clearing the good-form projection. Its sum over every finite set of primes is at most B by Problem 65.4.4.

This chapter has deduced the small twists from the polynomial input and the lemma on roots of unity, and the small ratios of a regular family from the twisting theorem. Taken as given: the polynomial input, the twisting theorem (Theorem 67.1.2), Theorem 65.4.1 and the existence of main summands used in the denominator clause, all read from the proof. Chapter 54 uses Theorem 67.2.1.

In the Lean formalization. In the Lean proof [GL] (`grh/src/`, namespace `New.Selmer` unless stated), the input of Section 67.1 is a specialization of `exists_twistPolynomials`, its objects are `SelmerDatum` and `StickelbergerSystem`, and the length bound is `SelmerDatum.TwistedLengthLe`. Theorem 67.1.1 is `exists_anticyclotomic_twist`, with conclusions `IsSmallTwist`; Theorem 67.1.2 is `exists_mFoldTwist_hasDivisibleSelmerLengthLe`; Theorem 67.2.1 is `New.exists_isRegularFamily`. Its clause on denominators is the field `New.Data.IsRegularFamily.exists_denominator_bound`; the proof uses `exists_mFoldTwist_hasDenominatorsLe` at each ι, and the sum over the primes is that of Problem 65.4.4. The selection of main summands, the two applications of Theorem 65.4.1 and the pairing estimate described in Section 67.2 are the steps of the proof of `exists_mFoldTwist_hasDenominatorsLe`; the main summands are supplied by `exists_isMainSummand_descentPair` and

`exists_isMainSummand_mainPair`. The passage from the values of a Stickelberger system to the ratios of a ramified critical pair is `exists_stickelbergerSystem_ellVal_ratio_le`.

Hints

Section 67.1.

67.1.1: For the last claim, the $\lg_{w'}$ with $w' \neq w$ are unramified at w because Q is auxiliary.

67.1.2: $\lg_w$ is trivial on wild inertia, and a generator of tame inertia at w maps to a generator of $\mathbb{Z}/\ell^{h_1}$; so $\chi_\zeta(s_w) = \zeta_w^a$ with a prime to ℓ, and ζ_w^{an}, ζ_w^n have the same order. At $\bar{w}$ use $\lg_w(g^c) = -\lg_w(g)$. Then Problem 68.2.5.

67.1.3: Choose s_0 as in the input, then a rational $\rho > 0$ with $s_0\rho \leq \varepsilon/2$, then h_0 by Problem 68.2.7 with the bounds $\mathrm{bd} + 1 \geq 0$ (note $0 \leq \mathrm{val}(F) \leq \mathrm{bd} + s_0\rho$) and $\varepsilon/2$, then a sufficiently large $h_1 \geq h_0$ and the auxiliary data at level ℓ^{h_1}. Use Problem 67.1.1; for the ramification, Problem 68.2.5; for the last sum, Problem 67.1.2 and $2\,\#Q \leq s_0$.

Theorem 67.1.1: Take $\chi = \chi_\zeta$ for $0 < \varepsilon < 1$. For $\varepsilon \geq 1$, apply the case $\varepsilon = 1/2$.

67.1.5: Factor n; for the last claim take $n = \mathcal{N}$.

Section 67.2.

67.2.1: Which multiplier leaves the local inequalities unchanged?

67.2.3: A place of Q has prime norm and does not lie above ℓ.

67.2.4: Problem 67.1.5, and count the factors of Int_b.

67.2.5: Write $a = xb$.

67.2.6: Problems 67.2.3, 67.2.2 and 67.2.1.

67.2.7: $\|\iota(C_1)\| = \ell^{-\,\mathrm{val}_\ell(C_1)}$.

References

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[Ne] J. Neukirch, *Algebraic Number Theory*, Grundlehren Math. Wiss. 322, Springer, 1999.

[Wa] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer, 1997.