THEOREM A: SHORT FORMS

Prerequisites. Modules over a discrete valuation ring: a submodule of finite index in $\mathbb{Z}_{(p)}^n$ is free of rank n, and a matrix over $\mathbb{Q}$ can be brought to diagonal form by invertible matrices over $\mathbb{Z}_{(p)}$ [La, Ch. III, §7]. From Chapter 5, the principle that size is compared with divisibility. From Chapter 33: the data (scales $x < x_1 < b$, $a = xb$, $L = \log b$; the CM field E with its set Φ of f infinite places; m, k, the weights κ, the principal level $M = p_0 p_1$, with $p_0 \neq p_1$ primes, and the prime level N), the amounts h_{main} and rem and the unit $U = faL^3$. From Chapter 34: the source forms, the group $\bar{G}$, the idempotent e_0, the target T, tame characters, twists and the lower chain. From Chapter 36: the Poincaré map. From Chapter 43: the composite lift and the seesaw identity. From Chapter 48: the gain $\mathrm{gain}(p)$, the set Π of primes $p < x_1$ with $\chi_K(p) \neq 1$, and the divisibility of the composite lift. From Chapter 51: the size of the composite lift. Chapter 23 treats small-rank examples of single definite lifts and their norms.

Theorem A says that the ramified source is spanned by integral forms whose translated images have short lifts at the trivial twist. It also bounds the index of every finite family of translated images of integral ramified forms in terms of the number of translates used. The last chapter of this part uses both bounds. The normalization multiplies by a positive rational number c_B, with exponent $-\lfloor \mathrm{gain}(p) - \mathrm{err}(p) \rfloor$ at each prime p in the product, including the level prime N; the price of the shortness is paid in index. We first do this with rational vectors, and then follow the exponents in the proof; the size of the composite lift is the subject of Chapter 51.

42.1. Index and colength over $\mathbb{Z}$

Let $\mathbb{Z}_{(p)}$ be the ring of rationals with denominator prime to p, and v_p the p-adic valuation, normalized by $v_p(p) = 1$, with $v_p(0) = +\infty$. Let $y = (y_i)_{i \in \mathcal{J}}$ be a finite family in $\mathbb{Q}^n$. A square matrix $u = (u_{ik})_{i,k \in \mathcal{J}}$ over $\mathbb{Z}_{(p)}$ *carries* y *with loss* δ_p if every $\sum_k u_{ik} y_k$ lies in $\mathbb{Z}_{(p)}^n$ and $v_p(\det u) \leq \delta_p$. The family *has index at most* δ if there are real numbers $\delta_p \geq 0$ with $\sum_p \delta_p \log p \leq \delta$ such that for every prime p some matrix carries y with loss δ_p.

Problem 42.1.1. The family $(1/6)$ in $\mathbb{Q}$ has index at most $\log 6$, and not at most δ for any $\delta < \log 6$.

Problem 42.1.2. A finite family y in $\mathbb{Q}^n$ has index at most δ if and only if $\delta \geq \log [\Lambda_y : \mathbb{Z}^n]$, where $\Lambda_y = \mathbb{Z}^n + \sum_i \mathbb{Z} y_i$. For the family $((\frac{1}{2}, \frac{1}{2}), (0, \frac{1}{4}))$ in $\mathbb{Q}^2$ one has $[\Lambda_y : \mathbb{Z}^2] = 8$.

Problem 42.1.3. If $\mathcal{J} = \mathcal{J}' \sqcup \mathcal{J}''$ and the two subfamilies have index at most δ' and δ'', then y has index at most $\delta' + \delta''$. Hence a family that is the union of h subfamilies of index at most δ has index at most $h\delta$. For the families $(\frac{1}{2}, \frac{1}{3})$ and $(\frac{1}{2}, \frac{1}{2})$ in $\mathbb{Q}$, split into singletons, the bound is $\log 6$ and $2 \log 2$, and the index is $\log 6$ and $\log 2$.

Date: November 26, 2026.

Problem 42.1.4. Let W be a submodule of $\mathbb{Z}_{(p)}^k$ with $\mathbb{Z}_{(p)}^k/W$ of order p^j. For every finite family $(\varphi_i)_{i\in\mathcal{J}}$ in $\mathbb{Z}_{(p)}^k$ there is a square matrix u over $\mathbb{Z}_{(p)}$ with $v_p(\det u)\le j$ and $\sum_k u_{ik}\varphi_k \in W$ for every i.

Problem 42.1.5. Let $A\colon \mathbb{Q}^k\to\mathbb{Q}^n$ be linear. Suppose that for every prime p there is a submodule $W_p\subseteq\mathbb{Z}_{(p)}^k$ of index p^{j_p} with $A(W_p)\subseteq\mathbb{Z}_{(p)}^n$, and $j_p=0$ for almost all p. Then every finite family in $A(\mathbb{Z}^k)$ has index at most $\sum_p j_p\log p$.

42.2. A model of Theorem A

Let $B\colon\mathbb{Q}^k\to\mathbb{Q}^n$ be linear; it stands for the chain of lifts. Let Π_0 be a finite set of primes, and suppose that for each $p\in\Pi_0$ we are given a real number γ_p and a submodule $W_p\subseteq\mathbb{Z}_{(p)}^k$ of index p^{j_p} on which B is divisible: $v_p(B\varphi)\ge\gamma_p$ coordinatewise for $\varphi\in W_p$. For $p\notin\Pi_0$ put $\gamma_p=j_p=0$ and $W_p=\mathbb{Z}_{(p)}^k$, and suppose $B(\mathbb{Z}_{(p)}^k)\subseteq\mathbb{Z}_{(p)}^n$ for these p. Put

$$g_p=\lfloor\gamma_p\rfloor,\qquad c_B=\prod_{p\in\Pi_0}p^{-g_p},\qquad A=c_BB.$$

Problem 42.2.1. For every prime p, $v_p(c_B)=-g_p$ and $A(W_p)\subseteq\mathbb{Z}_{(p)}^n$. Hence every finite family in $A(\mathbb{Z}^k)$ has index at most $\sum_p j_p\log p$, and $|A\varphi|^2=c_B^2|B\varphi|^2$ with $2\log c_B\le -2\sum_{p\in\Pi_0}\gamma_p\log p+2\sum_{p\in\Pi_0}\log p$.

Problem 42.2.2. Let $k=n=2$, $\Pi_0=\{2,3\}$ and $B(\varphi_1,\varphi_2)=(4\varphi_1+6\varphi_2,12\varphi_2)$.

(1) With $\gamma_2=1$, $W_2=\mathbb{Z}_{(2)}^2$ and $\gamma_3=1$, $W_3=\{\varphi:3\mid\varphi_1\}$, one has $c_B=1/6$; the least δ such that (Ae_1,Ae_2) has index at most δ is $\log 3$, and $|Ae_1|^2=4/9$, $|Ae_2|^2=5$.
(2) With $\gamma_2=2$, $W_2=\{\varphi:2\mid\varphi_2\}$ and the same choice at 3, one has $c_B=1/12$; this least δ is $\log 6$, and $|Ae_1|^2=1/9$, $|Ae_2|^2=5/4$.

Problem 42.2.3. The vectors of $\mathbb{Z}^k$ with all coordinates in $\{0,\pm1\}$ span $\mathbb{C}^k$. If $T_1,\dots,T_f$ are commuting complex-linear isometries of $\mathbb{C}^k$ preserving $\mathbb{Z}^k$, the image of $\prod_i(1-T_i)$ is spanned by integral vectors of squared norm at most 4^fk.

In Problem 42.2.2, increasing γ_2 by one halves c_B, shortens the image, and increases the index of the family by $\log 2$. For each prime p and each ring homomorphism $\mathbb{C}\to\mathbb{C}_p$, the divisibility theorem of Chapter 48 gives a submodule of the integral ramified source forms of colength exponent at most $\mathrm{err}(p)$ times the dimension of the full source. On this submodule the composite lift has valuation at least $\mathrm{gain}(p)-\mathrm{err}(p)$ for every twist of level prime to p and every chain datum for that twist.

42.3. Theorem A

Put $\Sigma:=\sum_{p\in\Pi}\mathrm{gain}(p)\log p$, as in Chapter 51. The composite lift $B_{\vartheta,\Psi}$ of Chapter 43 is defined on all source forms; for a twist ϑ it depends on a chain datum Ψ for ϑ, a finitely supported function on the translations. Write $G_f(V)$ for the group of finite adelic points of the unitary group of a space V. For a form F on X_0 or on Y_m and $\sigma\in\mathrm{Aut}(\mathbb{C})$, $|\sigma F(g)|^2$ denotes the Weyl squared norm of the conjugate value. By Theorem 51.3.6, if Ψ is a chain datum for the trivial twist,

$\sigma \in \mathrm{Aut}(\mathbb{C})$, $\varphi \in S$, $c \in \mathbb{R}$, and $|\sigma\varphi(g)|^2 \le e^c$ for every $g \in G_f(X_0)$, then for every $y \in G_f(Y_m)$

$$|\sigma(B_{1,\Psi}\varphi)(y)|^2 \le \exp\bigl(c + h_{\mathrm{main}} - m\,\mathrm{rem} + 2\Sigma + U\bigr).$$

This is a statement at the trivial twist only.

The spaces $S \supseteq S_{\mathrm{ram}}$ of source forms and ramified source forms, the set $S_{\mathrm{ram}}^{\mathrm{int}}$ of ramified forms integral at every ι, the dimension $D_X = \dim S$, the group $\bar{G}$ and its action ρ on the principal forms $H(Y_0)$, the target T, tame characters ξ, twists and m-fold twists ϑ with their moduli Q_ϑ, and the lower chain Θ_ξ are as in Chapter 34; the Poincaré map $\mathcal{P}\colon S \to H(Y_0)$ is that of Chapter 36. A form is integral at a ring homomorphism $\eta\colon \mathbb{C} \to \mathbb{C}_p$ if all its values have gauge at most 1 at η; integrality at ι is integrality at the homomorphism induced by ι, and $\mathcal{O}_\iota$ is the ring of $z \in \mathbb{C}$ with $|\iota(z)|_p \le 1$. For $Z > 0$ a form φ is *Z-short* if it is integral at every $\eta\colon \mathbb{C} \to \mathbb{C}_p$, for every prime p, and $|\sigma\varphi(g)|^2 \le Z$ for all $\sigma \in \mathrm{Aut}(\mathbb{C})$ and all g. For a form F on Y_m of specified level K and character, $\|F\|_\sigma^2$ is the sum over the double classes at level K of $|\sigma F(g)|^2$ at the chosen representatives g, each weighted by the reciprocal of the order of its stabilizer. For $\lambda \in \mathbb{C}$ the squared norm of $\sigma(\lambda F(g))$ is $|\sigma(\lambda)|^2$ times that of $\sigma F(g)$, and the gauge of $\lambda F(g)$ at η is $|\eta(\lambda)|_p$ times that of $F(g)$.

The text uses five inputs. Inputs 2 and 4 are theorems of the chapters named; input 1 is derived below from one statement read from the proof [GL]; inputs 3 and 5 are read from the proof, and no chapter develops them.

(1) The e^U-short forms in S_{ram} span S_{ram}. Problems 42.3.1 and 42.3.2 derive this from the statement before them (compare Problem 42.2.3).

(2) *Seesaw.* There is $c_{\mathrm{ss}} \in \mathbb{C}^\times$ such that for every twist ϑ there is a chain datum Ψ for ϑ with $\Theta_\vartheta(\mathcal{P}\varphi) = c_{\mathrm{ss}} B_{\vartheta,\Psi}\varphi$ for all $\varphi \in S_{\mathrm{ram}}$ (Theorem 43.4.1, at the point and the linear form that define $\mathcal{P}$).

(3) *Good part.* Let $z \in H(Y_0)$ and $s \in \bar{G}$. If $|\sigma(\Theta_1 z)(g)|^2 \le e^c$ for all $g \in G_f(Y_m)$, with $c \in \mathbb{R}$ and a fixed $\sigma \in \mathrm{Aut}(\mathbb{C})$, then $\|\Theta_1(\#\bar{G}\,\rho(e_0)\rho(s)z)\|_\sigma^2 \le e^{x^{99}+c}$. For every prime p, every ring homomorphism $\eta\colon \mathbb{C} \to \mathbb{C}_p$, every tame character ξ and every $\lambda \in \mathbb{C}$, if $\lambda\,\Theta_\xi z$ is integral at η, so is $\lambda\,\Theta_\xi(\#\bar{G}\,\rho(e_0)\rho(s)z)$. We use both estimates as inputs.

(4) *Divisibility.* Theorem 48.7.2. We write M_η for its module $S_{\mathrm{ram},\eta}$ of forms in S_{ram} integral at η, and $j_{p,\eta}$ and $S'_{p,\eta}$ for the integer l and the module S' of its part (d) at (p,η). That the colength of $S'_{p,\eta}$ in M_η divides $p^{j_{p,\eta}}$ means (Section 42.1) that every finite family in M_η is carried into $S'_{p,\eta}$ by a square matrix over $\mathcal{O}_\eta$, the ring of $z \in \mathbb{C}$ with $|\eta(z)|_p \le 1$, whose determinant divides $p^{j_{p,\eta}}$.

(5) $\dim S_{\mathrm{ram}} \ge (1 - f/(N-1))D_X$, and $f/(N-1) \le b^{-8}$.

Moreover the data satisfy (Chapter 33) $b \ge 2$, $N \ge x_1$, $\sum_{p \in \Pi \cup \{N\}} \log p \le b$ and $x^{99} + 4U + 2b \le faL^4$.

For input 1 the proof [GL] constructs, from bases of the lattice classes of X_0 whose vectors are short at every complex embedding, source forms supported on one class, and obtains: *the $4^{-f}e^U$-short forms in S span S. Status*: read from the proof.

Problem 42.3.1. Let $w \mid \pi_N$ be a prime of E, T_w the operator of Section 34.5, and $Z > 0$. If $\varphi \in S$ is Z-short, then $(1 - T_w)\varphi$ is $4Z$-short.

Problem 42.3.2. There are f primes $w \mid \pi_N$ of E. Hence $\prod_{w|\pi_N}(1-T_w)$ maps $4^{-f}e^U$-short forms to e^U-short forms, and the e^U-short forms in S_{ram} span S_{ram}.

Definition 42.3.1. Fix err as in input 4 and c_{ss} as in input 2. As in Section 42.2, put $g_p = \lfloor \mathrm{gain}(p) - \mathrm{err}(p) \rfloor$ and $c_B = \prod_{p \in \Pi \cup \{N\}} p^{-g_p}$, a positive rational number. For $s \in \bar{G}$ the *normalized translate* $A_s \colon S_{\mathrm{ram}} \to T$ is

$$A_s\varphi = c_B\, c_{\mathrm{ss}}^{-1}\, \#\bar{G}\, \rho(e_0)\rho(s)\, \mathcal{P}\varphi.$$

Problem 42.3.3. $\log c_B \le -\Sigma + U + b$.

Problem 42.3.4. For every prime p and every ι above p, $|\iota(c_B)|_p = p^{g_p}$, and $g_p = 0$ for $p \notin \Pi \cup \{N\}$.

Problem 42.3.5. $U + (h_{\mathrm{main}} - m\,\mathrm{rem} + 2\Sigma + U) + x^{99} + 2\log c_B \le h_{\mathrm{main}} - m\,\mathrm{rem} + x^{99} + 4U + 2b$.

Problem 42.3.6. Every e^U-short $\varphi \in S_{\mathrm{ram}}$ lies in $S_{\mathrm{ram}}^{\mathrm{int}}$ and satisfies $\|\Theta_1 A_s\varphi\|_\sigma^2 \le \exp(h_{\mathrm{main}} - m\,\mathrm{rem} + faL^4)$ for all $s \in \bar{G}$ and $\sigma \in \mathrm{Aut}(\mathbb{C})$.

Problem 42.3.7. $D_X \le 2 \dim S_{\mathrm{ram}}$.

Vectors of T integral at ι, and the index of a finite family in T, are those of the target lattice (Definition 34.11.1): $y \in T$ is integral at ι above p if $\Theta_\vartheta y$ is integral at ι for every m-fold twist ϑ of level prime to p, and a family has index at most δ if matrices over the rings $\mathcal{O}_\iota$, with determinants of total weighted valuation at most δ, carry it into the integral vectors. This is the carrying condition of Section 42.1 at each ι, with one matrix carrying the family into the vectors integral for all allowed twists at once.

Problem 42.3.8. Let ι lie above p, and let η be the homomorphism induced by ι. Then $A_s\varphi$ is integral at ι for every $\varphi \in S'_{p,\eta}$ and every $s \in \bar{G}$.

Problem 42.3.9. For each $s \in \bar{G}$, every finite family in $A_s(S_{\mathrm{ram}}^{\mathrm{int}})$ has index at most $\dim S_{\mathrm{ram}} \cdot 2U$.

The proof [GL] establishes the following two statements.

Theorem 42.3.2 (Theorem A)**.** (a) *The complex span of the set of $\varphi \in S_{\mathrm{ram}}^{\mathrm{int}}$ such that*

$$\|\Theta_1 A_s\varphi\|_\sigma^2 \le \exp\bigl(h_{\mathrm{main}} - m\,\mathrm{rem} + faL^4\bigr) \quad \textit{for all } s \in \bar{G} \textit{ and } \sigma \in \mathrm{Aut}(\mathbb{C})$$

is S_{ram}.

(b) *Let $J \subseteq \bar{G}$ be finite, $n \in \mathbb{N}$, and $y_1, \dots, y_n \in T$. If each y_i lies in $A_s(S_{\mathrm{ram}}^{\mathrm{int}})$ for some $s \in J$, then $(y_1, \dots, y_n)$ has index at most $\#J \cdot \dim S_{\mathrm{ram}} \cdot 2faL^3$.*

Neither part asks the forms to be independent or the images to span; Theorem B of Chapter 36 supplies few translates whose images span almost all of T. In the exponent of (a) the gains have disappeared and the remainder appears with the factor m. The last chapter of this part compares this upper bound with a lower bound in which the main amount h_{main} appears without the remainder.

In the Lean formalization. In the Lean proof [GL], Theorem 42.3.2 is `span_short_integralRamified_eq_top` (a) and `indexLe_normalizedPoincare` (b), with c_B, A_s and $S^{\mathrm{int}}_{\mathrm{ram}}$ the definitions `Data.invGainFactor`, `Data.normalizedPoincare` and `Data.integralRamified`. Input 1 is `Data.span_isShort_ramifiedSourceForms_eq_top`, the statement read for it is `Data.span_isShort_eq_top`, and Problem 42.3.1 is `IsShort.sub_translate`; input 3 is `normSqAt_goodProjTranslate_le` with `goodProjTranslate_mem_integralForms`, input 5 is `le_finrank_ramifiedSourceForms` with `f_div_N_sub_one_le`. The definitions of c_B and A_s use the witnesses `Data.divisibilityError` for err and `Data.seesawConst` for c_{ss}.

Hints

§42.1.

42.1.1: A 1×1 matrix u carries $1/6$ at p only if $v_p(u) \geq -v_p(1/6)$.

42.1.2: Write the matrix of the family as PDQ with P, Q invertible over $\mathbb{Z}_{(p)}$ and D diagonal.

42.1.3: Block diagonal matrices; Problem 42.1.2 for the examples.

42.1.4: Pull W back along $\mathbb{Z}_{(p)}^{\mathcal{J}} \to \mathbb{Z}_{(p)}^{k}$, $e_i \mapsto \varphi_i$, and take a basis of the preimage.

42.1.5: Choose preimages of the family in $\mathbb{Z}^k$. Which local matrices can act on these preimages?

§42.2.

42.2.1: How does multiplication by c_B change each coordinate valuation on W_p?

42.2.2: Problem 42.1.2.

42.2.3: The norm of $(1 - T_i)v$ is at most twice that of v.

§42.3.

42.3.1: z_w is an integral unit scalar: translation by it changes neither the gauges nor the set of values $\sigma\varphi(g)$. Then $|u - u'|^2 \leq 4\max(|u|^2, |u'|^2)$, and the gauge is ultrametric.

42.3.2: N splits completely in E and $[E : K] = f$. Problem 52.1.1: S_{ram} is the image of the product, so it is spanned by the images of a spanning set.

42.3.3: $-g_p \leq -\mathrm{gain}(p) + \mathrm{err}(p) + 1$, and $\mathrm{gain}(N) = 0$.

42.3.4: Which factors of c_B can have nonzero valuation at p? Compare with the support conditions on the gain and error.

42.3.5: Problem 42.3.3.

42.3.6: The seesaw at the trivial twist, Theorem 51.3.6 with $c = U$, the good part, and Problem 42.3.5.

42.3.7: Input 5.

42.3.8: Fix an m-fold twist of level prime to p. Compare the gauge bound from the seesaw and divisibility with the local absolute value of c_B, then use the good-part input.

42.3.9: As in Problem 42.1.5, with $\delta_p = D_X \mathrm{err}(p)$; then Problem 42.3.7.

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/`.

[La] S. Lang, *Algebra*, 3rd ed., Grad. Texts in Math. 211, Springer, 2002.