HECKE NONDEGENERACY ON THE TREE

Prerequisites. Modules over a discrete valuation ring and the elementary divisor theorem [La, Ch. III, §7]. Unramified extensions of $\mathbb{Q}_p$ and Teichmüller representatives. The tree of GL_2 over a local field [SeT, Ch. II, §1]. Legendre's formula $v_p(m!) = (m - s_p(m))/(p-1)$, where $s_p(m)$ is the sum of the base-p digits of m. From Chapter 5, *Size against divisibility*: Problem 5.4.4, and the colength of a submodule, defined before Theorem 5.4.1. Section 18.7 uses the notation of Chapter 33 and the collisions and exceptional primes of Chapter 48.

In Chapter 5 an index was bounded by colengths of submodules (Theorem 5.4.1). When a gain at a prime holds on a submodule spanned by images of a Hecke operator, how large is that colength? For GL_2 and weight k we compute, at one fixed lattice, the image of the normalized sum of the values at the neighbouring lattices. When $Q > k$ its elementary divisors are expressed by binomial coefficients, and Kummer's theorem bounds them.

Why Hecke operators? The proof passes through a chain of theta lifts. At an exceptional prime $p < x_1$, let S_η denote the module of integral source forms and $Y_{\mathfrak{M}}$ the product of the scaled Hecke operators at a full mark $\mathfrak{M}$, as in Chapter 48. Chapter 48 obtains the valuation bound for the composite lift on $Y_{\mathfrak{M}}^m S_\eta + p^{j_p} S_\eta$, where m is the number of lifts; Section 48.4 gives the hypotheses on the lift and the exponent j_p. Theorem 48.5.1 gives a colength bound for each factor modulo p^{j_p}. Adding these bounds over the m copies of the product and estimating their sum bounds the colength of $Y_{\mathfrak{M}}^m S_\eta + p^{j_p} S_\eta$ in S_η. The computation at one vertex is a model for this bound. Chapter 24, *Hecke operators and theta lifts*, relates a sum over the neighbours of a lattice on a class set to a Hecke operator on modular forms through the theta lift. This chapter uses nothing from Chapter 24.

In Sections 18.1–18.6, K is the unramified extension of $\mathbb{Q}_p$ of degree f, with ring of integers W, residue field $\mathbb{F}_Q$ where $Q = p^f$, and valuation v normalized by $v(p) = 1$. We fix an integer $k \geq 1$.

18.1. The tree and the integral forms

A *lattice* is a free W-submodule of rank 2 of K^2. For a lattice L, its *sources* are the lattices L'' with $pL \subset L'' \subset L$ and $L/L'' \cong \mathbb{F}_Q$. The vertices of the tree are the classes of lattices up to homothety, and the neighbours of the class of L are the classes of its sources [SeT, Ch. II, §1].

Problem 18.1.1. The sources of L correspond to the lines of $L/pL \cong \mathbb{F}_Q^2$. There are $Q+1$ of them, and their classes are pairwise distinct.

Let V be the space of homogeneous polynomial functions of degree k on K^2, on which $\mathrm{GL}_2(K)$ acts by $(gF)(u) = F(g^{-1}u)$. For a lattice L with dual $L^\vee = \mathrm{Hom}_W(L, W)$, put

$$H(L) := \mathrm{Sym}^k(L^\vee) \subset V.$$

If x, y is the basis of $L^\vee$ dual to a basis of L, then $H(L) = \bigoplus_{j=0}^{k} W x^{k-j} y^j$.

Date: November 25, 2026.

Problem 18.1.2. $H(gL) = gH(L)$ for $g \in \mathrm{GL}_2(K)$, and $H(cL) = c^{-k}H(L)$ for $c \in K^\times$. If $L'' \subset L$, then $H(L) \subset H(L'')$.

Problem 18.1.3. Let L'' be a source of L. There is a basis x, y of $L^\vee$ such that $L''^\vee = Wx + Wp^{-1}y$. Hence the elementary divisors of $H(L)$ in $H(L'')$ are $1, p, \dots, p^k$, we have $p^k H(L'') \subset H(L)$, and $\mathrm{length}_W H(L'')/H(L) = k(k+1)/2$.

A *form* is a function F from lattices to V. It is *integral* if $F(L) \in H(L)$ for every L. The Hecke operator and its normalization are

$$(TF)(L) := \sum_{L''} F(L''), \qquad Y := p^k T,$$

where the sum runs over the $Q+1$ sources of L. Let

$$S(L) := \sum_{L''} p^k H(L'') \subset H(L).$$

Problem 18.1.4. Y maps integral forms to integral forms, and $\{(YF)(L) : F \text{ integral}\} = S(L)$.

Problem 18.1.5. $S(L) = \sum_M \mathrm{Sym}^k(M)$, the sum over the $Q+1$ lattices M with $pL^\vee \subset M \subset L^\vee$ and $L^\vee/M \cong \mathbb{F}_Q$.

Problem 18.1.6. For $Q = 2$ and $k = 2$, $S(L) = Wx^2 + 2Wxy + Wy^2$. For $k = 1$ and every Q, $S(L) = H(L)$.

The *loss* at L is $\mathrm{length}_W H(L)/S(L)$. It does not depend on L, by Problem 18.1.2. By Problem 18.1.3 a single source costs $k(k+1)/2$. The question is how much the $Q+1$ sources save together.

18.2. Elementary divisors

Let H be a free W-module of rank t and $S \subset H$ a submodule of full rank. By the elementary divisor theorem [La, Ch. III, §7] there is a basis $h_1, \dots, h_t$ of H with $S = \bigoplus_i p^{e_i} W h_i$, and the exponents $e_1 \le \cdots \le e_t$ are unique. Then $\mathrm{length}_W H/S = e_1 + \cdots + e_t$. For an integer $D \ge 0$ and a real $\varrho \in [0,1]$, we say that S is *nondegenerate up to p^D on a share ϱ* when $\#\{i : e_i \le D\} \ge \varrho t$.

Problem 18.2.1. Let A be a matrix whose rows are the coordinates, in a basis of H, of a finite generating set of S. For every integer $1 \le l \le t$, the sum $e_1 + \cdots + e_l$ is the least valuation of an $l \times l$ minor of A. In particular the e_i do not change under a finite unramified extension of W.

Problem 18.2.2. $\#\{i : e_i \le D\}$ is the largest ν for which there are $s_1, \dots, s_\nu \in S$ and $\varphi_1, \dots, \varphi_\nu \in \mathrm{Hom}_W(H, W)$ with $\varphi_a(s_b) = p^D \delta_{ab}$.

The vectors s_b are *witnesses* and the functionals φ_a are *tests*. The next problem gives a criterion on linear combinations of the tests.

Problem 18.2.3. Let Λ be a W-module and $\varphi_1, \dots, \varphi_M \colon \Lambda \to W$ linear maps. Suppose that for every $c \in W^M$ with some c_i a unit there is $G \in \Lambda$ with $v\big(\sum_i c_i \varphi_i(G)\big) \le D$. Then the image of $G \mapsto (\varphi_i(G))_i$ contains $p^D W^M$.

Problem 18.2.4. Let A, A' be $t \times t$ matrices over W with $A \equiv A' \pmod{p^T}$ for an integer $T \ge 1$, and let e_i and e_i' be the exponents of their row spans in W^t (where $e_i = \infty$ for the zero elementary divisors). Then $\min(e_i, T) = \min(e_i', T)$ for every i.

Problem 18.2.4 lets one compute exponents below T modulo p^T; Section 18.6 measures a loss in this truncated way.

18.3. Kummer's theorem

Valuations of binomial coefficients enter the formula for the exponents.

Problem 18.3.1. For $0 \le j \le n$, $v_p\binom{n}{j} = \big(s_p(j) + s_p(n-j) - s_p(n)\big)/(p-1)$, and this is the number of carries in the addition of j and $n-j$ in base p.

This is due to Kummer [Ku]; see [Gra] for a survey.

Problem 18.3.2. For $1 \le j \le n$, $v_p\binom{n}{j} \le \lfloor \log_p n \rfloor - v_p(j)$. In particular $p^{v_p\binom{n}{j}} \le n$.

Problem 18.3.3. Every $\binom{Q-1}{j}$ with $0 \le j \le Q-1$ is prime to p. For $0 < j < p^m$, $v_p\binom{p^m}{j} = m - v_p(j)$, so Problem 18.3.2 is sharp.

18.4. The Fock form

For $F = \sum_m F_m x^m$ and $G = \sum_m G_m x^m$ in $K[x_1, \dots, x_{n'}]$, with multi-indices m and $m! = \prod_s m_s!$, let

$$\langle F, G \rangle := \sum_m F_m G_m \, m!, \qquad \text{that is,} \qquad \langle x^m, x^{m'} \rangle = m! \, \delta_{mm'}.$$

In one variable over $\mathbb{C}$, with complex conjugation on the coefficients of F, this is the Gaussian inner product of Problem 5.4.4; it is the inner product of the Fock model [Ba].

Problem 18.4.1. $\langle x_s F, G \rangle = \langle F, \partial_s G \rangle$ for every s. Hence $\langle F, G \rangle = \big(F(\partial)G\big)(0)$, where $F(\partial)$ is F with each x_s replaced by $\partial/\partial x_s$.

Problem 18.4.2. For $F \in K[x,y]$ homogeneous of degree k and $a, b \in K$, $\langle (ax + by)^k, F \rangle = k! \, F(a,b)$.

Let $H = \bigoplus_{j=0}^k W x^{k-j} y^j$, and let $H^\sharp := \{G \in K[x,y]$ homogeneous of degree k : $\langle G, F \rangle \in k! \, W$ for all $F \in H\}$.

Problem 18.4.3. $H^\sharp = \bigoplus_{j=0}^k \binom{k}{j} W x^{k-j} y^j$, and $p^{\lfloor \log_p k \rfloor} H \subset H^\sharp \subset H$.

So $\langle \cdot, \cdot \rangle / k!$ is a perfect pairing between $H^\sharp$ and H. The inclusion $H^\sharp \subseteq H$ is therefore nondegenerate up to $p^{\lfloor \log_p k \rfloor}$ on all of the rank.

18.5. The span at a vertex

Fix L and a basis x, y of $L^\vee$, so that $H(L) = H$ and $H(L)^\sharp = H^\sharp$ in the notation of Section 18.4. The lattices M of Problem 18.1.5 are $M_\alpha := W(x + \alpha y) + pL^\vee$ for $\alpha \in W$, which depends only on α modulo p, and $M_\infty := Wy + pL^\vee$.

Problem 18.5.1. (i) If $Q > k$, the W-span of $\{\lambda^k : \lambda \in L^\vee\}$ is $H(L)^\sharp$. (ii) If $Q = 2$ and $k = 3$, this span has colength 1 in $H(L)^\sharp = H(L)$.

Problem 18.5.2. $\mathrm{Sym}^k(M_\alpha)$ is spanned by the $(x + \alpha y)^{k-i}(py)^i$ with $0 \le i \le k$. If $Q > k$, then for each i the W-span of $\{(x + \alpha y)^{k-i} y^i : \alpha \in W\}$ is $\bigoplus_{j=i}^k \binom{k-i}{j-i} W x^{k-j} y^j$. For the remaining line, $\mathrm{Sym}^k(M_\infty) = \bigoplus_{j=0}^k p^{k-j} W x^{k-j} y^j$.

Problems 18.1.5 and 18.5.2 give the following theorem. Problem 18.3.2 gives its last two sentences.

Theorem 18.5.1. *Suppose $Q > k$. Then $S(L) = \bigoplus_{j=0}^{k} p^{\varepsilon_j} W x^{k-j} y^j$, where the exponent ε_j of the monomial $x^{k-j}y^j$ is*

$$\varepsilon_j = \min\Big(k-j,\ \min_{0\le i\le j}\Big(i + v_p\binom{k-i}{j-i}\Big)\Big).$$

In particular $\varepsilon_j \le \min\big(j,\, k-j,\, v_p\binom{k}{j}\big) \le \lfloor \log_p k \rfloor$. So $p^{\lfloor \log_p k\rfloor} H(L) \subset S(L)$, and the loss is at most $\sum_j v_p\binom{k}{j}$.

When $Q > k$, the inclusion $S(L) \subseteq H(L)$ is therefore nondegenerate up to $p^{\lfloor \log_p k\rfloor}$ on all of the rank. The exponents can be strictly smaller than the valuations $v_p\binom{k}{j}$.

Problem 18.5.3. Assume $Q > k$. Then $\varepsilon_j = \varepsilon_{k-j}$. For $k = Q-1$ the loss is 0. For $k = p < Q$ the loss is $p-1$. For $p = 3$, $k = 6$ and $Q \ge 9$ the ε_j, in the order $j = 0, \dots, k$, are $0, 1, 1, 0, 1, 1, 0$. For $p = 2$, $k = 8$ and $Q \ge 16$ they are $0, 1, 1, 1, 1, 1, 1, 1, 0$, so the loss is 7, although $\sum_j v_2\binom{8}{j} = 17$.

What if there are few edges?

Problem 18.5.4. If $Q \le k$, then at most $Q+1$ of the exponents of $S(L)$ in $H(L)$ vanish, and the loss is at least $k - Q$. More generally, for each integer $u \ge 1$ at most $(Q+1)u$ of the exponents are less than u.

So the largest exponent is at least $(k+1)/(Q+1) - 1$, and for fixed Q the loss grows quadratically in k, since at least $k + 1 - (Q+1)u$ exponents are $\ge u$ for each u. For $Q = 2$ and $k = 15$, a Smith form computation gives the exponents $0, 0, 0, 1, 1, 1, 2, 2, 2, 3, 3, 3, 4, 4, 4, 5$, a loss of 35. For $Q = 3$ and $k = 15$ it gives $0, 0, 0, 0, 1, 1, 1, 1, 2, 2, 2, 2, 4, 4, 4, 4$. The formula of Theorem 18.5.1 assumes $Q > k$.

When $Q > k$, every exponent is at most $\lfloor \log_p k \rfloor$. Conversely, if every exponent is at most D, then $Q + 1 \ge (k+1)/(D+1)$.

18.6. Onto up to colength

At an exceptional prime $p < x_1$, Chapter 48 bounds the colength of $Y_{\mathfrak{M}}^{m} S_\eta + p^{j_p} S_\eta$ in the module S_η of integral source forms. Problem 18.2.4 illustrates this truncation over W. In this chapter U denotes an endomorphism. The colength of Chapter 5 makes sense over any commutative ring. Let O be a commutative ring, $\mathcal{V}$ an O-module, $\mathcal{V}_1, \mathcal{V}_2 \subseteq \mathcal{V}$ submodules and $\zeta \in O$. We say that *the colength of $\mathcal{V}_2$ in $\mathcal{V}_1$ divides ζ* if for every $t \ge 0$ and every family $v_1, \dots, v_t$ of elements of $\mathcal{V}_1$ there is a $t \times t$ matrix C over O with $\det C \mid \zeta$ and $\sum_j C_{ij} v_j \in \mathcal{V}_2$ for every i. No inclusion between $\mathcal{V}_1$ and $\mathcal{V}_2$ is assumed. For $p \in O$, an integer $u \ge 0$, an endomorphism U of $\mathcal{V}$ and a real number c, we say that *U is onto $\mathcal{V}_1$ modulo p^u up to colength c* if $U\mathcal{V}_1 \subseteq \mathcal{V}_1$ and there is an integer $l \ge 0$ with $l \le c$ such that the colength of $U\mathcal{V}_1 + p^u \mathcal{V}_1$ in $\mathcal{V}_1$ divides p^l.

Problem 18.6.1. Let $\mathcal{V}_1$ be a free W-module of finite rank, $\mathcal{V}_2 \subseteq \mathcal{V}_1$ a submodule, possibly with $\mathcal{V}_1/\mathcal{V}_2$ of infinite length, and $l \ge 0$ an integer. The colength of $\mathcal{V}_2$ in $\mathcal{V}_1$ divides p^l if and only if $\operatorname{length}_W \mathcal{V}_1/\mathcal{V}_2 \le l$.

Problem 18.6.2. Suppose $Q > k$, and let U be an endomorphism of $H(L)$ with $UH(L) = S(L)$, for example the diagonal one that multiplies $x^{k-j}y^j$ by p^{ε_j}. Then U is onto $H(L)$ modulo p^u up to colength c if and only if $c \ge \sum_{j=0}^{k} \min(\varepsilon_j, u)$. For $p = 3$, $k = 6$, $Q \ge 9$ and every $u \ge 1$ the least such c is 4.

Problem 18.6.3. Let $\mathcal{V}_1$ be a free W-module of finite rank. If U_1 and U_2 are onto $\mathcal{V}_1$ modulo p^u up to colengths c_1 and c_2, then U_1U_2 is onto $\mathcal{V}_1$ modulo p^u up to colength $c_1 + c_2$.

18.7. Exceptional primes and the theorem on elementary divisors

We use the notation of Chapter 33: the parameters q_0 and d, with $d \equiv q_0/2 - 1 \pmod{q_0}$, the character χ_K of $K = \mathbb{Q}(\sqrt{-d})$, the a-places Φ_a, the place $[\nu]$ of an integer ν, and the number m of lifts; and from Section 48.2 the collisions, o_p, r_p and the exceptional primes. Here a collision means a collision outside the empty set. Since $q_0/2$ is divisible by $8 \cdot 3 \cdot 5 \cdot 7 \cdot 11$, quadratic reciprocity gives $\chi_K = 1$ at every prime factor of q_0; so a prime p with $\chi_K(p) = -1$ is prime to q_0, and o_p is the order of $-p$ in $(\mathbb{Z}/q_0)^\times$.

Problem 18.7.1. Let p be a prime with $\chi_K(p) = -1$, and $e \geq 1$ odd. Then (τ, e) is a collision for one, equivalently every, $\tau \in \Phi_a$ if and only if $o_p \mid e$. So collisions exist if and only if o_p is odd, and if o_p is odd and $o_p > r_p$, every collision has $p^e \geq pm$.

The theorem on elementary divisors, Theorem 48.5.1, is stated in Chapter 48, Section 48.5, with Problem 48.5.1 on the size of its hypotheses; the proof needs it only at the exceptional primes (Section 48.4). Theorem 18.5.1 is its model, not a case of it.

In the Lean formalization. In the Lean proof [GL], Theorem 48.5.1 is `FrobeniusCycle.elementary_divisors`, with the hypotheses `IsLargeDegree`, in `New/UpperBound/ElementaryDivisors/ElementaryDivisorTheorem.le` the notion of Section 18.6 is `IsOntoUpToColength` in `New/Reduction/Lattices/Colength.lean`. The underlying divisibility predicate is `ColengthDvd` in the same file. For the use at exceptional primes, see `IsMarked.isOntoUpToColength_scaledHeckeOperator` in `MarkOperator.lean`, and the product bound `IsMarked.isOntoUpToColength_prod_scaledHeckeOperator_pow` and the exceptional case of `Data.exists_colengthDvd_gaugeLe_compositeLift` in `LocalDivisibility.lean`.

Chapters 16 and 17 study the local gain, and this chapter the colength at an exceptional prime; Chapter 48 combines the local estimates for the composite lift. The next part, from Chapter 20 on, turns to periods, masses and norms of theta lifts.

Hints

§18.1.

18.1.1: $L'' \mapsto L''/pL$. For the last statement, compare the indices in L of two homothetic sources.

18.1.2: $(gL)^\vee = (g^{-1})^{\mathsf{T}} L^\vee$ under the pairing. An inclusion of lattices reverses on duals.

18.1.3: Choose a basis u_1, u_2 of L with $L'' = Wu_1 + Wpu_2$, by the elementary divisor theorem.

18.1.4: For the image, take F supported on the sources of L.

18.1.5: Dualize the two inclusions defining a source.

18.1.6: List the three lattices M and expand.

§18.2.

18.2.1: Multiplying A on either side by an invertible matrix does not change the ideal generated by its $l \times l$ minors.

18.2.2: To construct a family, use the dual basis of (h_i). To bound the size of any such family, reduce the witness and test maps modulo p^{D+1}.

18.2.3: The image is a submodule of W^M; compare it with $p^D W^M$.

18.2.4: Compare the cokernels of A and A' after tensoring with $W/p^T W$.

§18.3.

18.3.1: Legendre's formula, and each carry lowers the digit sum by $p-1$.

18.3.2: Between which digit positions can a carry occur?

18.3.3: Problem 18.3.1.

§18.4.

18.4.1: Check it on monomials. Then induct on the degree of F.

18.4.2: Problem 18.4.1, or expand both sides.

18.4.3: The monomials are orthogonal. For the inclusions, Problem 18.3.2.

§18.5.

18.5.1: Use the Vandermonde matrix of Teichmüller representatives. For $Q = 2$, look for a cubic form that takes values in $2\mathbb{Z}_2$ on $\mathbb{Z}_2^2$.

18.5.2: The same Vandermonde argument, applied to the vectors $\left(\binom{k-i}{j-i}\alpha^{j-i}\right)_j$.

18.5.3: The symmetry $x \leftrightarrow y$ of $H(L)$ permutes the lattices M. Then Problem 18.3.3.

18.5.4: Reduce modulo p. For the general statement, use Problem 18.1.3 modulo p^u.

§18.6.

18.6.1: For one direction take $v_1, \ldots, v_t$ a basis of $\mathcal{V}_1$. For the other, the vectors $c \in W^t$ with $\sum_j c_j v_j \in \mathcal{V}_2$ form a submodule whose quotient embeds in $\mathcal{V}_1/\mathcal{V}_2$.

18.6.2: Theorem 18.5.1 and Problem 18.6.1; then Problem 18.5.3.

18.6.3: U_1 maps $\mathcal{V}_1/(U_2\mathcal{V}_1 + p^u\mathcal{V}_1)$ onto $(U_1\mathcal{V}_1 + p^u\mathcal{V}_1)/(U_1U_2\mathcal{V}_1 + p^u\mathcal{V}_1)$.

§18.7.

18.7.1: For odd e, $-p^e = (-p)^e$, and $\tau \equiv 1 \pmod{q_0}$.

References

[Ba] V. Bargmann, *On a Hilbert space of analytic functions and an associated integral transform, Part I*, Comm. Pure Appl. Math. **14** (1961), 187–214.

[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/`.

[Gra] A. Granville, *Arithmetic properties of binomial coefficients I: Binomial coefficients modulo prime powers*, in: Organic Mathematics (Burnaby, 1995), CMS Conf. Proc. **20**, Amer. Math. Soc., 1997, 253–276.

[Ku] E. E. Kummer, *Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen*, J. reine angew. Math. **44** (1852), 93–146.

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

[SeT] J.-P. Serre, *Trees*, Springer, 1980.