PAIRINGS ON A FORMAL GROUP OF HEIGHT TWO

Prerequisites. Chapter 13, *Complex multiplication and reduction at an inert prime*: formal groups, their logarithms and the invariant derivation D (Section 13.2), and the statement of Lubin–Tate theory with the model logarithm (Section 13.3, Problem 13.3.7). Chapter 15, *The invariant derivation at a supersingular prime*: the function E_p and Theorem 15.4.1. Chapter 16, *The isotropic plane*, Theorem 16.3.1. Chapter 2, Problem 2.1.1. The ring $\mathbb{Z}_{p^2}$ of integers of the unramified quadratic extension of $\mathbb{Q}_p$, its Teichmüller roots of unity, and its Frobenius σ, which satisfies $\sigma(a) \equiv a^p \pmod p$. Legendre's formula $v_p(n!) = (n - s_p(n))/(p-1)$, where $s_p(n)$ is the sum of the base-p digits of n. Section 17.5 uses, besides, the field $\mathbb{C}_p$, the completion of an algebraic closure of $\mathbb{Q}_p$, with its valuation $v(p) = 1$ and ring of integers $\mathcal{O}_{\mathbb{C}_p}$, and the infinite places of a cyclotomic extension of an imaginary quadratic field.

Chapter 16 found the gain at the odd levels only for $p \equiv 3 \pmod 8$, because it needed a global element of the CM order acting by a non-unit on one eigenline. What structure, visible at p alone, forces a series to be divisible by about $p^{\alpha p/(p^2-1)}$, that is by $p^{\sum_{i \text{ odd}} \alpha/p^i}$, after α derivatives? This chapter studies series $\exp(-\beta(x,y))\,U(x,y)$ with U integral, where x and y are parameters of a formal group of height two and β is a pairing, biadditive and semilinear for Frobenius up to series with integral exponential. Sections 17.1–17.4 construct the family $Q_{c,\sigma c}$ ($c \in \mathcal{O}$) and derive two divisibility bounds for series with $\beta \simeq Q_{c,\sigma c}$, in the simplest setting: one variable x and one partner variable y. Section 17.5 puts $\exp(-Q_{c,\sigma c})U$, for a unit c, into the normal form of the proof by changing the partner coordinate (Problem 17.5.2), and states the count proved there for series in that form at the infinite places of a number field.

17.1. The formal module of height two

Throughout, p is an odd prime, $\mathcal{O} := \mathbb{Z}_{p^2}$, $L := \mathbb{Q}_{p^2}$, σ is the Frobenius of L, and v is the valuation with $v(p) = 1$. A power series over L, or over a finite extension of L, is *integral* if all its coefficients have valuation ≥ 0. Let

$$\lg(X) := \sum_{j \geq 0} \frac{X^{p^{2j}}}{p^j}, \qquad \lg^*(X) := \frac{1}{p}\lg(X^p) = \sum_{j \geq 0} \frac{X^{p^{2j+1}}}{p^{j+1}}.$$

In the notation of Chapter 13, $\lg = \ell_p$ is the model logarithm for the uniformizer p of $\mathcal{O}$, whose residue field has p^2 elements.

We use Hazewinkel's functional-equation lemma [Ha, §2.2], [Ha79, (2.5)–(2.8)] in the following case. Let $f(X) \in L[[X]]$ satisfy $f(X) - p^{-1}f(X^{p^2}) \in \mathcal{O}[[X]]$ and $f(X) \equiv X$ modulo degree 2. Then: $f^{-1}(f(X) + f(Y))$ has coefficients in $\mathcal{O}$; if $g(X) \in XL[[X]]$ also satisfies $g(X) - p^{-1}g(X^{p^2}) \in \mathcal{O}[[X]]$, then $f^{-1}(g(X)) \in \mathcal{O}[[X]]$; and for $\alpha, \beta \in X\mathcal{O}[[X]]$ and $r \geq 1$, $\alpha \equiv \beta \pmod{p^r}$ if and only if $f(\alpha) \equiv f(\beta) \pmod{p^r}$.

Date: November 25, 2026.

Let $F(X,Y) := \lg^{-1}(\lg X + \lg Y)$ and $[\alpha](X) := \lg^{-1}(\alpha \lg X)$ for $\alpha \in \mathcal{O}$.

Problem 17.1.1. $F \in \mathbb{Z}_p[[X,Y]]$ and $[\alpha] \in \mathcal{O}[[X]]$, so F is a formal $\mathcal{O}$-module. Modulo degree p^2+1,

$$F(X,Y) \equiv X + Y - \frac{1}{p} \sum_{0<k<p^2} \binom{p^2}{k} X^k Y^{p^2-k}.$$

For $\zeta \in \mathcal{O}$ with $\zeta^{p^2-1} = 1$, $[\zeta](X) = \zeta X$ and $F(\zeta X, \zeta Y) = \zeta F(X,Y)$.

Problem 17.1.2. $[p](X) \equiv X^{p^2} \pmod p$. So F has height two.

Problem 17.1.3. Let ω be a root of unity of order $2(p^2-1)$, so that $\omega^{p^2-1} = -1$ and $\omega \in \mathbb{Z}_{p^4}$. Then $\ell_{-p}(\omega X) = \omega \lg(X)$. Hence for $p \equiv 3 \pmod 4$ the formal group of $y^2 = x^3 - x$ is isomorphic to F over $\mathbb{Z}_{p^4}$.

For a series f over L let f^σ be the series obtained by applying σ to the coefficients, and $f^\phi(X) := f^\sigma(X^p)$, where X^p raises every variable to the power p.

Problem 17.1.4. For f integral over $\mathcal{O}$ in any number of variables, $f^\phi \equiv f^p \pmod p$. In particular $F(X^p, Y^p) \equiv F(X,Y)^p \pmod p$.

17.2. Pairings and their normal form

In this chapter L is $\mathbb{Q}_{p^2}$, U an integral series, and in Section 17.5 κ is a shape, ι a filling, N a number of rows, r a partner rule, $\Delta(\kappa)$ the predicted divisibility, B a number of boxes, t a height and S a set of exponents; elsewhere in the workbook these letters denote the weight, an isomorphism $\mathbb{C} \simeq \bar{\mathbb{Q}}_\ell$, the level, a rank, the gap, the budget, the number $5r$ and the source forms, and K is $\mathbb{Q}(\sqrt{-d})$.

For series f, g over L write $f \simeq g$ if $f - g$ has no constant term and $\exp(f-g)$ is integral. The basic tool is Dwork's lemma [Ko, §IV.2], in the following form, which has the same proof since $\sigma(a) \equiv a^p \pmod p$: for a series Ψ over L in finitely many variables without constant term,

$$\exp\Psi \text{ is integral} \iff \Psi^\phi - p\Psi \in p\,\mathcal{O}[[X]].$$

For a series H in two variables let $H^{\mathrm{sw}}(X,Y) := H(Y,X)$ and

$$(d_F H)(X_0, X_1, X_2) := H\big(F(X_0,X_1), X_2\big) - H(X_0,X_2) - H(X_1,X_2),$$

and for a series f in one variable let $\partial_F f := f(F(X_0,X_1)) - f(X_0) - f(X_1)$. A *pairing* is a series $\beta(X,Y)$ over L such that: (i) every monomial of β contains both variables; (ii) $d_F\beta \simeq 0$ and $d_F\beta^{\mathrm{sw}} \simeq 0$; (iii) $\beta(\zeta X, Y) \simeq \beta(X, \zeta^p Y)$ for every $\zeta \in \mathcal{O}$ with $\zeta^{p^2-1} = 1$. Condition (ii) says that β is additive in each variable up to $\simeq$. Condition (iii) is semilinearity for Frobenius, since $\zeta^p = \sigma(\zeta)$.

Problem 17.2.1. The relation $\simeq$ is an equivalence relation, stable under sums and under substitution of series over $\mathcal{O}$ without constant term for the variables. If $f \simeq g$, then $d_F f \simeq d_F g$.

Problem 17.2.2. (i) $\beta(\zeta X, Y) = \beta(X, \zeta^p Y)$ for all ζ as in (iii) if and only if every monomial $X^m Y^n$ of β has $m \equiv pn \pmod{p^2-1}$. (ii) Let β be a pairing, ζ a primitive (p^2-1)th root of unity, and $G := (p^2-1)^{-1} \sum_{k=0}^{p^2-2} \beta(\zeta^k X, \zeta^{-pk} Y)$. Then G is a pairing, $G \simeq \beta$, and G satisfies the condition of (i).

For $c, c' \in L$ let

$$A(X,Y) := \sum_{0\le i\le j} \frac{X^{p^{2i}}\, Y^{p^{2j+1}}}{p^{\,i+j+1}}, \qquad Q_{c,c'}(X,Y) := c\,A(X,Y) - c'\,A(Y,X).$$

In every monomial of A the exponent of Y is the exponent of X times an odd power of p.

Problem 17.2.3. For all c, c', $Q_{c,c'}(\zeta X, Y) = Q_{c,c'}(X, \zeta^p Y)$ for every ζ as in (iii). No monomial of $\lg(X)\lg(Y)$ satisfies the congruence of Problem 17.2.2(i), and $\lg(X)\lg(Y)$ fails condition (iii): $\lg(\zeta X)\lg(Y) \not\simeq \lg(X)\lg(\zeta^p Y)$ for ζ a primitive (p^2-1)th root of unity.

Problem 17.2.4. $A(X^p, Y^p) = p\big(\lg^*(X)\lg(Y) - A(Y,X)\big)$. Hence

$$Q_{c',c}(X^p, Y^p) - p\,Q_{c,c'}(X,Y) = p\big(c'\lg^*(X)\lg(Y) - c\lg(X)\lg^*(Y)\big).$$

Problem 17.2.5. If $c \in L$ and $Q_{c,\sigma c} \simeq 0$, then $c = 0$.

Problem 17.2.6. If $c \in \mathcal{O}$, β is a pairing and $\beta \simeq Q_{c,\sigma c}$, then $p\cdot[XY^p]\,\beta \in \mathcal{O}$ and $p\cdot[XY^p]\,\beta \equiv c \pmod p$.

For $c \in \mathcal{O}$, is $Q_{c,\sigma c}$ itself a pairing? For $c \neq 0$ it is not integral, and it is not biadditive on the nose. Problems 17.2.7–17.2.10 show that it is biadditive up to $\simeq$.

Problem 17.2.7. Let Ψ be a series over L whose partial derivative $\partial\Psi/\partial X_m$ is integral, let the entries of $\mathbf{g}$ and the series V have coefficients in $\mathcal{O}$ and zero constant term. Then $\Psi(\mathbf{g} + pV\mathbf{e}_m) - \Psi(\mathbf{g}) \in p\,\mathcal{O}[[X]]$, where $\mathbf{e}_m$ is the unit vector of the variable X_m.

Problem 17.2.8. $\partial_F \lg = 0$, and $\partial_F \lg^*$ is integral.

Problem 17.2.9. For $c, c' \in \mathcal{O}$, the series $\partial_X\big(Q_{c,c'}(X,Y) - c\lg(X)\lg^*(Y)\big)$ is integral.

Problem 17.2.10. For $c \in \mathcal{O}$, $Q_{c,\sigma c}$ is a pairing.

Since $c \mapsto Q_{c,\sigma c}$ is additive, Problems 17.2.5, 17.2.6 and 17.2.10 prove the following.

Theorem 17.2.1. *For every $c \in \mathcal{O}$ the series $Q_{c,\sigma c}$ is a pairing. If $c, c' \in \mathcal{O}$ and $Q_{c,\sigma c} \simeq Q_{c',\sigma c'}$, then $c = c'$. If a pairing β satisfies $\beta \simeq Q_{c,\sigma c}$ with $c \in \mathcal{O}$, then $c \equiv p\cdot[XY^p]\,\beta \pmod p$.*

Below we use only pairings $\beta \simeq Q_{c,\sigma c}$ with $c \in \mathcal{O}$. The exactly biadditive series $\lg(X)\lg(Y)$ is not a pairing: it fails condition (iii) (Problem 17.2.3). The denominators of $Q_{c,\sigma c}$ sit only on the monomials $X^{p^{2i}}Y^{p^{2j+1}}$ and $Y^{p^{2i}}X^{p^{2j+1}}$, at odd shifts.

17.3. Odd shifts and the credit

How much do these denominators cost after α derivatives? Let ϖ_p be a root of $\varpi_p^{p^2-1} = p$, and let $\mathcal{O}' := \mathcal{O}[\varpi_p]$, so that $v(\varpi_p) = \rho$ with

$$\rho := \frac{1}{p^2-1}, \qquad \gamma_p := \frac{p}{p^2-1}.$$

Problem 17.3.1. $\gamma_p = \sum_{e\ge 0} p^{-(2e+1)}$ and $\gamma_p + \rho = 1/(p-1)$. If $n = \sum_k \delta_k p^k$ in base p, then

$$\gamma_p n - E_p(n) = \gamma_p \sum_{k \text{ even}} \delta_k + \rho \sum_{k \text{ odd}} \delta_k, \qquad v(n!) - \rho n = \gamma_p n - \frac{s_p(n)}{p-1}.$$

Hence $v(n!) - \rho n \le E_p(n) \le \gamma_p n$.

If $g(\varpi_p x)$ is integral, then $v(g^{(n)}(0)) \ge v(n!) - \rho n$. For the formal group of Chapter 15 at $p \equiv 3 \pmod 4$, the nth invariant derivative at zero of an integral series has valuation at least $E_p(n)$ (Theorem 15.4.1). By Problem 17.3.1, both bounds are the credit $\gamma_p n = \sum_{i \text{ odd}} n/p^i$ up to digit terms.

Problem 17.3.2. In $Q_{c,c'}(\varpi_p X, \varpi_p Y)$ the coefficient of $X^{p^{2i}} Y^{p^{2j+1}}$ $(i \le j)$ has valuation $v(c) + (p^{2i} + p^{2j+1})\rho - (i + j + 1)$. For $i = j = 0$ this is $v(c) + \frac{1}{p-1} - 1$; otherwise it is at least $v(c) + \frac{1}{p-1} + p - 2$. The same holds for the coefficient of $Y^{p^{2i}} X^{p^{2j+1}}$, with c' in place of c.

Problem 17.3.3. Let Ψ be a series without constant term over a finite extension L' of $L(\varpi_p)$. If every coefficient of Ψ has valuation at least $1/(p-1)$, then every coefficient of $\exp \Psi$ has valuation at least 0; for $L' = L(\varpi_p)$ they lie in $\mathcal{O}'$. For every series h over $\mathcal{O}'$ without constant term, $\exp(\varpi_p^{p+1} h/p) = \sum_{k\ge 0} (h/p)^k\, g_k$ with $g_k \in \mathcal{O}'$.

For a series h without constant term, let $\mathcal{C}(h)$ be the set of series $\sum_{k\ge 0} p^{-k} h^k g_k$ with g_k integral over $\mathcal{O}'$, the sum being finite in each degree. It is stable under multiplication by integral series. Problems 17.2.1 and 17.3.2–17.3.3 prove the following.

Theorem 17.3.1. *Let $c \in \mathcal{O}$, let β be a pairing with $\beta \simeq Q_{c,\sigma c}$, let $U \in \mathcal{O}[[x,y]]$, and let $\Theta := \exp(-\beta(x,y))\, U(x,y)$. Then*

$$\Theta(\varpi_p x, \varpi_p y) \in \mathcal{C}(h), \qquad h := \sigma(c)\, x^p y - c\, x y^p.$$

17.4. Two local estimates

Fix Θ, β, c, h as in Theorem 17.3.1. We bound the mixed derivatives at 0 of Θ, of order a in x and w in y, in two ways: in the formal parameters, with $\partial_x^a \partial_y^w$, and in the logarithm coordinates, with $D_x^a D_y^w$, where $D_x := \lg'(x)^{-1} \partial_x$ is the invariant derivation of Chapter 13. Thus $(D_x^a D_y^w \Theta)(0) = a!\, w!\, [\xi^a \eta^w]\, \Theta(\lg^{-1} \xi, \lg^{-1} \eta)$. We call x the *top* and y its *partner*.

Problem 17.4.1. If $G(\varpi_p x, \varpi_p y) \in \mathcal{C}(h)$, then

$$v\big((\partial_x^a \partial_y^w G)(0)\big) \;\ge\; v(a!) + v(w!) - \rho(a+w) - \min\Big(w,\; \Big\lfloor \frac{a}{p} \Big\rfloor + \Big\lfloor \frac{w}{p} \Big\rfloor\Big).$$

In the formal parameters the multiplication by p on the partner, $y \mapsto [p](y)$, is not linear. In the logarithm coordinates it is $\eta \mapsto p\eta$, and its effect on D_y^w is the factor p^w.

Problem 17.4.2. $\beta(x, [p]y) \simeq p\, \beta(x,y)$, and $\exp\big(-p\, Q_{c,\sigma c}(\varpi_p x, \varpi_p y)\big)$ is integral over $\mathcal{O}'$.

Problem 17.4.3. If $G(\varpi_p x, \varpi_p y)$ is integral over $\mathcal{O}'$, then $v\big((D_x^a D_y^w G)(0)\big) \ge v(a!) + v(w!) - \rho(a+w)$.

Applying Problem 17.4.1 to Θ, and Problem 17.4.3 to $\Theta(x,[p]y)$, which is allowed by Problem 17.4.2, gives the following.

Theorem 17.4.1. *For all $a,w\ge 0$:*

(A) $v\big((\partial_x^a\partial_y^w\Theta)(0)\big) \;\ge\; v(a!)+v(w!)-\rho(a+w)-\min\big(w,\ \lfloor a/p\rfloor+\lfloor w/p\rfloor\big)$,

(B) $v\big(p^w(D_x^aD_y^w\Theta)(0)\big) \;\ge\; v(a!)+v(w!)-\rho(a+w)$.

By Problem 17.3.1, both right sides are at least $\gamma_p a-w-(s_p(a)+s_p(w))/(p-1)$: the top earns the credit $\gamma_p a=\sum_{i\ \mathrm{odd}} a/p^i$, and the partner pays at most one factor of p per derivative. In (B) the payment is the explicit factor p^w, the effect of $[p]$ on the partner. The bounds use the hypothesis $\beta\simeq Q_{c,\sigma c}$ with $c\in\mathcal{O}$, the integrality of U and the formal $\mathcal{O}$-module F, not any global element of a CM order.

How are the w factors of p spent? For $\Theta=\exp(-Q_{c,\sigma c})$ with c a unit, $1\le w<p$ and $a=p^{2e+1}w$ for an integer $e\ge 0$, the loss relative to $v(a!)$ is w at each of the levels $1,3,\dots,2e+1$.

Problem 17.4.4. Let $c\in\mathcal{O}$, let w,e be integers with $1\le w<p$ and $e\ge 0$, and let $a:=p^{2e+1}w$. Then

$$\big(\partial_x^a\partial_y^w\exp(-Q_{c,\sigma c}(x,y))\big)(0)=\frac{a!\,\sigma(c)^w}{p^{(e+1)w}},$$

of valuation $v(a!)-(e+1)w$ when c is a unit. (For $p=3$, $w=1$, $e=1$: $27!\,\sigma(c)/9$, of valuation 11.)

For these orders the loss is w at each of the odd levels through $2e+1$, as in the bound $\sum_{i\ \mathrm{odd}}(\lfloor a/p^i\rfloor-w)_+$ of Theorem 16.3.1. The odd powers p^i are exactly those at which $1-\chi_K(p^i)=2$ for p inert, where χ_K is the character of $K=\mathbb{Q}(\sqrt{-d})$ (written χ_d there) (Problem 2.1.1(ii)).

17.5. Couplings and the count

In the normal form of the proof each variable has a place index, and the exponent uses couplings between a place and its partners. The proof defines couplings and the normal form for every prime p; here p stays odd.

Let Φ and V be finite sets, and let $r=(r_e)_{e\ge0}$ be a sequence of maps $r_e\colon\Phi\to\Phi$, the *partner rule*. The variables are $z_{\tau i}$, $(\tau,i)\in\Phi\times V$, and a series is *integral* if its coefficients lie in $\mathcal{O}_{\mathbb{C}_p}$. The *couplings* are

$$\Gamma_e:=\sum_{(\tau,i)\in\Phi\times V} z_{\tau i}^{\,p^e}\,z_{r_e(\tau)i}\qquad(e\ge0).$$

Problem 17.5.1. (i) $\Gamma_e(\alpha z)=\alpha^{p^e+1}\Gamma_e(z)$ for $\alpha\in\mathcal{O}_{\mathbb{C}_p}$. (ii) Let $\Phi=(\mathbb{Z}/q\mathbb{Z})^\times$ with $p\nmid q$, let V be a point, and $r_e(\tau):=-p^e\tau$. If $p^2\equiv1\pmod q$ and $p\not\equiv-1\pmod q$, then for odd e the map r_e is an involution without fixed points, and Γ_e is the sum over its orbits $\{\tau,-p\tau\}$ of $z_\tau^{p^e}z_{-p\tau}+z_{-p\tau}^{p^e}z_\tau$. For $q=8$ and $p=3$, $\Gamma_1=z_1^3z_5+z_5^3z_1+z_3^3z_7+z_7^3z_3$.

Let S be a set of integers $e\ge0$, let $\varpi\in\mathbb{C}_p$, and let $\lambda=(\lambda_{ej})_{e,j\ge0}$ be a family in $\mathcal{O}_{\mathbb{C}_p}$. A series $\Theta\in\mathbb{C}_p[[z_{\tau i}]]$ has the *normal form* for (S,r,ϖ,λ) if there is an integral series W with

$$\Theta(\varpi z)=W(z)\exp\Big(\frac{\varpi^{p+1}}{p}\sum_{e\in S}\sum_{j\ge0}\lambda_{ej}\,\Gamma_e^{p^j}\Big).$$

The sum converges, as $\Gamma_e^{p^j}$ is homogeneous of degree $(p^e+1)p^j$. The λ_{ej} may be any elements of $\mathcal{O}_{\mathbb{C}_p}$, and ϖ any element of $\mathbb{C}_p$.

In the next problem $\Phi=\{1,2\}$, V is a point, r_e is the transposition for every e, S is the set of odd numbers, and $z_1=x$, $z_2=y$; so $\Gamma_1=x^py+xy^p$. The series $Q_{c,c'}$ and the root ϖ_p are those of Sections 17.2 and 17.3.

Problem 17.5.2. Let $c\in\mathcal{O}^\times$, $U\in\mathcal{O}[[x,y]]$ and $\Theta:=\exp(-Q_{c,\sigma c}(x,y))\,U(x,y)$. (i) Let $\epsilon\in\mathbb{C}_p$ satisfy $\epsilon^{p-1}=-\sigma(c)/c$. Then $\Theta(x,\epsilon y)$ has the normal form for (S,r,ϖ_p,λ) with $\lambda_{10}=\sigma(c)\epsilon$ and $\lambda_{ej}=0$ otherwise. For $p=3$, $c=1$, $U=1$, the coefficients of x^3y and of xy^3 in $\Theta(x,\epsilon y)$ are both $\epsilon/3$. (ii) If $U(0)=1$ and $c+\sigma(c)\in\mathcal{O}^\times$, then $\Theta(x,y)$ has the normal form for (S,r,ϖ_p,λ) for no λ.

The count measures jets of such a series along products of minors. Let $\mathcal{R}$ and $\mathcal{U}$ be finite sets, $N:=|\mathcal{R}|$, and take $V=\mathcal{R}\times\mathcal{U}$, so that the variables are $z_{\tau bu}$. A *shape* is a function κ on $\Phi\times\mathbb{Z}_{\geq 0}$ with values in $\mathbb{Z}_{\geq 0}$; $\kappa(\tau,t)$ is the number of columns of height t at τ, and only the heights $t<N$ will count. A *filling* ι of κ assigns a row $\iota_\tau(t,j,b)\in\mathcal{R}$ to every $\tau\in\Phi$, $t<N$, $j<\kappa(\tau,t)$ and $b<t$. For a family $\mu=(\mu_{\tau uk})$ in $\mathcal{O}_{\mathbb{C}_p}$ ($\tau\in\Phi$, $u\in\mathcal{U}$, $k\geq 0$) the product of minors is the polynomial

$$P_\mu(z):=\prod_{\tau\in\Phi}\prod_{t<N}\prod_{j<\kappa(\tau,t)}\det\Bigl(\sum_{u\in\mathcal{U}}\mu_{\tau uk}\,z_{\tau,\iota_\tau(t,j,b),u}\Bigr)_{0\leq b,k<t},$$

and the jet of Θ along it is $(P_\mu(\partial)\Theta)(0)=\sum_m m!\,[z^m]P_\mu\,[z^m]\Theta$, where $m!=\prod m_x!$ over the variables x. At each place the proof fixes a set of *standard* fillings: in a matrix of independent variables X_{bk}, their products of minors form a basis, over every commutative ring, of the span of the products for all fillings of that shape, and the sum over these fillings of the monomials $\prod_{\text{boxes}}x_{\text{entry}}$ satisfies the Weyl character formula. Substituting $X_{bk}=\sum_u\mu_{\tau uk}z_{\tau bu}$ gives the factors of P_μ at τ.

The predicted divisibility also depends on a prime d, which may equal p. In this formula $\chi_K(p):=\left(\frac{p}{d}\right)$ denotes the quadratic character of $\mathbb{Z}/d\mathbb{Z}$, evaluated at p; for $d\equiv 3\pmod 4$ it agrees with the character of $K=\mathbb{Q}(\sqrt{-d})$ used above. Put $c_p:=1/2$ if $p=d$ and $c_p:=1$ otherwise, and let I_p° be the set of $e\geq 0$ such that $p=d$, or $\chi_K(p)=-1$ and e is odd; let $I_p:=I_p^\circ\setminus\{0\}$. For a shape κ let

$$a_\tau:=\sum_{t<N,\ t=1}\kappa(\tau,t),\qquad a'_\tau:=\sum_{t<N,\ t\neq 1}\kappa(\tau,t),\qquad l_\tau:=\sum_{t<N,\ t\neq 1}t\,\kappa(\tau,t)$$

be the numbers of columns of height one, of the other columns, and of the boxes in these. With $\tau_e:=r_e(\tau)$ and $x_+:=\max(x,0)$, the *predicted divisibility* is the real number

$$\begin{aligned}\Delta(\kappa):=c_p\sum_{e\in I_p}\sum_{\tau\in\Phi}\Bigl[\Bigl(\frac{a_\tau}{p^e}-a_{\tau_e}-a'_{\tau_e}\Bigr)_+&+\Bigl(\frac{l_\tau}{p^e}-l_{\tau_e}\Bigr)_+-\frac{a'_\tau}{p^e}\Bigr]\\&-[p=d]\,\frac{1}{2}\sum_{\tau\in\Phi}\bigl[\min(a_\tau,a_{\tau_0}+a'_{\tau_0})+a'_\tau+\min(l_\tau,l_{\tau_0})\bigr],\end{aligned}$$

where $[p=d]$ is 1 if $p=d$ and 0 otherwise.

Problem 17.5.3. Let $\chi_K(p)=-1$, $\Phi=\{1,2\}$ with r_e the transposition for odd e (and any r_e for even e), $N\geq 2$, $\kappa(1,1)=a$, $\kappa(2,1)=w$, and $\kappa=0$ otherwise.

Then

$$\Delta(\kappa) = \sum_{e\ge 1,\ e \text{ odd}} \Big[\Big(\frac{a}{p^e} - w \Big)_+ + \Big(\frac{w}{p^e} - a \Big)_+ \Big].$$

For one column ($a = 1$, $w = 0$) this is γ_p; for $p = 13$, $a = 200$, $w = 1$ it is $187/13$.

For $w = 0$ this is the credit $\gamma_p a$ of Section 17.3, without the loss from the digits (Problem 17.3.1); the bound of Theorem 16.3.1 has the same shape, with $\lfloor a/p^i \rfloor$ in place of a/p^i.

The count uses all infinite places of a cyclotomic extension of $\mathbb{Q}(\sqrt{-d})$. Let q_0 be a positive integer divisible by 18480, and d a prime with $q_0 \mid 2(d+1)$ and $q_0 \nmid d+1$. For an integer $s \ge 0$ let $q_1 := q_0 \cdot 3^{\lfloor \log_3 s \rfloor + 5}\, 2^s$, with $\lfloor \log_3 0 \rfloor := 0$, and let Φ be the set of infinite places of $\mathbb{Q}(\sqrt{-d}, \zeta_{q_1})$. It is a group, identified with $\mathrm{Gal}(\mathbb{Q}(\sqrt{-d}, \zeta_{q_1})/\mathbb{Q}(\sqrt{-d})) \cong (\mathbb{Z}/q_1\mathbb{Z})^\times$ through the place of a fixed embedding. Every prime factor of q_1 splits in $\mathbb{Q}(\sqrt{-d})$, so a prime p with $\chi_K(p) \ne 1$ is prime to q_1; for such p the partner rule is $r_e(\tau) := (-p^e)\,\tau$. Let $\rho(d,p) := c_p/(N_p - 1)$, where $N_p := p^2$ if $\chi_K(p) = -1$ and $N_p := p$ if $p = d$; for p inert, $\rho(d,p) = \rho$.

Theorem 17.5.1. *Let q_0, d, s, Φ be as above, let p be a prime with $\chi_K(p) \ne 1$, and fix an embedding of $\mathbb{C}$ into $\mathbb{C}_p$. Let $\mathcal{R}$, $\mathcal{U}$ be finite sets, $N := |\mathcal{R}|$, κ a shape, $\varpi \in \mathbb{C}_p$ with $v(\varpi) = \rho(d,p)$, λ a family in $\mathcal{O}_{\mathbb{C}_p}$, and $\Theta \in \mathbb{C}_p[[z_{\tau b u} : (\tau, b, u) \in \Phi \times \mathcal{R} \times \mathcal{U}]]$ a series with the normal form for $(I_p^\circ, r, \varpi, \lambda)$. Then for every standard filling of κ and every family μ in $\mathcal{O}_{\mathbb{C}_p}$,*

$$v\big((P_\mu(\partial)\Theta)(0)\big) \;\ge\; \Delta(\kappa) - fN^3\big(1 + \log_p \max(B,1)\big), \qquad B := \sum_{\tau\in\Phi} \sum_{t<N} t\,\kappa(\tau,t),$$

where $f := |\Phi|$, $\log_p$ is the real logarithm to the base p, and $v(0) = \infty$.

For a single column of height one the right side of Theorem 17.5.1 is negative: there $B = 1$, $N \ge 2$ and $\Delta(\kappa) \le 1/(p-1)$, while the error term is at least $8f$. Which series have the normal form is a separate statement; see the remark below. In the Lean formalization. In the Lean proof [GL], the couplings, their sum and the normal form are `New.coupling`, `New.couplingSum` and `New.HasNormalForm`, in `New/Derivatives/Divisibility/NormalForm.lean`. Theorem 17.5.1 is `New.Parameters.norm_jet_minorProd_le_of_hasNormalForm`, in `New/Derivatives/Divisibility/Count.lean`, stated as the upper bound $p^{-(\Delta(\kappa) - fN^3(1+\log_p \max(B,1)))}$ for the norm of the jet; there P_μ for a standard filling is `New.minorProd` and Δ is `New.predictedDivisibility`. The jet is `New.jet`, the standard filling at one place is an element of `New.BasisTableau`, and a standard filling over all the places is an element of `New.WeylIndex`, in `Lib/GLn/SchurModule/Basic.lean`; I_p°, I_p, c_p, $\rho(d,p)$ are `New.partnerExponents`, `New.positivePartnerExponents`, `New.piPrimeValuation`, `New.varpiValuation`, in `Lib/CM/FormalGroup/PrimeNotation.lean`; the data q_0, d are `New.Parameters` and the partner rule is `New.Parameters.partner`. `New.rescale_coupling` gives the homogeneity of Γ_e, and `New.hasSum_couplingSum` gives the convergence of the sum defining the normal form; `New.IsTableauBasis` states the basis and character conditions, and `New.isTableauBasis_epsilon` proves them for the chosen set of fillings; $a_\tau, a'_\tau, l_\tau, B$ are `New.heightOneColumns`, `New.lowColumnCount`, `New.lowBoxCount`, `New.boxes`; χ_K and N_p are `New.chiK` and `New.primeNorm`; q_1/q_0 is `New.towerDeg` evaluated at s, the field is `New.Parameters.E`, and `New.Parameters.placeMulEquiv` identifies Φ with $(\mathbb{Z}/q_1\mathbb{Z})^\times$; the splitting of

the prime factors of q_1 is `New.Parameters.chiK_eq_one_of_dvd`. The corresponding statement of the Lean proof on which series have the normal form is `New.Parameters.exists_hasNormalForm`, in `New/Derivatives/FormalGroup/ThetaProducts.lean`.

Hints

§17.1.

17.1.1: Apply the functional-equation lemma with $f = \lg$ and $g = \alpha \lg$. Modulo degree p^2+1, $\lg(X) \equiv X + X^{p^2}/p$. For ζ, use $\zeta^{p^{2j}} = \zeta$. The coefficients of F lie in $\mathbb{Q}_p \cap \mathcal{O} = \mathbb{Z}_p$.

17.1.2: Compare $\lg([p]X)$ with $\lg(X^{p^2})$, using the last part of the functional-equation lemma.

17.1.3: $\omega^{p^{2j}} = (-1)^j \omega$. Then use Problem 13.3.7.

17.1.4: $(f+g)^p \equiv f^p + g^p$ and $\sigma(a) \equiv a^p$.

§17.2.

17.2.1: An integral series with constant term 1 has an integral inverse. For the last statement, express $\exp(d_F(f-g))$ through $\exp(f-g)$.

17.2.2: (i) Compare ζ^m with ζ^{pn}. (ii) Apply (iii) with ζ^k in place of ζ, and use the binomial series $(1+T)^{1/(p^2-1)}$.

17.2.3: $\zeta^{p^2} = \zeta$. For the last assertion, look at the terms linear in X of the exponential of the difference.

17.2.4: Expand $\lg^*(X)\lg(Y)$ as a double sum and split it according to the relative size of the two indices.

17.2.5: Dwork's lemma and Problem 17.2.4. Look at the coefficients of $X^p Y^{p^{2j}}$.

17.2.6: Set $\Psi := \beta - Q_{c,\sigma c}$, and use condition (i) of a pairing: which powers of Ψ contribute terms linear in X to $\exp\Psi$?

17.2.7: Expand one monomial in the changed variable, and compare the nth binomial term with the derivative.

17.2.8: For $\lg^*$, use Problems 17.1.4 and 17.2.7, and that $\lg'$ is integral.

17.2.9: Compare each exponent with its denominator.

17.2.10: The second variable follows from the first, since $Q^{\mathrm{sw}}_{c,\sigma c} = Q_{c'',\sigma c''}$ with $c'' = -\sigma c$. For the first, apply Dwork's lemma to $d_F Q_{c,\sigma c}$. The series $(d_F Q)^\phi$ differs from $d_F(Q^\phi)$ by evaluating $Q^\sigma = Q_{\sigma c,c}$ at $F(X_0^p, X_1^p)$ instead of $F(X_0,X_1)^p$. Split $Q_{\sigma c,c}$ as in Problem 17.2.9, and use Problems 17.2.4, 17.2.7, 17.2.8 and $\lg^*(Y^p) = \lg(Y) - Y$.

§17.3.

17.3.1: $\gamma_p n - E_p(n) = \sum_{i \text{ odd}} \{n/p^i\}$, the fractional parts. Legendre's formula.

17.3.3: $v(k!) < k/(p-1)$ for $k \geq 1$.

§17.4.

17.4.1: $\partial_x^a \partial_y^w$ commutes with the rescaling up to ϖ_p^{a+w}. Count the factors $x^p y$ and xy^p in a monomial of h^k of degree at most a in x and at most w in y.

17.4.2: $[p]$ is the p-fold sum for F. Problems 17.3.2 and 17.3.3.

17.4.3: The series $\varpi_p^{-1}\lg(\varpi_p T)$ has coefficients in $\mathbb{Z}_p$.

17.4.4: Only the terms of $A(y,x)$ with $i=0$ have degree less than p in y.

§17.5.

17.5.2: (i) Split off the terms $i=j=0$ of $Q_{c,\sigma c}$; Problems 17.3.2 and 17.3.3.
(ii) Compare the coefficients of $x^p y$ and xy^p on both sides.

17.5.3: Here $a'_\tau = l_\tau = 0$.

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/`.

[Ha] M. Hazewinkel, *Formal Groups and Applications*, Academic Press, 1978.

[Ha79] M. Hazewinkel, *On formal groups. The functional equation lemma and some of its applications*, Astérisque **63** (1979), 73–82.

[Ko] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, 2nd ed., Grad. Texts in Math. 58, Springer, 1984.