PAIRINGS ON A FORMAL GROUP OF HEIGHT TWO

Prerequisites. Chapter 14, *Complex multiplication and reduction at an inert prime*: formal groups, their logarithms and the invariant derivation D (Section 14.2), and the statement of Lubin–Tate theory with the model logarithm (Section 14.3, Problem 14.3.7). Chapter 16, *The invariant derivation at a supersingular prime*: the function E_p and Theorem 16.4.1. Chapter 17, *The isotropic plane*, Theorem 17.3.1 and Section 17.4; Chapter 19 is mentioned once, for orientation. 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.

Chapter 17 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. The argument needs the gain at every inert prime. What structure, visible at p alone, forces a theta kernel 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? In the argument a theta kernel at an inert prime has the form $\exp(-\beta(x,y))\,U(x,y)$ 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. This chapter classifies such pairings and derives the divisibility from the normal form, in the simplest setting: one variable x and one partner variable y.

18.1. The formal module of height two

Throughout, p is an odd prime, $\mathcal{O} := \mathbb{Z}_{p^2}$, $K := \mathbb{Q}_{p^2}$, σ is the Frobenius of K, and v is the valuation with $v(p) = 1$. A power series over K, or over a finite extension of K, 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 14, $\lg = \ell_p$ is the model logarithm for the uniformizer p of $\mathcal{O}$, with $q = p^2$.

We use Hazewinkel's functional-equation lemma [Ha, §2.2], [Ha79, (2.5)–(2.8)] in the following case. Let $f(X) \in K[[X]]$ 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 $g(X) \in XK[[X]]$ 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 $f(\alpha) \equiv f(\beta) \pmod{p^r}$.

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

Date: November 25, 2026.

Problem 18.1.1. $F \in \mathbb{Z}_p[[X,Y]]$ 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 18.1.2. $[p](X) \equiv X^{p^2} \pmod{p}$. So F has height two.

Problem 18.1.3. Let u be a root of unity of order $2(p^2-1)$, so that $u^{p^2-1} = -1$ and $u \in \mathbb{Z}_{p^4}$. Then $\ell_{-p}(uX) = u \lg(X)$. 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 K 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 18.1.4. For f integral over $\mathcal{O}$ in any number of variables, $f^\phi \equiv f^p \pmod{p}$. In particular $F(X^p, Y^p) \equiv F(X,Y)^p \pmod{p}$.

18.2. Pairings and their normal form

For series f, g over K 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 [Adr, Lemma 9.1(i)], which has the same proof: for a series Ψ over K 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 K 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 $\exp\beta$ is biadditive up to integral cocycles. Condition (iii) is semilinearity for Frobenius, since $\zeta^p = \sigma(\zeta)$.

Problem 18.2.1. The relation $\simeq$ is an equivalence relation, stable under sums and under substitution of integral series without constant term for the variables. If $f \simeq g$, then $d_F f \simeq d_F g$.

Problem 18.2.2. (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, $N := p^2-1$, ζ a primitive Nth root of unity, and $G := N^{-1} \sum_{k=0}^{N-1} \beta(\zeta^k X, \zeta^{-pk} Y)$. Then G is a pairing, $G \simeq \beta$, and G satisfies the condition of (i).

For $c, c' \in K$ 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 18.2.3. 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 18.2.2(i).

Problem 18.2.4. $A(X^p, Y^p) = p\big(\lg^*(X)\lg(Y) - A(Y, X)\big)$. 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 18.2.5. If $c \in K$ and $Q_{c,\sigma c} \simeq 0$, then $c = 0$.

Problem 18.2.6. 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 $p \cdot [XY^p]\,\beta \equiv c \pmod{p}$.

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 18.2.7–18.2.10 show that it is biadditive up to $\simeq$.

Problem 18.2.7. Let Φ be a series over K whose partial derivative $\partial\Phi/\partial X_e$ is integral, let φ be a tuple of integral series without constant terms, and let V be an integral series without constant term. Then $\Phi(\varphi + pV\mathbf{e}_e) - \Phi(\varphi) \in p\,\mathcal{O}[[X]]$, where $\mathbf{e}_e$ is the unit vector of the variable X_e.

Problem 18.2.8. $\partial_F \lg = 0$, and $\partial_F \lg^*$ is integral.

Problem 18.2.9. 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 18.2.10. For $c \in \mathcal{O}$, $Q_{c,\sigma c}$ is a pairing.

Conversely, every pairing has this form.

Theorem 18.2.1 ([Adr, Thm. 9.3])**.** *For every pairing β there is a unique $c \in \mathcal{O}$ with $\beta \simeq Q_{c,\sigma c}$.*

Problems 18.2.5 and 18.2.10 give the uniqueness and show that every $Q_{c,\sigma c}$ occurs. For the existence, Adriazola replaces β by the average G of Problem 18.2.2, finds c from the coefficient of X in G, as in Problem 18.2.6, and applies Dwork's lemma to $G - Q_{c,\sigma c}$, using Problem 18.2.4; we do not reproduce the argument. The exactly bilinear pairing $\lg(X)\lg(Y)$ is excluded by semilinearity (Problem 18.2.3). So, up to $\simeq$, the denominators of a pairing sit only on the monomials $X^{p^{2i}}Y^{p^{2j+1}}$ and $Y^{p^{2i}}X^{p^{2j+1}}$, at odd shifts.

18.3. 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 18.3.1. $\gamma_p = \sum_{e\geq 0} p^{-(2e+1)}$ and $\gamma_p + \rho = 1/(p-1)$. If $n = \sum_k d_k p^k$ in base p, then

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

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

So a derivative of order n in a formal parameter gains $v(n!)$, and after the rescaling $x \mapsto \varpi_p x$ the gain is $\gamma_p n$ up to the digits of n; for the formal group of Chapter 16, a derivative of order n in the logarithm gains $E_p(n)$ on integral series (Theorem 16.4.1). Both are the credit $\gamma_p n = \sum_{i \text{ odd}} n/p^i$ up to digits.

Problem 18.3.2. 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 18.3.3. If every coefficient of a series Ψ without constant term has valuation $\ge 1/(p-1)$, then $\exp \Psi$ is integral over $\mathcal{O}'$. 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. Theorem 18.2.1 and Problems 18.3.2–18.3.3 prove the following.

Theorem 18.3.1. *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*

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

18.4. Two local estimates

Fix Θ, β, c, h as in Theorem 18.3.1. 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 14. Thus $(D_x^a D_y^w \Theta)(0) = a!\, w!\, [z^a t^w]\, \Theta(\lg^{-1} z, \lg^{-1} t)$. We call x the *top* and y its *partner*.

Problem 18.4.1. 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 $t \mapsto pt$, and its effect on D_y^w is the factor p^w.

Problem 18.4.2. $\beta(x, [p]y) \simeq p\, \beta(x, y)$, and $\exp\big(-p\, Q_{c,\sigma c}(\varpi_p x, \varpi_p y)\big)$ is integral over $\mathcal{O}'$.

Problem 18.4.3. 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 18.4.1 to Θ, and Problem 18.4.3 to $\Theta(x, [p]y)$, which is allowed by Problem 18.4.2, gives the following.

Theorem 18.4.1. *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) $v\big(p^w (D_x^a D_y^w \Theta)(0)\big) \;\ge\; v(a!) + v(w!) - \rho(a + w)$.

By Problem 18.3.1, both right sides are at least $\gamma_p a - w - (s_p(a)+s_p(w))/(p-1)$: the top earns the credit $\gamma_p a = \sum_{i \text{ odd}} a/p^i$, 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; in the argument this factor becomes a Hecke operator, whose elementary divisors are the loss computed in Chapter 19. The bounds use only the formal $\mathcal{O}$-module F and the semilinearity (iii) for the Teichmüller roots of unity, as in hypothesis (iii) of [Adr, Thm. 9.3], not any global element of a CM order.

How are the w factors of p spent? For $\Theta = \exp(-Q_{c,\sigma c})$ and $w < p$ they are spent once at each odd level.

Problem 18.4.4. Let $c \in \mathcal{O}$, $1 \le w < p$, $e \ge 0$, and $a := p^{2e+1}w$. 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.)

So the term $x^{p^{2e+1}} y/p^{e+1}$ of $A(y,x)$ charges w at each of the levels $1, 3, \dots, 2e+1$; this is the charge of w at each odd level in the bound $\sum_{i \text{ odd}} (\lfloor a/p^i \rfloor - w)_+$ of Theorem 17.3.1. The odd powers p^i are exactly those at which $1 - \chi_d(p^i) = 2$ for p inert (Problem 2.1.1(ii)), and the credit $\gamma_p \alpha$ at a top of weight α is matched against them in [Adr, §3.2].

In the argument, x and y are the parameters along a hyperbolic pair f, f' of the hermitian form at p, as in Section 17.4, transported to F by the Lubin–Tate isomorphism [Adr, Prop. 8.11], as in Problem 18.1.3. For the CM curve used there and every prime $p \ge 5$ inert in its CM field, Adriazola shows that the coboundary of the logarithm of the reduced theta function is a pairing [Adr, Thm. 8.12], that the theta kernels are $c_0 \exp(-\sum \beta(x,y))\, U$ with U integral [Adr, Thm. 8.21], and, with many tops and partners and with minors in place of single derivatives, proves lower bounds of the kind of Theorem 18.4.1 [Adr, Thm. 9.6]; its part (iii), with an explicit power of p attached to the partners, corresponds to (B). That the constant c_0 is integral is assumed there: in [Adr] this is [Adr, Hyp. 11.42, (N3)]; see the ledger in Section 58.7 of Chapter 58. The Lean formalization [Lean] does not assume it: it proves an integral kernel law of this shape for the kernels it uses, by a different route, in which the exponent is a torus average of a coboundary of the logarithm of the sigma function of one CM curve, and the integrality comes from a factorization of the fourth tensor power of the kernel into sigma functions.

Hints

§18.1.

18.1.1: 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 $\zeta^{p^{2j}} = \zeta$.

18.1.2: The last part of the functional-equation lemma, with $\lg([p]X) - \lg(X^{p^2}) = pX$.

18.1.3: $u^{p^{2j}} = (-1)^j u$. Then use Problem 14.3.7.

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

§18.2.

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

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

18.2.3: $\zeta^{p^2}=\zeta$.

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

18.2.5: Dwork's lemma and Problem 18.2.4. Look at the coefficients of $X^pY^{p^{2j}}$.

18.2.6: By condition (i) of a pairing, the coefficient of XY^n in $\exp\Psi$ equals that of Ψ.

18.2.7: Reduce to a monomial aX_e^kM with $v(ka)\geq 0$. Use $\binom{k}{n}=\frac{k}{n}\binom{k-1}{n-1}$ and $v(p^n/n)\geq 1$.

18.2.8: For $\lg^*$, use Problems 18.1.4 and 18.2.7, and that $\lg'$ is integral.

18.2.9: Compare each exponent with its denominator.

18.2.10: 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 $d_FQ_{c,\sigma c}$. The series $(d_FQ)^\phi$ 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 18.2.9, and use Problems 18.2.4, 18.2.7, 18.2.8 and $\lg^*(Y^p)=\lg(Y)-Y$.

§18.3.

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

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

§18.4.

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

18.4.2: $[p]$ is the p-fold sum for F. Problems 18.3.2 and 18.3.3.

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

18.4.4: Only the terms of $A(y,x)$ with $i=0$ have degree less than p in y. Then use the uniqueness of base-p digits.

References

[Adr] J. Adriazola, *The Alpöge proof of the Riemann hypothesis*, manuscript, revised 24 November 2026, `https://github.com/jimjamzola/RH-Alpoge-Reconstruction`.

[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.

[Lean] The Lean community, *riemann-hypothesis*, a Lean formalization of Alpöge's argument, `https://github.com/leanprover-community/riemann-hypothesis`.