COMMUTATIVE FORMAL GROUPS – EXERCISES

Notation: R is usually a commutative ring with 1; k is usually a field; p is usually a prime number; q is usually a power of p; $F(X,Y)$ is usually a commutative 1-dim formal group law;

(1) Let R be a reduced commutative ring (no nonzero nilpotent elements). Classify all 1-dimensional commutative formal group laws over R which are polynomials.
(2) Give an example of a 1-dim polynomial group law over $\mathbb{Z}[\epsilon]/\epsilon^2$ which is not $\widehat{\mathbb{G}}_a$ or $\widehat{\mathbb{G}}_m$.
(3) Show that formal group laws over R have formal inverses; i.e., there exists a unique $i(X) \in R[[X]]$ such that $F(X, i(X)) = 0$.
(4) Show that over a field k of char $p > 0$, $\widehat{\mathbb{G}}_a$ is not isomorphic to $\widehat{\mathbb{G}}_m$.
(5) Let F be a formal group over R. If an integer n is invertible in R, show that the multiplication by n map $[n] : F \to F$ is an isomorphism. Therefore, F is naturally a $\mathbb{Z}_S$-module, where S is the multiplicative subset of $\mathbb{Z}$ consisting of invertible numbers in R.
(6) Prove the $\mathbb{Q}$-theorem by finding an explicit isomorphism $\phi : \widehat{\mathbb{G}}_a \to F$ inductively degree by degree.
(7) (Noncommutative 1-dim formal groups). Let $D = k[\epsilon]/\epsilon^2$ where k is a field of char $p > 0$. Show that $F(X,Y) = X + Y + \epsilon XY^p$ is a noncommutative formal group.
(8) Let $B_n(x,y) = (x+y)^n - x^n - y^n$ (n is a natural number). Find the gcd d_n of the coefficients of $B_n(x,y)$.
(9) Suppose $\phi : F \to G$ is a homomorphism with leading term $cX^n, n > 1, c \in R - \{0\}$. Show that n is a power of some prime p and c is p-torsion.
(10) Describe the rings $\mathrm{End}_R(\mathbb{G}_a)$ and $\mathrm{End}_R(\widehat{\mathbb{G}}_a)$.
(11) Let F be a formal group law over $\mathbb{Z}_p$. Then its logarithm $\log_F(X) \in \mathbb{Q}_p[[X]]$ can be computed by $\log_F(X) = \lim_{n\to\infty} p^{-n}[p^n](X)$.
(12) Let E be the elliptic curve $y^2 = x^3 + ax + b$, $a, b \in R$. The identity of E is at ∞. Using the local coordinate $u = x/y$ at ∞, write down the first few terms of the logarithm of the formal group $\hat{E}$. Hint: first find an invariant differential on E.
(13) Let $C_n(x,y) = \frac{1}{d_n} B_n(x,y) \in \mathbb{Z}[X,Y]_{\deg=n}$. Suppose F_1 and F_2 are n-buds over R extending the same $(n-1)$-bud F, show that $F_1(x,y) - F_2(x,y)$ is an R-multiple of $C_n(x,y)$.
(14) Let $F_{\le 2}(X,Y) = X + Y + c_2XY$ be the universal 2-bud over $\mathbb{L}_{\le 2} = \mathbb{Z}[c_2]$, find an explicit 3-bud $f_{\le 3}(X,Y)$ (again over $\mathbb{L}_{\le 2}$) extending $F_{\le 2}$. Now $F_{\le 3}(X,Y) = f_{\le 3}(X,Y) + c_3(X^2Y + XY^2)$ is a universal 3-bud over $\mathbb{L}_{\le 3} = \mathbb{Z}[c_2, c_3]$, find an explicit 4-bud $f_{\le 4}(X,Y)$ (again over $\mathbb{L}_{\le 3}$) extending $F_{\le 3}$. If you have trouble sleeping, do three more steps.
(15) Write down the first few terms of the logarithm of the universal formal group over the Lazard ring $\mathbb{L}$.
(16) Let S be a set of primes. Let $E_S(X) = \exp(\sum_{n \text{ only has prime divisors in } S} \frac{X^n}{n})$ be the Artin-Hasse exponential with respect to S. Show that for $p \in S$, we have $E_S(X)^p / E_S(X^p) = E_{S-\{p\}}(X)^p$.
(17) Prove Dwork's lemma: a power series $f(X) \in 1 + X\mathbb{Q}[[X]]$ has p-integral coefficients if and only if $f(X)^p/f(X^p)$ is p-integral and $\equiv 1 \mod p$.
(18) Let F and G be formal groups over a field k of char $p > 0$. If $\phi : F \to G$ is a homomorphism with vanishing linear term, then ϕ is a power series in X^p. In other words ϕ factors as $F \xrightarrow{\mathrm{Fr}_p} F^{(p)} \to G$.
(19) Let k be a field of char $p > 0$. Let $F(X,Y) = X + Y + C_{p^h}(X,Y) +$ (higher terms) be a formal group law over k. Show that the height of F is h.
(20) Let F and F' be p^i-buds over k of char p. Show that $F \equiv F' + aC_{p^i}(X,Y)$ if and only if $[p](X) \equiv [p]'(X) + aX^{p^i}$.
(21) Let p be a prime. Let R be a $\mathbb{Z}_{(p)}$-algebra and F a formal group over R with $[p](X) = 0$. Show that $F \cong \widehat{\mathbb{G}}_a$ over R.

(22) Let $q = p^h$. Let $\widetilde{F}_h$ be the formal group law with logarithm $\sum_{n\geq 0} \frac{X^{q^n}}{p^n}$. Show that $\widetilde{F}_h$ is indeed a formal group over $\mathbb{Z}$.
(23) Let F_h be the reduction of $\widetilde{F}_h$ mod p (so F_h is a formal group over $\mathbb{F}_p$). Show that F_h satisfies $[p](X) = X^q$. Therefore it has height h.
(24) Show that the monomials appearing in F_h all have total degrees $\equiv 1 \mod (q-1)$.
(25) Let $\widetilde{F}$ be a formal group over $\mathbb{Z}_p$ and F be its reduction modulo p. Show that the reduction map $\mathrm{End}_{\mathbb{Z}_p}(\widetilde{F}) \to \mathrm{End}_{\mathbb{F}_p}(F)$ is injective provided that F has finite height.
(26) For the elliptic curve $y^2 = x^3 + 1$ over $\mathbb{Z}[1/6]$, use the first few terms of the logarithm (see Exercise 12) of $\hat{E}$ to find the height of the reduction modulo $p = 5, 7, 11$.
(27) Let F_h be the formal group over $\mathbb{F}_p$ in Exercise 22. Show that $X \mapsto aX$ is an endomorphism of F_h over $\overline{\mathbb{F}}_p$ if and only if $a \in \mathbb{F}_q$ $(q = p^h)$. (Hint: use Exercise 24).
(28) Show that $E = \mathrm{End}_{\overline{\mathbb{F}}_p}(F_h)$ is p-adically separated and complete, i.e., $E \xrightarrow{\sim} \varprojlim_n E/p^nE$.
(29) Show that the endomorphisms ring $\mathrm{End}_{\mathbb{F}_p}(F_h)$ (endos over the prime field $\mathbb{F}_p$!) is a $\mathbb{Z}_p$-algebra generated by the Frobenius element Fr_p.
(30) Let k be a field of char $p > 0$ and R be a k-algebra. Let F be a formal k-module over R. Show that F is isomorphic to $\widehat{\mathbb{G}}_a$ over R *as formal k-modules*. (*Hint:* first show that F is isomorphic to $\widehat{\mathbb{G}}_a$ as a formal group using Exercise 21, then study how k could possibly act on $\widehat{\mathbb{G}}_a$ using the structure of $\mathrm{End}(\widehat{\mathbb{G}}_a)$ worked out in Exercise 10).
(31) Let R be complete with respect to the I-adic topology ($I \subset R$ is an ideal). Let F be a formal A-module over R. Let $J \subset A$ and $I \subset R$ be ideals such that the structure map $A \to R$ sends J into I. Then the A-mod structure on F uniquely extends to an $\hat{A} = \varprojlim_n A/J^n$-module structure on F (with respect to the tautological extension $\hat{A} \to R$).
(32) Let $\mathcal{O}$ the integer ring of a local non-archimedean field. Let F_π and F_ω be Lubin-Tate $\mathcal{O}$-modules (defined using uniformizers π and ω of $\mathcal{O}$) over $\mathcal{O}^{ur}$ (the completion of the integers in the maximal unramified extension of $\mathcal{O}$). Show that there exists an isomorphism $\theta : F_\pi \xrightarrow{\sim} F_\omega$ of formal $\mathcal{O}$-modules over $\mathcal{O}^{ur}$ such that $\theta^\sigma(X) = \theta([u]_{F_\pi}(X))$. Here $u \in \mathcal{O}^\times$ is defined by $\omega = u\pi$.
(33) (Weierstrass preparation theorem) Let $\mathcal{O}$ be a complete DVR, π a uniformizer of $\mathcal{O}$ and $f(X) \in \mathcal{O}[[X]]$. Show that there is a unique way to write $f(X) = \pi^n g(X)u(X)$ such that: (1) $n \in \mathbb{Z}_{\geq 0}$; (2) $g(X) \in \mathcal{O}[X]$ is a monic polynomial whose non-leading coefficients are in $\pi\mathcal{O}$; (3) $u(X)$ is a unit in $\mathcal{O}[[X]]$, i.e., the constant term of $u(X)$ is in $\mathcal{O}^\times$. (*Hint*: first determine n and the degree of $g(X)$, then solve for $g(X)$ and $u(X)$ mod π, mod π^2, etc.)
(34) Solving π^n-torsion points of a Lubin-Tate $\mathcal{O}$-module $F_{\pi,f}$ for a general $f \in \mathcal{O}[[X]]$ satisfying $f(X) \equiv \pi X (\mod \deg 2)$ and $f(X) \equiv X^q (\mod \pi)$. Using the Weierstrass preparation theorem (see Exercise 33) to show that $[\pi^n](X) = 0$ can be solved in a separable closure of K. [*Note*: for different choices of f, we get different solutions for the π^n-torsion points, but the field extension of K they generate is independent of f.]
(35) (Formal inverse function theorem.) A morphism $\Phi : \hat{\mathbb{A}}^n \to \hat{\mathbb{A}}^n$ is given by n-tuple of formal power series $(X_1, \cdots, X_n) \mapsto (\Phi_1(X_1, \cdots, X_n), \cdots, \Phi_n(X_1, \cdots, X_n))$ where $\Phi_i(X_1, \cdots, X_n) \in R[[X_1, \cdots, X_n]]$ has no constant term. The linear coefficients of $\Phi_1, \cdots, \Phi_n$ form a matrix $J(\Phi) \in M_n(R)$, called the Jacobian of Φ. Show that Φ is invertible if and only if $\det(J(\Phi)) \in R^\times$ (i.e., $J(\Phi)$ is invertible).
(36) Prove an n-dimensional version of the $\mathbb{Q}$-theorem by finding a basis of invariant differentials.
(37) (Curvilinear formal group laws.) An n-dimensional formal group law $F_i(X_1, \cdots, X_n; Y_1, \cdots, Y_n)$ is *curvilinear* if $(X_1, 0, \cdots, 0) +_F (0, X_2, 0, \cdots) +_F + \cdots +_F (0, \cdots, 0, X_n) = (X_1, \cdots, X_n)$. Show that F is curvilinear if and only if $X^\lambda Y^\mu$ doesn't appear in any F_i, for all multi-indices λ and μ with disjoint support (nonzero positions).
(38) Show that every formal group law is strictly isomorphic to a curvilinear one.
(39) In the Cartier ring, write $\langle a \rangle + \langle b \rangle$ as $\langle c_1 \rangle + \mathbf{V}_2 \langle c_2 \rangle \mathbf{F}_2 + \cdots$. Express c_1, c_2, c_3, c_4 as polynomials of a and b.

(40) Let $\mathfrak{C}(F)$ be the group of curves on a formal group F. Define a filtration on $\mathfrak{C}(F)$ by $V^{\geq k}\mathfrak{C}(F) = \{\gamma(X) \equiv 0 \mod \deg k\}$. Show that $\mathfrak{C}(F)$ is separated and complete with respect to this filtration, i.e., $\mathfrak{C}(F) \xrightarrow{\sim} \varprojlim_k \mathfrak{C}(F)/V^{\geq k}\mathfrak{C}(F)$.

(41) Show that $\mathfrak{C}(F)/V^{\geq 2}\mathfrak{C}(F) \cong F(R\epsilon)$. Here $R\epsilon$ is the nilpotent R-algebra freely generated by ϵ with $\epsilon^2 = 0$.

(42) Define a filtration by right ideals $V^{\geq k}\mathrm{End}(\mathfrak{C}) = \{\phi | \phi(F)(\mathfrak{C}(F)) \subset V^{\geq k}\mathfrak{C}(F)\}$. Show that $\mathrm{End}(\mathfrak{C})$ is separated and complete with respect to this filtration, i.e., $\mathrm{End}(\mathfrak{C}) \xrightarrow{\sim} \varprojlim_k \mathrm{End}(\mathfrak{C})/V^{\geq k}\mathrm{End}(\mathfrak{C})$.

(43) Check using definition and relations in $\mathrm{Cart}(R)$ that $W(R)$ is a commutative ring.

(44) Check the right actions of $\mathbf{V}_m, \langle c \rangle$ and $\mathbf{F}_m$ on $\underrightarrow{W}$ indeed give a right action of $\mathrm{Cart}(R)$ on $\underrightarrow{W}$. From this, deduce a formula for the $\underleftarrow{W}$ action on $\underrightarrow{W}$.

(45) Show that every element in $\underrightarrow{W}(R\epsilon)$ can be written uniquely as a finite sum $\sum_n (1-\epsilon t) \cdot \langle a_n \rangle \mathbf{F}_n$ (for $a_n \in R$) using the right action of $\mathrm{Cart}(R)$ on $\underrightarrow{W}$. Show that $\underrightarrow{W}(R\epsilon)$ is isomorphic to the quotient right-$\mathrm{Cart}(R)$-module $V^{\geq 2}\mathrm{Cart}(R) \backslash \mathrm{Cart}(R)$.

(46) Let $1 + \sum_{i \geq 1} a_i t^i, 1 + \sum_{i\geq 1} b_i t^i \in \underleftarrow{W}(R)$ be two elements, compute the first few coefficients of their product (in the ring structure of $\underleftarrow{W}(R)$) expressed in power series.

(47) Check that the $\mathbf{V}_n, \langle c \rangle$ and $\mathbf{F}_n$ actions on the ghosts $(\Phi_1, \Phi_2, \cdots)$ are as described in the class.

(48) Show that $\exp(-t) = \prod_{n\geq 1}(1-t^n)^{\mu(n)/n}$ where μ is the Möbius function.

(49) Show that the Artin-Hasse $E_p(-t) = \exp(-t - \frac{t^p}{p} - \cdots) = \prod_{(m,p)=1}(1-t^m)^{\mu(m)/m}$.

(50) Suppose F is a formal group over R, R is a ring of char p. Then $\mathbf{V}_p\mathbf{F}_p = p \in \mathrm{Cart}(R)$.

(51) Show that a curve $\gamma \in \mathfrak{C}(F)$ is p-typical if and only if $\mathbb{F}_\ell \gamma = 0$ for all primes $\ell \neq p$.

(52) Suppose R is torsion free and a formal group F over R is defined using a logarithm $\ell_F(X) \in \mathrm{Frac}(R)[[X]]$. Show that a curve $\gamma(X)$ into F is p-typical if and only if all monomials appearing in $\ell_F(\gamma(X))$ have p-power degrees.

(53) Figure out how $\mathbf{F}$ and $\langle c \rangle$ and $\mathbf{V}$ act on the p-adic phantom components.

(54) Check that the right $\mathbf{V}$-action on $W_p(R)$ (which we also denote by σ) is the same as conjugation by $\mathbf{F}$ in $\mathrm{Cart}_p(R)$: $\sigma(x)\mathbf{F} = \mathbf{F}x$ for all $x \in W_p(R)$. Deduce from this that it is a ring endomorphism of $W_p(R)$.

(55) Show that for $x, y \in W_p(R)$ where R is a $\mathbb{Z}_{(p)}$-algebra, we have $x \cdot \tau(y) = \tau(\sigma(x) \cdot y)$. Here $x \cdot y$ denotes the ring multiplication in $W_p(R)$.

(56) If k is a perfect field of char p, is $\mathrm{Cart}_p(k)$ a noetherian ring? If R is a noetherian $\mathbb{Z}_{(p)}$-algebra, is $\mathrm{Cart}_p(R)$ noetherian?

(57) Show that any finite free R-group of order 2 is of the form $G_{a,b} = \mathrm{Spec} R[X]/(X^2 + aX)$ with comultiplication $\Delta(X) = X \otimes 1 + 1 \otimes X - bX \otimes X$, and $a, b \in R, ab = 2$. Moreover, $G_{a,b} \cong G_{a',b'}$ if and only if there is a unit $u \in R^\times$ such that $a' = au, b' = bu^{-1}$.

(58) Show that the Cartier dual of $G_{a,b}$ is $G_{b,a}$.

(59) Let $A \subset B$ be an inclusion of finite dimensional commutative and cocommutative Hopf algebras over a field k. Show that B is a free A-module.

(60) Let k be a field of char $p > 0$. Let k'/k be a degree p inseparable extension by adjoining p-th root of $u \in k$. Let $G_i = \mathrm{Spec} k[x]/(x^p - u^i)$ for $i = 0, \cdots, p-1$. Construct a group scheme structure on $G = \sqcup_{i=0}^{p-1} G_i$ such that G such that $G^0 = G_0 = \mu_p$ and that the connected-étale exact sequence $1 \to G_0 \to G \to \mathbb{Z}/p\mathbb{Z} \to 1$ does not split.

(61) Let V be a vector space over k (char p). Let $C^p(V)$ (resp. $C_p(V)$) be the invariants (resp. coinvariants) of $V^{\otimes p}$ under the action of cyclic permutation of length p. Show that the natural map $C^p(V) \to C_p(V)$ factors as $C^p(V) \twoheadrightarrow V^{(p)} \hookrightarrow C_p(V)$.

(62) Let G be a finite group scheme over k and $G^\vee$ its Cartier dual. Show that F_G is the adjoint of $V_{G^\vee}$ and V_G is the adjoint of $F_{G^\vee}$.

(63) Consider the composition $G^{(p)} \xrightarrow{V_G} G \xrightarrow{F_G} G^{(p)}$. Show that this composition is also multiplication by p on $G^{(p)}$. Can you see this explicitly from the Hopf algebra?

(64) Show that the contravariant Dieudonné functor intertwines F_G (resp. V_G) with the operator $\mathbf{F}$ (resp. $\mathbf{V}$) on $M(G)$.
(65) Let M be the contravariant Dieudonné module of a p-divisible group G over a perfect field k of char p. Show that there canonical k-linear isomorphisms $(\mathrm{Lie}G)^* \cong M/\mathbf{F}M^{(p)}$ (which respects $\mathbf{V}$) and $\mathrm{Lie}G^* \cong M^{(p)}/\mathbf{V}M$ (which respects $\mathbf{F}$).
(66) Using Dieudonné theory, show that there exists one-dimensional height two p-divisible groups over $\mathbb{F}_q$ which are not isogenous to the p-divisible groups of any (supersingular) elliptic curve over $\mathbb{F}_q$.
(67) Let (M,ϕ) be an isocrystal over $W(\mathbb{F}_q)$ where $q = p^r$. Let $\{x_1, \cdots, x_n\}$ be the multi-set of eigenvalues of ϕ^r (which is a linear operator on M). Show that the slopes of (M,ϕ) are given by the multi-set $\{\lambda_1, \cdots, \lambda_n\}$ where $\lambda_i = \frac{1}{r}\mathrm{val}_p(x_i)$.
(68) Show that the isocrystal $M_\lambda \in \mathrm{Isocry}(k)$ is simple (k algebraically closed, $\lambda \in \mathbb{Q}$).
(69) Consider isocrystals over k algebraically closed. How is the tensor product $M_\lambda \otimes M_\mu$ decomposed into simple objects?
(70) Let M a finitely generated $W(k)$-module and $\phi : M \to M$ be a σ-linear map. Show that M is a direct sum of $W(k)$-submodules $M_1 \oplus M_2$, both stable under ϕ and ϕ acts bijectively on M_1 and topologically nilpotently on M_2. Such a decomposition is unique.
(71) Let k be a perfect field of char p. Classify p-divisible groups over k with height two and dimension one.