Exercises

1 Preliminaries

1.1 Finite flat group schemes in coordinates

All group schemes in these notes are commutative. Let R be a ring. The examples to keep in mind are a perfect field k of characteristic p, the dual numbers $k[\epsilon]/(\epsilon^2)$, the rings $W(k)/p^m$ and $W(k)$, and a field of characteristic 0.

A *finite flat group scheme over* R is an affine scheme $G = \operatorname{Spec} A$, where A is a finite locally free R-module, together with multiplication

$$m : G \times_R G \longrightarrow G,$$

an identity section $e : \operatorname{Spec} R \to G$, and an inverse $i : G \to G$, satisfying the usual group laws. If A has constant rank h, we call h the *order* of G. For every R-algebra S, these maps make

$$G(S) = \operatorname{Hom}_{R\text{-alg}}(A, S)$$

into an abelian group. Working with arbitrary S, rather than only fields, allows nilpotent elements to be detected.

Exercises

1. Show that m, e, i, with their arrows reversed, give R-algebra maps

$$\Delta : A \longrightarrow A \otimes_R A, \qquad \varepsilon : A \longrightarrow R, \qquad \iota : A \longrightarrow A.$$

   Translate associativity, the identity law, and the inverse law into equations involving Δ, ε, and ι. These equations define a Hopf algebra.

2. Given $f, g \in G(S) = \operatorname{Hom}_{R\text{-alg}}(A, S)$, express fg, the identity element, and f^{-1} in terms of Δ, ε, and ι. Check the group laws using the equations in the preceding exercise.

1.2 The additive and multiplicative groups

Two group schemes which are not finite, but which contain many of our basic examples, are

$$\mathbb{G}_{a,R} = \operatorname{Spec} R[x] \qquad \text{and} \qquad \mathbb{G}_{m,R} = \operatorname{Spec} R[t, t^{-1}].$$

The multiplication, identity, and inverse maps on $\mathbb{G}_{a,R}$ are defined, on coordinate rings, by

$$\begin{aligned} \Delta_a &: R[x] \longrightarrow R[x] \otimes_R R[x], & x &\longmapsto x \otimes 1 + 1 \otimes x, \\ \varepsilon_a &: R[x] \longrightarrow R, & x &\longmapsto 0, \\ \iota_a &: R[x] \longrightarrow R[x], & x &\longmapsto -x. \end{aligned}$$

The multiplication, identity, and inverse maps on $\mathbb{G}_{m,R}$ are defined, on coordinate rings, by

$$\begin{aligned} \Delta_m &: R[t,t^{-1}] \longrightarrow R[t,t^{-1}] \otimes_R R[t,t^{-1}], & t &\longmapsto t \otimes t, \\ \varepsilon_m &: R[t,t^{-1}] \longrightarrow R, & t &\longmapsto 1, \\ \iota_m &: R[t,t^{-1}] \longrightarrow R[t,t^{-1}], & t &\longmapsto t^{-1}. \end{aligned}$$

Exercises

1. Verify directly that these formulas satisfy the Hopf-algebra identities.
2. For an R-algebra S, show that

$$\mathbb{G}_{a,R}(S) = S \qquad \text{and} \qquad \mathbb{G}_{m,R}(S) = S^\times.$$

Use the displayed Hopf-algebra maps to compute the group laws, identity elements, and inverses induced on these sets.

1.3 Basic finite group schemes

Let C be a finite abelian group. The constant group scheme C_R is the disjoint union of one copy of $\operatorname{Spec} R$ for each $c \in C$; thus

$$\mathcal{O}(C_R) = \prod_{c \in C} R.$$

For an R-algebra S, its S-points are the locally constant maps $\operatorname{Spec} S \to C$. If $\operatorname{Spec} S$ is connected, this is just C.

For every positive integer n, set

$$\mu_{n,R} = \operatorname{Spec} R[t]/(t^n - 1), \qquad \mu_{n,R}(S) = \{u \in S^\times : u^n = 1\}.$$

If R is an $\mathbb{F}_p$-algebra, also set

$$\alpha_{p,R} = \operatorname{Spec} R[x]/(x^p), \qquad \alpha_{p,R}(S) = \{s \in S : s^p = 0\},$$

with addition as the group law.

These presentations exhibit $\mu_{n,R}$ as the closed subgroup $\ker([n] : \mathbb{G}_{m,R} \to \mathbb{G}_{m,R}) \subset \mathbb{G}_{m,R}$ and, when R is an $\mathbb{F}_p$-algebra, $\alpha_{p,R}$ as the closed subgroup $\ker(F : \mathbb{G}_{a,R} \to \mathbb{G}_{a,R}) \subset \mathbb{G}_{a,R}$, where F is given on coordinate rings by $x \mapsto x^p$.

Exercises

1. For C_R, describe multiplication, identity, and inverse on the components indexed by C. If $e_c \in \prod_{c \in C} R$ is the characteristic function of c, calculate $\Delta(e_c), \varepsilon(e_c)$, and $\iota(e_c)$.
2. Starting with multiplication of units, calculate multiplication, identity, and inverse on $\mu_{n,R}(S)$. Translate these into formulas for $\Delta(t), \varepsilon(t)$, and $\iota(t)$ on $R[t]/(t^n - 1)$, and verify the Hopf-algebra identities.
3. Do the same calculation for $\alpha_{p,R}$, beginning with addition in S. Where is the assumption that R is an $\mathbb{F}_p$-algebra used?
4. Show that C_R, $\mu_{n,R}$, and $\alpha_{p,R}$ (when defined) are finite locally free, and calculate their orders. Show that this order is unchanged by base change.
5. Let k be an algebraically closed field of characteristic p. Show that $(\mathbb{Z}/p\mathbb{Z})_k$, $\mu_{p,k}$, and $\alpha_{p,k}$ are pairwise non-isomorphic. Compare their k-points, connected components, and coordinate rings.

1.4 Group schemes in characteristic zero

Exercises

1. Let K be a field of characteristic 0. Prove that every group scheme locally of finite type over K is reduced. For the purposes of these notes, it is enough to prove this when the group scheme is finite over K.

2. Let $G = \operatorname{Spec} A$ be a finite flat group scheme over K. Deduce from the preceding exercise that A is a finite product of finite separable field extensions of K, and hence that G is finite étale over K.

3. If K is algebraically closed, conclude that G is non-canonically isomorphic to the constant group scheme associated with a finite abelian group.

1.5 Cartier duality

Let $G = \operatorname{Spec} A$ be finite flat and commutative over R. Since A is finite locally free, its R-linear dual $A^* = \operatorname{Hom}_R(A, R)$ is finite locally free. Dualizing the multiplication and comultiplication of A makes A^* into a Hopf algebra. The resulting group scheme

$$G^\vee = \operatorname{Spec} A^*$$

is the *Cartier dual* of G.

Exercises

1. Write out all the structure maps on A^*. Check that $(G^\vee)^\vee \cong G$ and that Cartier duality commutes with base change $R \to R'$.

2. Calculate $(\mathbb{Z}/n\mathbb{Z})^\vee_R$ directly and show that it is $\mu_{n,R}$. Conclude that $\mu^\vee_{n,R} \cong (\mathbb{Z}/n\mathbb{Z})_R$ over every base ring R.

3. If R is an $\mathbb{F}_p$-algebra, show directly from the Hopf algebra that $\alpha^\vee_{p,R} \cong \alpha_{p,R}$.

2 The Moret–Bailly family

Moret–Bailly constructs a non-constant family of supersingular abelian surfaces over $\mathbb{P}^1_{/\mathbb{F}_p}$. The following exercises develop the group-scheme calculations used in his construction. Fix a supersingular elliptic curve E_{ss} over $\overline{\mathbb{F}}_p$.

Recall the group schemes α_p and μ_p from §1.3.

Exercises

1. Calculate $\operatorname{End}(\alpha_p)$, $\operatorname{Aut}(\alpha_p)$.

2. Calculate $\operatorname{Hom}(\alpha_p, \alpha_p \times \alpha_p)$.

3. Prove that two homomorphisms $f, g \in \operatorname{Hom}(\alpha_p, \alpha_p \times \alpha_p)$ have the same image if and only if there exists an element $\lambda \in \mathbb{G}_m$ such that $\lambda f = g$.

4. Take as a black-box the fact that $\alpha_p \subset E_{ss}[p]$. Finish Moret–Bailly's construction.

5. Do the first two steps with α_p replaced by μ_p.

6. Deduce that there is an abelian surface over a positive-dimensional base which has CM.

3 Dieudonné theory

3.1 p-divisible groups

A *p-divisible group of height h over R* is a system

$$G_1 \hookrightarrow G_2 \hookrightarrow G_3 \hookrightarrow \cdots$$

of finite flat commutative group schemes over R such that G_n has order p^{nh} and G_n is the kernel of multiplication by p^n on G_{n+1}. Equivalently, multiplication by p gives a faithfully flat map $G_{n+1} \to G_n$ with kernel G_1. We write $G[p^n] = G_n$.

The two basic examples, both of height 1, are

$$\mathbb{Q}_p/\mathbb{Z}_p = (\mathbb{Z}/p^n\mathbb{Z})_{n\geq 1}, \qquad \mu_{p^\infty} = (\mu_{p^n})_{n\geq 1}.$$

The transition map $\mathbb{Z}/p^n\mathbb{Z} \hookrightarrow \mathbb{Z}/p^{n+1}\mathbb{Z}$ sends a to pa, and the transition map for the second system is the natural closed immersion $\mu_{p^n} \hookrightarrow \mu_{p^{n+1}}$. We use the same notation after base change to any ring R. A homomorphism of p-divisible groups is a compatible collection of homomorphisms at every finite level.

Exercises

1. Write both transition maps on coordinate rings. Check that multiplication by p maps level $n+1$ onto level n, with kernel respectively $\mathbb{Z}/p\mathbb{Z}$ and μ_p.

2. Show that Cartier duality exchanges $\mathbb{Q}_p/\mathbb{Z}_p$ and μ_{p^∞} level by level.

3. Suppose $\operatorname{Spec} R$ is connected. Calculate the endomorphisms of $(\mathbb{Z}/p^n\mathbb{Z})_R$ and of $\mu_{p^n,R}$. Then impose compatibility at all finite levels and prove

$$\operatorname{End}_R((\mathbb{Q}_p/\mathbb{Z}_p)_R) \cong \mathbb{Z}_p, \qquad \operatorname{End}_R(\mu_{p^\infty,R}) \cong \mathbb{Z}_p.$$

   Explain why the answer is unchanged when R is k, $k[\epsilon]/(\epsilon^2)$, $W(k)/p^m$, or $W(k)$.

3.2 Dieudonné modules

Let k be a perfect field of characteristic p, and put $W = W(k)$. Let $\sigma : W \to W$ be the Witt-vector Frobenius.

A *Dieudonné module* is a finitely generated W-module D equipped with a σ-linear endomorphism F and a σ^{-1}-linear endomorphism V satisfying

$$FV = VF = p.$$

A homomorphism of Dieudonné modules is a W-linear map commuting with F and V.

The basic examples are

G	$D(G)$	F	V
$\frac{1}{p^n}\mathbb{Z}/\mathbb{Z}$	W/p^n	σ	$p\sigma^{-1}$
μ_{p^n}	W/p^n	$p\sigma$	σ^{-1}
α_p	W/pW	0	0.

At infinite level, set

$$D(\mathbb{Q}_p/\mathbb{Z}_p) = \varprojlim_n D(\tfrac{1}{p^n}\mathbb{Z}/\mathbb{Z}), \qquad D(\mu_{p^\infty}) = \varprojlim_n D(\mu_{p^n}).$$

Theorem 3.1. *The Dieudonné functor D gives an anti-equivalence from finite flat commutative group schemes over k killed by a power of p to finite-length Dieudonné modules, and an anti-equivalence from p-divisible groups over k to Dieudonné modules which are finite free over W. In particular, it sends the group schemes displayed above to the indicated modules.*

If $f : G_1 \to G_2$ induces $D(f) : D(G_2) \to D(G_1)$, then $D(\ker f)$ is the cokernel of $D(f)$.

Assume now that k contains $\mathbb{F}_{p^2}$, and let E_s/k be a supersingular elliptic curve. We use the following description:

$$D(E_s[p^\infty]) = We \oplus Wf, \qquad F(e) = f, \quad F(f) = pe.$$

Exercises

1. Calculate (the Dieudonné modules of) all order p group schemes over $\overline{\mathbb{F}}_p$. Do this over $\mathbb{F}_q$ as well.
2. Calculate $\mathrm{Hom}(\alpha_p, E_s)$.
3. Calculate all Dieudonné sub-modules of $D(E_s[p^\infty])$. Conclude that E_s has a unique order p^n-subgroup scheme for every n. What is this subgroup scheme if n is even?
4. Calculate $\mathrm{End}(E_s[p^\infty])$.
5. Calculate $\mathrm{Hom}(\alpha_p, E_s \times E_s)$.
6. For every homomorphism as above, calculate the Dieudonné module of the (p-divisible group of the) quotient $\mathscr{G} = E_s[p^\infty] \times E_s[p^\infty]/\alpha_p$.
7. For every such quotient $\mathscr{G}$, calculate $\mathrm{Hom}(\alpha_p, \mathscr{G})$. Conclude that $\mathscr{G}$ is defined over $\mathbb{F}_{p^2}$ if and only if the number you calculated equals 2. Otherwise, this number must be 1.
8. Calculate $\mathrm{End}(\mathbb{Q}_p/\mathbb{Z}_p)$ and $\mathrm{End}(\mu_{p^\infty})$ over each connected base ring R considered in §1.1. Do this without using Dieudonné modules.
9. Deduce that, for every such R, the ring $\mathrm{End}((\mathbb{Q}_p/\mathbb{Z}_p)^a \times (\mu_{p^\infty})^b)$ is independent of R.
10. Do the calculation over k using Dieudonné modules as a consistency check.

4 The Serre–Tate theorem

Let k be a perfect field of characteristic p, let A/k be an abelian variety, and let R be a local Artinian $W(k)$-algebra with residue field k. Define $\mathrm{Def}_A(R)$ to be the category whose objects are pairs $(\widetilde{A}, \varphi)$, where $\widetilde{A}/R$ is an abelian scheme and

$$\varphi : \widetilde{A} \times_R k \xrightarrow{\sim} A$$

is an identification of its special fiber with A. Morphisms are isomorphisms of abelian schemes over R compatible with the identifications of the special fibers.

Similarly, define $\mathrm{Def}_{A[p^\infty]}(R)$ to be the category of pairs $(\widetilde{G}, \psi)$, where $\widetilde{G}/R$ is a p-divisible group and

$$\psi : \widetilde{G} \times_R k \xrightarrow{\sim} A[p^\infty].$$

Taking the associated p-divisible group defines a functor

$$\begin{aligned} \mathrm{Def}_A(R) &\longrightarrow \mathrm{Def}_{A[p^\infty]}(R), \\ (\widetilde{A}, \varphi) &\longmapsto (\widetilde{A}[p^\infty], \varphi[p^\infty]). \end{aligned}$$

Theorem 4.1 (Serre–Tate)**.** *For every such R, this functor is an equivalence of categories. In particular, deforming an abelian variety, together with its morphisms, is equivalent to deforming its p-divisible group together with its morphisms.*

For a complete Noetherian local $W(k)$-algebra R with residue field k, define both deformation categories by taking compatible systems over $R/\mathfrak{m}^n$; the same conclusion then follows by passage to the inverse limit. More generally, if $\widetilde{A}$ and $\widetilde{B}$ lift abelian varieties A and B, then homomorphisms $\widetilde{A} \to \widetilde{B}$ are in bijection with homomorphisms $\widetilde{A}[p^\infty] \to \widetilde{B}[p^\infty]$ whose reductions come from homomorphisms $A \to B$.

Exercises

1. Let $(R, \mathfrak{m})$ be a complete Noetherian local $W(k)$-algebra with residue field k. One may also take $R = \mathcal{O}_L$, where $L/W(k)[1/p]$ is a finite totally ramified extension. If A/R is an abelian scheme, show that the image of
$$\mathrm{End}_R(A) \longrightarrow \mathrm{End}_k(A \times_R k)$$
is ℓ-co-torsion free for every prime $\ell \neq p$.

2. Let $k = \overline{\mathbb{F}}_p$, put $W = W(k)$, and let A/k be a g-dimensional ordinary abelian variety. Thus
$$A[p^\infty] \cong (\mathbb{Q}_p/\mathbb{Z}_p)^g \times (\mu_{p^\infty})^g.$$
Define the *canonical lift* $\widetilde{A}/W$ of A.

3. Use the Serre–Tate theorem to show that $\mathrm{End}_W(\widetilde{A}) = \mathrm{End}_k(A)$.

4. If A and B are ordinary abelian varieties over k, show that
$$\mathrm{Hom}_k(A, B) = \mathrm{Hom}_W(\widetilde{A}, \widetilde{B}).$$

5. Let A and B be ordinary g-dimensional abelian varieties over k with no nonzero homomorphisms between them. One has $\widetilde{A}[p^\infty] \cong \widetilde{B}[p^\infty]$. Why does the Serre–Tate theorem not imply that there is a nonzero homomorphism $\widetilde{A} \to \widetilde{B}$?

6. You may assume that every simple CM abelian variety over $\mathbb{C}$ has commutative endomorphism algebra. Prove that a simple ordinary abelian variety over $\overline{\mathbb{F}}_p$ has commutative endomorphism algebra.

5 Lifting

5.1 Grothendieck–Messing theory over mildly ramified extensions

Let k be a perfect field of characteristic p and put $W = W(k)$. Let $L/W[1/p]$ be a finite extension, with ring of integers $\mathcal{O}_L$ and maximal ideal $\mathfrak{m}$. We say that L is *mildly ramified* if its ramification index satisfies $e(L) < p - 1$.

Theorem 5.1 (Grothendieck–Messing theory over $\mathcal{O}_L$)**.** *1. Let $\mathscr{G}/k$ be a p-divisible group. Its lifts to $\mathcal{O}_L$ are in bijection with co-torsion-free submodules*
$$\mathrm{Fil}_{\mathscr{G}} \subset D(\mathscr{G}) \otimes_W \mathcal{O}_L$$
whose reduction modulo $\mathfrak{m}$ is $\ker(F : D(\mathscr{G})/pD(\mathscr{G}) \to D(\mathscr{G})/pD(\mathscr{G}))$.

2. *Two filtrations* Fil *and* Fil′ *give isomorphic lifts modulo* $\mathfrak{m}^n$ *if and only if*

$$\mathrm{Fil} \bmod \mathfrak{m}^n = \mathrm{Fil}' \bmod \mathfrak{m}^n.$$

3. *Let* $f : \mathscr{G} \to \mathscr{H}$*, and let* $\widetilde{\mathscr{G}}$ *and* $\widetilde{\mathscr{H}}$ *be lifts corresponding to* $\mathrm{Fil}_{\mathscr{G}}$ *and* $\mathrm{Fil}_{\mathscr{H}}$*. Then* f *lifts to a homomorphism* $\widetilde{\mathscr{G}} \to \widetilde{\mathscr{H}}$ *if and only if*

$$D(f)(\mathrm{Fil}_{\mathscr{H}}) \subset \mathrm{Fil}_{\mathscr{G}}\,.$$

The *Deuring lifting theorem* says the following. Let E be an elliptic curve over a finite field k, and let $f \in \mathrm{End}_k(E)$. After replacing k by a finite extension k', there exist a complete discrete valuation ring R of characteristic 0 with residue field k', an elliptic curve $\widetilde{E}/R$ lifting $E_{k'}$, and an endomorphism $\widetilde{f} \in \mathrm{End}_R(\widetilde{E})$ lifting f.

Exercises

1. Let $\widetilde{\mathscr{G}}/\mathcal{O}_L$ be a lift of $\mathscr{G}/k$. Prove that the image of

$$\mathrm{End}_{\mathcal{O}_L}(\widetilde{\mathscr{G}}) \longrightarrow \mathrm{End}_k(\mathscr{G})$$

   is co-torsion free.

2. Show that $\mathbb{Q}_p/\mathbb{Z}_p$ and μ_{p^∞} each have a unique lift to $\mathcal{O}_L$.

3. Define the canonical lift of an ordinary p-divisible group using Grothendieck–Messing theory.

4. Prove the Deuring lifting theorem stated above.

5. Consider the supersingular p-divisible group over $k = \mathbb{F}_{p^2}$. Prove that every lift to $W(\mathbb{F}_{p^2})$ admits an extra endomorphism.

References