Generalised Weierstrass equations, and some elementary universal families

J. Jin

April 11, 2012

Table of contents

Version history

Thanks to everyone who pointed out mistakes to me, either in these notes, or during the lectures themselves.

11-04 Corrected some minor mistakes.
Changed title of Section 0.4.
Removed a superfluous argument in Section 1.1 saying that $(f_*\Omega_{E/S})^E = f_*\Omega_{E/S}$.
Added this version history.

05-04 Fixed the hyperlinks in the Table of contents.

27-03 Fixed arrow label positioning.

20-03 Corrected some minor mistakes.

14-03 First version.

0 Preliminaries

In sections 1, 2 and 3, we give the theory of relative differentials, first over modules over a ring (which, throughout this talk, will always be assumed to be associative, commutative and unital), and then over a morphism of schemes. These sections will follow the Stacks Project [2, Sect. 7.118] for the module of Kähler differentials, Hartshorne [1, Sect. II.8] for the module of relative differentials in the scheme-theoretic context. The Stacks Project [2, Sect. 16.29] covers the same subject, but in the more general context of sheaves of rings on a site.

In section 4, we give some of the elementary theory of group schemes needed in the second part of the talk. This section follows and expands the beginning of Chapter 3 of the upcoming book of van der Geer and Moonen [3].

1 Kähler differentials

Definition 0.1. Let A be a ring, let B be an A-algebra, and let M be a B-module. An *A-derivation* of B into M is a map $\mathrm{d}\colon B \to M$ such that the following properties hold for all $a \in A$ and all $b_1, b_2 \in B$.

(1) $\mathrm{d}(b_1 + b_2) = \mathrm{d}b_1 + \mathrm{d}b_2$,
(2) $\mathrm{d}(b_1 b_2) = b_1 \mathrm{d}b_2 + b_2 \mathrm{d}b_1$,
(3) $\mathrm{d}a = 0$.

Definition 0.2. Let A be a ring, let B be an A-algebra, and let M be a B-module. The *module of relative Kähler differentials* of B over A is, if it exists, a pair $(\Omega_{B/A}, \mathrm{d}_{B/A})$ of a B-module $\Omega_{B/A}$, together with an A-derivation $\mathrm{d}_{B/A}\colon B \to \Omega_{B/A}$ into it, that satisfies the following universal property.

For any pair (M, d) of a B-module M and an A-derivation $\mathrm{d}\colon B \to M$ into it, there exists a unique B-linear map $f\colon \Omega_{B/A} \to M$ such that $\mathrm{d} = f \circ \mathrm{d}_{B/A}$.

Example 0.3. Let A be a ring, and let $B = A[x_1, \ldots, x_n]/(f_1, \ldots, f_r)$. Then

$$\Omega_{B/A} = \bigoplus_i B\mathrm{d}x_i \Big/ \sum_j B\Big(\sum_i \tfrac{\partial f_j}{\partial x_i}\mathrm{d}x_i\Big),$$

together with the A-derivation $\mathrm{d}_{B/A} f = \sum_i \frac{\partial f}{\partial x_i}\mathrm{d}x_i$, is the module of relative Kähler differentials. (Checking that $(\Omega_{B/A}, \mathrm{d}_{B/A})$ is indeed universal is left to the reader.)

Proposition 0.4. *Let A be a ring, let B be an A-algebra. Then the module of relative Kähler differentials exists.*

Proof. We construct a pair $(\Omega_{B/A}, \mathrm{d}_{B/A})$ that satisfies the universal property given in Definition 0.2. Let F be the free B-module $B^{(B)}$, and let $\mathrm{d}\colon B \to F$ be the map $b \mapsto (\delta_{ib})_{i \in B}$. Let G be the B-submodule of F generated by, for all $a \in A$ and all $b_1, b_2 \in B$,

(1) $\mathrm{d}(b_1 + b_2) - \mathrm{d}b_1 - \mathrm{d}b_2$,

(2) $\mathrm{d}(b_1 b_2) - b_1 \mathrm{d}b_2 - b_2 \mathrm{d}b_1$,
(3) $\mathrm{d}a$.

Let $\Omega_{B/A} = F/G$, and let $\mathrm{d}_{B/A} \colon B \to \Omega_{B/A}$, $b \mapsto \mathrm{d}b + G$. Then the pair $(\Omega_{B/A}, \mathrm{d}_{B/A})$ is indeed universal. The proof of this is left to the reader. □

From this description of the module of relative Kähler differentials, we can deduce the following.

Corollary 0.5. *The B-module $\Omega_{B/A}$ is generated by elements of the form $\mathrm{d}_{B/A} b$ with $b \in B$.*

This corollary has a number of consequences.

Corollary 0.6. *If $A \to B$ is surjective, then $\Omega_{B/A} = 0$.*

Proof. This follows as $\mathrm{d}_{B/A} b = 0$ for all $b \in B$. □

Let

$$\begin{array}{ccc} B & \longrightarrow & B' \\ \uparrow & & \uparrow \\ A & \longrightarrow & A' \end{array}$$

be a commutative diagram of rings and morphisms. Then the composition of $A \to A'$ with $\mathrm{d}_{B'/A'}$ is an A-derivation. This gives a B-linear map $f \colon \Omega_{B/A} \to \Omega_{B'/A'}$ which is the unique B-linear map such that $\mathrm{d}_{B'/A'} = f \circ \mathrm{d}_{B/A}$. Hence for all $b \in B$, we have $f(\mathrm{d}_{B/A} b) = \mathrm{d}_{B'/A'} b$.

Corollary 0.7. *If $B \to B'$ is surjective, then so is the B-linear map $\Omega_{B/A} \to \Omega_{B'/A'}$.*

We now study the kernel of the B-linear map $f \colon \Omega_{B/A} \to \Omega_{B'/A'}$.

Lemma 0.8. *The B-module $\ker(\Omega_{B/A} \to \Omega_{B'/A'})$ is generated by all $\mathrm{d}_{B/A} b$ of which the image of $b \in B$ is in the image of A' (in the ring B').*

Proof. Let F, G, and F', G' be as in the proof of Proposition 0.4, for B/A and B'/A', respectively. Then the B-linear map $\Omega_{B/A} \to \Omega_{B'/A'}$ comes from the B-linear map $F \to F'$, $\mathrm{d}b \to \mathrm{d}'b$. Let $I = \ker(B \to B')$. Then the inverse image of G' under this map is generated by G, the elements $\mathrm{d}b$ such that the image of $b \in B$ is in the image of A', and the elements $i\mathrm{d}b$ with $i \in I$ and $b \in B$. But note that $i, bi \in I$, so their images in B' are 0, which is also in the image of A'. Hence $i\mathrm{d}b \in \mathrm{d}(bi) - b\mathrm{d}i + G$, so the inverse image of G' is generated by G and the elements $\mathrm{d}b$ such that the image of $b \in B$ is in the image of A'. The result follows. □

The following propositions are useful later on for considering the module of differentials over schemes.

Proposition 0.9. *Let $\{A_i \to B_i\}$ be a directed system of ring maps, and let $A = \operatorname{colim}_i A_i$, $B = \operatorname{colim}_i B_i$. Then the pair $(\operatorname{colim}_i \Omega_{B_i/A_i}, \operatorname{colim}_i \mathrm{d}_{B_i/A_i})$ is the module of relative Kähler differentials of B over A.*

Proof. First note that $\mathrm{d} = \operatorname{colim}_i \mathrm{d}_{B_i/A_i}$ is itself an A-derivation, as every d_{B_i/A_i} is a derivation; as we have a directed system, any pair of elements of B comes from a pair of elements of some B_i, and any element of A comes from an element of some A_i.

Now let M be a B-module, and let $\mathrm{d}' \colon B \to M$ be an A-derivation. Then, for all i, we get an A_i-derivation $\mathrm{d}'_i \colon B_i \to M$, and hence a unique B_i-module map $f_i \colon \Omega_{B_i/A_i} \to M$ such that $\mathrm{d}'_i = f_i \circ \mathrm{d}_{B_i/A_i}$. The f_i are compatible with the system of ring maps, by the universal property of the module of relative Kähler differentials. This gives a unique B-linear map $f \colon \operatorname{colim}_i \Omega_{B_i/A_i} \to M$ such that $\mathrm{d}' = f \circ \mathrm{d}_{B/A}$. □

Proposition 0.10. *Let A be a ring, and let B and A' be A-algebras. Let B' denote the B-algebra $B \otimes_A A'$. Then $\Omega_{B'/A'} \cong \Omega_{B/A} \otimes_A A'$.*

Proof. Note that the map $B \times A' \to \Omega_{B/A} \otimes_A A'$, $(b, a) \mapsto \mathrm{d}_{B/A} b \otimes a$ is A-bilinear, so this gives a morphism $\mathrm{d}\colon B' = B \otimes_A A' \to \Omega_{B/A} \otimes_A A'$ of abelian groups. As $\mathrm{d}_{B/A}$ is an A-derivation, it follows that d is an A'-derivation as well.

We now show that the pair $(\Omega_{B/A} \otimes_A A', \mathrm{d})$ is universal. Let M' be a B'-module, and let $\mathrm{d}'\colon B' \to M'$ be an A'-derivation. Then the composition $B \to B' \to M'$ gives an A-derivation on M', viewed as a B-module, hence a B-linear map $f\colon \Omega_{B/A} \to M'$. Note that the map $\Omega_{B/A} \times A' \to M'$, $(b, a) \mapsto af(b)$ is A-bilinear, so this gives a map $f'\colon \Omega_{B/A} \otimes_A A' \to M'$. Since on pure tensors $b \otimes a \in B' = B \otimes_A A'$, we have $f' \circ \mathrm{d}(b \otimes a) = af(\mathrm{d}_{B/A} b) = a\mathrm{d}'(b \otimes 1) = \mathrm{d}'(b \otimes a)$, it follows that $\mathrm{d}' = f \circ \mathrm{d}$. Moreover, f' is the unique B'-linear map such that $\mathrm{d}' = f' \circ \mathrm{d}$, as $\Omega_{B/A} \times A'$ is generated by elements of the form $\mathrm{d}_{B/A} b \otimes a$ with $b \in B$ and $a \in A'$. The result follows. □

Corollary 0.11. *Let A be a ring, and let B and A' be A-algebras. Let B' denote the B-algebra $B \otimes_A A'$. Then $\Omega_{B'/A'} \cong \Omega_{B/A} \otimes_B B'$.*

Proposition 0.12. *Let A be a ring, and let B be an A-algebra. Let S be a multiplicative system in A mapping into the unit group of B. Then $\Omega_{B/S^{-1}A} = \Omega_{B/A}$.*

Proof. Since there is a natural map $A \to S^{-1}A$, we deduce that every $S^{-1}A$-derivation of B also is an A-derivation of B. Conversely, if M is a B-module, and $\mathrm{d}\colon B \to M$ is an A-derivation, then for all $s \in S$, we have $0 = \mathrm{d}1 = s\mathrm{d}(1/s) + (1/s)\mathrm{d}s = s\mathrm{d}(1/s)$. As s is invertible in B, it follows that $\mathrm{d}(1/s) = 0$, and hence, by the Leibniz rule, that d is an $S^{-1}A$-derivation of B. □

Proposition 0.13. *Let A be a ring, and let B be an A-algebra. Let S be a multiplicative system in B, then $\Omega_{S^{-1}B/A} = S^{-1}\Omega_{B/A}$.*

Proof. Let $\mathrm{d}\colon S^{-1}B \to S^{-1}\Omega_{B/A}$, $b/s \mapsto \mathrm{d}_{B/A} b/s - b\mathrm{d}_{B/A} s/s^2$. Then d is an A-derivation, so there exists a unique $S^{-1}B$-linear map $f\colon \Omega_{S^{-1}B/A} \to S^{-1}\Omega_{B/A}$ such that $\mathrm{d} = f \circ \mathrm{d}_{S^{-1}B/A}$. This $S^{-1}B$-linear map sends $\mathrm{d}_{S^{-1}B/A} b$ to $\mathrm{d}_{B/A} b$ for all $b \in B$.

On the other hand, the sequence $A \to B \to S^{-1}B$ of rings induces a B-linear map $g\colon \Omega_{B/A} \to \Omega_{S^{-1}B/A}$, which sends $\mathrm{d}_{B/A} b$ to $\mathrm{d}_{S^{-1}B/A} b$ for all $b \in B$. Hence the map $\Omega_{B/A} \times S^{-1}B \to \Omega_{S^{-1}B/A}$, $(x, b) \mapsto bg(x)$ is B-bilinear, so it induces a map $f'\colon S^{-1}\Omega_{B/A} = \Omega_{B/A} \otimes_B S^{-1}B \to \Omega_{S^{-1}B/A}$ of abelian groups. This map is $S^{-1}B$-linear, and it sends $\mathrm{d}_{B/A} b$ to $\mathrm{d}_{S^{-1}B/A} b$ for all $b \in B$.

As $\mathrm{d}_{S^{-1}B/A}(b/s)$ is in the $S^{-1}B$-submodule of $\Omega_{S^{-1}B/A}$ generated by $\mathrm{d}_{S^{-1}B/A} b$ and $\mathrm{d}_{S^{-1}B/A} s$ for all $b \in B$ and $s \in S$, by the Leibniz rule, it follows that f and f' are inverses, and hence the result follows. □

Now let $A \to B \to C$ be a sequence of rings. Note that $\mathrm{d}_{C/B}$ is a B-derivation, so in particular, it is an A-derivation. Hence there is a unique C-linear map $g\colon \Omega_{C/A} \to \Omega_{C/B}$ such that $\mathrm{d}_{C/B} = g \circ \mathrm{d}_{C/A}$. Also note that $\mathrm{d}_{C/A}$ is an A-derivation, and that $\Omega_{C/A}$ has a natural B-module structure. Hence there is a unique B-linear map $f'\colon \Omega_{B/A} \to \Omega_{C/A}$ such that $\mathrm{d}_{C/A} = f' \circ \mathrm{d}_{B/A}$. Now the map $\Omega_{B/A} \times C \to \Omega_{C/A}$, $(b, c) \mapsto cf'(b)$ is B-bilinear, so we obtain a morphism $f\colon \Omega_{B/A} \otimes_B C \to \Omega_{C/A}$ of abelian groups. This morphism is C-linear.

Proposition 0.14 (First Exact Sequence). *The sequence of C-modules*

$$\Omega_{B/A} \otimes_B C \to \Omega_{C/A} \to \Omega_{C/B} \to 0$$

is exact.

Proof. First note that g is surjective, as $\mathrm{d}_{C/A} = g \circ \mathrm{d}_{C/B}$, and $\Omega_{C/B}$ is generated by the elements of the form $\mathrm{d}_{C/B}c$ with $c \in C$.

Also note that $g \circ f = 0$, as $\Omega_{B/A} \otimes_B C$ is generated as a C-module by the elements of the form $\mathrm{d}_{B/A}b \otimes 1$ with $b \in B$, and $g \circ f$ vanishes for those elements.

It follows from Lemma 0.8 that $\ker g$ is generated by elements of the form $\mathrm{d}_{C/A}b$ with $b \in B$. As $\mathrm{d}_{B/A}b \otimes 1 \mapsto \mathrm{d}_{C/A}b$ under f, it follows that $\operatorname{im} f = \ker g$.

We conclude that the given sequence is exact. □

Let A be a ring, let B be an A-algebra, and let I be an ideal of B. Let $C = B/I$. View I/I^2 as a C-module. Consider the morphism $B \to \Omega_{B/A} \otimes_B C$, $b \mapsto \mathrm{d}_{B/A}b \otimes 1$ of abelian groups. This morphism induces a well-defined morphism $\delta \colon I/I^2 \to \Omega_{B/A} \otimes_B C$, as for all $i_1, i_2 \in I$, we have $\delta(i_1 i_2) = \mathrm{d}_{B/A}(i_1 i_2) \otimes 1 = \mathrm{d}_{B/A}i_1 \otimes (i_2 + I) + \mathrm{d}_{B/A}i_2 \otimes (i_1 + I) = 0$. The map δ is C-linear, as for all $b \in B$ and $i \in I$, $\delta(b + I)(i + I^2) = \mathrm{d}_{B/A}bi \otimes 1 = \mathrm{d}_{B/A}i \otimes (b + I) + \mathrm{d}_{B/A}b \otimes (i + I) = (b + I)\delta(i + I^2)$.

Proposition 0.15 (Second Exact Sequence)**.** *The sequence of C-modules*

$$I/I^2 \to \Omega_{B/A} \otimes_B C \to \Omega_{C/A} \to 0$$

exact. Moreover, if the map $B \to C$ admits a section $C \to B$ which is an A-algebra morphism, then the C-linear map $I/I^2 \to \Omega_{B/A} \otimes_B C$ is injective, and the sequence is split.

Proof. First note that, as $B \to C$ is surjective, $\Omega_{C/B} = 0$. Then it immediately follows from the First Exact Sequence that f is surjective. Also note that $f \circ \delta = 0$.

To see that $\operatorname{im} \delta = \ker f$, note that by a similar argument to the one used to prove Lemma 0.8, $\ker f'$ is generated by the elements of the form $\mathrm{d}_{B/A}b \otimes 1$, with $b \in B$ such that its image in C is in the image of A. Such elements are of the form $a + i$ with $a \in A$ and $i \in I$, so $\ker f'$ is generated by the elements of the form $\mathrm{d}_{B/A}i \otimes 1$ with $i \in I$. Hence by definition of δ, it follows that $\operatorname{im} \delta = \ker f$. We deduce that the given sequence is exact.

Now suppose that $B \to C$ admits a section. Let α denote the map $B \to C$, and let β denote its section. The map β gives a C-linear map $\Omega_{C/A} \to \Omega_{B/A}$ such that its composition with $\Omega_{B/A} \to \Omega_{B/A} \otimes_B C$ is a section of the C-linear map $\Omega_{B/A} \otimes_B C \to \Omega_{C/A}$.

Now consider the map $B \to I/I^2$, $b \mapsto b - \beta\alpha b$. As α, β both are morphisms of A-algebras, it follows that this map is an A-derivation, hence gives a B-linear map $\Omega_{B/A} \to I/I^2$. As $I\Omega_{B/A}$ is in the kernel of this map, this gives a C-linear map $\Omega_{B/A}/I\Omega_{B/A} = \Omega_{B/A} \otimes_B C \to I/I^2$. Note that this map sends an element of the form $\mathrm{d}b \otimes 1$ to $b - \beta\alpha b$, hence is a retraction of the C-linear map $I/I^2 \to \Omega_{B/A} \otimes_B C$. We deduce that this map is injective, and that the exact sequence is split. □

2 Pullbacks of morphisms of sheaves on topological spaces

Before we define the module of relative differentials on schemes, we will define what pullbacks of morphisms of sheaves are. We first fix some terminology.

Let $f \colon X \to Y$ be a morphism of topological spaces, let $\mathcal{F}$ be a sheaf of sets on X, and let $\mathcal{G}$ be a sheaf of sets on Y. Then an *f-morphism* $\phi \colon \mathcal{G} \to \mathcal{F}$ consists of for all opens $V \subseteq Y$ and $U \subseteq X$ such that $fU \subseteq V$, a map $\phi_{V/U} \colon \mathcal{G}(V) \to \mathcal{F}(U)$, such that the $\phi(V)$ are compatible with the restriction maps of both $\mathcal{F}$ and $\mathcal{G}$. Note that giving an f-morphism $\mathcal{G} \to \mathcal{F}$ is equivalent to giving a morphism $\mathcal{G} \to f_*\mathcal{F}$ of sheaves on Y, and hence, as the pair (f^{-1}, f_*) is an adjoint pair of functors, also equivalent to giving a morphism $f^{-1}\mathcal{G} \to \mathcal{F}$ of sheaves on X. If f is an isomorphism, then an f-isomorphism is an f-morphism $\phi \colon \mathcal{G} \to \mathcal{F}$ such that there exists an f^{-1}-morphism $\psi \colon \mathcal{F} \to \mathcal{G}$ satisfying $\phi\psi = \mathrm{id}_{\mathcal{F}}$ and $\psi\phi = \mathrm{id}_{\mathcal{G}}$.

The notion of an f-morphism is really convenient for defining compositions, and as an added bonus, the universal property for $f^{-1}\mathcal{G}$, obtained from adjointness, takes the following convenient form.

Let $f\colon X \to Y$ be a morphism of topological spaces, and let $\mathcal{G}$ be a sheaf of sets on Y. Then there is a natural f-morphism $f^{-1}\colon \mathcal{G} \to f^{-1}\mathcal{G}$ which satisfies the following. For all morphisms $g\colon Z \to X$ of topological spaces, for all sheaves of sets $\mathcal{H}$ on Z, and for all fg-morphisms $\phi\colon \mathcal{G} \to \mathcal{H}$, there is a unique g-morphism $\phi'\colon f^{-1}\mathcal{G} \to \mathcal{H}$ such that $\phi = \phi' f^{-1}$.

$$\begin{array}{ccc} \mathcal{G} & \xrightarrow{f^{-1}} & f^{-1}\mathcal{G} \\ & \searrow^{\phi} & \vdots\, \phi' \\ & & \mathcal{H} \end{array}$$

As an immediate consequence, we have the following.

Proposition 0.16. *Let*

$$\begin{array}{ccc} X' & \xrightarrow{f'} & Y' \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle h} \\ X & \xrightarrow{f} & Y \end{array}$$

be a commutative diagram of ringed spaces, and let $\mathcal{F}$ and $\mathcal{G}$ be sheaves of sets on X and Y, respectively. Let $\phi\colon \mathcal{G} \to \mathcal{F}$ be an f-morphism. Then there exists a unique f'-morphism $\phi'\colon \mathcal{G}_{Y'} = h^{-1}\mathcal{G} \to \mathcal{F}_{X'} = g^{-1}\mathcal{F}$, such that $g^{-1}\phi = \phi' h^{-1}$.

Note that we only have used the adjointness of the pair (f^{-1}, f_*), so this proposition still holds if all the sheaves are sheaves of abelian groups, rather than sheaves of sets, if f-morphisms are defined accordingly.

Similarly, as for a morphism f of ringed spaces, the pair (f^*, f_*) is adjoint, Proposition 0.16 still holds if "sheaf of sets" is replaced by "modules", and f^{-1} is replaced by f^*. (Again, if f-morphisms are defined accordingly.)

Definition 0.17. In the situation of Proposition 0.16, the morphism ϕ' is called the *pullback along* (g, h) of ϕ, or if $g = h$, simply the *pullback along* g.

Example 0.18. If g and h both are open immersions, then ϕ' is simply the restriction map.

We list some elementary properties in the following proposition.

Proposition 0.19. *Let*

$$\begin{array}{ccc} X'' & \xrightarrow{f''} & Y'' \\ {\scriptstyle g'}\downarrow & & \downarrow{\scriptstyle h'} \\ X' & \xrightarrow{f'} & Y' \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle h} \\ X & \xrightarrow{f} & Y \end{array}$$

be a commutative diagram of ringed spaces, and let $\mathcal{F}$ and $\mathcal{G}$ be sheaves of sets on X and Y, respectively. Let $\phi\colon \mathcal{G} \to \mathcal{F}$ be an f-morphism, and let ϕ' denote its pullback along (g, h).

(1) *If f and f' are isomorphisms, and ϕ is an f-isomorphism, then ϕ' is an f'-isomorphism, and its inverse is the pullback of ϕ^{-1}.*

(2) The pullback of ϕ along (gg', hh') is equal to the pullback of ϕ' along (g', h').
(3) The composition of two pullbacks is the pullback of the composition.

3 The module of relative differentials

Let $f\colon X \to S$ be a morphism of schemes. We first generalise the concept of derivations to this more general context. Note that we view $f^\#$ as an f-morphism $\mathcal{O}_S \to \mathcal{O}_X$.

Definition 0.20. Let $f\colon X \to S$ be a morphism of schemes, and let $\mathcal{F}$ be an $\mathcal{O}_X$-module. A morphism $\mathrm{d}\colon \mathcal{O}_X \to \mathcal{F}$ of sheaves of sets is an *S-derivation* if for all open subsets $V \subseteq S$ and $U \subseteq X$ with $fU \subseteq V$, the map $\mathrm{d}_{U/V}$ is a $\mathcal{O}_S(V)$-derivation of $\mathcal{O}_X(U)$.

As the open affine subsets of X and S form a basis for the topology of X and S respectively, to check that d is an S-derivation, one only needs to check this for all open affine U and V.

Definition 0.21. Let $f\colon X \to S$ be a morphism of schemes. The *module of relative differentials*, if it exists, is a pair $(\Omega_{X/S}, \mathrm{d}_{X/S})$ of an $\mathcal{O}_X$-module $\Omega_{X/S}$ and an S-derivation $\mathrm{d}_{X/S}\colon \mathcal{O}_X \to \Omega_{X/S}$ that satisfies the following universal property.

For all $\mathcal{O}_X$-modules $\mathcal{F}$, and all S-derivations $\mathrm{d}\colon \mathcal{O}_X \to \mathcal{F}$, there exists a unique $\mathcal{O}_X$-linear map $\phi\colon \Omega_{X/S} \to \mathcal{F}$ such that $\mathrm{d} = \phi \circ \mathrm{d}_{X/S}$.

Proposition 0.22. *Let $f\colon X \to S$ be a morphism of schemes. Then the module of relative differentials exists.*

Proof. We do this by gluing.

First, fix an affine open subset $V = \operatorname{Spec} A$ of S. Then for all affine open subsets $U = \operatorname{Spec} B$ of X with $fU \subseteq V$, we define $\Omega_{U/V} = \widetilde{\Omega_{B/A}}$ on U. We show that the $\Omega_{U/V}$ glue to an $\mathcal{O}_{f^{-1}V}$-module $\Omega_{f^{-1}V/V}$. This comes down to showing that if $U' = \operatorname{Spec} B'$ is a standard affine open of U, that $\Omega_{U/V}|_{U'} \cong \Omega_{U'/V}$. But this follows directly from Proposition 0.13, as B' is the localisation of B by a single element.

Next, we want to show that the $\Omega_{f^{-1}V/V}$ for all affine opens V in S glue to a $\mathcal{O}_X$-module $\Omega_{X/S}$. Again, this comes down to showing that for all standard affine opens $V' = \operatorname{Spec} A'$ of V we have $\Omega_{f^{-1}V/V}|_{V'} \cong \Omega_{f^{-1}V'/V'}$, or equivalently, for all affine opens $V' = \operatorname{Spec} A'$ of V, and all affine opens $U = \operatorname{Spec} B$ of $f^{-1}V'$, we have $\Omega_{U/V} = \Omega_{U/V'}$. But this follows directly from Proposition 0.12, as A' is the localisation of A by a single element, which maps to an invertible element in B.

So we have an $\mathcal{O}_X$-module $\Omega_{X/S}$. Now we define the S-derivation $\mathrm{d}_{X/S}$. Let $V = \operatorname{Spec} A$ be an affine open subset of S, and let $U = \operatorname{Spec} B$ be an affine open subset of X with $fU \subseteq V$. Then we define $\mathrm{d}_{X/S}(U) = \mathrm{d}_{B/A}$. By the above, this does not depend on the affine open V chosen. This rule is compatible with the restriction maps, as by the proof of Proposition 0.13, for a standard affine open subset $U' = \operatorname{Spec} B'$ of U, the restriction $\Omega_{X/S}(U) = \Omega_{B/A} \to \Omega_{X/S}(U') = \Omega_{B'/A}$, which is simply the localisation map, is compatible with A-derivations. Hence this defines a morphism of sheaves of sets $\mathrm{d}_{X/S}$, which by construction is an S-derivation.

Finally, to check that $\mathrm{d}_{X/S}$ is universal, let $\mathcal{F}$ be an $\mathcal{O}_X$-module, and let $\mathrm{d}\colon \mathcal{O}_X \to \mathcal{F}$ be an S-derivation. Let $U = \operatorname{Spec} A \subseteq S$ and $V = \operatorname{Spec} B \subseteq X$ be affine open. Then we obtain A-derivations $\mathrm{d}(V)\colon B \to \mathcal{F}(V)$, hence we obtain unique B-linear maps $\phi(V)\colon \Omega_{X/S}(V) = \Omega_{B/A} \to \mathcal{F}(V)$ such that $\mathrm{d}(V) = \phi(V) \circ \mathrm{d}_{X/S}(V)$. These maps are compatible with restrictions by the universal property of the module of relative Kähler differentials. Hence the maps $\phi(V)$ give a unique $\mathcal{O}_X$-linear map $\phi\colon \Omega_{X/S} \to \mathcal{F}$ satisfying $\mathrm{d} = \phi \circ \mathrm{d}_{X/S}$. □

Corollary 0.23. *Let $f\colon X \to S$ be a morphism of schemes. Then $\Omega_{X/S}$ is quasi-coherent, and for all affine open subsets $V = \operatorname{Spec} A$ of S and all affine open subsets $U = \operatorname{Spec} B$ of X with $fU \subseteq V$, we have $\Omega_{X/S}(V) = \Omega_{B/A}$ and $\mathrm{d}_{X/S}(U) = \mathrm{d}_{B/A}$.*

Example 0.24. If $f\colon X \to S$ is a closed immersion, then locally, f is given by a surjective morphism of rings, so $\Omega_{X/S} = 0$.

Example 0.25. Let $S = \operatorname{Spec} A$ be an affine scheme, and let $X = \operatorname{Spec} B$, where B is the ring $A[x_1, \ldots, x_n]/(f_1, \ldots, f_r)$ from Example 0.3. Then $\Omega_{X/S}$ is the sheaf associated to the B-module given in Example 0.3

Remark 0.26. Note that if $\mathrm{d}\colon \mathcal{O}_X \to \mathcal{F}$ is an S-derivation, then this induces an $\mathcal{O}_{S,f(x)}$-derivation $\mathrm{d}_x\colon \mathcal{O}_{X,x} \to \mathcal{F}_x$ for every point of x. By Proposition 0.9, this derivation is universal if d is universal.

The following is the scheme-theoretic equivalent of Proposition 0.10.

Proposition 0.27. *Let $f\colon X \to S$ and $g\colon T \to S$ be morphisms of schemes. Then $\Omega_{X_T/T} = g_X^*\Omega_{X/S}$.*

Proof. First note that the composition $\mathrm{d}\colon \mathcal{O}_X \to g_{X,*}\mathcal{O}_{X_T} \to g_{X,*}\Omega_{X_T/T}$ is an S-derivation. Hence this gives rise to a unique $\mathcal{O}_X$-linear map $\phi\colon \Omega_{X/S} \to g_{X,*}\Omega_{X_T/T}$ compatible with S-derivations. View ϕ as a g_X-morphism $\Omega_{X/S} \to \Omega_{X_T/T}$, and let $\phi'\colon g_X^*\Omega_{X/S} \to \Omega_{X_T/T}$ be the pullback of ϕ along (id, g_X).

Let $x_T \in X_T$, let $x = g_X(x_T) \in X$, let $t = f_T(x_T) \in T$ and let $s = gf_T(x_T) = fg_X(x_T)$. Then the pullback diagram defining ϕ' viewed on stalks, becomes

$$\begin{array}{ccc} \Omega_{B'/A'} & \xleftarrow{\phi'^{\#}} & \Omega_{B/A} \otimes_B B' \\ \uparrow{\scriptstyle \mathrm{id}} & & \uparrow{\scriptstyle \mathrm{id} \otimes g_X^{\#}} \\ \Omega_{B'/A'} & \xleftarrow[\phi^{\#}]{} & \Omega_{B/A} \end{array}$$

where $A = \mathcal{O}_{S,s}$, $B = \mathcal{O}_{X,x}$, $A' = \mathcal{O}_{T,t}$ and $B' = \mathcal{O}_{X_T,x_T}$. Note that $\phi'^{\#}$ is the unique B'-linear map making this diagram commute, hence $\phi'^{\#}$ is the canonical isomorphism $\Omega_{B/A} \otimes_B B' \cong \Omega_{B'/A'}$ from Proposition 0.10. From this, we deduce that ϕ' is an isomorphism. □

Corollary 0.28. *Let $f\colon X \to S$ and $g\colon T \to S$ be morphisms of schemes, let $\mathcal{F}$ be an $\mathcal{O}_X$-module, and let $\mathrm{d}\colon \mathcal{O}_X \to \mathcal{F}$ be an S-derivation. Then there is a unique T-derivation $\mathrm{d}'\colon \mathcal{O}_{X_T} \to g_X^*\mathcal{F}$ such that $\mathrm{d}'g_X^* = g_X^*\mathrm{d}$.*

Next, we have the scheme-theoretic equivalent of the Exact Sequences. Let $f\colon X \to Y$ and $g\colon Y \to Z$ be morphisms of schemes. Then $\mathrm{d}_{X/Y}$ is also a Z-derivation, and this gives the canonical $\mathcal{O}_X$-linear map $\Omega_{X/Z} \to \Omega_{X/Y}$. And in the same way as in the proof of Proposition 0.27, we construct the canonical map $f^*\Omega_{Y/Z} \to \Omega_{X/Z}$, which on stalks is given by the canonical morphism $\Omega_{\mathcal{O}_{Y,fx}/\mathcal{O}_{Z,gfx}} \otimes_{\mathcal{O}_{Y,fx}} \mathcal{O}_{X,x} \to \Omega_{\mathcal{O}_{X,x}/\mathcal{O}_{Z,gfx}}$.

Hence the following follows from the First Exact Sequence for modules of relative differentials over rings.

Proposition 0.29 (First Exact Sequence)**.** *Let $f\colon X \to Y$ and $g\colon Y \to Z$ be morphisms of schemes. Then the sequence of $\mathcal{O}_X$-modules*

$$f^*\Omega_{Y/Z} \to \Omega_{X/Z} \to \Omega_{X/Y} \to 0$$

is exact.

Now suppose that f is a closed immersion with sheaf of ideals $\mathcal{I}$. Then we have a morphism of sheaves

$$I \xrightarrow{\mathrm{d}} \Omega_{Y/Z} \longrightarrow f_*f^*\Omega_{Y/Z}$$

which is actually an $\mathcal{O}_Y$-linear map, as multiplication by a local section of I in $f_*f^*\Omega_{Y/Z}$ is the zero map. This gives by adjunction, a $\mathcal{O}_X$-linear map $f^*\mathcal{I} \to f^*\Omega_{Y/Z}$, which on stalks is given by the map $\mathcal{I}_{fx} \otimes_{\mathcal{O}_{Y,fx}} \mathcal{O}_{X,x} = \mathcal{I}_{fx}/\mathcal{I}_{fx}^2 \to \Omega_{\mathcal{O}_{Y,fx}/\mathcal{O}_{Z,gfx}} \otimes_{\mathcal{O}_{Y,fx}} \mathcal{O}_{X,x}$ of the Second Exact Sequence.

Hence the following follows from the Second Exact Sequence for modules of relative differentials over rings.

Proposition 0.30 (Second Exact Sequence)**.** *Let $i\colon X \to Y$ be a closed immersion with sheaf of ideals $\mathcal{I}$, and let $g\colon Y \to Z$ be a morphism of schemes. Then the sequence of $\mathcal{O}_X$-modules*

$$i^*\mathcal{I} \to i^*\Omega_{Y/Z} \to \Omega_{X/Z} \to 0$$

is exact. Moreover, if i admits a retraction, which is a morphism of Z-schemes, then the map $i^*\mathcal{I} \to i^*\Omega_{Y/Z}$ is injective, and the sequence is split.

Example 0.31. For any scheme S, we have $\Omega_{\mathbb{A}^n_S/S} \cong \mathcal{O}^n_{\mathbb{A}^n_S}$.

We can now also finally formulate what it means for a morphism of schemes $f\colon X \to S$ to be smooth of relative dimension $d \in \mathbb{Z}_{\geq 0}$.

Definition 0.32. Let $f\colon X \to S$ be a morphism of schemes, and let $d \in \mathbb{Z}_{\geq 0}$. Then f is *smooth of relative dimension d* is f is smooth, and $\Omega_{X/S}$ is locally free of constant rank d.

4 Translation actions on modules over group schemes

Let us first recall the definition of a group scheme.

Definition 0.33. Let S be a scheme. A *group scheme* is a scheme G over S, together with three S-morphisms $\mu\colon G \times_S G \to G$, $1\colon S \to G$ and $\iota\colon G \to G$ such that the following three diagrams commute (where the unlabelled arrows in (2) are the canonical isomorphisms).

(1)
$$\begin{tikzcd} G \times_S G \times_S G \arrow[r, "\mathrm{id}\times\mu"] \arrow[d, "\mu\times\mathrm{id}"'] & G \times_S G \arrow[d, "\mu"] \\ G \times_S G \arrow[r, "\mu"'] & G \end{tikzcd}$$

(2)
$$\begin{tikzcd} G \times_S G \arrow[dr, "\mu"] & G \times_S S \arrow[l, "\mathrm{id}\times 1"'] \arrow[d] \\ S \times_S G \arrow[u, "1\times\mathrm{id}"] \arrow[r] & G \end{tikzcd}$$

(3)
$$\begin{tikzcd} G \arrow[r, "(\mathrm{id},\iota)"] \arrow[d, "(\iota,\mathrm{id})"'] \arrow[dr, "1\circ f"] & G \times_S G \arrow[d, "\mu"] \\ G \times_S G \arrow[r, "\mu"'] & G \end{tikzcd}$$

Remark 0.34. Note that by Yoneda's Lemma, giving a group scheme G is equivalent to giving a factorisation of the functor of points of G via the forgetful functor $\mathfrak{Ab} \to \mathfrak{Set}$, and hence also to giving a group structure on $G(T)$ which is functorial in the S-scheme T.

Definition 0.35. Let G be a group scheme over a scheme S, and let T be an S-scheme. Let $g \in G(T)$. Then the *(right) translation* $t_g\colon G_T \to G_T$ by g is the morphism given on the functor of points as $G_T(T') \to G_T(T')$, $(x, \phi) \mapsto \big(x \cdot (g \circ \phi), \phi\big)$. Here, we view $G_T(T')$ as $G(T') \times T(T')$.

The *universal (right) translation* $\tau\colon G \times_S G \to G \times_S G$ is the translation by $\mathrm{id} \in G(G)$, where we view $G \times_S G$ as a G-scheme via the second projection.

Remark 0.36. It follows immediately from the definition that for any S-scheme T, all translations of G_T are translations of G (as for all T-schemes T', we have $G_T(T') = G(T')$).

In this context, it is interesting to describe the universal G_T-translation τ_T in terms of the universal G-translation τ, in the case that $T \to S$ is an open immersion. In this case, $G_T = f^{-1}T$, and τ_T is the restriction of τ to the open subscheme $G_T \times_T G_T$ of $G \times_S G$.

The following proposition justifies the term "universal".

Proposition 0.37. *Let G be a group scheme over a scheme S. Then every translation arises as a base change of τ.*

Proof. Let T be an S-scheme, and let $g \in G(T)$. Then note that we have a commutative diagram

$$\begin{array}{ccc} G \times_S T & \xrightarrow{\mathrm{id} \times g} & G \times_S G \\ {\scriptstyle t_g}\downarrow & & \downarrow{\scriptstyle \tau} \\ G \times_S T & \xrightarrow[\mathrm{id} \times g]{} & G \times_S G \end{array}$$

which is Cartesian, as the vertical arrows are isomorphisms. ☐

We now turn our attention to modules on group schemes.

Definition 0.38. Let G be a group scheme over a scheme S, and let $\mathcal{F}$ be an $\mathcal{O}_G$-module. Then an *action of G on $\mathcal{F}$ over the (right) translation action of G on G* (or simply, a *(right) translation action*) consists of for all S-schemes T, and all $g \in G(T)$, a t_g-isomorphism $\alpha_T(g)\colon \mathcal{F}_{G_T} \to \mathcal{F}_{G_T}$ of sheaves of modules with the following properties.

(1) The data is functorial in T, i.e. for all morphisms $\phi\colon T' \to T$ of S-schemes, $\alpha_{T'}(g \circ \phi)$ is the pullback of $\alpha_T(g)$ along $\mathrm{id} \times \phi\colon G_{T'} \to G_T$.
(2) For all S-schemes T, and for all $g, h \in G(T)$, we have $\alpha_T(g)\alpha_T(h) = \alpha_T(gh)$.

Example 0.39. The $\mathcal{O}_G$-module of relative differentials $\Omega_{G/S}$ has a natural translation action. Let T be an S-scheme, and let $g \in G(T)$. Then note that as t_g fits in a Cartesian diagram

$$\begin{array}{ccc} G_T & \xrightarrow{t_g} & G_T \\ {\scriptstyle f_T}\downarrow & & \downarrow{\scriptstyle f_T} \\ T & \xrightarrow[\mathrm{id}]{} & T \end{array}$$

so by Proposition 0.27, we have a canonical isomorphism $t_g^*\Omega_{G_T/T} = \Omega_{G_T/T}$. This gives us a natural t_g-isomorphism $t_g^*\colon \Omega_{G_T/T} \to \Omega_{G_T/T}$ with inverse $t_{g^{-1}}^*$. Hence we can define $\alpha_T(g) = t_g^*$.

Note that for every S-morphism $\phi\colon T' \to T$, we have $(\mathrm{id} \times \phi)t_{g\circ\phi} = t_g(\mathrm{id} \times \phi)$, so $\alpha_T(g)$ is indeed functorial in T. Also note for all S-schemes T, and for all $g, h \in G(T)$, we have $t_{gh} = t_h t_g$, so the $\alpha_T(g)$ indeed define a translation action on $\Omega_{G/S}$.

Example 0.40. Let $\mathcal{G}$ be an $\mathcal{O}_S$-module. Then $f^*\mathcal{G}$ has a natural translation action. Let T be an S-scheme, and let $g \in G(T)$. Then $f_T t_g = f_T$, and this implies that there is a canonical isomorphism $t_g^*(f^*\mathcal{G})_T = (f^*\mathcal{G})_T$. Hence taking $\alpha_T(g) = t_g^*$ defines a translation action on $f^*\mathcal{G}$, as seen in the previous example.

Example 0.41. Let $\mathcal{F}$ be an $\mathcal{O}_G$-module with a translation action of G. Let $\phi\colon T \to S$ be a morphism of schemes. Then $\mathcal{F}_{G_T}$ has an induced translation action of G_T, as translations of G_T are also translations of G.

Definition 0.42. Let G be a group scheme over a scheme S, and let $\mathcal{F}$ be an $\mathcal{O}_G$-module with a translation action α. A global section $s \in \Gamma(G, \mathcal{F})$ is *invariant under translations* if for all S-schemes T, and all $g \in G(T)$, we have $\alpha_T(g)s_{G_T} = s_{G_T}$. The subset of $\Gamma(G, \mathcal{F})$ consisting of the global sections that are invariant under translations is denoted $\Gamma(G, \mathcal{F})^G$.

To check that global sections of $\mathcal{O}_G$-modules $\mathcal{F}$, with a translation action α, are invariant under translations, one only needs to check that those global sections are invariant under the universal one, as every translation arises as a base change from the universal one, and as α is functorial in the S-scheme T. Hence, we have the following.

Proposition 0.43. *Let G be a group scheme over a scheme S, and let $\mathcal{F}$ be an $\mathcal{O}_G$-module with a translation action α. Then a global section $s \in \Gamma(G, \mathcal{F})$ is invariant under translations if and only if $\alpha_G(\mathrm{id})s_{G\times_S G} = s_{G\times_S G}$.*

We give an alternate description of a translation action.

Proposition 0.44. *Let G be a group scheme over a scheme S, and let $\mathcal{F}$ be an $\mathcal{O}_G$-module. Then giving a translation action α on G is equivalent to giving for all S-schemes T, and all $g_1, g_2 \in G(T)$, an $\mathcal{O}_T$-linear isomorphism $\alpha_T(g_1, g_2)\colon g_1^*\mathcal{F} \to g_2^*\mathcal{F}$ functorial in T, satisfying for all $g_1, g_2, g_3 \in G(T)$ the relation $\alpha_T(g_2, g_3)\alpha_T(g_1, g_2) = \alpha_T(g_1, g_3)$.*

Proof. First, let α be a translation action on $\mathcal{F}$, and consider for all S-schemes T and all $g_1, g_2 \in G(T)$, the following commutative diagram.

$$\begin{array}{ccc} T & \xrightarrow{\mathrm{id}} & T \\ {\scriptstyle (g_2,\mathrm{id})}\downarrow & & \downarrow{\scriptstyle (g_1,\mathrm{id})} \\ G_T & \xrightarrow[t_{g_2^{-1}g_1}]{} & G_T \end{array}$$

Then note that $(g_i, \mathrm{id})^*\mathcal{F}_{G_T} = (g_i, \mathrm{id})^*\pi_1^*\mathcal{F} = g_i^*\mathcal{F}$, so the pullback of $\alpha_T(g_2^{-1}g_1)$ along $\big((g_2, \mathrm{id}), (g_1, \mathrm{id})\big)$ defines an $\mathcal{O}_T$-linear isomorphism $\alpha_T(g_1, g_2)\colon g_1^*\mathcal{F} \to g_2^*\mathcal{F}$. We leave the proof that these $\alpha_T(g_1, g_2)$ satisfy the desired properties to the reader.

Now suppose that we have, for all S-schemes T, and all $g_1, g_2 \in G(T)$, an $\mathcal{O}_T$-linear isomorphism $\alpha_T(g_1, g_2)\colon g_1^*\mathcal{F} \to g_2^*\mathcal{F}$. Let T be an S-scheme, and let $g \in G(T)$. Let $\pi_1\colon G_T \to G$ denote the canonical projection. Then define $\alpha_T(g) = \alpha_{G_T}(\pi_1 \circ t_g, \pi_1)\colon t_g^*\pi_1^*\mathcal{F} \to \pi_1^*\mathcal{F}$. Note that $\pi_1^*\mathcal{F} = \mathcal{F}_{G_T}$, so $\alpha_T(g)$ defines a t_g-isomorphism $\mathcal{F}_{G_T} \to \mathcal{F}_{G_T}$. Again, we leave the proof that these $\alpha_T(g)$ define a translation action to the reader. □

Example 0.45. We give the translation action on $\Omega_{G/S}$ of Example 0.39 with respect to this alternate description. Let T be an S-scheme, and let $g_1, g_2 \in G(T)$. Then, as $t_{g_2^{-1}g_1}^*\Omega_{G_T/T} = \Omega_{G_T/T}$, we have

$$\begin{aligned} g_1^*\Omega_{G/S} = (g_1, \mathrm{id})^*\Omega_{G_T/T} &= (g_2, \mathrm{id})^* t_{g_2^{-1}g_1}^*\Omega_{G_T/T} \\ &= (g_2, \mathrm{id})^*\Omega_{G_T/T} = g_2^*\Omega_{G/S}, \end{aligned}$$

and $\alpha_T(g_1, g_2)$ is the identity, as the identity makes the pullback diagram defining $\alpha_T(g_1, g_2)$ commute.

Similarly, for an $\mathcal{O}_S$-module $\mathcal{G}$, the translation action on $f^*\mathcal{G}$ of Example 0.40 can be given by identity maps, as for all S-schemes T, and all $g_1, g_2 \in G(T)$, we have $g_2^* f^* \mathcal{G} = g_1^* f^* \mathcal{G}$.

Example 0.46. Let $\mathcal{F}$ be an $\mathcal{O}_G$-module with a translation action α of G, and let T be an S-scheme. Then the induced translation action β of G_T on $\mathcal{F}_{G_T}$ is given by $\beta_{T'}(g_1, g_2) = \alpha_{T'}(g_1, g_2)$, for all T-schemes T' and all $g_1, g_2 \in G_T(T') = G(T')$.

Now let $f\colon G \to S$ be a group scheme, and let $\mathcal{F}$ be an $\mathcal{O}_G$-module with a translation action α. We want to construct an $\mathcal{O}_S$-submodule of $f_*\mathcal{F}$ "consisting of elements that are invariant under translation".

Let U be an open subset of S. Then note that $f^{-1}U/U$ is a base change of G/S, this induces a natural group scheme structure on $f^{-1}U/U$ and a natural translation action on $\mathcal{F}|_{f^{-1}U}$. Also note that an element of $f_*\mathcal{F}(U)$ can also be viewed as a global section of the $\mathcal{O}_{f^{-1}U}$-module $\mathcal{F}|_{f^{-1}U}$. Then let $\mathcal{G}(U)$ denote the subgroup of $f_*\mathcal{F}(U)$ consisting of the local sections that are invariant under translations with respect to the group scheme $f^{-1}U/U$.

Note that $\mathcal{G}$ is a subsheaf of $\mathcal{O}_S$-modules by Example 0.18 and by the fact that, as for every open cover $\{U_i\}$ of an open U of S, the set $\{G_{U_i} \times_{U_i} G_{U_i}\}$ is an open cover of $G_U \times_U G_U$. We denote this subsheaf by $(f_*\mathcal{F})^G$.

Proposition 0.47. *Let $f\colon G \to S$ be a group scheme, and let $\mathcal{F}$ be a $\mathcal{O}_G$-module with a translation action α. Let β be the natural translation action on f^*1^*F. Then there is a canonical $\mathcal{O}_G$-linear isomorphism $f^*1^*\mathcal{F} = \mathcal{F}$ compatible with the translation actions α and β.*

Proof. Note that we have a commutative diagram

$$\begin{array}{ccc} G & \xrightarrow{\ \mathrm{id}\ } & G \\ {\scriptstyle (1\circ f,\mathrm{id})}\downarrow & & \downarrow{\scriptstyle \Delta} \\ G \times_S G & \xrightarrow[\ \tau\ ]{} & G \times_S G \end{array}$$

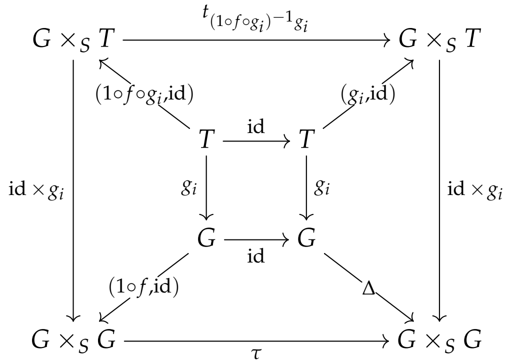
where the horizontal arrows are isomorphisms. Note that $\Delta^*\mathcal{F}_{G\times_S G} = \Delta^*\pi_1^*\mathcal{F} = \mathcal{F}$, and that $(1 \circ f, \mathrm{id})^*\mathcal{F}_{G\times_S G} = f^*1^*\mathcal{F}$. Consider $\alpha_G(\mathrm{id})\colon \mathcal{F}_{G\times_S G} \to \mathcal{F}_{G\times_S G}$. This is a τ-isomorphism. Hence by Proposition 0.19(1), its pullback $\phi\colon \mathcal{F} \to f^*1^*\mathcal{F}$ along $\big((1 \circ f, \mathrm{id}), \Delta\big)$ is a $\mathcal{O}_G$-linear isomorphism.

We now show that this isomorphism ϕ is compatible with the translation actions of G, i.e. that for all S-schemes T and all $g_1, g_2 \in G(T)$, the following diagram of $\mathcal{O}_T$-modules commutes, where $g_i^*\phi$ denotes the pullback of ϕ along g_i.

$$\begin{array}{ccc} g_2^* f^* 1^* \mathcal{F} & \xleftarrow{\ g_2^*\phi\ } & g_2^*\mathcal{F} \\ {\scriptstyle \beta_T(g_1,g_2)}\uparrow & & \uparrow{\scriptstyle \alpha_T(g_1,g_2)} \\ g_1^* f^* 1^* \mathcal{F} & \xleftarrow[\ g_1^*\phi\ ]{} & g_1^*\mathcal{F} \end{array}$$

First note that, by Example 0.45, we have $1 \circ f \circ g_1 = 1 \circ f \circ g_2$, and $\beta_T(g_1, g_2) = \mathrm{id} = \alpha_T(1 \circ f \circ g_1, 1 \circ f \circ g_2)$. Hence to prove that the diagram commutes, it suffices to show that $g_i^*\phi = \alpha_T(g_i, 1 \circ f \circ g_i)$.

To do this, we consider the following commutative cube.



Note that the $\mathcal{O}_T$-linear map $g_i^*\phi$ is the pullback of the τ-morphism $\alpha_G(\mathrm{id})$ along

$$\big((1\circ f,\mathrm{id})\circ g_i, \Delta\circ g_i\big) = \big((\mathrm{id}\times g_i)\circ(1\circ f\circ g_i,\mathrm{id}), (\mathrm{id}\times g_i)\circ(g_i,\mathrm{id})\big).$$

Also note that the $t_{(1\circ f\circ g_i)^{-1}g_i}$-morphism $\alpha_T\big((1\circ f\circ g_i)^{-1}g_i\big)$ is the pullback of $\alpha_G(\mathrm{id})$ along $\mathrm{id}\times g_i$. Hence $g_i^*\phi$ is the pullback of the $t_{(1\circ f\circ g_i)^{-1}g_i}$-morphism $\alpha_T\big((1\circ f\circ g_i)^{-1}g_i\big)$, in other words, $g_i^*\phi = \alpha_T(g_i, 1\circ f\circ g_i)$, as desired. □

Corollary 0.48. *Let $f\colon G\to S$ be a group scheme, and let $\mathcal{F}$ be a $\mathcal{O}_G$-module with a translation action. Then $(f_*\mathcal{F})^G = (f_*f^*1^*\mathcal{F})^G$.*

Proposition 0.49. *Let $f\colon G\to S$ be a group scheme, and let $\mathcal{F}$ be a $\mathcal{O}_G$-module with a translation action. Then the canonical map $f^*\colon 1^*\mathcal{F}\to f_*f^*1^*\mathcal{F} = f_*\mathcal{F}$ induces an isomorphism $1^*\mathcal{F}\to(f_*\mathcal{F})^G$.*

Proof. It suffices to show that f^* induces an $\Gamma(S,\mathcal{O}_S)$-linear isomorphism on global sections, as for all open subsets $U\subseteq S$, $f^{-1}U/U$ is a group scheme as well.

Let $s\in 1^*\Gamma(S,\mathcal{F})$. Then $f^*s\in\Gamma(S, f^*1^*\mathcal{F})$ is invariant under translations; for all S-schemes T and all $g\in G(T)$, t_g is an S-morphism, so $f\pi_1 t_g = f\pi_1$, which implies that $t_g^*(f^*s)_{G_T} = (f^*s)_{G_T}$. This gives an $\Gamma(S,\mathcal{O}_S)$-linear map $\Gamma(S,1^*\mathcal{F})\to\Gamma(S,f^*1^*\mathcal{F})^G$, which we will also denote by f^*.

We now show that f^* is an $\Gamma(S,\mathcal{O}_S)$-linear isomorphism. We do this by showing that its inverse is given by 1^*. First note that 1^*f^* is the identity on $\Gamma(S,1^*\mathcal{F})$. Now suppose that $s\in\Gamma(S,f^*1^*\mathcal{F})^G$. Then in particular, we have $\tau^*s_{G\times_S G} = s_{G\times_S G}$, so

$$f^*1^*s = (1\circ f,\mathrm{id})^*\pi_1^*s = (1\circ f,\mathrm{id})^*\tau^*\pi_1^*s = \Delta^*\pi_1^*s = s.$$

Hence f^*1^* is the identity on $\Gamma(G,f^*1^*\mathcal{F})^G$, so f^* is an isomorphism. □

1 Generalised Weierstrass equations

In the case of elliptic curves over algebraically closed fields, it is a basic fact that all elliptic curves can be given by a Weierstrass polynomial, and conversely, that all (non-singular) Weierstrass polynomials give rise to an elliptic curve. In the situation over arbitrary schemes, the situation is not as nice. We do have the following.

Proposition 1.1. *Let S be a scheme, and let $a_1, a_2, a_3, a_4, a_6 \in \mathcal{O}_S(S)$ with $\Delta(a_1, a_2, a_3, a_4, a_6) \in \mathcal{O}_S(S)^\times$ (where Δ denotes the usual elliptic discriminant). Then*

$$E = \operatorname{Proj}_S \mathcal{O}_S[x, y, z]/(y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6)$$

is an elliptic curve over S, together with the section $0 = (0 : 1 : 0) \in E(S) \subseteq \mathbb{P}^2_S$.

Here, for a graded $\mathcal{O}_S$-algebra $\mathcal{A}$, $\operatorname{Proj}_S \mathcal{A}$ denotes the *relative projective spectrum* obtained by gluing for all affine opens of U of A, the S-schemes $\operatorname{Proj} \mathcal{A}(U)$. For a proof of its existence, see the Stacks Project [2, Sect. 22.15].

We will call such elliptic curves *Weierstrass curves*. Unfortunately, not every elliptic curve will be a Weierstrass curve, but something a bit weaker will still be true, namely that *locally* on the base, every elliptic curves will be Weierstrass.

Theorem 1.2. *Let $f : E \to S$ be an elliptic curve. Then affine locally on $S = \operatorname{Spec} A$, there are $a_1, a_2, a_3, a_4, a_6 \in A$ with $\Delta(a_1, a_2, a_3, a_4, a_6) \in A^\times$ (where Δ denotes the usual elliptic discriminant) such that f is given by*

$$E = \operatorname{Proj} A[x, y, z]/(y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6) \to \operatorname{Spec} A,$$

and such that 0 is given by $(0 : 1 : 0) \in E(A) \subseteq \mathbb{P}^2_A$.

We prove this theorem in the following section.

1 Generalised Weierstrass equations

We first start off with a general fact about sheaves of modules that we will use often, see for example Hartshorne [1, Ex. II.5.1d].

Lemma 1.3 (Projection Formula)**.** *Let $f : X \to S$ be a morphism of ringed spaces, let $\mathcal{F}$ be an $\mathcal{O}_X$-module, and let $\mathcal{E}$ be a locally free $\mathcal{O}_S$-module of finite rank, then*

$$f_*(\mathcal{F} \otimes_{\mathcal{O}_X} f^*\mathcal{E}) = f_*\mathcal{F} \otimes_{\mathcal{O}_S} \mathcal{E}.$$

Let $f : E \to S$ be an elliptic curve. In René's talks, we have seen that E is an abelian group scheme over S.

Note that as elliptic curves are smooth of relative dimension 1, by definition it follows that $\Omega_{E/S}$ is invertible. Define the invertible $\mathcal{O}_S$-module $\omega_{E/S} = 0^*\Omega_{E/S}$. Then, by the Second Exact Sequence for the sequence $S \to E \to S$, we have $\omega_{E/S} = 0^*\mathcal{I}(0)$. By Proposition 0.47, we also have $f_*\Omega_{E/S} = f_*f^*\omega_{E/S}$. From the Projection Formula, it follows that $f_*f^*\omega_{E/S} = f_*\mathcal{O}_E \otimes_{\mathcal{O}_S} \omega_{E/S}$. As $f_*\mathcal{O}_E = \mathcal{O}_S$, it follows that $f_*\Omega_{E/S} = \omega_{E/S}$.

For now, assume that $S = \operatorname{Spec} A$ is affine, and that $\omega_{E/S}$ is trivial. Recall that $I(0)$ is a relative Cartier divisor of E, in particular, it is invertible. So, by making S smaller if necessary, we may assume that $U = \operatorname{Spec} B$ is an affine open subset of E such that $U \supseteq 0S$, and on which $I(0)$ is trivial. Then note that $U - 0S$ is a standard affine subset of U, namely it is $D(t)$ where t is a generator of $I(0)$ on U. This gives a split short exact sequence of B-modules

$$0 \longrightarrow I \longrightarrow B \underset{f^\#}{\overset{0^\#}{\rightleftarrows}} A \longrightarrow 0$$

where I is a free B-submodule of B. Let t_0 be a generator of I. As I is free, t_0 is not a zero divisor. We say that t_0 is a *parameter* at 0. Then we have an isomorphism $\phi\colon B \to A \oplus t_0 B$ of abelian groups, which gives an injective ring map $B \to A[[T]]$, $t_0 \mapsto T$ by repeated application of ϕ, hence also an injective ring map $F_\psi\colon B_{t_0} = \mathcal{O}_E(U - 0S) \to A((T))$ which we will call the *expansion map*.

This expansion map is independent of the open affine U chosen; by this, we mean that for any $x \in \mathcal{O}_E(E)$, the expansion of $x|_U$ is independent of U. This follows as for any element $b \in B$ with $0^\# b$ invertible in a, we have the following commutative diagram, where the map λ is the localisation map.

$$\begin{array}{ccc} B & \xrightarrow{\ \phi\ } & A \oplus t_0 B \\ {\scriptstyle\lambda}\downarrow & & \downarrow{\scriptstyle \mathrm{id} \oplus \lambda} \\ B_b & \xrightarrow{\ \phi_b\ } & A \oplus t_0 B_b \end{array}$$

This expansion map has the property that expansion of elements in $t_0^n B$ are in $T^n A[[T]]$. Furthermore, the composition $t_0^n B \to T^n A[[T]] \to A$, where the latter map sends a series to its T^n-coefficient, induces an isomorphism $t_0^n B / t_0^{n+1} B \to A$, hence the T^n-coefficient of a B-basis of $t_0^n B$ must be invertible in A.

Now let $\mathrm{d}\colon A((T)) \to A((T))\mathrm{d}T$ be the A-derivation

$$\sum_{i=r}^{\infty} a_i T^i \mapsto \sum_{i=r-1}^{\infty} (i+1) a_{i+1} T^i \mathrm{d}T.$$

This gives a unique B_t-linear map $F'_\psi\colon \Omega_{E/S}(U - 0S) = (\Omega_{B/A})_{t_0} \to A((T))\mathrm{d}T$ compatible with derivations, which we again call the *expansion map*. By a similar argument as before, this expansion map is independent of the open affine U chosen, in the same sense as before.

Note that the kernel of the composition $\Omega_{B/A} \to A[[T]]\mathrm{d}T \to A\mathrm{d}T$ contains $I\Omega_{B/A}$, where the latter map sends a series to its constant coefficient. Hence this gives a map $\Omega_{B/A} \otimes_B A \to A$. A straightforward check using the given derivations shows that this map is actually an isomorphism. Hence if ω is an $\mathcal{O}_S$-basis of $\omega_{E/S}$, viewed as element of $\Omega_{B/A}$, then its expansion has constant coefficient invertible in A.

Hence given a parameter t_0 at 0, there is a unique $\mathcal{O}_S$-basis ω of $\omega_{E/S}$ *adapted to* t_0, i.e. with expansion in $\big(1 + TA[[T]]\big)\mathrm{d}T$, and conversely, given an $\mathcal{O}_S$-basis ω of $\omega_{E/S}$, there is a unique parameter t_0 such that ω is adapted to t_0.

Proposition 1.4. *Let $f\colon E \to S$ be an elliptic curve, and let $n \in \mathbb{Z}_{\geq 1}$. Then $f_*\mathcal{I}^{-n}(0)$ is locally free of rank n. If $\omega_{E/S}$ is free and S is affine, then $f_*\mathcal{I}^{-n}(0)$ is free.*

Proof. We prove this by induction on n. The case $n = 1$ is proved by René. So suppose that for some $k \in \mathbb{Z}_{\geq 1}$, we have that $f_*\mathcal{I}^{-k}(0)$ is locally free of rank k. Consider the following canonical short exact sequence of $\mathcal{O}_E$-modules.

$$0 \longrightarrow \mathcal{I}(0) \longrightarrow \mathcal{O}_E \longrightarrow 0_*\mathcal{O}_S \longrightarrow 0$$

Note that $\mathcal{I}^{-k-1}(0)$ is locally free, hence flat over $\mathcal{O}_E$. Taking tensor products with $\mathcal{I}^{-k-1}(0)$ now gives the short exact sequence of $\mathcal{O}_E$-modules

$$0 \longrightarrow \mathcal{I}^{-k}(0) \longrightarrow \mathcal{I}^{-k-1}(0) \longrightarrow 0_*\mathcal{O}_S \otimes_{\mathcal{O}_E} \mathcal{I}^{-k-1}(0) \longrightarrow 0.$$

By the Projection Formula, $0_*\mathcal{O}_S \otimes_{\mathcal{O}_E} \mathcal{I}^{-k-1}(0) = 0_*0^*\mathcal{I}^{-k-1}(0)$, so as f_* is left exact and $R^1 f_*\mathcal{I}^{-k}(0) = 0$, we get a short exact sequence of $\mathcal{O}_S$-modules

$$0 \longrightarrow f_*\mathcal{I}^{-k}(0) \longrightarrow f_*\mathcal{I}^{-k-1}(0) \longrightarrow 0^*\mathcal{I}^{-k-1}(0) \longrightarrow 0.$$

Note that $0^*\mathcal{I}^{-k-1}(0)$ is invertible, and that by the induction hypothesis, $f_*\mathcal{I}^{-k}(0)$ is locally free of rank k. Hence it follows that $f_*\mathcal{I}^{-k-1}(0)$ is locally free of rank $k+1$.

If $\omega_{E/S} = 0^*\mathcal{I}(0)$ is free and S is affine, then so are all the $0^*\mathcal{I}^{-n}(0)$, which implies by induction that all the $f_*\mathcal{I}^{-n}(0)$ are free too. ☐

Now assume that $S = \operatorname{Spec} A$ is affine, and that $\omega_{E/S}$ is trivial with basis ω. Then $f_*\mathcal{I}^{-n}(0)$ is free of rank n for all $n \in \mathbb{Z}_{\geq 1}$.

Note that $f_*\mathcal{I}^{-1}(0)$ has basis 1. Hence $f_*\mathcal{I}^{-2}(0)$ has a basis containing 1, say $1, X$. The element X necessarily has expansion in $T^{-2}A[[T]]$, and its T^{-2}-coefficient is invertible. So we may choose X in such a way that its expansion is in $T^{-2} + T^{-3}A[[T]]$ (we say that such an X is *adapted to* ω). This X is unique up to $X \mapsto X + a$, where $a \in A$. Next, note that $f_*\mathcal{I}^{-3}(0)$ has a basis $1, X, Y$. Similar as before, we may assume that Y has expansion in $T^{-3} + T^{-4}A[[T]]$ (we say that such Y is *adapted to* ω). This Y is unique up to $Y \mapsto Y + bX + c$, where $b, c \in A$.

Now it follows that

(4) $f_*\mathcal{I}^{-4}(0)$ has basis $1, X, Y, X^2$;
(5) $f_*\mathcal{I}^{-5}(0)$ has basis $1, X, Y, X^2, XY$;
(6) $f_*\mathcal{I}^{-6}(0)$ has basis $1, X, Y, X^2, XY, X^3$ or basis $1, X, Y, X^2, XY, Y^2$.

Moreover, it follows that $Y^2 - X^3 \in f_*\mathcal{I}^{-5}(0)$, hence there exist $a_1, a_2, a_3, a_4, a_6 \in A$ such that for

$$W = y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3 \in A[x, y, z],$$

we have $W(X, Y, 1) = 0$.

Proof of Theorem 1.2. We show that, affine locally on $S = \operatorname{Spec} A$ such that $\omega_{E/S}$ is trivial, E is isomorphic to $Z = \operatorname{Proj} A[x, y, z]/(W)$, with W obtained in the way given above.

The 4-tuple $(\mathcal{I}^{-3}(0), X, Y, 1)$ defines a morphism $E \to \mathbb{P}^2_S$ which factors via $Z \to \mathbb{P}^2_S$, hence this gives a morphism $E \to Z$. On all fibres of E/S, this gives an isomorphism. Hence, as E is of finitely presentation over S, by reducing to the noetherian case, we are done if we show the following lemma. ☐

Lemma 1.5. *Let $\phi\colon X \to Y$ be a morphism of locally noetherian, proper, flat S-schemes, where S is also locally noetherian. Suppose that $\phi_s\colon X_s \to Y_s$ is an isomorphism for all points $s \in S$. Then ϕ is an isomorphism.*

Proof. As X and Y are proper S-schemes, it follows that ϕ is proper as well, and hence closed. As ϕ is an isomorphism on all fibres, it follows that ϕ is a bijection. So ϕ is a homeomorphism, hence affine. (See the Stacks Project [2, Lem. 04DE])

Now note that as ϕ is proper, ϕ_* sends coherent sheaves to coherent sheaves, so $\phi_*\mathcal{O}_X$ is a coherent $\mathcal{O}_Y$-module. Also, as on every fibre, $\phi_*\mathcal{O}_X$ is isomorphic to $\mathcal{O}_Y$, it follows in particular that $\phi_* \mathcal{O}_X$ is flat over Y, by the fibre-wise criterion for flatness. Hence $\phi_* \mathcal{O}_X$ is flat and coherent, so locally free of finite rank, and we can read off this rank from all of its fibres. This implies that $\phi_* \mathcal{O}_X$ is invertible, and hence that the $\mathcal{O}_Y$-linear map $\mathcal{O}_Y \to \phi_* \mathcal{O}_X$ is an isomorphism. □

Now let $f \colon E \to S$ be an arbitrary elliptic curve, and suppose that ω is a basis of $\omega_{E/S}$. Then we define for all $P \in E(S)$, in light of the above, the global sections $x(P) = P^* X$, $y(P) = P^* Y$ and $z(P) = P^* 1$ of $P^* \mathcal{I}^{-3}(0)$. Furthermore, we define the discriminant Δ of the pair $(E/S, \omega)$ to be the usual elliptic discriminant in terms of the Weierstrass coefficients. Note that the discriminant does not depend on which X, Y adapted to ω we chose.

2 Some elementary universal elliptic curves

Example 1.6. By now, we have already seen the first example of a universal family of elliptic curves. Namely, for every elliptic curve E/S with $\omega_{E/S}$ trivial, say with $\mathcal{O}_S$-basis ω, we get a homogeneous Weierstrass equation

$$W = y^2 z + a_1 xyz + a_3 yz^2 - x^3 - a_2 x^2 - a_4 x - a_6$$

with $\Delta(a_1, a_2, a_3, a_4, a_6) \in \mathcal{O}_S(S)^\times$, and an embedding $\phi \colon E \to \mathbb{P}^2_S$, inducing an isomorphism $E \to \operatorname{Proj} \mathcal{O}_S[x, y, z]/(W)$.

In this case, consider the elliptic curve

$$\mathbb{E} = \operatorname{Proj} A[x, y, z]/(W)$$

over $\operatorname{Spec} A$, where $A = \mathbb{Z}[a_1, a_2, a_3, a_4, a_6, 1/\Delta]$, together with the canonical embedding $F \colon \mathbb{E} \to \mathbb{P}^2_A$, and an $\mathcal{O}_S$-basis Ω of $\omega_{\mathbb{E}/A}$. This triple $(\mathbb{E}/A, F, \Omega)$ is *universal*, i.e. all triples $(E/S, \phi, \omega)$, where ϕ is an embedding of E into $\mathbb{P}^2_S$, and ω is an $\mathcal{O}_S$-basis of $\omega_{E/S}$, arise as a *unique* base change of the universal triple, compatible with the extra data, i.e. there are *unique* morphisms $E \to \mathbb{E}$ and $S \to \mathbb{S}$, making the following diagram Cartesian, and which are compatible with the extra data.

$$\begin{array}{ccc} E & \longrightarrow & \mathbb{E} \\ \downarrow & & \downarrow \\ S & \longrightarrow & \mathbb{S} \end{array}$$

If furthermore 6 is invertible in S, then there are unique X, Y adapted to ω such that $Y^2 = X^3 + aX + b$ with $a, b \in \mathcal{O}_S(S)$ such that $\Delta = -16(4a^3 + 27b^2)$ is invertible in S.

Now consider the elliptic curve

$$\mathbb{E} = \operatorname{Proj} A[x, y, z]/(y^2 z - x^3 - axz^2 - bz^3),$$

over A, where $A = \mathbb{Z}[1/6, a, b, 1/\Delta]$, and fix a basis Ω of $\omega_{\mathbb{E}/R}$. Then the pair $(\mathbb{E}/A, \Omega)$ is universal for pairs $(E/S, \omega)$, where 6 is invertible in S, and ω is an $\mathcal{O}_S$-basis of $\omega_{E/S}$.

Replacing A above by the ring $\mathbb{Z}[1/6, a, b]/(\Delta - 1)$ gives a universal pair for pairs $(E/S, \omega)$ where 6 is invertible in S, ω is an $\mathcal{O}_S$-basis of $\omega_{E/S}$, and the discriminant of E with respect to ω is equal to 1.

Example 1.7. Let E/S be an elliptic curve such that $\omega_{E/S}$ is trivial with basis ω, and let $P \in E(S)$ be *everywhere of order* 2, i.e. annihilated by 2, and of order 2 in every fibre of E/S. Then $z(P)$ is non-zero in all fibres of E/S, which implies that $z(P)$ generates $P^* \mathcal{I}^{-3}(0)$. Hence we can write $P = (x : y : 1)$.

Suppose that 2 is invertible in S, then there is a unique Y adapted to ω making both a_1 and a_3 zero. Then the automorphism $Q \mapsto -Q$ is given on the functor of points by $(\mathcal{L}, s_0, s_1, s_2) \mapsto$

$(\mathcal{L}, s_0, -s_1, s_2)$. Hence we can even write $P = (x : 0 : 1)$, so there is a unique X adapted to ω making P the point $(0 : 0 : 1)$. Then the Weierstrass equation becomes of the form

$$y^2 z = x(x^2 + a_2 xz + a_4 z^2),$$

and its discriminant is $\Delta = 16(a_2^2 a_4^2 - 4a_4^3)$.

Hence the triple $(\mathbb{E}/A, \Omega, \mathbb{P})$, where $A = \mathbb{Z}[1/2, a_2, a_4, 1/\Delta]$,

$$\mathbb{E} = \operatorname{Proj} A[x, y, z]/(y^2 z - x^3 - a_2 x^2 z - a_4 xz^2)$$

and $\mathbb{P} = (0 : 0 : 1)$ is the universal triple for triples $(E/S, \omega, P)$ for which 2 is invertible in S.

Example 1.8. Let E/S be an elliptic curve, and suppose that $\omega_{E/S}$ is trivial with $\mathcal{O}_S$-basis ω. Let P be a point on E that is *nowhere annihilated* by 2 or 3, i.e. not annihilated by 2 or 3 on any fibre of E/S. Then, as in previous cases, we may assume that $P = (0 : 0 : 1)$, and that in the Weierstrass equation of E, we have $a_6 = 0$. Note that $-P = (0 : -a_3 : 1)$, so P being nowhere annihilated by 2 implies that a_3 is invertible in S. Hence taking $Y = Y - (a_4/a_3)X$ makes a_4 zero. (Moreover, note that X, Y are now unique.)

Now note that P is nowhere annihilated by 3, so a_2 is everywhere non-zero. This implies that a_2 is invertible in S. So for a unique choice of ω, we get $a_2 = a_3$. This makes the Weierstrass equation of the form

$$y^2 z + sxyz + tyz^2 = x^3 + tx^2 z,$$

for some $s, t \in \mathcal{O}_S$ with $\Delta = -t^3\big(16t^2 + (8s^2 - 36s + 27)t + (s-1)s^3\big)$ invertible in S.

Hence the pair $(\mathbb{E}/A, \mathbb{P})$, where $A = \mathbb{Z}[s, t, 1/\Delta]$,

$$\mathbb{E} = \operatorname{Proj} A[x, y, z]/(y^2 z + sxyz + tyz^2 - x^3 - tx^2),$$

and $\mathbb{P} = (0 : 0 : 1)$ is universal for all pairs $(E/S, P)$ with P nowhere annihilated by 2 or 3.

We now would like to know, in the last example, for example what subscheme of $\mathbb{E}$ is the universal one if we also require P to be everywhere of order N for some fixed $N \geq 4$. To do this, we need to study the multiplication-by-N map first, and this is what Johan will do next week.

Bibliography

[1] R. Hartshorne. *Algebraic Geometry*, volume 52 of *Grad. Texts in Math.* Springer, 2006. ISBN 978-0-387-90244-9.

[2] Stacks Project. http://math.columbia.edu/algebraic_geometry/stacks-git, 2012.

[3] G. van der Geer and B. Moonen. http://staff.science.uva.nl/~bmoonen/boek/BookAV.html, 2012.