Notes on group schemes and Cartier duality

Spencer Dembner

2 February, 2020

In this note, we record some basic facts about group schemes, and work out some examples.

1 Definition of a group scheme

Let $\mathbf{Sch}/S$ be the category of schemes over S, where $S = \mathrm{Spec}(R)$ is a fixed affine base scheme. Let $U\colon \mathbf{Ab} \to \mathbf{Set}$ be the forgetful functor.

Definition 1.1. A group scheme is a contravariant functor $G\colon \mathbf{Sch}/S \to \mathbf{Ab}$, such that the composition $U \circ G$, a functor from $\mathbf{Sch}/S$ to $\mathbf{Set}$, is representable. We will also call the object representing the functor G a group scheme.

Let $G \in \mathbf{Sch}/S$ be any object, and by abuse of notation let G denote the representable functor defined by $G(X) = \mathrm{Hom}_{\mathbf{Sch}/S}(X, G)$ (we will usually avoid explicit subscripts for the category). Then giving G the structure of a group scheme is the same thing as defining, for each $X \in \mathbf{Sch}/S$, a group structure on $G(X)$ which is functorial in the obvious ways: a map $X \to X'$ induces a group homomorphism $G(X') \to G(X)$, and so on. The functor is contravariant because maps *into* a group have an obvious group structure, while maps out of a group do not.

If G is a group object, then in particular G induces a group structure on the set $G(G \times G) = \mathrm{Hom}(G \times G, G)$. We define $m\colon G \times G \to G$ by $m = \mathrm{pr}_1 \mathrm{pr}_2$, where pr_i denotes projection onto the i-th factor and the two maps are multiplied according to the group scheme structure; this represents the multiplication. We take $\varepsilon\colon S \to G$ to be the identity of $G(S)$, and we think of it as identifying a point of of G. The maps m, ε satisfy the natural categorical generalizations of the group axioms. For instance, ε is the identity in the sense that the following diagram commutes (here, note that since $S \in \mathbf{Sch}/S$ is the final object, $G \times S = G$.

$$\begin{array}{ccccc} G & = & G \times S & \xrightarrow{\mathrm{id}\times\varepsilon} & G \times G \\ \| & & & \searrow^{\mathrm{id}} & \downarrow{\scriptstyle m} \\ S \times G & & & & \\ \downarrow{\scriptstyle \varepsilon\times\mathrm{id}} & & & & \\ G \times G & & \xrightarrow{\quad m \quad} & & G \end{array} \tag{1.0.1}$$

Note also that the map $m\colon G \times G \to G$ determines the group $G(X)$ for any scheme X. Indeed, given $f, g\colon X \to G$, there is a corresponding map $f \times g\colon X \to G \times G$. Since $f \times g$ is a map $X \to G \times G$, by functoriality it determines a homomorphism $G(G \times G) \to G(X)$. Thus, we have:

$$m \circ (f \times g) = (f \times g)^*(m) = (f \times g)^*(\mathrm{pr}_1\, \mathrm{pr}_2) = (f \times g)^*(\mathrm{pr}_1)(f \times g)^*(\mathrm{pr}_2) = fg$$

Thus, the map m determines the group scheme structure. It's not too hard to see that given any m satisfying the appropriate axioms, we obtain a group scheme structure defined by $fg = m \circ (f \times g)$, for any scheme X and any $f, g \colon X \to G$. For a more explicit discussion of this point, see section 1 of [Tat97].

Now, specialize to the case where G is an affine scheme, so $G = \mathrm{Spec}(A)$ for some R-algebra A. Since the category of affine R-schemes is opposite to the category of R-algebras, we can explicitly state the conditions which the map m needs to satisfy, more or less by dualizing the axioms for multiplication in a ring. The resulting structure is known as a *Hopf algebra*.

Proposition 1.2. *Giving $G = \mathrm{Spec}(A)$ the structure of a group scheme is the same as giving A the structure of a Hopf algebra.*

In general terms, a Hopf algebra has two compatible structures, an algebra structure and a "coalgebra" structure. It has a multiplication coming from its algebra structure, and a comultiplication, expressing its group scheme structure. There is also a counit, which here takes the form of an R-algebra map $\varepsilon \colon A \to R$ (the unit can be expressed by the unique R-algebra map $\pi R \to A$, which sends 1 to the unit of the algebra A). Finally, there is an inversion map $\mathrm{inv} \colon A \to A$, expressing the existence of inverses in the group $G(X)$ for each X. The additional maps are required to make the following diagrams commute:

$$\begin{array}{ccccc} A & & \xrightarrow{\quad\Delta\quad} & & A \otimes A \\ \Big\downarrow{\scriptstyle \Delta} & & & & \Big\downarrow{\scriptstyle \Delta\times \mathrm{id}} \\ & & & & (A \otimes A) \otimes A \\ & & & & \Big\| \\ A \otimes A & \xrightarrow{\mathrm{id}\times\Delta} & A \otimes (A \otimes A) & = & A \otimes A \otimes A \end{array} \tag{1.0.2}$$

$$\begin{array}{ccccc} A & & \xrightarrow{\quad\Delta\quad} & & A \otimes A \\ \Big\downarrow{\scriptstyle \Delta} & \searrow^{\mathrm{id}} & & & \Big\downarrow{\scriptstyle \varepsilon\times \mathrm{id}} \\ & & & & R \otimes A \\ & & & & \Big\| \\ A \otimes A & \xrightarrow{\mathrm{id}\times\varepsilon} & A \otimes R & = & A \end{array} \tag{1.0.3}$$

$$\begin{array}{ccc} A & \xrightarrow{\pi\circ\varepsilon} & A \\ \Big\downarrow{\scriptstyle \Delta} & & \Big\uparrow{\scriptstyle m} \\ A \otimes A & \xrightarrow{\mathrm{inv}\times \mathrm{id}} & A \otimes A \end{array} \tag{1.0.4}$$

Here, the diagrams correspond, respectively, to the duals of associativity, identity and the existence of inverses. There are additional axioms, expressing the requirement that the algebra and "coalgebra" maps be compatible, so for instance $\Delta \colon A \to A \otimes A$ is required to be an algebra homomorphism. For exact statements of these, again see section 1 of [Tat97]. The Hopf algebra A is *commutative* if the underlying algebra is commutative, and *cocommutative* if Δ is invariant under

permuting tensor factors. More explicitly, there exists an algebra automorphism $T\colon A\otimes A \to A\otimes A$ characterized by $T(x\otimes y) = y\otimes x$. The Hopf algebra A is cocommutative if $T\circ\Delta = \Delta$. We will also call a group scheme commutative if the underlying Hopf algebra is cocommutative. The role of these various axioms will hopefully become clearer as we discuss some examples.

2 Basic examples of Hopf algebras and group schemes

A fundamental example of a Hopf algebra is the group algebra $A := R[G]$, where G is a finite group. This is the algebra spanned by elements e_g for $g \in G$, with multiplication characterized by $e_g e_h = e_{gh}$. It also has a natural comultiplication, characterized by $\Delta(e_g) = e_g \otimes e_g$. Note that this *does not* say that $\Delta(a) = a\otimes a$ for all $a \in A$; in fact, the elements a in a Hopf algebra which satisfy this property will play a special role later in our discussion of Cartier duality. One can check directly, using linearity and the fact that G is a group, that all the required diagrams commute.

The algebra $R[G]$ is not commutative unless G is, and thus is not a scheme. However, it is cocommutative: for all g, we have $T(\Delta(e_g)) = e_g\otimes e_g = \Delta(e_g)$, which shows by linearity that $\Delta = T\circ\Delta$. Another example, in some ways similar, is the universal enveloping algebra $A := U(\mathfrak{g})$ of a Lie algebra $\mathfrak{g}$, with the usual algebra structure. Here, the comultiplication is given by $a \mapsto a\otimes 1 + 1\otimes a$.

Now, we consider examples whose multiplication is commutative, making them group schemes. Again letting G be any finite group, let R^G be the set of functions from G to R, spanned by the indicator functions 1_g for $g \in G$. This has a natural structure as a commutative R-algebra, coming from the ring structure on R. It also has a natural comultiplication, characterized by the condition $\Delta(1_g) = \sum_{ab=g} 1_a \otimes 1_b$.

In general, to describe the comultiplication in a group scheme, we can make use of the functorial description we gave above. Thinking of a group scheme as a representable functor from (affine) schemes to groups, we observed that the multiplication map $m\colon G\times G \to G$ is given by the product $\mathrm{pr}_1\,\mathrm{pr}_2$ of the two projection maps, in the group $G(G\times G)$. Thinking in the category of commutative R-algebras, we obtain a group structure on $\mathrm{Hom}(A,B)$ for any commutative R-algebra B, by identifying it with $\mathrm{Hom}(\mathrm{Spec}\,B, G)$. The comultiplication $\Delta\colon A\to A\otimes A$ is the product, in $\mathrm{Hom}(A, A\otimes A)$ of the algebra maps $\tilde{\mathrm{pr}}_1, \tilde{\mathrm{pr}}_2\colon A\to A\otimes A$, which are defined by $\tilde{\mathrm{pr}}_1(a) = a\otimes 1$, $\tilde{\mathrm{pr}}_2(a) = 1\otimes a$.

For example, in the case of R^G discussed above, for any algebra X there is a group structure on $\mathrm{Hom}(R^G, X)$ characterized by the following condition: for all $x, y\colon R^G \to X$ and all $g \in R^G$, $(xy)(1_g) = \sum_{ab=g} x(1_a)y(1_b)$. Note that if X has no nontrivial idempotents, there are in fact only $|G|$ algebra homomorphisms $R^G \to X$, corresponding to a choice of factor in R^G. With respect to this group law, the identity is the algebra map $i\colon R^G \to P$ characterized by $i(1_e) = 1$, $i(1_g) = 0$ for all other g (this is an algebra map, since it's given by projection onto the 1_e factor, followed by the unique algebra map $R\to P$). Likewise, given any algebra map $x\colon R^G\to X$, define y by $y(1_g) = x(1_{g^{-1}})$. One checks that x and y are inverses with regard to this group law. If we didn't already know the map Δ, we could recover it as the product $\tilde{\mathrm{pr}}_1\tilde{\mathrm{pr}}_2$, which gives the formula we defined above.

Two other basic examples of group schemes are the schemes $\mathbb{G}_a$ and $\mathbb{G}_m$, the additive and multiplicative group schemes. The scheme $\mathbb{G}_a$ is just $R[x]$, with comultiplication characterized by $\Delta(x) = x\otimes 1 + 1\otimes x$. The scheme $\mathbb{G}_m$ is $R[x, x^{-1}]$, with comultiplication characterized by $x\mapsto x\otimes x$.

3 Finite flat group schemes and Cartier duality

Since the axioms for a Hopf algebra were obtained by dualizing those for an algebra, we might expect that taking the vector space dual of a Hopf algebra gives us yet another Hopf algebra. This is not quite true, but in many situations we care about it will be. For the rest of the note, we work over a fixed field k unless we state otherwise.

Let A be a Hopf algebra over k, and let $A' = \mathrm{Hom}_k(A, k)$, which so far is only a k-vector space. We have a comultiplication $\Delta\colon A \to A \otimes A$, and a multiplication, which we can think of as a map $m\colon A \otimes A \to A$. Passing to vector space duals, we have a map $\Delta'\colon (A \otimes A)' \to A'$. This is not quite a multiplication yet, but there is an obvious map $A' \otimes A' \to (A \otimes A)'$; given $f, g\colon A \to k$, it sends them to the function on $A \otimes A$ characterized by $(fg)(x \otimes y) = f(x)g(y)$. Composing with this map yields a multiplication on A', so any coalgebra structure gives an algebra structure on the dual space.

The situation with the algebra structure is slightly different. Now, the map $m\colon A \otimes A \to A$ gives rise to a map $A' \to (A \otimes A)'$, but there is no obvious map $(A \otimes A)' \to A' \otimes A'$. However, if A is finite-dimensional over k, then there is a canonical isomorphism $A' \otimes A' \cong (A \otimes A)'$. Thus, the dual of a finite-dimensional Hopf algebra is once again a finite-dimensional Hopf algebra.

Definition 3.1. A finite flat group scheme over the ring R is an R-group scheme G such that the morphism $G \to \mathrm{Spec}(R)$ is finite and flat.

In the case where k is a field, the definition of a finite morphism shows that G must be an affine scheme. Likewise, every morphism $k \to A$, where A is a k-algebra, is flat, since vector spaces are flat. It follows that over a field, the flatness condition is trivial, and a finite flat group scheme over k is just a finite-dimensional Hopf algebra over k, thought of contravariantly.

Let G be a finite flat group scheme over k. By our discussion above, the dual A' is also a Hopf algebra. In general, A' will not be commutative, and thus will not be a scheme. However, if G is *commutative*, so that its Hopf algebra A is both commutative and cocommutative, then the dual A' can once again be thought of as a commutative group scheme.

Definition 3.2. Let G be a commutative group scheme over k. Its Cartier dual is the group scheme $G' = \mathrm{Spec}(A')$, corresponding to the dual Hopf algebra A'.

We can give a more explicit characterization of Cartier duality in terms of the notion of a character. Letting $G = \mathrm{Spec}(A)$ and $H = \mathrm{Spec}(B)$ be affine group schemes, a morphism of group schemes $G \to H$ is the same as a morphism of Hopf algebras $B \to A$.

Definition 3.3. Let $G = \mathrm{Spec}(A)$ be an affine group scheme. A character of G is a morphism of group schemes $\chi\colon G \to \mathbb{G}_m$.

We say that an element $a \in A$ is *grouplike* if it's invertible and $\Delta(a) = a \otimes a$.

Proposition 3.4. *Characters of $G = \mathrm{Spec}(A)$ correspond to grouplike elements $a \in A$. The grouplike elements in A form a group under multiplication.*

Proof. A character corresponds to a Hopf algebra homomorphism $\chi\colon R[x, x^{-1}] \to A$, which is determined by the image of the element x. Any choice for $\chi(x)$ which is invertible defines an algebra homomorphism, and so we only need to ensure it preserves the comultiplication. That is, we need the following condition to hold:

$$\chi^{\otimes 2}(\Delta(x)) = \chi(x) \otimes \chi(x) = \Delta(\chi(x))$$

But this is exactly the condition for $\chi(x)$ to be grouplike. Finally, note that the grouplike elements form a group under multiplication, because the comultiplication is required to be an algebra homomorphism. That is, for any grouplike elements a, b, we have $\Delta(ab) = \Delta(a)\Delta(b) = (a \otimes a)(b \otimes b) = ab \otimes ab$. □

Given a group scheme G, this allows us to define a related functor G_c, in the following way: given any affine scheme $X = \mathrm{Spec}(B)$ over k, write $X \times G = \mathrm{Spec}(B \otimes G)$ for the base change to X. Then $G_c(X)$ is the set of characters $\chi\colon X \times G \to \mathbb{G}_m$, with multiplication given by multiplication of grouplike elements.

Lemma 3.5. *Suppose that $G = \mathrm{Spec}(A)$ is a finite flat group scheme over k. Then the functors G', G_c are isomorphic.*

Proof.[Sketch] By finite-dimensionality, it's enough to show the dual fact that the functors G and $(G')_c$ are isomorphic. Let $X = \mathrm{Spec}(B)$ be an affine scheme over k. Then $G' \otimes B$ can be identified with the space of k-linear maps $G \to B$. On the other hand, $G(X)$ is the group of k-algebra maps $G \to B$, so we have a natural inclusion $G(X) \subset G' \otimes B$. We claim that this inclusion exactly identifies $G(X)$ with the grouplike elements in G'. In one direction, suppose $f\colon G \to B$ is a k-algebra homomorphism. Recall that the comultiplication on G' was the dual of the multiplication on G. Explicitly, this means that for all x, y, $\Delta(f)(x, y) = f(xy)$. Since f is an algebra homomorphism, $\Delta(f)(x, y) = f(xy) = f(x)f(y)$, so $\Delta(f) = f \otimes f$, and f is grouplike. It's clear that all steps are reversible, so the converse holds as well. [1]

Note also that the group laws are the same: given algebra homomorphims $f, g\colon G \to B$, they multiply via the rule $fg(x) = (f \otimes g)(\Delta(x))$. But this is exactly the multiplication in the algebra $G' \otimes B$. □

What this lemma tells us is that the "character functor" defined abstractly above is representable, and in fact is represented by the group scheme G'. If G is not finite flat, then there is still a well-defined functor which may still be representable, but the theory does not guarantee that it will be.

4 Examples of Cartier duality

A fundamental example of a finite flat group scheme is the scheme $\mu_n := \mathrm{Spec}(A)$, where $A = k[x]/(x^n - 1)$. This is a subscheme of $\mathbb{G}_m$, and its comultiplication is likewise given by $\Delta(x) = x \otimes x$.

The dual Hopf algebra is spanned by the dual basis y_i, for $0 \leq i < n$, such that $y_i(x^i) = 1$, $y_i(x^j) = 0$ when $i \neq j$. The multiplication, dual to the comultiplication, is characterized by $(y_i y_j)(x^k) = (y_i \otimes y_j)(\Delta(x^k)) = y_i(x^k)y_j(x^k) = 1$ if $i = j = k$, and 0 otherwise. Thus, as an algebra, $A' \cong k^n$. The comultiplication, dual to the multiplication, is given by $(\Delta(y_i))(x^j, x^k) = y_i(m(x^j, x^k)) = y_i(x^{j+k})$; thus, $\Delta(y_i) = \sum_j y^j \otimes y^{i-j}$.

This is a special case, for G a commutative group, of two Hopf algebras we've seen before, namely $k[G]$ and k^G. A generalized version of our calculation above shows that for any Abelian group G, the group schemes $\mathrm{Spec}(k[G])$ and $\mathrm{Spec}(k^G)$ are dual to each other. We call the schemes

[1] For simplicity, we're ignoring some details: for instance, a grouplike element ought to satisfy conditions related to the identity which would ensure that $f(1) = 1$.

k^G *constant group schemes.* The motivation for the name is that whenever $\mathrm{Spec}(B)$ is connected (that is, when B does not split into a direct sum) and $|G| = n$, there are exactly n homomorphisms $k^G \to B$, corresponding to the choice of a k-factor. The composition law on these homomorphisms turns them into a group, which will be isomorphic to G. In the case we considered above, we can observe that $\mu_n = k[\mathbb{Z}/n\mathbb{Z}]$, while its Cartier dual is $k^{\mathbb{Z}/n\mathbb{Z}}$.

When the underlying field k has characteristic $p > 0$, we have a (non-reduced) group scheme $\alpha_p = \mathrm{Spec}(A)$, where $A = k[x]/(x^p)$. The map $\Delta(x) = x \otimes 1 + 1 \otimes x$ induces a well-defined map $\Delta\colon A \to A \otimes A$, and we take this map to be our comultiplication. Explicitly, for any k, we have:

$$\Delta(x^k) = (\Delta(x))^k = \sum_{i+j=k} \binom{k}{i} x^i \otimes x^j$$

The Cartier dual A' is spanned by a dual basis y_i as above, where $y_i(x^i) = 0$ and $y_i(x^j) = 0$ otherwise. We have comultiplication defined by $\Delta(y_i)(x^j, x^k) = y_i(x^{j+k})$, so $\Delta(y_i) = \sum_j y_j y_{i-j}$. We have multiplication defined by:

$$(y_i y_j)(x^k) = (y_i \otimes y_j)(\Delta(x^k)) = \sum_{a+b=k} \binom{k}{a} y_i(x^a) y_j(x^b)$$

This sum equals $\binom{n}{i}$ if $n = i + j$, and 0 otherwise. Thus, $y_i y_j = \binom{i+j}{i} y_{i+j}$. Define a k-algebra map $A' \to A$ by $y_i \mapsto \frac{x^i}{i!}$. This preserves the comultiplication, and the definition of a binomial coefficient shows that it preserves the multiplication as well, so we obtain an isomorphism of the Hopf algebra A with its dual A', showing that α_p is Cartier self-dual. For another discussion, see [Sno].

In the case of group schemes which are not finite flat, we can still consider characters and grouplike elements. For instance, considering the group scheme $\mathbb{G}_m$, the definition makes clear that x^n is grouplike for each n. For any polynomial $f(x) = \sum a_i x^i$, we have:

$$f(x) \otimes f(x) = \sum_{i,j} a_i a_j x^i \otimes x^j$$

This can't equal $\Delta(f(x))$ unless f is a monomial, so we conclude that the elements x^i are the only grouplike elements in $k[x, x^{-1}]$. They form a group isomorphic to $\mathbb{Z}$, which is not surprising, since $k[x, x^1] = k[\mathbb{Z}]$, the group algebra of $\mathbb{Z}$. In fact, the dual of $\mathbb{G}_m$ is none other than $k^{\mathbb{Z}}$, as our discussion above leads us to expect.

In the case $k = \mathbb{R}$, another interesting example to consider is $S = \mathrm{Spec}(A)$, where $A = \mathbb{R}[x, y]/(x^2 + y^2 - 1)$. This has comultiplication coming from the group structure on S^1. Writing $A = \mathbb{R}[x_1, y_1]/(x_1^2 + y_1^2 - 1)$, and letting $A \otimes A$ be generated by variables x_2, y_2, x_3, y_3, we can give it explicitly by:

$$\Delta(x_1) = x_2 \otimes y_3 - y_2 \otimes x_3, \Delta(y_1) = x_2 \otimes y_3 + y_2 \otimes x_3$$

Over $\mathbb{C}$, $x^2 + y^2$ factors as $(x + iy)(x - iy)$. Setting $u = x + iy, v = x - iy$, we have:

$$\mathbb{C}[x, y]/(x^2 + y^2 - 1) = \mathbb{C}[u, v]/(uv - 1) = \mathbb{C}[u, u^1]$$

Computing the comultiplication and setting $u_j = x_j + iy_j$, $v_j = x_j - iy_j$, we have:

$$\Delta(u_1) = \Delta(x_1)+i\Delta(y_1) = x_2\otimes x_3 - y_2\otimes y_3 + i(x_2\otimes y_3 + y_2\otimes x_3) = x_2\otimes x_3 + ix_2\otimes y_3 + iy_2\otimes y_3 - y_2\otimes y_3$$

Likewise, we have:

$$u_2 \otimes u_3 = (x_2 + iy_2) \otimes (x_3 + iy_3) = x_2 \otimes x_3 + ix_2 \otimes y_3 + iy_2 \otimes y_3 - y_2 \otimes y_3$$

This shows that the base change of S to $\mathbb{C}$ is just $\mathbb{G}_m$, although the two group schemes are not isomorphic over $\mathbb{R}$. The resulting base change has an action of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$, permuting $u = x + iy$ and $u^{-1} = x - iy$, which suggests that we should think of S as a "twisted" version of $\mathbb{G}_m$.

We close by considering one more example which is slightly more involved.

Example 4.1. Let $E/\mathbb{F}_2$ be the elliptic curve defined by $y^2 + y = x^3$. We have a finite flat group scheme $A := E[2]$, the two-torsion group scheme for the curve E.

Every elliptic curve in characteristic 2 has either 1 or 2 two-torsion points, including the identity. Let $P = (x, y) = [x : y : 1]$ be any point on $E[\overline{\mathbb{F}}_2]$ aside from the origin. Then $-P$ is the unique second point (x, y') satisfying $x = x', y'^2 + y' = x'^3 = x^3$. The equation $y^2 = y$ factors as $(y + 1)y$, so we see that the inversion map is $[X : Y : Z] \mapsto [X : Y + Z : Z]$. In particular, this shows that the origin is the only 2-torsion point, so E is supersingular (has trivial 2-torsion subgroup).

In order to find coordinates for A, we first change coordinates to include the origin $[0 : 1 : 0]$, which is automatically 2-torsion. To this end, work with affine coordinates $(X/Z, Z/Y)$, with respect to which the origin is the point $(0, 0)$; note that these coordinates make sense, since there are no 2-torsion points whose y-coordinate is zero.

Now, we write down the algebraic condition for a point to be two-torsion, trying very hard to forget that there are no nontrivial two-torsion points. If $[X : Y : Z] = [X : Y + Z : Z]$, this tells us that $Y/X = (Y + Z)/X$, so $XY = XY + XZ, XZ = 0$. Likewise, $Z/Y = Z/(Z + Y)$, so $Z^2 + YZ + YZ = 0$, $Z^2 = 0$. Along with the equation for the elliptic curve, we obtain the following affine scheme:

$$\begin{aligned}\mathbb{Z}/2\mathbb{Z}[X, Z]/(Z + Z^2 - X^3, Z^2, XZ) &= \mathbb{Z}/2\mathbb{Z}[X, Z]/(Z - X^3, Z^2, XZ) \\ &= \mathbb{Z}/2\mathbb{Z}[X]/(X^6, X^4) = \mathbb{Z}/2\mathbb{Z}[X]/(X^4)\end{aligned}$$

In order to write down the comultiplication, we use II.2.3 from [Sil09], which tells us that if λ is the line through two points $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ on an elliptic curve E, and if E is given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

then the point $P_3 = -(P_1 + P_2)$, which is the unique third intersection point of the line between P_1 and P_2 with E, satisfies:

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$$

In (x, z) coordinates, the curve E has equation $z^2 + z = x^3$, which is once again (the same) Weierstrass equation. Applying the result above, we find that the x-coordinate of $-(P_1 + P_2)$ is given by:

$$x_3 = \left(\frac{z_2 + z_1}{x_1 + x_1}\right)^2 + x_1 + x_2 = x_2^4 + x_1^2 x_2^2 + x_1^4 + x_1 + x_2$$

Here, the second equality follows by expanding and using that $z_i = z_i^3$ for 2-torsion points. Now, the origin is not at infinity, so inversion will not have the usual form. Instead, inversion in these coordinates (excluding the line $z = 1$) is given by $(x, z) \mapsto (x/(1 + z), z/(1 + z))$. However, since this is the group scheme of 2-torsion points, and since $P = -P$ when P is 2-torsion, we can ignore this complication. It follows that the comultiplication is given explicitly by the formula:

$$\Delta(x) = x_2^4 + x_1^2 x_2^2 + x_1^4 + x_1 + x_2.$$

References

[Sil09] Silverman, Joseph H. *The Arithmetic of Elliptic Curves*. Second. Vol. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009.

[Sno] Snowden, Andrew. *Lecture 6: Group Schemes 2*. URL: `http://www-personal.umich.edu/~asnowden/teaching/2013/679/L06.html`.

[Tat97] Tate, John. "Finite flat group schemes". In: *Modular forms and Fermat's last theorem (Boston, MA, 1995)*. Springer, New York, 1997, pp. 121–154.