Cartier duality with examples

CJ Dowd

January 20, 2024

1 Cartier duality over a field

Let k be a field. When we refer to an algebra, we mean a commutative algebra.

We consider finite k-groups, i.e. group objects in the category of k-schemes that are also finite over $\operatorname{Spec} k$ (and automatically flat). These are always the spectrum of some finite dimensional ring over k (necessarily artinian and noetherian). From the basic theory of group schemes, the category of finite k-groups is dual to the category of *finite-dimensional Hopf algebras* over k. These are finite-dimensional k-algebras A equipped with a comultiplication map $c : A \to A \otimes_k A$, a counit homomorphism $\eta : A \to k$, and an antipode morphism $i : A \to A$, all of which are k-algebra homomorphisms and satisfy commutative diagrams dual to those required for group schemes.

Now suppose that $G = \operatorname{Spec} A$ is a *commutative* finite group scheme. Given such an algebra A, we may form its dual $A^* = \operatorname{Hom}_k(A, k)$. Dualizing is well-behaved under the assumption that A is finite-dimensional. We endow A^* with the structure of a Hopf algebra by dualizing the Hopf algebra structure on A:

- The multiplicative structure $A^* \otimes A^* \to A^*$ is the dual of the comultiplicative structure $c : A \to A \otimes A$. This law is commutative by the assumption that X is a commutative group scheme. This assumption means that A is *cocommutative*, i.e. $\operatorname{im}(c) \subseteq \operatorname{Sym}^2 A \subseteq A \otimes A$; hence c^* is invariant under precomposition with the switch morphism. This is the main reason why we restrict ourselves to the case of commutative group schemes, since otherwise the dual construction would not give a scheme.
- The k-algebra structure $k = k^* \to A^*$ is given by the dual of the unit map $\eta : A \to k$.
- The antipode $A^* \to A^*$ is given by the dual of the antipode $i : A \to A$.
- The comultiplication map $A^* \to A^* \otimes A^*$ is the dual of the multiplication map $A \otimes A \to A$.
- The counit map $A^* \to k = k^*$ is the dual of the structure morphism $k \to A$.

Here, we naturally identify $k^* = k$ by identifying the element $\lambda \in k$ with the functional $a \mapsto \lambda a$. These choices of maps are precisely the ones that make A^* into a Hopf algebra by reversing the arrows in the commutative diagrams that make A into a Hopf algebra.

Definition 1. The *Cartier dual* X^* of a commutative finite k-group $X = \operatorname{Spec} A$ is the k-group $\operatorname{Spec} A^*$ via the Hopf algebra structure on A^* described above. It is again a finite commutative group.

2 Examples

Example 2. Let $\mu_m = \operatorname{Spec} A = \operatorname{Spec} k[x]/(x^m - 1)$. The coalgebra structure on the coordinate ring is given by $x \mapsto x \otimes x$, which we think of as corresponding to the multiplicative group law $(x, y) \mapsto xy$. The antipode is $x \mapsto x^{m-1} = x^{-1}$, and the counit map is $x \mapsto 1$.

Abstractly, the linear dual of A is just an m-dimensional vector space over k. It has basis $\{y_0, y_1, \ldots, y_{m-1}\}$ defined by $y_i(x^j) = \delta_{ij}$. Hence the dual to the bialgebra morphism $A \to A \otimes_k A$ is the map $A^* \otimes A^* \to A$

defined by $c^* : y_i \otimes y_i \mapsto y_i$, $y_i \otimes y_j \mapsto 0$ for $i \neq j$, endowing A^* with the structure of a commutative algebra. The counit map $\eta : A \to k : x \mapsto 1$ is dual to $k \to A^* : 1 \mapsto \sum_{i=0}^{m-1} y_i$, which we take as the structure morphism. To see this, note that the dual of η is the unique linear functional $\varphi : k \to A^*$ satisfying $(\varphi(\lambda))(x^i) = \lambda \cdot \eta(x^i) = \lambda$, so the image of 1 must yield 1 upon evaluating at any of the x_i. As a sanity check, we observe that

$$c^* \left(\left(\sum_{i=0}^{m-1} y_i \right) \otimes z \right) = z$$

since this is true when $z = y_i$, and this good since we expect since $\sum_{i=0}^{m-1} y_i$ to act as the multiplicative identity.

This already gives enough information to identify the algebra structure of A^*: it is the ring k^m, the m-fold product of k. The isomorphism is given by sending $y_i \to e_i$, the i-th standard basis vector of this ring. The multiplicative structures clearly match, and the element $\sum_{i=0}^{m-1} y_i$ gets sent to $(1, 1, \ldots, 1)$, which is the multiplicative identity of k^m, so this is indeed an isomorphism of k-algebras. Hence, as a scheme, $(\mu_m)^*$ is the disjoint union of m copies of $\operatorname{Spec} k$.

We now identify the coalgebra structure, and hence the group law on $(\mu_m)^*$. The structure morphism $k \hookrightarrow A$ dualizes to the counit morphism $y_0 \mapsto 1$, $y_i \mapsto 0$ for $i \neq 0$, which canonically identifies one of the points on $\operatorname{Spec} A^*$ as the identity element. The dual of the multiplication map $\Delta : x \otimes x' \to xx'$ is the unique map Δ^* such

$$\Delta^*(y_i)(x^j \otimes x^k) = y_i(x^j x^k) = \delta_{i(j+k)},$$

where the indices are understood to be modulo m and δ denotes the Kronecker delta. This determines $\Delta^*(y_i) = \sum_{j=0}^{m-1} y_j \otimes y_{i-j}$. Finally, we can extract the group law on X^* at the level of points: let P_i be the points on X^* corresponding to the prime ideals $\mathfrak{p}_i = \bigoplus_{j \neq i} k$. The preimage of the prime ideal $\mathfrak{p}_{ij} = \bigoplus_{\substack{0 \leq i', j' < m \\ (i', j') \neq (i, j)}} k$ corresponding to the point $(P_i, P_j) \in (\mu_m)^* \times (\mu_m)^*$ under the coalgebra homomorphism is $\mathfrak{p}_{i+j}$, corresponding to P_{i+j}. We can verify directly that $(\mu_m)^*$ is the constant group scheme $\mathbb{Z}/m\mathbb{Z}$ by verifying that that coalgebra homomorphism on this scheme matches the one we found for $(\mu_m)^*$. Using the identification $A^{**} \simeq A$, we also conclude $(\mathbb{Z}/m\mathbb{Z})^* \simeq \mu_m$.

Note that our previous discussion was completely independent of the characteristic of the base field. If $\operatorname{char}(k) = p > 0$, we get a curious result in the case $m = p^n$: the group scheme μ_{p^n} is a nonreduced group scheme consisting of one point, but its dual is a constant group scheme consisting of p^n points, illustrating:

- The dual of a constant group scheme may not be constant;
- The dual of a smooth group scheme may not be smooth;
- The dual of a connected group scheme may not be connected.

Example 3. Let α_p be the kernel of the relative Frobenius endomorphism on the scheme $\mathbb{G}_a$ over some field k of characteristic p. As a scheme, this is the spectrum of $A = k[x]/(x^p)$, and its group structure is defined by the comultiplication $c : x \mapsto x \otimes 1 + 1 \otimes x$, inherited from $\mathbb{G}_a$; this means that $c(x^n) = (x \otimes 1 + 1 \otimes x)^n = \sum_{i=0}^{n} \binom{n}{i} x^i \otimes x^{n-i}$. The counit morphism is associated to $x \mapsto 0$, and the antipode is defined by $x \mapsto -x$.

Again let A^* have basis $y_0, \ldots, y_{p-1}$ dual to the basis $x^0, x^1, \ldots, x^{p-1}$ of A. The dual to the comultiplication of A is the unique map $c^* : A^* \otimes A^* \to A^*$ satisfying, for all $0 \leq n < p$,

$$\begin{aligned} c^*(y_i \otimes y_j)(x^n) &= (y_i \otimes y_j) \left(\sum_{k=0}^{n} \binom{n}{k} x^k \otimes x^{n-k} \right) \\ &= \sum_{k=0}^{n} \binom{n}{k} \delta_{ik} \delta_{j(n-k)} \\ &= \binom{n}{i} \delta_{j(n-i)}, \end{aligned}$$

so this sum is nonzero only if $n = i + j$. We conclude that $c^*(y_i \otimes y_j) = \binom{i+j}{i} y_{i+j}$. Meanwhile, the dual to the counit morphism is $1 \mapsto y_0$; again, as a sanity check, we indeed have $c^*(y_0 \otimes y_i) = y_i$ for any y_i. We also note that $y_i^p = 0$ for any $i \neq 0$, since this is $\prod_{j=1}^p \binom{ji}{i} y_{ji}$, and the last term is divisible by p unless $i = 0$.

We claim that the algebra structure on A^* is in fact isomorphic to A. This isomorphism $\varphi : A \to A^*$ is given by

$$x^i \mapsto i! \cdot y_i$$

for each $0 \leq i < p$. This is an algebra homomorphism since

$$(i+j)! \cdot y_{i+j} = \frac{(i+j)!}{\binom{i+j}{i}} y_i y_j = (i! \cdot y_i)(j! \cdot y_j),$$

and it sends $1 = x^0 \mapsto y_0$.

The comultiplication structure on A^* is defined by $\Delta^*(y_i)(x^j \otimes x^k) = y_i(x^{j+k}) = \delta_{i(j+k)}$—note that we *do not* consider indices modulo p, unlike the case of Example 2, since now $x^n = 0$ if $n \geq p$, so we interpret $\delta_{i(j+k)} = 1$ if and only $i = j + k$ as integers. We conclude that $\Delta^*(y_i) = \sum_{j=0}^i y_j \otimes y_{i-j}$, with the indexing stopping at i. We observe something remarkable: the algebra isomorphism $A \to A^*$ we described previously is also a coalgebra isomorphism, since

$$\begin{aligned} \varphi(c(x^n)) &= \varphi\left(\sum_{i=0}^n \binom{n}{i} x^i \otimes x^{n-i}\right) \\ &= \sum_{i=0}^n \binom{n}{i} \cdot i! \cdot (n-i)! \cdot y_i \otimes y_{n-i} \\ &= n! \cdot \sum_{i=0}^n y_i \otimes y_{n-i} \\ &= n! \cdot \Delta^*(y_n) \\ &= \Delta^*(\varphi(x^n)). \end{aligned}$$

We conclude that α_p is its own Cartier dual!

Note that computing the Cartier dual of α_{p^n} for $n \geq 2$ is trickier. The map $\varphi : x^i \mapsto i! \cdot y_i$ described previously is no longer an isomorphism if we allow $i \geq p$ since $i! = 0$ in this range.

3 Cartier duality over a general base

Now let S be an arbitrary scheme.

Definition 4. A *finite group* G over S is a group object in the category of S-schemes that is finite locally free over S. That is, $f_*\mathcal{O}_G$ is a locally free $\mathcal{O}_S$-algebra of finite rank, where $f : G \to S$ is the structure morphism. If this rank r is constant, then we say that r is the *order* of G.

We will refer to such schemes simply as finite group schemes, with the local freeness assumed. If S is locally noetherian, then local freeness of $f : G \to S$ is equivalent to saying that G is flat over S.

The category of finite S-group schemes is dually equivalent to the category of locally free and finite $\mathcal{O}_S$-Hopf algebras via $G \mapsto f_*\mathcal{O}_G$, where $f : G \to S$ is the structure morphism, and, in the other direction, $\mathcal{A} \mapsto \underline{\mathrm{Spec}}\, \mathcal{A}$, where $\mathcal{A}$ is a sheaf of $\mathcal{O}_S$-Hopf algebras.

Definition 5. The *Cartier dual* G^* of a finite commutative group scheme G over S is S-group

$$\underline{\mathrm{Spec}} \mathscr{H}om_{\mathcal{O}_S}(f_*\mathcal{O}_G, \mathcal{O}_S),$$

with Hopf algebra structure given by dualizing the Hopf structure on $\mathcal{O}_G$ as described in the case over a field.

Again, cocommutativity of the coalgebra structure of $\mathcal{O}_G$ guarantees that $\mathscr{H}om_{\mathcal{O}_S}(f_*\mathcal{O}_G, \mathcal{O}_S)$ is a commutative $\mathcal{O}_S$-algebra, hence G^* is a scheme. Commutativity of G^* follows from the assumption that $f_*\mathcal{O}_G$ is a commutative $\mathcal{O}_S$-algebra.

Implicit in this discussion is the following:

Lemma 6. *Let $f : G \to S$ be a group scheme over an arbitrary scheme S. If $U \subseteq S$ is an open subscheme, then $V = f^{-1}(U)$ is an open subgroup scheme of G over U.*

Proof. It suffices to show that the morphisms $\mu|_V : V \times V \to G, i|_V : V \to G$, and $e|_U : U \to G$ factor through the open immersion $V \to G$. The morphisms μ, i, and e are all morphisms of S-schemes, so their restrictions are all morphisms of U-schemes, which automatically implies that the images of all of these restrictions land in V. ∎

Therefore, there exists a covering $\{U_i\}$ of S such that $U_i = \operatorname{Spec} R_i$ for some ring R and such that $f^{-1}(U_i) = \operatorname{Spec} A_i$ for some finite free R_i-algebras A_i. By the lemma, the A_i inherit an R_i-Hopf algebra structure—this follows from the fact that the $f^{-1}(U_i)$ are themselves group schemes over their respective U_i. We may therefore locally describe G^* as the spectrum of $\operatorname{Hom}_{R_i}(A_i, R_i)$, which is again a free R_i-Hopf algebra of the same rank as A_i, so we also conclude that G^* is finite free over S. The gluing morphisms bewteen such charts are dual to the corresponding gluing morphisms between the various $\operatorname{Spec} A_i$. This description also shows that $G^{**} = G$ via the local natural isomorphisms $\operatorname{Hom}_{R_i}(\operatorname{Hom}_{R_i}(A_i, R_i), R_i) \simeq A_i$ of finite free R_i-Hopf algebras.

Practically, this means that the theory over an arbitrary base is not terribly more complicated than the theory over a field as long as we work affine-locally and glue. For example, our computations of $(\mu_m)^*$ and $(\alpha_p)^*$ are essentially the same as before.

4 The functor of points

There is an alternative useful description of the Cartier dual: it represents the functor that sends a commutative finite group scheme to its group of characters. This description makes the Cartier dual a scheme-theoretic analogue of the Pontryagin dual for (abstract) finite abelian groups. The advantage of our original definition is that it gives an explicit construction of the Cartier dual, showing that it is representable by a finite locally free commutative group scheme, but the functorial definition is often more useful in practice.

Proposition 7. *Let G be a finite commutative group scheme over a base S. Then G^* represents the functor $T \mapsto \operatorname{Hom}_{T-\mathrm{Gp}}(G_T, \mathbb{G}_{m,T})$ on the category of S-schemes. Here, $\operatorname{Hom}_{T-\mathrm{Gp}}$ refers to homomorphisms of T-group schemes.*

Proof. It suffices to prove this when $S = \operatorname{Spec} R$ is affine, since we can cover a general base scheme by affines and glue. It also suffices to give a natural isomophism of functors $G^*(T) \simeq \operatorname{Hom}_{T-\mathrm{Gp}}(G_T, \mathbb{G}_{m,T})$ when T is the spectrum of an affine R-algebra, since the restriction of the two functors to this subcategory determines the functor of points for more general S-schemes, again by a covering argument. For this case, we follow [2, Section 14].

So let $S = \operatorname{Spec} R, T = \operatorname{Spec} B$, and $G = \operatorname{Spec} A$, where B is an R-algebra and A is a finite free R-Hopf algebra. Then $G^*(T) = G^*_T(T) = \operatorname{Hom}_{B-\mathrm{alg}}(A^*_B, B)$ (homomorphisms of B-algebras) and $\operatorname{Hom}_{T-\mathrm{Gp}}(G_T, \mathbb{G}_{m,T}) = \operatorname{Hom}_{B-\mathrm{Hopf}}(B[x, x^{-1}], A_B)$ (homomorphisms of B-Hopf algebras; recall that the Hopf algebra structure on $B[x, x^{-1}]$ is determined by $x \mapsto x \otimes x$). Our goal is to establish a bijection between these two Hom sets that is natural in B, and we will do this by identifying both sets with a certain subset of A_B.

We start by identifying $\operatorname{Hom}_{B-\mathrm{Hopf}}(B[x, x^{-1}], A_B)$ with a subset of A_R. Any element

$$\phi \in \operatorname{Hom}_{B-\mathrm{Hopf}}(B[x, x^{-1}], A_B)$$

is determined by $\alpha = \phi(T)$. Conversely, an arbitrary element $\alpha \in A_B$ determines a Hopf algebra homomorphism ϕ if and only if $\alpha \in A_B^\times$ and $c_B(\alpha) = \alpha \otimes \alpha$, where $c_B : A_B \to A_B \otimes A_B$ is the comultiplication associated to the group law on G_T. (Elements α satisfying $c_B(\alpha) = \alpha \otimes \alpha$ are called *grouplike*.) Therefore we may identify

$$\operatorname{Hom}_{B-\mathrm{Hopf}}(B[x, x^{-1}], A_B) = \{\alpha \in A_B^\times : c_T(\alpha) = \alpha \otimes \alpha\}.$$

We massage this description a bit. Let $\eta_T : A_B \to B$ be the B-algebra homomorphism associated to the unit map $T \to G_T$. We have a Cartesian diagram

$$\begin{array}{ccc} A_B & \xrightarrow{c_T} & A_B \otimes A_B \\ \downarrow{\scriptstyle \eta_T} & & \downarrow{\scriptstyle \eta_T \times \eta_T} \\ B & \longrightarrow & B \otimes_B B = B \end{array}$$

with the identification $B \otimes_B B = B$ given by $b_1 \otimes b_2 \mapsto b_1 b_2$. Therefore our two previous observations imply that $\eta_T(\alpha) \in B^\times$ and $\eta_T(\alpha)^2 = \eta_T(\alpha)$, hence $\eta_T(\alpha) = 1$. Conversely, suppose $\alpha \in A_B$ satisfies $\eta_T(\alpha) = 1$ and $c_T(\alpha) = \alpha \otimes \alpha$. Letting $i_T : A_B \to A_B$ be the antipode map, we have a commutative diagram

$$\begin{array}{ccc} A_B & \xrightarrow{c_T} & A_B \otimes_B A_B \\ \downarrow{\scriptstyle \eta_T} & & \downarrow{\scriptstyle a_1 \otimes a_2 \mapsto a_1 \cdot i_T(a_2)} \\ B & \longrightarrow & A_B \end{array}$$

as part of the Hopf algebra axioms. Tracing the image of α under this commutative diagram, we conclude that we must have $\alpha \cdot i_T(\alpha) = 1$, so $\alpha \in A_B^\times$. Hence, we may alternatively identify

$$\operatorname{Hom}_{B-\mathrm{Hopf}}(B[x, x^{-1}], A_B) = \{\alpha \in A_B : c_T(\alpha) = \alpha \otimes \alpha, \eta_T(\alpha) = 1\}.$$

These are the *grouplike elements that pull back to* 1.

Meanwhile, we consider which element of $\operatorname{Hom}_{B-\mathrm{mod}}(A_B^*, B)$ correspond to B-*algebra* homomorphisms, not just B-module homomorphisms. In order for a B-module homomorphism $\varphi : A_B^* \to B$ to be a B-algebra homomorphism, it is necessary and sufficient to require $\varphi(\eta_T^*(1)) = 1$, since $\eta_T^*(1)$ acts as the multiplicative unit in A_B^*, and that $\varphi(c^*(a_1^* \otimes a_2^*)) = \varphi(a_1^*)\varphi(a_2^*)$, preserving the multiplicative structure. There is a natural identification of A_B with its double dual $\operatorname{Hom}_{B-\mathrm{mod}}(A_B^*, B)$ sending $\alpha \in A_B$ to the homomorphism $a^* \mapsto a^*(\alpha)$. Identifying φ with an element $\alpha \in A_B$, the two requirements for φ to be an algebra homomorphism translate to requiring $\eta_T(\alpha) = 1$ and $c(\alpha) = \alpha \otimes \alpha$. We conclude that we have a natural bijection

$$\begin{aligned} G^*(T) = \operatorname{Hom}_{B-\mathrm{alg}}(A_B^*, B) &= \{\alpha \in A_B : c_T(\alpha) = \alpha \otimes \alpha, \eta_T(\alpha) = 1\} \\ &= \operatorname{Hom}_{B-\mathrm{Hopf}}(B[x, x^{-1}], A_B) = \operatorname{Hom}_{T-\mathrm{Gp}}(G_T, \mathbb{G}_{m,T}), \end{aligned}$$

as desired. This bijection is also a group isomorphism, where the group structure on both sides is identified with multiplication in $A_B^\times$. ■

Corollary 8. *The Cartier dual $(-)^*$ defines an additive dual equivalence on the category of finite commutative S-groups.*

Proof. Contravariant functoriality is clear, either from the direct construction or the functor of points. For additivity, it suffices to show that $(G \times_S H)^* \simeq G^* \times_S H^*$ naturally as group schemes for any finite commutative S-groups G and H. This follows immediately from the functor of points characterization of the Cartier dual. Since $(-)^*$ is its own essential inverse, it defines a dual equivalence of categories. ■

Example 9. If G is the constant group scheme associated to a finite abelian group of the form $\prod \mathbb{Z}/m_i\mathbb{Z}$, then $G^* = \prod \mu_{m_i}$.

Example 10. Let $f : A \to B$ be an isogeny of abelian schemes with dual $\hat{f} : \hat{B} \to \hat{A}$. Then the Weil pairing identifies $\ker f = (\ker \hat{f})^*$. For example, $A[n] = (\hat{A}[n])^*$. In characteristic p, we have $\ker F = (\ker \hat{V})^*$, where F is the Frobenius and $\hat{V}$ is the Verschiebung on the dual. For ordinary abelian varieties over an algebraically closed field of characteristic p, $\ker F$ is local while $\ker V$ is étale, and the Weil pairing in this case is the starting point for the construction of the canonical lifting for ordinary abelian varieties, along with the Serre-Tate Theorem; for more details see [1, Section 2].

References

[1] N. Katz. "Serre-Tate local moduli". In: *Algebraic surfaces (Orsay, 1976–78)*. Vol. 868. Lecture Notes in Math. Springer, Berlin, 1981, pp. 138–202. ISBN: 3-540-10842-4.

[2] David Mumford. *Abelian varieties*. Vol. 5. Tata Institute of Fundamental Research Studies in Mathematics. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition. Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008.