NOTES ON CARTIER DUALITY

Let k be a commutative ring with 1, and let $G = \mathrm{Spec}(A)$ be a commutative finite locally free group scheme over k. We have the following k-linear maps

$$\begin{array}{llll} \text{(unity)} & i\colon k \to A, & \text{(multiplication)} \quad m\colon A \otimes_k A \to A, & \text{(inverse)} \quad \tau\colon A \to A, \\ \text{(co-unity)} & \varepsilon\colon A \to k, & \text{(co-multiplication)} \quad \mu\colon A \to A \otimes_k A & \end{array}$$

satisfying the axioms for a commutative co-commutative Hopf algebra over k. Recall that A is a projective k-module of finite rank. Let $A' := \mathrm{Hom}_k(A,k)$. Dualizing the structure maps for A, we get k-linear maps

$$\begin{array}{llll} \text{(unity)} & i'\colon k \to A', & \text{(multiplication)} \quad m'\colon A \otimes_k A' \to A', & \text{(inverse)} \quad \tau'\colon A' \to A', \\ \text{(co-unity)} & \varepsilon'\colon A' \to k, & \text{(co-multiplication)} \quad \mu\colon A' \to A' \otimes_k A' & \end{array}$$

making A' a commutative co-commutative Hopf algebra over k. Here i' is the transpose of ε, m' is the transpose of μ, τ' is the transpose of τ, ε' is the transpose of i and μ' is the transpose of m. Let $\widehat{G} = \mathrm{Spec}(A')$ be the commutative finite locally free group scheme attached to A'.

For every commutative k-algebra R, we use a subscript R to denote the base-changed objects like $A_R := A \otimes_k R$, $A'_R = A' \otimes_k R = \mathrm{Hom}_R(A_R, R)$ and for morphisms like $\mu'_R\colon A'_R \to A'_R \otimes_R A'_R$, $\varepsilon'_R\colon A'_R \to R$. The set of R-valued points

$$G(R) = \mathrm{Hom}_{k\text{-alg}}(A,R) \hookrightarrow \mathrm{Hom}_k(R, A'_R) = A'_R$$

of G is identified with the set of all $\hat{\phi} \in A'_R$ satisfying the properties (i) and (ii) below.

(i) $\mu'_R(\hat{\phi}) = \hat{\phi} \otimes \hat{\phi} \ \in \ A'_R \otimes_R A'_R$

(ii) $\varepsilon'_R(\hat{\phi}) = 1 \ \in \ R$.

(ii)′ $\hat{\phi} \in (A'_R)^\times$.

Note that (i) says that the transpose $\phi\colon A_R \to R$ of $\hat{\phi}$ respects multiplication, while (ii) says that $\phi \circ i_R = \mathrm{id}_R$. So (i) and (ii) says that ϕ is an homomorphism of k-algebras. On the other hand, the set $\mathrm{Hom}_{R\text{-grp}}(\widehat{G} \times_{\mathrm{Spec}(k)} \mathrm{Spec}(R), \mathbb{G}_m \times \mathrm{Spec}R)$ of all R-homomorphisms from $\widehat{G} \times_{\mathrm{Spec}(k)} \mathrm{Spec}(R)$ to $\mathbb{G}_m \times \mathrm{Spec}R$ is naturally identified with the set of all elements $\hat{\phi} \in A'_R$ satisfying conditions (i) and (ii)′.

Lemma. Suppose that $\hat{\phi} \in A'_R$ satisfies (i). Then (ii) $\Longleftrightarrow$ (ii)′. In other words, $G(R)$ is in natural bijection with $\mathscr{H}om_k(G, \mathbb{G}_m)(R)$.

PROOF. (ii′) $\Longrightarrow$ (ii). Apply the identity ($1 \cdot 1 = 1$ in A_R)

$$(\varepsilon'_R \otimes \varepsilon'_R) \circ \mu'_R = \varepsilon'_R$$

to $\hat{\phi}$, we get

$$\varepsilon'_R(\hat{\phi})^2 = \varepsilon'_R(\hat{\phi})$$

Hence $\varepsilon'_R(\hat{\phi}) = 1$ because $\varepsilon'_R(\hat{\phi})$ is a unit in A'_R by (ii′).

(ii) $\Longrightarrow$ (ii′). Apply the identity (for the additive inverse in $\widehat{G}_R := \mathrm{Spec}(A'_R)$)

$$m'_R \circ (1_{A'} \otimes \tau'_R) \circ \mu'_R = i'_R \circ \varepsilon'_R$$

to $\hat{\phi}$, we get $\hat{\phi} \cdot \tau'_R(\hat{\phi}) = 1$ in A'_R. So $\hat{\phi}$ is a unit in A'_R. □

Apply the above Lemma to $\widehat{G}$, we see that sheaf $\mathscr{H}om_k(G,\mathbb{G}_m)$ of commutative groups over $\mathrm{Spec}(k)$ is representable, and naturally identified with $\widehat{G}=\mathrm{Spec}(A')$ (as schemes at this point). One can reformulate this as a morphism

$$\mathrm{can}_G\colon G\times_{\mathrm{Spec}(k)}\widehat{G}\longrightarrow \mathbb{G}_m\times\mathrm{Spec}(k)$$

obtained from the above Lemma applied to the tautological element in $G(A)$ with $R=A$. This morphism corresponds to the k-algebra homomorphism

$$k[T,T^{-1}]\longrightarrow A\otimes_k A'$$

which sends T to the "*diagonal element*" $\delta\in A\otimes_k A'$ which corresponds to Id_A. Since δ also corresponds to $\mathrm{Id}_{A'}$, the canonical morphism $\mathrm{can}_G\colon$ is naturally identified with $\mathrm{can}_{\widehat{G}}$. Moreover the Lemma tells us that

$$(\dagger)\qquad \mu'_A(\delta)=\delta\otimes_A\delta\in A\otimes_k A'\otimes_k A',\quad \varepsilon'_A(\delta)=i(1)\in A,\quad\text{and}\quad \delta\cdot\tau'_A(\delta)=1.$$

The same argument (because δ also correspond to the tautological element in $\widehat{G}(A')$ gives

$$(\ddagger)\qquad \mu_{A'}(\delta)=\delta\otimes_{A'}\delta\in A\otimes_k A\otimes_k A',\quad \varepsilon_{A'}(\delta)=i'(1)\in A'\quad\text{and}\quad \delta\cdot\tau_{A'}(\delta)=1.$$

Note that $\delta\otimes_A\delta$ is the product of $\mathrm{pr}_{12}(\delta)$ and $\mathrm{pr}_{13}(\delta)$ in $A\otimes_k A'\otimes_k A'$, and $\delta\otimes_{A'}\delta$ is the product of $\mathrm{pr}_{13}(\delta)$ and $\mathrm{pr}_{23}(\delta)$ in $A\otimes_k A\otimes_k A'$. The formulas (†) and (‡) gives the multiplicative inverse of δ in $A\otimes_k A'$, namely $\tau'_A(\delta)=\tau_{A'}(\delta)$. More importantly they also show that the canonical map $\mathrm{can}\colon G\times_{\mathrm{Spec}(k)}\widehat{G}\longrightarrow\mathbb{G}_m\times\mathrm{Spec}(k)$ is bi-multiplicative.

Example 1. Let H be an abstract commutative finite group. Write k^H for the set of all k-valued functions on H, and $k[H]$ be the group algebra of H over k. The delta functions δ_h at $h\in H$ form a k-basis of k^H, and we have $\delta_x\cdot\delta_y=\delta(x,y)\delta_x$ for all $x,y\in H$, where $\delta(x,y)$ denotes the Kronecker's symbol. The co-multiplication, co-unit and inverse in k^H are given by

$$\mu\colon\delta_h\mapsto\sum_{x,y\in H,\ x\cdot y=h}\delta_x\otimes\delta_y,\qquad \varepsilon\colon\delta_x\mapsto\delta(x,0)\,\delta_x,\qquad \tau\colon\delta_x\mapsto\delta_{-x}.$$

The group algebra $k[H]$ is best thought of as the convolution algebra of all k-valued measures on H, where the basis element $[h]$ corresponding to an element $h\in H$ is "evaluation at h". The co-multiplication, co-unit and inverse are given by

$$\mu'\colon[x]\mapsto[x]\otimes[x],\qquad \varepsilon'\colon[x]\mapsto 1,\qquad \tau'\colon[x]\mapsto[-x].$$

Some samples of the equalities in (†) and (‡) are:

$$\mu_{k[H]}\left(\sum_{x\in H}\delta_x\otimes[x]\right)=\sum_{y,z\in H}\delta_y\otimes\delta_z\otimes[y+z]=\left(\sum_{y\in H}\delta_y\otimes 1\otimes[y]\right)\cdot\left(1\otimes\sum_{z\in H}\delta_z\otimes 1\otimes[z]\right)$$

in $k^H\otimes_k k^H\otimes_k k[H]$,

$$\varepsilon_{k^H}\left(\sum_{x\in H}\delta_x\otimes[x]\right)=\sum_{x\in H}\delta_x=i_{k^H}(1)$$

in k^H, and

$$\left(\sum_{x\in H}\delta_x\otimes[x]\right)\cdot\left(\sum_{y\in H}\delta_y\otimes[y]\right)=\sum_{x,y\in H}\delta(x,y)\,\delta_x\otimes[x-y]=\left(\sum_x\delta_x\right)\otimes[0]=i_{k^H\otimes k[H]}(1)$$

in $k^H\otimes_k k[H]$. When $H=\mathbb{Z}/n\mathbb{Z}$ we have $\mathrm{Spec}(k[\mathbb{Z}/n\mathbb{Z}])=\mathrm{Spec}(k[T]/(T^n-1))=\mu_n\times\mathrm{Spec}(k)$.

Example 2. Let p be a prime number, $k \supset \mathbb{F}_p$ be a field, $G = \alpha_p \times \mathrm{Spec}(k) = \mathrm{Spec}(k[X]/(X^p))$. Let $x \in A = k[X]/(X^p)$ be the image of X in A. The co-multiplication and co-unity are determined by

$$\mu\colon x \mapsto x \otimes 1 + 1 \otimes x \qquad \text{and} \qquad \varepsilon\colon x \mapsto 0\,.$$

Let $y_0, y_1, \ldots, y_{p-1} \in A' = \mathrm{Hom}_k(A,k)$ be the dual basis of $1, x, x^2, \ldots, x^{p-1}$. Then we have

$$\mu'\colon y_i \mapsto \sum_{0 \le a \le i} y_a \otimes y_{i-a}\,, \qquad y_1^i = i!\, y_i \quad \forall i = 0,1,\ldots,p-1\,,\ y^p = 0\,.$$

Then $x \mapsto y_1$ establishes an isomorphism $A \cong A'$ of Hopf-algebras. The diagonal element

$$\delta = \sum_{i=0}^{p-1} x^i \otimes y_i \ \in\ A \otimes_k A'$$

is equal to

$$\exp(x \otimes y_1) = 1 + x \otimes y_1 + \frac{x^2 \otimes y_1^2}{2!} + \cdots + \frac{x^{p-1} \otimes y_1^{p-1}}{(p-1)!} = E_p(xy)\,,$$

where $E_p(T)$ is the truncated exponential

$$E_p(T) := 1 + T + \frac{T^2}{2!} + \cdots + \frac{T^{p-1}}{(p-1)!} \ \in\ k[T]$$

In other words, the formula $(x,y) \mapsto E(xy)$ gives an auto-duality pairing

$$\alpha_a \times \alpha_p \ \longrightarrow \mathbb{G}_m$$

which identifies α_p with its own Cartier dual.

Example 2′. Let $k \supset \mathbb{F}_p$ be a field of characteristic p. Let $\mathrm{Fr}_{p^n}\colon \mathbb{G}_m \times \mathrm{Spec}(k) \longrightarrow \mathbb{G}_m \times \mathrm{Spec}(k)$ be the Frobenius homomorphism defined by $X \mapsto X^{p^n}$. Denote by $\alpha_{p^n} = \mathrm{Spec}(k[X]/(X^{p^n}))$ the kernel of Fr_{p^n}. We have short exact sequences

$$0 \longrightarrow \alpha_{p^n} \xrightarrow{j_{n,n+m}} \alpha_{p^{n+m}} \xrightarrow{\beta_{n+m,m}} \alpha_{p^m} \longrightarrow 0$$

for positive integers m, n, where $j_{n,n+m}$ is the natural inclusion and $\beta_{n+m,m}$ is induced by Fr_{p^n}.

Write $A := k[X]/(X^{p^n})$ and let x be the image of X in A. Let $y_0, y_1, \ldots, y_{p^n-1}$ be the k-basis in $A' := \mathrm{Hom}_k(A,k)$ dual to the k-basis $1, x, x^2, \ldots, x^{p^n-1}$ of A. The co-multiplication on A is given by

$$\mu\colon x \mapsto x \otimes 1 + 1 \otimes x\,.$$

The co-multiplication, unity and co-unity on A' are given by

$$\mu'\colon y_i \mapsto \sum_{0 \le a \le i} y_a \otimes y_{i-a}\ \ i = 0,1,\ldots,p^n-1\,; \qquad i'\colon 1 \mapsto y_0\,, \qquad \varepsilon'\colon y_i \mapsto 0 \ \ \forall i > 0\,.$$

It is straight forward to deduce from $\mu(x) = x \otimes 1 + 1 \otimes x$ that

$$y_1^2 = 2y_2\,,\ \ y_1^3 = 3!\, y_3\,, \ldots, y_1^{p-1} = (p-1)! \cdot y_{p-1}\,,\ \ y_1^p = 0\,.$$

Similarly we have

$$y_{p^a}^j = j! \cdot y_{jp^a} \quad \text{and} \quad y_{p^a}^p = 0 \quad \forall a = 0,1,\ldots,n-1, \ \forall j = 0,1,\ldots,p-1\,.$$

More generally, for every natural number i with $0 \le i \le p^n - 1$, written in p-adic expansion in the form $i = \sum_{0\le a\le n-1} j_a\, p^a$, then

$$y_i = y_{j_0 + j_1 p + \cdots + j_{n-1}p^{n-1}} = \prod_{0\le a\le n-1} \frac{y_{p^a}^{j_a}}{j_a!}\,.$$

So A' is isomorphic to $k[Z_0, Z_1, \ldots, Z_{n-1}]/(Z_0^p, Z_1^p, Z_2^p, \ldots, Z_{n-1}^p)$ as k-algebras, such that y_{p^a} corresponds to the image of Z_a for $a = 0,1,\ldots,n-1$. The diagonal element

$$\delta = \sum_{i=0}^{p^n-1} x^i \otimes y_i \in A \otimes_k A' \cong k[X, Z_0, Z_1, \ldots, Z_{n-1}]/(X^{p^n}, Z_0^p, Z_1^p, \ldots, Z_{n-1}^p)$$

can be written in terms of the truncated exponential $E_p(T) = 1 + T + T^2/2! + \cdots + T^{p-1}/(p-1)!$ as the image of the polynomial

$$\delta(X, \underline{Z}) = \delta(X, Z_0, Z_1, \ldots, Z_{n-1}) = \prod_{a=0}^{n-1} E_p(X^{p^a} \cdot Z_a)$$

in $k[X, Z_0, Z_1, \ldots, Z_{n-1}]/(X^{p^n}, Z_0^p, Z_1^p, \ldots, Z_{n-1}^p)$. The group law of the Cartier dual $\widehat{\alpha_{p^{n-1}}}$ of α_{p^n} is completely determined by the polynomial $\delta(X, \underline{Z})$ as follows. Using $Z_0, Z_1, \ldots Z_{n-1}$ as the coordinates on $\widehat{\alpha_{p^{n-1}}}$, then the the sum of two points in $\widehat{\alpha_{p^n}}$ with coordinates $\underline{z} = (z_0, z_1, \ldots, z_{n-1})$, $\underline{w} = (w_0, w_1, \ldots, w_{n-1})$ is the point with coordinates $\underline{\Phi}(\underline{z}, \underline{w})$ where

$$\begin{array}{rcl} \underline{\Phi}(\underline{Z},\, \underline{W}) & = & (\Phi_0(\underline{Z},\, \underline{W}), \ldots, \Phi_{n-1}(\underline{Z}, \underline{W})) \\ & \in & \Big(k[Z_0, Z_1, \ldots, Z_{n-1}, W_0, W_1, \ldots, W_{n-1}]/(Z_0^p, \ldots, Z_{p-1}^p, W_0^p, \ldots, W_{n-1}^p)\Big)^n \end{array}$$

is determined by the equation

$$\prod_{a=0}^{n-1} E_p\left(X^{p^a}\, \Phi_a(\underline{Z}, \underline{W})\right) = \prod_{a=1}^{n-1} E_p\left(X^{p^a} \cdot Z_a\right) \cdot \prod_{a=1}^{n-1} E_p\left(X^{p^a} \cdot W_a\right)$$

in $k[X, Z_0, Z_1, \ldots, Z_{n-1}, W_0, W_1, \ldots, W_{n-1}]/(X^{p^n}, Z_0^p, \ldots, Z_{p-1}^p, W_0^p, \ldots, W_{n-1}^p)$. Notice that

$$E_p(XZ + XW) \equiv E_p(XZ) \cdot E_p(XW) \pmod{(X^p, Z^p, W^p)}\,,$$

but

$$E_p(X(Z_0 + W_0) + X^p(Z_1 + W_1)) \not\equiv E_p(XZ_0 + X^pZ_1) \cdot E_p(XW_0 + X^pW_1) \pmod{(X^{p^2}, Z_0^p, Z_1^p, W_0^p, W_1^p)}\,.$$

So the usual "exponential rule" does not hold for the truncated exponential when applied to rings like $k[X, Z_0, Z_1, W_0, W_1]/(X^{p^2}, Z_0^p, Z_1^p, W_0^p, W_1^p)$.

The Cartier dual of the homomorphism $\beta_{n+m,m}\colon \alpha_{p^{n+m}} \to \alpha_{p^m}$ induced by $\mathrm{Fr}_{p^n}\colon x \mapsto x^{p^n}$, the n-th power of the Frobenius, corresponds to the homomorphism

$$\beta'_{n+m,m}\colon k[Y_0, \ldots, Y_{n+m-1}]/(Y_0^p, \ldots, Y_{n+m-1}^p) \longrightarrow k[Y_0, \ldots, Y_{m-1}]/(Y_0^p, \ldots, Y_{m-1}^p)$$

of Hopf algebras such that

$$\beta'_{n+m,m}\colon Y_0,\dots,Y_{n-1}\ \mapsto\ 0\,;\qquad \beta'_{n+m,m}\colon Y_{n+a}\ \mapsto\ Y_a,\ a=0,\dots m-1\,.$$

Similarly the natural embedding $j_{n,n+m}\colon \alpha_{p^n}\ \hookrightarrow \alpha_{p^{n+m}}$ corresponds to the homomorphism

$$j'_{n,n+m}\colon k[Y_0,\dots,Y_{n-1}]/(Y_0^p,\dots,Y_{n-1}^p)k[Y_0,\dots,Y_{n+m-1}]/(Y_0^p,\dots,Y_{n+m-1}^p)$$

of Hopf algebras which sends each Y_a to Y_a for all $a=0,1,\dots,n-1$. Using the maps j'_{m_1,m_2} it is easy to see that for each natural number a with $0\le a\le n$, the a-th component $\Phi_a(\underline{Z},\ \underline{W})$ of the group law comes from a unique polynomial in $\mathbb{F}_p[Z_0,\dots,Z_a,W_0,\dots,W_a]$ independent of n whose degree in each variable is $\le p-1$. For instance

$$\Phi_0(\underline{Z},\ \underline{W})=Z_0+W_0,\qquad \Phi_1(\underline{Z},\ \underline{W})=Z_1+W_1+\sum_{i=1}^{p-1}\frac{Z_0^i}{i!}\cdot\frac{W_0^{p-i}}{(p-i)!}\,.$$