Title	Finite Group Schemes I(Deformations of Group Schemes and Number Theory)
Author(s)	Nakkajima{Nakajima}, Yukiyoshi
Citation	数理解析研究所講究録 (1996), 942: 1-13
Issue Date	1996-04
URL	http://hdl.handle.net/2433/60160
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

数理解析研究所講究録
942巻 1996年 1-13

Finite Group Schemes I

Yukiyoshi Nakkajima*

December 4, 1995

1 Introduction

In this report I give some definitions and state fundamental facts on group schemes which are used in [S], [Su] and [N]. The main topics of this report are exact sequences of commutative group schemes and Cartier duality of finite commutative group schemes. The proofs are not given here. I write this report mainly for persons who have not studied these topics. Fundamental results on group schemes can be seen in [SGA3 Tome 1,2,3], [DG], [Sh], [W] etc. To motivate the reader to study finite group schemes, I give a reason why finite group schemes are fundamental in the study of arithmetic geometry. Abelian schemes are very important objects in arithmetic geometry. We can get a p-divisible group from an abelian scheme which is an inverse limit of finite commutative group schemes. It is easier to study p-divisible groups rather than abelian schemes itself. I assume the reader is acquainted with fundamental facts about schemes which are written in [EGA I,II,III,IV] or [H]. But I sometimes review them for him. I hope this report is useful for him and encourage him to read books and papers on group schemes.

Acknowledgment I would like to express my gratitude to Professors T. Sekiguchi and N. Suwa for giving me an opportunity for making a survey of group schemes. I thank Doctor A. Shiho very much for pointing out some mistakes.

*Department of Mathematical Sciences of University of Tokyo, 3-8-1 Komaba Meguro-ku, Tokyo 153, Japan

2 Definition of group schemes

In this section we give the definition of group schemes over any base and formulate it in the view of Hopf algebras when they are affine over bases. Let S be a scheme and (Sch/S) be the category of the schemes over S. Let $G \in (\mathrm{Sch}/S)$, i.e. a morphism $\pi : G \longrightarrow S$, and $m : G \underset{S}{\times} G \longrightarrow G$, $e : S \longrightarrow G$, and $\mathrm{inv} : G \longrightarrow G$ be morphisms over S.

Definition 2.1. *1) A quadruplet (G, m, e, inv) (we often this simply by G) is called a group scheme over S if the following diagrams commute:*
a) (associative law)

$$\begin{array}{ccc} G \underset{S}{\times} G \underset{S}{\times} G & \xrightarrow{m\times 1} & G \underset{S}{\times} G \\ {\scriptstyle 1\times m}\downarrow & & \downarrow{\scriptstyle m} \\ G \underset{S}{\times} G & \xrightarrow[m]{} & G \end{array}$$

b) (unit)

$$\begin{array}{ccc} G \underset{S}{\times} S & \xrightarrow{1\times e} & G \underset{S}{\times} G \\ {\scriptstyle 1}\downarrow & & \downarrow{\scriptstyle m} \\ G & \xrightarrow[1]{} & G \end{array}$$

$$\begin{array}{ccc} S \underset{S}{\times} G & \xrightarrow{e\times 1} & G \underset{S}{\times} G \\ {\scriptstyle 1}\downarrow & & \downarrow{\scriptstyle m} \\ G & \xrightarrow[1]{} & G \end{array}$$

c) (inverse)

$$\begin{array}{ccc} G & \xrightarrow{(1,inv)} & G \underset{S}{\times} G \\ {\scriptstyle \pi}\downarrow & & \downarrow{\scriptstyle m} \\ S & \xrightarrow[e]{} & G \end{array}$$

$$\begin{array}{ccc} G & \xrightarrow{(inv,1)} & G \underset{S}{\times} G \\ {\scriptstyle \pi}\downarrow & & \downarrow{\scriptstyle m} \\ S & \xrightarrow[e]{} & G \end{array}$$

2) Let $G = (G, m, e, inv)$ be a group scheme over S. G is called commutative if the following diagram commutes:

$$\begin{array}{ccc} G \underset{S}{\times} G & \xrightarrow{twist} & G \underset{S}{\times} G \\ {\scriptstyle m}\downarrow & & \downarrow{\scriptstyle m} \\ G & \xrightarrow[1]{} & G \end{array}$$

Remark 2.2.

1) We do not use the word "abelian" in (2.1) 2) contrary to in the theory of abstract group theory, for it is used for the other objects stated in (3.1) 7) below.
2) Let G (resp. T) be a group scheme (resp. scheme) over S. Then the base change scheme $G \underset{S}{\times} T$ is a group scheme over T. Especially if we take T as a point of S, we obtain a group scheme over it and we can consider G/S as a family of group schemes with parameter space S.
3) Let G, H be group schemes over S. Then the fiber product $G \underset{S}{\times} H$ is naturally endowed with a group structure.
4) Let G and T be as in 2). We can consider G as a functor from (Sch/S) to the category of sets (Sets). The T-valued points $G(T) := \mathrm{Hom}_{S\text{-Sch}}(T, G)$ can be endowed with a group structure: a) The multiplication law is given as follows: $G(T) \times G(T) = (G \underset{S}{\times} G)(T) \xrightarrow{m} G(T)$. b) The unit element is $T = T \underset{S}{\times} S \xrightarrow{1\times e} T \underset{S}{\times} G$. Note that $G(T) = (G \underset{S}{\times} T)(T)$. c) The inverse is induced by inv. Then the commutative diagrams as in (2.1) correspond to a) $(ab)c = a(bc)$, b) $a \cdot 1 = a$, $1 \cdot a = a$, c) $aa^{-1} = 1$, $a^{-1}a = 1$ for $a, b, c \in G(T)$.

Next we consider an affine group scheme G over a scheme S. In general for affine schemes over S $f : X \longrightarrow S$, $g : Y \longrightarrow S$, we have the equality $\mathrm{Hom}_{S\text{-Sch}}(X, Y) = \mathrm{Hom}_{\mathcal{O}_S\text{-alg}}(g_*(\mathcal{O}_Y), f_*(\mathcal{O}_X))$ by [EGA II] Prop.(1.2.7). Let $\pi : G \longrightarrow S$ be the structure morphism and we put $\mathcal{A}(G) := \pi_*(\mathcal{O}_G)$, $\Delta := m^* : \mathcal{A}(G) \longrightarrow \mathcal{A}(G) \underset{\mathcal{O}_S}{\otimes} \mathcal{A}(G)$, $\varepsilon := e^* : \mathcal{A}(G) \longrightarrow \mathcal{O}_S$, and $a := \mathrm{inv}^* : \mathcal{A}(G) \longrightarrow \mathcal{A}(G)$. Then by the above general fact, the commutative diagrams in (2.1) correspond to the following commutative diagrams:
a) (coassociativity)

$$\begin{array}{ccc} \mathcal{A}(G) \underset{\mathcal{O}_S}{\otimes} \mathcal{A}(G) \underset{\mathcal{O}_S}{\otimes} \mathcal{A}(G) & \xleftarrow{\Delta\otimes 1} & \mathcal{A}(G) \underset{\mathcal{O}_S}{\otimes} \mathcal{A}(G) \\ \uparrow{\scriptstyle 1\otimes\Delta} & & \uparrow{\scriptstyle \Delta} \\ \mathcal{A}(G) \underset{\mathcal{O}_S}{\otimes} \mathcal{A}(G) & \xleftarrow[\Delta]{} & \mathcal{A}(G) \end{array}$$

b) (counit)

$$\begin{array}{ccc} \mathcal{A}(G) \underset{\mathcal{O}_S}{\otimes} \mathcal{O}_S & \xleftarrow{1\otimes\varepsilon} & \mathcal{A}(G) \underset{\mathcal{O}_S}{\otimes} \mathcal{A}(G) \\ \uparrow{\scriptstyle 1} & & \uparrow{\scriptstyle \Delta} \\ \mathcal{A}(G) & \xleftarrow[1]{} & \mathcal{A}(G) \end{array}$$

$$\begin{array}{ccc} \mathcal{O}_S \underset{\mathcal{O}_S}{\otimes} \mathcal{A}(G) & \xleftarrow{\varepsilon\otimes 1} & \mathcal{A}(G) \underset{\mathcal{O}_S}{\otimes} \mathcal{A}(G) \\ \uparrow{\scriptstyle 1} & & \uparrow{\scriptstyle \Delta} \\ \mathcal{A}(G) & \xleftarrow[1]{} & \mathcal{A}(G) \end{array}$$

c) (antipode)

$$\begin{array}{ccc} \mathcal{A}(G) & \xleftarrow{(1,a)} & \mathcal{A}(G) \underset{\mathcal{O}_S}{\otimes} \mathcal{A}(G) \\ \uparrow{\scriptstyle \pi^*} & & \uparrow{\scriptstyle \Delta} \\ \mathcal{O}_S & \xleftarrow[\varepsilon]{} & \mathcal{A}(G) \end{array}$$

$$\begin{array}{ccc} \mathcal{A}(G) & \xleftarrow{(a,1)} & \mathcal{A}(G) \underset{\mathcal{O}_S}{\otimes} \mathcal{A}(G) \\ \uparrow{\scriptstyle \pi^*} & & \uparrow{\scriptstyle \Delta} \\ \mathcal{O}_S & \xleftarrow[\varepsilon]{} & \mathcal{A}(G) \end{array}$$

Such $(\mathcal{A}(G), \Delta, \varepsilon, a)$ satisfying the above axioms a), b), and c) is called a (commutative) Hopf algebra over $\mathcal{O}_S$, Δ a comultiplication or coproduct, ε a counit and a an antipode (An antipode is usually written as S, but we use S as a base scheme, so that we denote it by a.)

3 Examples

We give examples of group schemes in this section.

Example 3.1.

1) Additive group scheme $\mathbb{G}_a$.
As a scheme $\mathbb{G}_a$ is a line over $\mathbb{Z}$, i.e. $\operatorname{Spec}\mathbb{Z}[X]$. The structure of the Hopf algebra is given as follows:

$$\mathbb{Z}[X] \ni X \overset{\Delta}{\longmapsto} X \otimes 1 + 1 \otimes X \in \mathbb{Z}[X]^{\otimes 2},$$
$$\mathbb{Z}[X] \ni X \overset{\varepsilon}{\longmapsto} 0 \in \mathbb{Z},$$
$$\mathbb{Z}[X] \ni X \overset{a}{\longmapsto} -X \in \mathbb{Z}[X].$$

The additive group scheme over a base scheme S is obtained by the base change $\mathbb{G}_{a/S} := \mathbb{G}_a \underset{\operatorname{Spec}\mathbb{Z}}{\times} S$.
2) (See [M] Lecture 26.) Witt scheme $\mathbb{W}_n$ ($n \in \mathbb{Z}_{\geq 1}$): A generalization of 1) .
The Witt scheme $\mathbb{W}_n$ is $\operatorname{Spec}\mathbb{Z}[X_0, \cdots, X_{n-1}]$ as a scheme. We consider n-th product of $\mathbb{G}_a$ $\mathbb{G}_a^n = \operatorname{Spec}\mathbb{Z}[W_0, \cdots, W_{n-1}]$ (Here we take W_i as coordinates of $\mathbb{G}_a$.) and a morphism $\mathbb{W}_n \longrightarrow \mathbb{G}_a^n$ given by $\mathbb{Z}[W_0, \cdots, W_{n-1}] \ni W_i \longmapsto X_0^{p^i} + pX_1^{p^{i-1}} + \cdots + p^i X_i \in \mathbb{Z}[X_0, \cdots, X_{n-1}]$. Since $\mathbb{W}_n \otimes \mathbb{Z}\left[\frac{1}{p}\right] \overset{\simeq}{\longrightarrow} \mathbb{G}_a^n \otimes \mathbb{Z}\left[\frac{1}{p}\right]$, the group structure on $\mathbb{G}_a^n \otimes \mathbb{Z}\left[\frac{1}{p}\right]$ induces that on $\mathbb{W}_n \otimes \mathbb{Z}\left[\frac{1}{p}\right]$. The following says that not only $\mathbb{W}_n \otimes \mathbb{Z}\left[\frac{1}{p}\right]$ but also $\mathbb{W}_n$ has a group structure.

Theorem (Witt). $\mathbb{W}_n$ has a unique group structure which induces the above on the dense open set $\mathbb{W}_n \otimes \mathbb{Z}\left[\frac{1}{p}\right]$.

This is the reformulation of the classical theorem of Witt [Se] §6 Th. 5. If the reader knows the theorem, he shall know that $\mathbb{W}_n$ has a not only group structure but also ring structure (The definition of ring schemes can be easily defined.). If n goes infinity, the group scheme $\mathbb{W}$ is obtained.
3) General linear group GL_n.
As a scheme GL_n is $\operatorname{Spec}\mathbb{Z}[X_{1,1}, \cdots, X_{n,n}]\left[\frac{1}{D}\right]$, where D is the determinant $\det(X_{i,j})$. The structure of Hopf algebra is given as follows:

$$\mathbb{Z}[X_{1,1}, \cdots, X_{n,n}]\left[\frac{1}{D}\right] \ni X_{ij} \overset{\Delta}{\longmapsto} \sum_{k=1}^{n} X_{ik} \otimes X_{kj} \in \mathbb{Z}[X_{1,1}, \cdots, X_{n,n}]\left[\frac{1}{D}\right]^{\otimes 2},$$

$$\mathbb{Z}[X_{1,1},\cdots,X_{n,n}]\left[\frac{1}{D}\right] \ni X_{ij} \overset{\varepsilon}{\longmapsto} \delta_{ij} \in \mathbb{Z},$$

$$\mathbb{Z}[X_{1,1},\cdots,X_{n,n}]\left[\frac{1}{D}\right] \ni X_{ij} \overset{a}{\longmapsto} \frac{A_{ij}}{D} \in \mathbb{Z}[X_{1,1},\cdots,X_{n,n}]\left[\frac{1}{D}\right],$$

where A_{ij} is the cofactor of the matrix (X_{ij}). Some closed subschemes of GL_n (e.g, SL_n, Sp_n) can be defined. GL_1 is denoted by $\mathbb{G}_m$.
4) Constant groups.
Let Γ be an abstract finite group. The functor

$$(\mathrm{Sch}/\mathbb{Z}) \ni T \longmapsto \Gamma \in (\mathrm{Groups})$$

is not representable. But the functor

$$(\mathrm{Sch}/\mathbb{Z}) \ni T \longmapsto \Gamma^{\pi_0(T)} \in (\mathrm{Groups})$$

is representable. The scheme which represents it is as follows: As a scheme it is the spectrum of the ring of the maps from Γ to $\mathbb{Z}$, in other words the group ring of Γ over $\mathbb{Z}$. We denote it by $\mathrm{Map}(\Gamma, \mathbb{Z})$. Since $\mathbb{Z}$ has a ring structure, $\mathrm{Map}(\Gamma, \mathbb{Z})$ also has the structure. $\mathrm{Map}(\Gamma, \mathbb{Z})$ is a free $\mathbb{Z}-$module of finite rank and $\mathrm{Map}(\Gamma, \mathbb{Z})\otimes\mathrm{Map}(\Gamma, \mathbb{Z})$ is canonically isomorphic to $\mathrm{Map}(\Gamma\times\Gamma, \mathbb{Z})$. Let f be an element of $\mathrm{Map}(\Gamma, \mathbb{Z})$ and $\sigma, \tau \in \Gamma$. Then the comultiplication, counit and antipode is given as follows:

$$(\Delta f)(\sigma,\tau) = f(\sigma\tau), \quad (\varepsilon f)(\sigma) = f(1), \quad (af)(\sigma) = f(\sigma^{-1}).$$

If one notes that $\mathrm{Map}(\Gamma, \mathbb{Z})$ has the idempotents $e_\sigma :=$ ((the characteristic function of σ)), and in general an idempotent of a structure sheaf of a scheme corresponds to a connected connected component of it, one sees that $\mathrm{Spec}\,(\mathrm{Map}(\Gamma, \mathbb{Z}))$ represents the functor

$$(\mathrm{Sch}/\mathbb{Z}) \ni T \longmapsto \Gamma^{\pi_0(T)} \in (\mathrm{Groups}).$$

5) Group scheme of n-th root of unity μ_n.
As a scheme $\mu_n = \mathrm{Spec}\,\mathbb{Z}[X]/(X^n - 1)$ ($n \in \mathbb{Z}_{>0}$). The Hopf algebra structure is the same of $\mathbb{G}_m$. In the notation of §4, $\mu_n = \mathrm{Ker}(\mathbb{G}_m \overset{n}{\longrightarrow} \mathbb{G}_m)$.
6) Let p be a prime number and S be a scheme of characteristic p.
Let $\alpha_{p^r} = \underline{\mathrm{Spec}}\,(\mathcal{O}_S[X]/(X^{p^r}))$ ($r \in \mathbb{Z}_{>0}$). The Hopf algebra structure is the same of $\mathbb{G}_a$. In the notation of §4, α_{p^r} is $\mathrm{Ker}(\mathbb{G}_a \overset{\mathrm{Fr}^r}{\longrightarrow} \mathbb{G}_a)$, where Fr is the Frobenius of $\mathbb{G}_a$, i.e. p-th power homomorphism.

7) Abelian schemes
Let $\mathcal{A}$ be a group scheme over a scheme S. $\mathcal{A}$ is called an abelian (group) scheme over S if it is proper and smooth over S whose geometric fibers are connected. It is one of the most important group schemes in arithmetic geometry.

The following theorem says that the study of a connected group variety reduces to that of an abelian variety, a closed variety of a general linear group and of an extension:

Theorem 3.2 (Chevalley). *Let k be a field and G be a connected group variety over k. Then there exists an extension of an abelian variety A by a connected closed normal subgroup variety H of G which can be embedded in $GL_{n/k}$ for some $n \in \mathbb{N}$ as a closed variety. (Exact sequences of group schemes are explained in §4.)*

4 Kernels and cokernels

The definition of the kernel is very easy. Let $f : G \longrightarrow H$ be a morphism of group schemes over a scheme S. Then $\mathrm{Ker}\, f$ is defined as the fiber product:

$$\begin{array}{ccc} \mathrm{Ker}\, f & \longrightarrow & S \\ \downarrow & & \downarrow \text{unit section} \\ G & \xrightarrow[f]{} & H. \end{array}$$

The definition of the cokernel of f is somewhat difficult. A naive question arises: Is the following contravariant functor

$$F : (\mathrm{Sch}/S) \ni T \longmapsto H(T)/f(G(T)) \in (\mathrm{Sets})$$

representable, i.e. does there exist a scheme $\mathcal{G}$ over S such that $\mathcal{G}(T) = H(T)/f(G(T))$ ($T \in (\mathrm{Sch}/S)$) in a functorial way? But this does not hold usually. Descent theory [SGA-1] Exposé VIII Cor.1.2 says that, if a contravariant functor F is representable, it must satisfy the following condition: For a faithfully flat and quasi-compact(=:f.p.q.c = fidèlment plat et quasi-compact in French) morphism of S-schemes $\coprod T_\alpha \longrightarrow T$:

$$(*) \qquad F(T) \longrightarrow \prod F(T_\alpha) \rightrightarrows \prod F(T_\beta \underset{T}{\times} T_\gamma).$$

is exact, i.e. $F(T)$ is isomorphic to the equalizer of $\rightrightarrows$. Let n be a natural number greater than 1 and let us consider $\mu_n \hookrightarrow \mathbb{G}_m$ over a field k which contains n-th root of unity. Let K be a Galois extension of k of finite degree d. If $\mathbb{G}_{m/k}/\mu_{n/k}$ is representable in the naive sense, the following sequence is exact by $(*)$ (we take a f.p.q.c morphism $\operatorname{Spec} K \longrightarrow \operatorname{Spec} k$).

$$k^*/\mu_n(k) \longrightarrow K^*/\mu_n(K) \rightrightarrows (K^*/\mu_n(K))^d.$$

One of the maps $\rightrightarrows$ is the diagonal embedding and the other is the map of the conjugations. We assume there exist an element of $a \in k$ such that n-th root of a is not contained in k. Then $\sqrt[n]{a}$ is an element of the equalizer of $\rightrightarrows$, but it is not an element of the image of $k^*/\mu_n(k)$.

(If one knows the etale topology of Grothendieck, he sees immediately that the naive idea is not right. In fact, if $\mathbb{G}_{m/k}/\mu_{n/k}$ is representable by a commutative group scheme $\mathcal{G}$ in the naive sense, we have an exact sequence

$$1 \longrightarrow \mu_{n/k} \longrightarrow \mathbb{G}_{m/k} \longrightarrow \mathcal{G} \longrightarrow 1$$

in the category of the abelian sheaves of the Zariski site on $\operatorname{Spec} k$, also of the etale site on $\operatorname{Spec} k$. The long exact sequence of the above sheaves on the etale topology and the Hilbert's theorem 90 ([SGA 4 Tome 3] Exp. IX Th.3.3) show $H^1_{\text{et}}(\operatorname{Spec} k, \mu_{n/k}) = 0$. But this is contrary to $H^1_{\text{et}}(\operatorname{Spec} k, \mu_{n/k}) = H^1(\operatorname{Gal}(k_s/k), \mu_n(k)) = k^*/(k^*)^n \neq 0$.)

If one takes every map $T_\alpha \longrightarrow T$ as an open immersion, the exactness of $(*)$ says that F is a sheaf on T. As stated above one should consider not only open immersions but also f.p.q.c morphisms and we take not only open coverings but also f.p.q.c. coverings as coverings of a scheme. We call a contravariant functor $G : (\mathrm{Sch}/S) \longrightarrow (\mathrm{Sets})$ a sheaf (to be more precise, sheaf of the f.p.q.c. topology on S) if $(*)$ for G instead of F is exact. (The author does not define the definition of the coverings and Grothendieck topology, but one should consult SGA 3 Exp. IV, SGA 4 Tome 1, or SGA $4\frac{1}{2}$ I.6 if one wants to know the f.p.q.c. sheaves well). Anyway, at last one can come to the definition of the cokernel:

Definition 4.1. *Let $f : H \longrightarrow G$ be a morphism of group schemes over S.* $\operatorname{Coker} f$ *is defined to be the cokernel of $H \overset{f}{\underset{e}{\rightrightarrows}} G$ in the category of the sheaves on S. Here e is the composite of the structure morphism of H/S and the unit section of G/S.*

The next problem is to give sufficient conditions for the representability of cokernels.

Theorem 4.2 ([R]). *Let G/S be a group scheme of finite type and H be a closed subgroup scheme of finite type. One of the following conditions is sufficient for the representability of G/H.*
1) S is artinean.
2) G is smooth over S and S is regular of dimension≤ 1.
3) G is quasi-projective and H is proper and flat.

Example 4.3.

1) Let n be a positive integer and S be a scheme. Then $\mathbb{G}_{m/S}/\mu_{n/S} \xrightarrow{\simeq} \mathbb{G}_{m/S}$.
2) Let p be a prime number and S be a scheme of characteristic $p > 0$. Then $\mathbb{W}_{n/S}/(\mathbb{Z}/p^n)_S \xrightarrow{\simeq}{}^{\mathrm{Fr}-1} \mathbb{W}_{n/S}$. Here Fr is the Frobenius(=p-th power homomorphism) of $\mathbb{W}_{n/S}$.
3) Examples given in [S] and [Su].
(If the reader knows the etale and f.p.p.f(=fidèlement plat et presentation fini in French, faithfully flat and of finite presentaion in English) topology , he sees the above are obtained by exact sequences of etale or f.p.p.f-sheaves (etale $\leq$ f.p.p.f $\leq$ f.p.q.c).)

5 Cartier duality

In this section Cartier duality for finite group schemes is explained. It is convenient sometimes for the reader to remember Pontrjagin duality for locally compact topological groups. First we must review the definition of finite group schemes.

Definition 5.1. *1) Let G/S be a group scheme. G is called finite if the structure sheaf $\mathcal{O}_G$ is a locally free $\mathcal{O}_S-$module of finite rank.*
2) Let G/S be a finite group scheme. Then the order function of G is defined as $rk_{\mathcal{O}_S}(\mathcal{O}_G) : \pi_0(S) \longrightarrow \mathbb{N}$. It is denoted by $\sharp G$.

Let G/S be a finite group scheme. Then $\mathcal{O}_G$ is a locally free $\mathcal{O}_S-$module of finite rank. We put $\mathcal{O}_G^D := \mathcal{H}om_{\mathcal{O}_S-\mathrm{mod}}(\mathcal{O}_G, \mathcal{O}_S)$. Let us recall the algebra structure and the Hopf-algebra structure of $\mathcal{O}_G$ in the left of the table below.

G	"G^D"
prod. of ring : $\mathcal{O}_G^{\otimes 2} \longrightarrow \mathcal{O}_G$	$\mathcal{O}_G^{D\otimes 2} \longleftarrow \mathcal{O}_G^D$; coproduct
stru. morph. : $\mathcal{O}_S \longrightarrow \mathcal{O}_G$	$\mathcal{O}_S \longleftarrow \mathcal{O}_G^D$; counit
coproduct; $\Delta : \mathcal{O}_G \longrightarrow \mathcal{O}_G^{\otimes 2}$	$\mathcal{O}_G^D \longleftarrow \mathcal{O}_G^{D\otimes 2}$; prod. of ring
counit; $\varepsilon : \mathcal{O}_G \longrightarrow \mathcal{O}_S$	$\mathcal{O}_G^D \longleftarrow \mathcal{O}_S$; structure morph.
antipode; $a : \mathcal{O}_G \longrightarrow \mathcal{O}_G$	$\mathcal{O}_G^D \longleftarrow \mathcal{O}_G^D$; antipode

Dualizing the left we obtained the right of the table. With these structures $\mathcal{O}_G^D$ defines a finite commutative group scheme:

Propositon 5.2 (Cartier duality). *Let G/S, H/S be finite commutative group schemes. Then the followings hold:*
1) $G^D = \underline{\mathrm{Spec}}(\mathcal{O}_G^D)$ is a finite commutative group scheme of order $\sharp G$.
2) $(G^D)^D = G$
3) $\mathrm{Hom}_S(G^D, H^D) = \mathrm{Hom}_S(H, G)$
4) $G^D = \underline{\mathrm{Hom}}(G, \mathbb{G}_{m/S})$, where $\underline{\mathrm{Hom}}(G, \mathbb{G}_{m/S})$ is the functor from (Sch/S) to (Ab) whose T-valued point $(T \in (\mathrm{Sch}/S))$ is $\mathrm{Hom}_{T-\mathrm{gp}}(G_T, \mathbb{G}_{m/T})$.
5) $(G \underset{S}{\times} H)^D = G^D \underset{S}{\times} H^D$.
6) $(G \underset{S}{\times} T)^D = G^D \underset{S}{\times} T$.
7) Let $1 \longrightarrow K \longrightarrow G \longrightarrow H \longrightarrow 1$ be an exact sequence of finite commutative group schemes over S. Then the sequence $1 \longleftarrow K^D \longleftarrow G^D \longleftarrow H^D \longleftarrow 1$ is exact.

Definition 5.3. *G^D is called the Cartier dual of G.*

If one shows something on the Cartier dual G^D, one often gets some information on G itself, e.g. extensions over nilpotent bases, the existence of Jordan-Hölder sequence in [R] Prop. (3.2.1) and etc.

Example 5.4.

1) $(\mathbb{Z}/n)^D = \mu_n$. If one remembers the Pontrjagin duality, it seems evident. To show it we (must ?) use (5.2) 4).
2) Examples given [OT] and [R1]. The author shall take these examples in [N] (3.8) 2).
3) We want to give dualities of Witt schemes. Before doing so, let us remember the Pontrjagin duality of the direct sum indexed by $\mathbb{N}$ of the real group $\mathbb{R}$. Let $\mathbb{C}_1$ be the Lie group of the complex numbers of absolute value 1. The pairing $\bigoplus_{\mathbb{N}} \mathbb{R} \times \prod_{\mathbb{N}} \mathbb{R} \ni (x, y) \longrightarrow e^{2\pi i \sum xy} \in \mathbb{C}_1$ gives

duality $\mathrm{Hom}(\bigoplus_{\mathrm{N}}\mathbb{R}, \mathbb{C}_1) \simeq \prod_{\mathrm{N}}\mathbb{R}$. Here $\sum(\cdot)$ is the sum of $\cdot \in \bigoplus_{\mathrm{N}}\mathbb{R}$. Formally $e^U = \prod_{n=1}^{\infty}(1-U^n)^{-\frac{\mu(n)}{n}}$, where μ is the Möbius function. Let p be a prime number. Mimicking the equation, we define the Artin-Hasse exponential $E_p(U)$ by $E_p(U) := \prod_{(n,p)=1}(1-U^n)^{-\frac{\mu(n)}{n}}$. As shown in [DG] Chap.V, §4, n°4, $E_p(U)$ has another expression $E_p(U) = \exp(\sum_{r=0}^{\infty}\frac{U^{p^r}}{p^r})$. Let $\mathcal{X} = (X_0, X_1, \cdots)$ be a sequence of variables. We define $E_p(U;\mathcal{X}) = E_p(UX_0)E_p(U^pX_1)E_p(U^{p^2}X_2)\cdots \in \mathbb{Z}_{(p)}[\mathcal{X}][[U]]^*$. As the classical exponential gives a group homomorphism

$$(\bigoplus_{\mathrm{N}}\mathbb{R}, +) \xrightarrow{e^{2\pi i(\cdot)}} \mathbb{C}_1,$$

$E_p(U;\cdot)$ does a homomorphism of group schemes

$$(\mathbb{W}_{\mathbb{Z}_{(p)}[[U]]}, +) \xrightarrow{E_p(U;\cdot)} \mathbb{G}_{m/\mathbb{Z}_{(p)}[[U]]}.$$

To avoid infinite sums, we consider a sub-functor $\widehat{\mathbb{W}}$ of $\mathbb{W}$ whose T-valued point is $\{(a_1, \cdots, a_n, \cdots) \in \mathbb{W}(T) | a_i = 0(\text{a.a}), a_i \in \Gamma(T, \mathcal{O}_T) : \text{nilpotent}\}$. $\widehat{\mathbb{W}}$ is an analogy of $\bigoplus_{\mathrm{N}}\mathbb{R}$. $\widehat{\mathbb{W}}$ is an ideal of $\mathbb{W}$ and for $a \in \widehat{\mathbb{W}}(T)$ ($T \in (\mathrm{Sch}/\mathbb{Z}_{(p)})$), $E_p(U;a)$ is a polynomial of U over $\Gamma(T, \mathcal{O}_T)$. Hence we have a pairing

$$\widehat{\mathbb{W}}_{\mathbb{Z}_{(p)}} \underset{\mathbb{Z}_{(p)}}{\times} \mathbb{W}_{\mathbb{Z}_{(p)}} \ni (a,b) \longmapsto E_p(1, a\cdot b) \in \mathbb{G}_{m/\mathbb{Z}_{(p)}}.$$

Here $\cdot$ between a and b means the multiplication of the Witt ring. Finally we have a duality which is used in [S]:

Theorem 5.5 ([DG] Chap.V, §4). *Let S be a scheme of characteristic p.*
1) The above pairing induces the isomorphism $(\mathbb{W}_{n/S})^D \simeq {}_{\mathrm{Fr}^n}\widehat{\mathbb{W}}_S$. Here ${}_{\mathrm{Fr}^n}\widehat{\mathbb{W}}_S := \mathrm{Ker}(\mathrm{Fr}^n : \widehat{\mathbb{W}}_S \longrightarrow \widehat{\mathbb{W}}_S)$.
2) The above pairing induces the isomorphism ${}_{\mathrm{Fr}^m}(\mathbb{W}_{n/S})^D \simeq {}_{\mathrm{Fr}^n}\mathbb{W}_{m/S}$. Here ${}_{\mathrm{Fr}^n}\mathbb{W}_{m/S} := \mathrm{Ker}(\mathrm{Fr}^n : \mathbb{W}_{m/S} \longrightarrow \mathbb{W}_{m/S})$.

Remark 5.6.

Note that $\mathbb{W}_{n/S}$ is not a finite scheme over S. $\mathbb{W}^D_{n/S}$ is defined as the functor $\underline{\mathrm{Hom}}(\mathbb{W}_{n/S}, \mathbb{G}_{m/S})$.

References

[DG] M. Demazure and P. Gabriel. *Groupes algébriques.* North-Holland Publ. Amsterdam, (1970).

[EGA I,II,III,IV] A. Grothendieck and J. Dieudonné. *Éléments de géométrie algébrique I,II,III,IV.* Publ. Math. IHES 4 (1960), 8 (1961), 11 (1961), 17 (1963), 20 (1964), 24 (1965), 28 (1966), 32 (1967).

[H] R. Hartshorne, *Algebraic Geometry.* G.T.M. 52, Springer-Verlag, (1977).

[M] D. Mumford. *Lectures on Curves on Algebraic Surfaces.* Annals of Math. Studies 59, Princeton Univ. Press.

[N] Y. Nakkajima. *Finite Group Schemes II.* In this volume.

[OT] F. Oort and J. Tate. *Group schemes of finite order.* Ann. Sci. École Norm. Sup.3, (1970), pp. 1-21.

[R] M. Raynaud. *Passage au quotient par une rélation d'équivalence plate.* Proceedings of a Conference on Local Fields, Driebergen, 1966. Springer-Verlag, 1967, pp.78-85

[R1] M. Raynaud. *Schémas en groupes de type* $(p, , \cdots, p)$. Bull. Soc. Math. Fr. 102, (1974), pp.241-280.

[S] T. Sekiguchi. *Kummer-Artin-Schreier-Witt theory II.* In this volume.

[Se] J.-P. Serre. *Corps Locaux.* Hermann, Paris (1968).

[SGA-1] A. Grothendieck et M. Raynaud. *Revetements étales et Groupe Fondamental.* Lecture Notes in Math. 224, Springer-Verlag, (1971).

[SGA-3 Tome 1,2,3] M. Demazure et A. Grothendieck. *Schemas en Groupes.* Lecture Notes in Math. 151,152,153, Springer-Verlag (1970).

[SGA-4 Tome 1, 3] M. Artin, A. Grothendieck et J.L. Verdier. *Théorie des Topos et Cohomologie Etales des Schéma.* Lecture Notes in Math. 269, 305, Springer-Verlag, (1972), (1973).

[SGA $4\frac{1}{2}$] P. Deligne. *Cohomologie Etale.* Lecture Notes in Math. 569, Springer-Verlag, (1971).

[Sh] S. S. Shatz. *Group Schemes, Formal Groups, and p-Dividible Groups.* In Arithmetic Geometry edited by G. Cornell and J.H. Silverman, Springer-Verlag, (1986), pp. 29-78.

[Su] N. Suwa. *Kummer-Artin-Schreier-Witt theory I.* In this volume.

[W] W. Waterhouse. *Introduction to Affine Group Schemes.* G.T.M. 66, Springer-Verlag, (1979).