Hiroshima Math. J.
42 (2012), 325–354

Artin-Schreier-Witt extensions and normal bases

Noriyuki Suwa

(Received August 17, 2010)
(Revised May 10, 2011)

Abstract. We establish the Artin-Schreier-Witt theory in connection with the unit group scheme of a group algebra, following a method presented by Serre in ⟨Groupes algébriques et corps de classes⟩. The argument is developed not only over a field but also over a ring, as generally as possible.

Introduction

The Kummer and Artin-Schreier theories are important items in the classical Galois theory to describe explicitly cyclic extensions of a field. We have an elementary way to verify the Kummer theory by the Lagrange resolvants. Serre [8, Ch.VI, 8] formulated this method, combining the normal basis theorem and the unit group scheme of a group algebra. His argument raises a problem if the following assertion holds true:

(A) Let Γ be a finite group and R a ring. Suppose given an affine group R-scheme G and a homomorphism $i : \Gamma \to G$. Then there exists a commutative diagram

$$\begin{tikzcd}
\Gamma \arrow[r] \arrow[d, "\wr"] & U(\Gamma)_R \arrow[d] \\
\Gamma \arrow[r, "i"] & G.
\end{tikzcd}$$

(For the notation, see Section 1.) As is mentioned by Serre, if (A) holds true, we obtain a conclusion:

(a) Let S/R be an unramified Galois extension with group Γ. If the Galois extension S/R has a normal basis, then there exists a cartesian diagram

$$\begin{tikzcd}
\operatorname{Spec} S \arrow[r] \arrow[d] & G \arrow[d] \\
\operatorname{Spec} R \arrow[r] & G/\Gamma.
\end{tikzcd}$$

2010 *Mathematics Subject Classification.* Primary 13B05; Secondary 14L15, 12G05.
Key words and phrases. Artin-Schreier-Witt extensions, Witt vectors, Artin-Hasse exponetial series.

In the previous article [9] we formulated Serre's argument in the framework of the group scheme theory, adding a problem if the following assertion holds true:

(B) Let Γ be a finite group and R a ring. Suppose given an affine group R-scheme G and a homomorphism $i : \Gamma \to G$. Then there exist a commutative diagram

$$\begin{tikzcd}
\Gamma \arrow[r, "i"] \arrow[d, "\wr"] & G \arrow[d] \\
\Gamma \arrow[r] & U(\Gamma)_R.
\end{tikzcd}$$

If (B) holds true, we obtain a conclusion:

(b) Let S/R be the unramified Galois extension with group Γ defined by a cartesian diagram

$$\begin{tikzcd}
\mathrm{Spec}\, S \arrow[r] \arrow[d] & G \arrow[d] \\
\mathrm{Spec}\, R \arrow[r] & G/\Gamma.
\end{tikzcd}$$

Then the Galois extension S/R has a normal basis.

We shall call the problems (A) and (B) *sculpture problem* and *embedding problem* respectively. In [9] we examined both the problems when Γ is a cyclic group:

(1) the Kummer theory (Proposition 2.2);
(2) the Kummer-Artin-Schreier theory (Proposition 2.6);
(3) the Artin-Schreier theory in characteristic $p > 0$ (Proposition 2.9);
(4) the quadratic-twisted Kummer theory of odd degree (Proposition 3.5);
(5) the quadratic-twisted Kummer theory of even degree (Proposition 3.11);
(6) the quadratic-twisted Kummer-Artin-Schreier theory (Proposition 4.3).

In this article we examine the Artin-Schreier-Witt theory in characteristic $p > 0$. In fact, it is verified that the sculpture and embedding problems are affirmative when R is a ring of characteristic p, Γ is a cyclic group of order p^n and $G = W_n$, the group scheme of Witt vectors of length n:

Main theorem = Theorem 2.5. *Let Γ be a cyclic group of order p^n. Then we have commutative diagrams of group schemes over $\mathbf{F}_p$ with exact rows*

$$\begin{tikzcd}
0 \arrow[r] & \Gamma \arrow[r] \arrow[d, "\wr"] & U(\Gamma)_{\mathbf{F}_p} \arrow[r] \arrow[d] & (U(\Gamma)/\Gamma)_{\mathbf{F}_p} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathbf{Z}/p^n\mathbf{Z} \arrow[r] & W_{n,\mathbf{F}_p} \arrow[r, "F-1"] & W_{n,\mathbf{F}_p} \arrow[r] & 0
\end{tikzcd}$$

and

$$\begin{tikzcd}
0 \arrow[r] & \mathbf{Z}/p^n\mathbf{Z} \arrow[r] \arrow[d, "\wr"] & W_{n,\mathbf{F}_p} \arrow[r, "F-1"] \arrow[d] & W_{n,\mathbf{F}_p} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \Gamma \arrow[r] & U(\Gamma)_{\mathbf{F}_p} \arrow[r] & (U(\Gamma)/\Gamma)_{\mathbf{F}_p} \arrow[r] & 0.
\end{tikzcd}$$

It is crucial to use a variant of the Artin-Hasse exponential series for construction of homomorphisms $U(\Gamma)_{\mathbf{F}_p} \to W_{n,\mathbf{F}_p}$ and $W_{n,\mathbf{F}_p} \to U(\Gamma)_{\mathbf{F}_p}$. It should be mentioned that Serre [8, Ch.VI, 9] gave an affirmative answer for the sculpture problem, using the Artin-Hasse exponential series.

Now we explain the organization of the article. In Section 1, we recall needed facts on Witt vectors and variants of the Artin-Hasse exponential series. In Section 2, we prove the main theorem after recalling Serre's argument. Section 3 presents a few examples of normal bases for Artin-Schreier-Witt extensions. We conclude the article, giving two remarks in Section 4. One is concerned with Noether's problem on the rationality of invariant function fields. The other is concerned with the sculpture and embedding problems for the Grothendieck resolution of a finite flat commutative group scheme.

Notation

Throughout the article, p denotes a prime number. For a group scheme G over a ring of characteristic p, we denote by $F : G \to G^{(p)}$ the Frobenius homomorphism of G.

For a ring R, $R^\times$ denotes the multiplicative group of invertible elements of R. A ring is commutative unless otherwise mentioned.

For a scheme X and a group scheme G over X, $H^1(X, G)$ denotes the set of isomorphism classes of right G-torsors over X. (For details we refer to Demazure-Gabriel [2, Ch.III, 4].)

1. Witt vectors and the Artin-Hasse exponential series

We start with reviewing relevant facts on Witt vectors and the Artin-Hasse exponential series. For details, see [2, Chap. V] or [4, Chap. III].

1.1. For each $r \geq 0$, we denote by $\Phi_r(\boldsymbol{T}) = \Phi_r(T_0, T_1, \dots, T_r)$ the so-called Witt polynomial

$$\Phi_r(\boldsymbol{T}) = T_0^{p^r} + pT_1^{p^{r-1}} + \cdots + p^rT_r$$

in $\mathbf{Z}[\boldsymbol{T}] = \mathbf{Z}[T_0, T_1, \ldots]$. We define polynomials

$$S_r(\boldsymbol{X}, \boldsymbol{Y}) = S_r(X_0, \ldots, X_r, Y_0, \ldots, Y_r)$$

in $\mathbf{Z}[\boldsymbol{X}, \boldsymbol{Y}] = \mathbf{Z}[X_0, X_1, \ldots, Y_0, Y_1, \ldots]$ inductively by

$$\Phi_r(S_0(\boldsymbol{X}, \boldsymbol{Y}), S_1(\boldsymbol{X}, \boldsymbol{Y}), \ldots, S_r(\boldsymbol{X}, \boldsymbol{Y})) = \Phi_r(\boldsymbol{X}) + \Phi_r(\boldsymbol{Y})$$

Then, as is well-known, the addition of the scheme of Witt vectors

$$W_{\mathbf{Z}} = \operatorname{Spec} \mathbf{Z}[T_0, T_1, T_2, \ldots]$$

is defined by

$$\begin{aligned}(T_0, T_1, T_2, \ldots) &\mapsto S(\boldsymbol{T} \otimes 1, 1 \otimes \boldsymbol{T}) \\ &= (S_0(\boldsymbol{T} \otimes 1, 1 \otimes \boldsymbol{T}), S_1(\boldsymbol{T} \otimes 1, 1 \otimes \boldsymbol{T}), S_2(\boldsymbol{T} \otimes 1, 1 \otimes \boldsymbol{T}), \ldots).\end{aligned}$$

The additive group scheme $W_{n,\mathbf{Z}}$ of Witt vectors of length n is also defined by

$$W_{n,\mathbf{Z}} = \operatorname{Spec} \mathbf{Z}[T_0, T_1, \ldots, T_{n-1}]$$

with the addition

$$\begin{aligned}&(T_0, T_1, \ldots, T_{n-1}) \\ &\quad\mapsto (S_0(\boldsymbol{T} \otimes 1, 1 \otimes \boldsymbol{T}), S_1(\boldsymbol{T} \otimes 1, 1 \otimes \boldsymbol{T}), \ldots, S_{n-1}(\boldsymbol{T} \otimes 1, 1 \otimes \boldsymbol{T})).\end{aligned}$$

The Frobenius endomorphism

$$F : W_{n,\mathbf{F}_p} = \operatorname{Spec} \mathbf{F}_p[T_0, T_1, \ldots, T_{n-1}] \to W_{n,\mathbf{F}_p} = \operatorname{Spec} \mathbf{F}_p[T_0, T_1, \ldots, T_{n-1}]$$

is given by

$$(T_0, T_1, \ldots, T_{n-1}) \mapsto (T_0^p, T_1^p, \ldots, T_{n-1}^p).$$

1.2. Recall now the definition of the Artin-Hasse exponential series

$$E_p(T) = \exp\left(\sum_{r\geq 0} \frac{T^{p^r}}{p^r}\right) \in \mathbf{Z}_{(p)}[[T]].$$

For $\boldsymbol{U} = (U_r)_{r\geq 0}$, put

$$E_p(\boldsymbol{U}; T) = \prod_{r\geq 0} E_p(U_r T^{p^r}) = \exp\left(\sum_{r\geq 0} \frac{1}{p^r} \Phi_r(\boldsymbol{U}) T^{p^r}\right).$$

It is readily seen that

$$E_p(\boldsymbol{U}; T) E_p(\boldsymbol{V}; T) = E_p(S(\boldsymbol{U}, \boldsymbol{V}); T).$$

Let R be a $\mathbf{Z}_{(p)}$-algebra and $\boldsymbol{a} = (a_0, a_1, a_2, \dots) \in W(R)$. A formal power series $E_p(\boldsymbol{a}; T) \in R[[T]]$ is defined by

$$E_p(\boldsymbol{a}; T) = \prod_{k=0}^{\infty} E_p(a_k T^{p^k}).$$

For $\boldsymbol{a}, \boldsymbol{b} \in W(R)$, we have a functional equation

$$E_p(\boldsymbol{a} + \boldsymbol{b}; T) = E_p(\boldsymbol{a}; T) E_p(\boldsymbol{b}; T).$$

Let $F(T) \in R[[T]]^{\times}$. Then $F(T)$ is expressed uniquely in the form

$$c \prod_{j=1}^{\infty} E_p(a_j; T^j) \text{ with } c \in R^{\times} \text{ and } a_j \in R \text{ for } j \geq 1.$$

For each positive integer j prime to p, put $\boldsymbol{a}_j = (a_j, a_{pj}, a_{p^2 j}, \dots) \in W(R)$. Then we obtain a factorization

$$F(T) = c \prod_{(j,p)=1} E_p(\boldsymbol{a}_j; T^j) \text{ with } c \in R^{\times} \text{ and } \boldsymbol{a}_j \in W(R) \text{ for } j \geq 1,\ (j,p) = 1.$$

The correspondence

$$F(T) = c \prod_{(j,p)=1} E_p(\boldsymbol{a}_j; T^j) \mapsto (c, (\boldsymbol{a}_j)_{(j,p)=1})$$

gives rise to an isomorphism of groups $R[[T]]^{\times} \xrightarrow{\sim} R^{\times} \times W(R)^{\mathbf{N}}$.

Now we generalize the argument mentioned above. For details we refer to [7, Section 2].

1.3. Define a formal power series $E_p(U, \Lambda; T)$ in $\mathbf{Q}[U, \Lambda][[T]]$ by

$$E_p(U, \Lambda; T) = (1 + \Lambda T)^{U/\Lambda} \prod_{k=1}^{\infty} (1 + \Lambda^{p^k} T^{p^k})^{(1/p^k)\{(U/\Lambda)^{p^k} - (U/\Lambda)^{p^{k-1}}\}}.$$

Then we have

$$E_p(U, \Lambda; T) = \begin{cases} \displaystyle\prod_{(k,p)=1} E_p(U\Lambda^{k-1} T^k)^{(-1)^{k-1}/k} & \text{if } p > 2, \\ \displaystyle\prod_{(k,2)=1} [E_p(U\Lambda^{k-1} T^k) E_p(U\Lambda^{2k-1} T^{2k})^{-1}]^{1/k} & \text{if } p = 2. \end{cases}$$

It follows that the formal power series $E_p(U, \Lambda; T)$ has its coefficients in $\mathbf{Z}_{(p)}[U, \Lambda]$.

Let R be a $\mathbf{Z}_{(p)}$-algebra and $a, \lambda \in R$. We define a formal power series $E_p(a, \lambda; T)$ in $R[[T]]$ by

$$E_p(a, \lambda; T) = \begin{cases} \prod_{(k,p)=1} E_p(a\lambda^{k-1}T^k)^{(-1)^{k-1}/k} & \text{if } p > 2, \\ \prod_{(k,2)=1} [E_p(a\lambda^{k-1}T^k)E_p(a\lambda^{2k-1}T^{2k})^{-1}]^{1/k} & \text{if } p = 2. \end{cases}$$

For example, we have
(1) $E_p(1, 0; T) = E_p(T)$;
(2) $E_p(1, 1; T) = 1 + T$.

Furthermore, for $\lambda \in R$ and $\boldsymbol{a} = (a_0, a_1, a_2, \dots) \in W(R)$, we define a formal power series $E_p(\boldsymbol{a}, \lambda; T) \in R[[T]]$ by

$$E_p(\boldsymbol{a}, \lambda; T) = \prod_{k=0}^{\infty} E_p(a_k, \lambda^{p^k}; T^{p^k}).$$

For $\boldsymbol{a}, \boldsymbol{b} \in W(R)$, we have a functional equation

$$E_p(\boldsymbol{a} + \boldsymbol{b}, \lambda; T) = E_p(\boldsymbol{a}, \lambda; T)E_p(\boldsymbol{b}, \lambda; T).$$

Let $F(T) \in R[[T]]^{\times}$. Then $F(T)$ is expressed uniquely in the form

$$c \prod_{(j,p)=1} E_p(\boldsymbol{a}_j, \lambda^j; T^j) \text{ with } c \in R^{\times} \text{ and } \boldsymbol{a}_j \in W(R) \text{ for } j \geq 1,\ (j, p) = 1.$$

It is verified also that that the correspondence

$$F(T) = c \prod_{(j,p)=1} E_p(\boldsymbol{a}_j, \lambda^j; T^j) \mapsto (c, (\boldsymbol{a}_j)_{(j,p)=1})$$

gives rise to an isomorphism of groups $R[[T]]^{\times} \xrightarrow{\sim} R^{\times} \times W(R)^{\mathbf{N}}$.

Remark 1.4. The formal power series $E_p(U, 1; T)$ was introduced by Dwork [3, Section 1] as $F(t, Y)$. Furthermore he proved that $E_p(U, 1; T) \in \mathbf{Z}_{(p)}[U][[T]]$ by a different method.

1.5. Put $A = \mathbf{Z}[T]/(T^N)$. Then the Weil restriction $G = \prod_{A/\mathbf{Z}} \mathbf{G}_{m,A}$ is represented by the affine scheme

$$\operatorname{Spec} \mathbf{Z}\left[U_0, U_1, \dots, U_{N-1}, \frac{1}{U_0}\right]$$

with multiplication

$$U_k \mapsto \sum_{i+j=k} U_i \otimes U_j \qquad (0 \leq k < N).$$

Let R be a $\mathbf{Z}_{(p)}$-algebra. Then $F(T) \in (R[T]/(T^N))^\times$ is expressed uniquely in the form

$$F(T) = c \prod_{\substack{1 \le j < N \\ (j,p)=1}} E_p(\boldsymbol{a}_j, \lambda^j; T^j) \bmod T^N,$$

where $c \in R^\times$ and $\boldsymbol{a}_j \in W_k(R)$ if j is prime to p and $p^{k-1} < N/j \le p^k$. Here the formal power series $E_p(\boldsymbol{a}, \lambda; T)$ for $\boldsymbol{a} = (a_0, a_1, \dots, a_{n-1}) \in W_n(R)$ is defined by

$$E_p(\boldsymbol{a}, \lambda; T) = \prod_{k=0}^{n-1} E_p(a_k, \lambda^{p^k}; T^{p^k}).$$

For j with $1 \le j < N$ and $(j,p) = 1$, we put $U_j = W_{k,\mathbf{Z}_{(p)}}$ if $p^{k-1} < N/j \le p^k$. Then the correspondence

$$F(T) = c \prod_{\substack{1 \le j < N \\ (j,p)=1}} E_p(\boldsymbol{a}_j, \lambda^j; T^j) \mapsto (c, (\boldsymbol{a}_j)_{\substack{1 \le j < N \\ (j,p)=1}})$$

gives rise to an isomorphism of groups

$$\chi_R^{(\lambda)} : G(R) = (R[T]/(T^N))^\times \xrightarrow{\sim} R^\times \times \prod_{\substack{1 \le j < N \\ (j,p)=1}} U_j(R).$$

The map $\chi_R^{(\lambda)}$ is represented by an isomorphism of group schemes over $\mathbf{Z}_{(p)}$

$$\chi^{(\lambda)} : G_{\mathbf{Z}_{(p)}} = \left(\prod_{A/\mathbf{Z}} \mathbf{G}_{m,A} \right) \otimes_{\mathbf{Z}} \mathbf{Z}_{(p)} \xrightarrow{\sim} \mathbf{G}_{m,\mathbf{Z}_{(p)}} \times \prod_{\substack{1 \le j < N \\ (j,p)=1}} U_j.$$

In fact, a homomorphism of group schemes

$$\varepsilon : G = \prod_{A/\mathbf{Z}} \mathbf{G}_{m,A} = \operatorname{Spec} \mathbf{Z}\left[U_0, U_1, \dots, U_{N-1}, \frac{1}{U_0}\right] \to \mathbf{G}_{m,\mathbf{Z}} = \operatorname{Spec} \mathbf{Z}\left[U, \frac{1}{U}\right]$$

is defined by $U \mapsto U_0$.

Consider now the factorization

$$U_0 + U_1 T + U_2 T^2 + \cdots + U_{N-1} T^{N-1} = U_0 \prod_{j=1}^{N-1} E_p(c_j(\boldsymbol{U}), \lambda^j; T^j)$$

in $\left(\mathbf{Z}_{(p)}\left[U_0, U_1, \dots, U_{N-1}, \dfrac{1}{U_0}\right]\Big/(T^N)\right)^{\times}$. Here

$$c_j(\boldsymbol{U}) = c\left(\frac{U_1}{U_0}, \frac{U_2}{U_0}, \dots, \frac{U_j}{U_0}\right) \in \mathbf{Z}_{(p)}\left[\frac{U_1}{U_0}, \frac{U_2}{U_0}, \dots, \frac{U_j}{U_0}\right].$$

Then a homomorphism of group schemes

$$\chi_j^{(\lambda)} : G_{\mathbf{Z}_{(p)}} = \left(\prod_{A/\mathbf{Z}} \mathbf{G}_{m,A}\right) \otimes_{\mathbf{Z}} \mathbf{Z}_{(p)} = \operatorname{Spec} \mathbf{Z}_{(p)}\left[U_0, U_1, \dots, U_{N-1}, \frac{1}{U_0}\right]$$
$$\to U_{j,R} = W_{k,R} = \operatorname{Spec} \mathbf{Z}_{(p)}[X_0, X_1, \dots, X_{k-1}]$$

is defined by

$$(X_0, X_1, \dots, X_{k-1}) \mapsto (c_j(\boldsymbol{U}), c_{pj}(\boldsymbol{U}), \dots, c_{p^{k-1}j}(\boldsymbol{U})).$$

At last, we obtain an isomorphism of group schemes

$$\chi^{(\lambda)} = ((\varepsilon, (\chi_j^{(\lambda)})_{\substack{1 \le j < N \\ (j,p)=1}}) : G_{\mathbf{Z}_{(p)}} \xrightarrow{\sim} \mathbf{G}_{m,\mathbf{Z}_{(p)}} \times \prod_{\substack{1 \le j < N \\ (j,p)=1}} U_{j,\mathbf{Z}_{(p)}}.$$

2. Main theorem

First we recall the argument of Serre [8, Ch.VI, 8] in terms of the group scheme theory. We refer to [9, Section 1] for details.

2.1. Let Γ be a finite group. The functor $R \mapsto R[\Gamma]$ is represented by the ring scheme $A(\Gamma)$ defined by

$$A(\Gamma) = \operatorname{Spec} \mathbf{Z}[T_\gamma; \gamma \in \Gamma]$$

with
(a) the addition: $T_\gamma \mapsto T_\gamma \otimes 1 + 1 \otimes T_\gamma$;
(b) the multiplication: $T_\gamma \mapsto \sum_{\gamma'\gamma''=\gamma} T_{\gamma'} \otimes T_{\gamma''}$.

Put now

$$U(\Gamma) = \operatorname{Spec} \mathbf{Z}\left[T_\gamma, \frac{1}{\Delta_\Gamma}; \gamma \in \Gamma\right],$$

where $\Delta_\Gamma = \det(T_{\gamma\gamma'})$ denotes the determinant of the matrix $(T_{\gamma\gamma'})_{\gamma,\gamma' \in \Gamma}$ (the group determinant of Γ). Then $U(\Gamma)$ is an open subscheme of $A(\Gamma)$, and the functor $\Gamma \mapsto R[\Gamma]^{\times}$ is represented by the group scheme $U(\Gamma)$.

We denote also by Γ, for the abbreviation, the constant group scheme defined by Γ. More precisely, $\Gamma = \operatorname{Spec} \mathbf{Z}^{\Gamma}$ and the law of multiplication is defined by $e_{\gamma} \mapsto \sum_{\gamma'\gamma''=\gamma} e_{\gamma'} \otimes e_{\gamma''}$. Here $\mathbf{Z}^{\Gamma}$ denotes the functions from Γ to $\mathbf{Z}$, and $(e_{\gamma})_{\gamma \in \Gamma}$ is a basis of $\mathbf{Z}^{\Gamma}$ over $\mathbf{Z}$ defined by

$$e_{\gamma}(\gamma') = \begin{cases} 1 & (\gamma' = \gamma) \\ 0 & (\gamma' \neq \gamma). \end{cases}$$

The canonical injection $\Gamma \to R[\Gamma]^{\times}$ is represented by the homomorphism of group schemes $i : \Gamma \to U(\Gamma)$, which is defined by

$$T_{\gamma} \mapsto e_{\gamma} : \mathbf{Z}\left[T_{\gamma}, \frac{1}{\Delta_{\Gamma}}\right] \to \mathbf{Z}^{\Gamma}.$$

It is readily seen that $\Gamma \to U(\Gamma)$ is a closed immersion. Moreover the right multiplication by $\gamma \in \Gamma$ on $U(\Gamma)$ is defined by the automorphism $\gamma : T_{\gamma'} \mapsto T_{\gamma'\gamma^{-1}}$ of $\mathbf{Z}[T_{\gamma}, 1/\Delta_{\Gamma}]$.

Terminology 2.2. Let R be a ring, Γ a finite group and S an R-algebra. We shall say that:

(1) S/R is an *unramified Galois extension with group* Γ if $\operatorname{Spec} S$ has a structure of right Γ-torsor over $\operatorname{Spec} R$;

(2) an unramified Galois extension S/R with group Γ has a *normal basis* if there exists $s \in S$ such that $(\gamma s)_{\gamma \in \Gamma}$ is a basis of R-module S.

In particular, an unramified Galois extension S/R with group Γ is called an *unramified cyclic extension of degree* n if Γ is a cyclic group of order n.

2.3. Let R be a ring and Γ a finite group. Then the exact sequence

$$1 \to \Gamma \to U(\Gamma) \to U(\Gamma)/\Gamma \to 1$$

yields an exact sequence of pointed sets

$$U(\Gamma)(R) \to (U(\Gamma)/\Gamma)(R) \to H^1(R, \Gamma) \to H^1(R, U(\Gamma))$$

(cf. [2, Ch.III, 4.4]). Furthermore, an unramified Galois extension S/R with group Γ has a normal basis if and only if the class $[S]$ in $H^1(R, \Gamma)$ is contained in $\operatorname{Ker}[H^1(R, \Gamma) \to H^1(R, U(\Gamma))]$ ([9, 1.8]).

More concretely, let R be a ring, Γ a finite group and S/R an unramified Galois extension with group Γ. Then the Galois extension S/R has a normal basis if and only if there exist morphisms Spec $S \to U(\Gamma)$ and Spec $R \to U(\Gamma)/\Gamma$ such that the diagram

$$\begin{tikzcd}
\operatorname{Spec} S \arrow[r] \arrow[d] & U(\Gamma) \arrow[d] \\
\operatorname{Spec} R \arrow[r] & U(\Gamma)/\Gamma
\end{tikzcd}$$

is cartesian.

2.4. Let Γ be a cyclic group of order p^n, and take a generator γ of Γ. Let R be an $\mathbf{F}_p$-algebra. Then $\sum_{k=0}^{p^n-1} a_k\gamma^k \in R[\Gamma]$ is invertible if and only if $\sum_{k=0}^{p^n-1} a_k$ is invertible in R. Hence the functor $R \mapsto R[\Gamma]^\times$ is represented by the affine group scheme

$$U(\Gamma)_{\mathbf{F}_p} = \operatorname{Spec} \mathbf{F}_p\left[T_0, T_1, \dots, T_{p^n-1}, \frac{1}{T_0 + T_1 + \cdots + T_{p^n-1}}\right]$$

with multiplication

$$T_k \mapsto \sum_{\substack{i+j \equiv k \\ \bmod p^n}} T_i \otimes T_j \qquad (0 \le k < p^n).$$

For an $\mathbf{F}_p$-algebra R, the correspondence $\gamma \mapsto 1 + T$ gives rise to an isomorphism of multiplicative groups $\xi_R : R[\Gamma]^\times \xrightarrow{\sim} (R[T]/(T^{p^n}))^\times$. The map ξ_R is represented by the isomorphism of group schemes over $\mathbf{F}_p$

$$\begin{aligned}
\xi : U(\Gamma)_{\mathbf{F}_p} &= \operatorname{Spec} \mathbf{F}_p\left[T_0, T_1, \dots, T_{p^n-1}, \frac{1}{T_0 + T_1 + \cdots + T_{p^n-1}}\right] \\
&\xrightarrow{\sim} \left(\prod_{A/\mathbf{Z}} \mathbf{G}_{m,A}\right) \otimes_{\mathbf{Z}} \mathbf{F}_p = \operatorname{Spec} \mathbf{F}_p\left[U_0, U_1, \dots, U_{p^n-1}, \frac{1}{U_0}\right]
\end{aligned}$$

defined by

$$U_k \mapsto \sum_{j=k}^{p^n-1} \binom{j}{k} T_j \qquad (0 \le k < p^n).$$

In fact, we have

$$\xi_R\left(\sum_{k=0}^{p^n-1} a_k\gamma^k\right) = \sum_{k=0}^{p^n-1} a_k(1+T)^k = \sum_{k=0}^{p^n-1}\left\{\sum_{j=k}^{p^n-1}\binom{j}{k}a_j\right\}T^k.$$

Moreover the inverse of ξ is given by

$$T_j \mapsto \sum_{k=j}^{p^n-1} (-1)^{k-j} \binom{k}{j} U_k :$$

$$\mathbf{F}_p\left[T_0, T_1, \dots, T_{p^n-1}, \frac{1}{T_0 + T_1 + \cdots + T_{p^n-1}}\right] \to \mathbf{F}_p\left[U_0, U_1, \dots, U_{N-1}, \frac{1}{U_0}\right].$$

Taking $N = p^n$ and $\lambda = 1$ in 1.5, we obtain also an isomorphism of group schemes over $\mathbf{F}_p$

$$\chi = \chi^{(1)} : G_{\mathbf{F}_p} = \left(\prod_{A/\mathbf{Z}} \mathbf{G}_{m,A}\right) \otimes_{\mathbf{Z}} \mathbf{F}_p \xrightarrow{\sim} \mathbf{G}_{m,\mathbf{F}_p} \times \prod_{\substack{1 \le j < p^n \\ (j,p)=1}} U_{j,\mathbf{F}_p}.$$

In particular, we have a homomorphism of group schemes

$$\chi_1 : G_{\mathbf{F}_p} = \left(\prod_{A/\mathbf{Z}} \mathbf{G}_{m,A}\right) \otimes_{\mathbf{Z}} \mathbf{F}_p \overset{\chi}{\xrightarrow{\sim}} \mathbf{G}_{m,\mathbf{F}_p} \times \prod_{\substack{1 \le j < p^n \\ (j,p)=1}} U_{j,\mathbf{F}_p} \xrightarrow{\substack{\text{canonical} \\ \text{projection}}} U_{1,\mathbf{F}_p} = W_{n,\mathbf{F}_p}.$$

We define also a homomorphism of group schemes over $\mathbf{F}_p$

$$\sigma_1 : W_{n,\mathbf{F}_p} \to G_{\mathbf{F}_p} = \left(\prod_{A/\mathbf{Z}} \mathbf{G}_{m,A}\right) \otimes_{\mathbf{Z}} \mathbf{F}_p$$

as the composite

$$W_{n,\mathbf{F}_p} = U_{1,\mathbf{F}_p} \xrightarrow{\substack{\text{canonical} \\ \text{injection}}} \mathbf{G}_{m,\mathbf{F}_p} \times \prod_{\substack{1 \le j < p^n \\ (j,p)=1}} U_{j,\mathbf{F}_p} \overset{\chi^{-1}}{\xrightarrow{\sim}} G_{\mathbf{F}_p} = \left(\prod_{A/\mathbf{Z}} \mathbf{G}_{m,A}\right) \otimes_{\mathbf{Z}} \mathbf{F}_p.$$

Then σ_1 is a section of χ_1.

Theorem 2.5. *Let Γ be a cyclic group of order p^n. Then we have commutative diagrams of group schemes over $\mathbf{F}_p$ with exact rows*

$$\begin{tikzcd}
0 \arrow[r] & \Gamma \arrow[r] \arrow[d] & U(\Gamma)_{\mathbf{F}_p} \arrow[r] \arrow[d, "\chi_1 \circ \xi"] & (U(\Gamma)/\Gamma)_{\mathbf{F}_p} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathbf{Z}/p^n\mathbf{Z} \arrow[r] & W_{n,\mathbf{F}_p} \arrow[r, "F-1"] & W_{n,\mathbf{F}_p} \arrow[r] & 0
\end{tikzcd}$$

and

$$\begin{tikzcd}
0 \arrow[r] & \mathbf{Z}/p^n\mathbf{Z} \arrow[r] \arrow[d, "\wr"] & W_{n,\mathbf{F}_p} \arrow[r, "F-1"] \arrow[d, "\xi^{-1} \circ \sigma_1"] & W_{n,\mathbf{F}_p} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \Gamma \arrow[r] & U(\Gamma)_{\mathbf{F}_p} \arrow[r] & (U(\Gamma)/\Gamma)_{\mathbf{F}_p} \arrow[r] & 0.
\end{tikzcd}$$

Proof. Let R be an $\mathbf{F}_p$-algebra. Then by definition we have $\xi_R(\gamma) = 1 + T \in (R[T]/(T^{p^n}))^{\times}$. Put now $\mathbf{1} = (1, 0, \dots, 0) \in W_n(R)$. Noting that $E_p(\mathbf{1}, 1; T) = E_p(1, 1; T) = 1 + T$, we obtain $(\chi_1 \circ \xi)_R(\gamma) = \mathbf{1}$ in $W_n(R)$. This implies the commutativity of the first diagram. We have also $E_p(l\mathbf{1}, 1; T) = (1 + T)^l$ for $l \in \mathbf{Z}$. It follows that $(\xi^{-1} \circ \sigma_1)_R(l\mathbf{1}) = \gamma^l$, which implies the commutativity of the second diagram.

Corollary 2.6 (Artin-Schreier-Witt theory). *Let R be an $\mathbf{F}_p$-algebra and S/R an unramified cyclic extension of degree p^n. Then there exist morphisms* $\operatorname{Spec} S \to W_{n,\mathbf{F}_p}$ *and* $\operatorname{Spec} R \to W_{n,\mathbf{F}_p}$ *such that the diagram*

$$\begin{tikzcd}
\operatorname{Spec} S \arrow[r] \arrow[d] & W_{n,\mathbf{F}_p} \arrow[d, "F-1"] \\
\operatorname{Spec} R \arrow[r] & W_{n,\mathbf{F}_p}
\end{tikzcd}$$

is cartesian. Moreover the cyclic extension S/R has a normal basis.

Proof. It is known that we have $H^1(R, W_n) = 0$. This implies the first assertion. On the other hand, it follows from the theorem that

$$\operatorname{Ker}[H^1(R, \Gamma) \to H^1(R, U(\Gamma))] = \operatorname{Ker}[H^1(R, \Gamma) \to H^1(R, W_n)] = H^1(R, \Gamma).$$

2.7. We can give a more concrete description of Corollary 2.6.

For $\boldsymbol{X} = (X_0, X_1, \dots, X_{n-1}) \in W_n(\mathbf{F}_p[X_0, X_1, \dots, X_{n-1}])$, put

$$(F - 1)(\boldsymbol{X}) = (\tilde{F}_0(X_0), \tilde{F}_1(X_0, X_1), \dots, \tilde{F}_{n-1}(X_0, X_1, \dots, X_{n-1})).$$

Let R be an $\mathbf{F}_p$-algebra and S a cyclic unramified extension of R of degree p^n. Then there exists $\boldsymbol{a} = (a_0, a_1, \dots, a_{n-1}) \in W_n(R)$ such that S is isomorphic to

$$R[X_0, X_1, \dots, X_{n-1}]/ \\ (\tilde{F}_0(X_0) - a_0, \tilde{F}_1(X_0, X_1) - a_1, \dots, \tilde{F}_{n-1}(X_0, X_1, \dots, X_{n-1}) - a_{n-1}).$$

Let α_i denote the image X_i in S for each i. Then the Galois group of S/R is generated by

$$\gamma : (\alpha_0, \alpha_1, \dots, \alpha_{n-1}) \mapsto (\alpha_0, \alpha_1, \dots, \alpha_{n-1}) + (1, 0, \dots, 0) \in W_n(S).$$

Furthermore, develop

$$E_p(\boldsymbol{X}, 1; T) = \sum_{j=0}^{p^n-1} b_j(\boldsymbol{X}) T^j$$

in $\mathbf{F}_p[T]/(T^{p^n})$. Then $b_0(\boldsymbol{X}) = 1$, and $b_j(\boldsymbol{X}) = b_j(X_0, X_1, \dots, X_{k-1})$ if $p^{k-1} \leq j < p^j$. For $0 \leq l < p^n$ we define a polynomial $\Psi_l(X_0, X_1, \dots, X_{n-1}) \in \mathbf{F}_p[X_0, X_1, \dots, X_{n-1}]$ by

$$\Psi_l(X_0, X_1, \dots, X_{n-1}) = \sum_{j=l}^{p^n-1} (-1)^{l+j} \binom{j}{l} b_j(\boldsymbol{X}).$$

The homomorphism of group schemes

$$\begin{aligned} \xi^{-1} \circ \sigma_1 : W_{n,\mathbf{F}_p} &= \operatorname{Spec} \mathbf{F}_p[X_0, X_1, \dots, X_{n-1}] \\ &\to U(\Gamma)_{\mathbf{F}_p} = \operatorname{Spec} \mathbf{F}_p\left[T_0, T_1, \dots, T_{p^n-1}, \frac{1}{T_0 + T_1 + \cdots + T_{p^n-1}}\right] \end{aligned}$$

is given by

$$\begin{aligned} T_l \mapsto \Psi_l(X_0, X_1, \dots, X_{n-1}) :& \\ \mathbf{F}_p&\left[T_0, T_1, \dots, T_{p^n-1}, \frac{1}{T_0 + T_1 + \cdots + T_{p^n-1}}\right] \\ &\to \mathbf{F}_p[X_0, X_1, \dots, X_{n-1}] \qquad (0 \leq l < p^n). \end{aligned}$$

A normal basis of the cyclic extension S/R is generated by $\Psi_0(\alpha_0, \alpha_1, \dots, \alpha_{n-1})$. More precisely, we have

$$\gamma^{-j} \Psi_0(\alpha_0, \alpha_1, \dots, \alpha_{n-1}) = \Psi_j(\alpha_0, \alpha_1, \dots, \alpha_{n-1})$$

for $0 \leq j < p^n$.

Remark 2.8. Taking $N = p^n$ and $\lambda = 0$ in 1.4, we obtain another isomorphism of group schemes over $\mathbf{F}_p$

$$\tilde{\chi} = \chi^{(0)} : U(\Gamma)_{\mathbf{F}_p} \xrightarrow{\sim} \mathbf{G}_{m,\mathbf{F}_p} \times \prod_{1 \leq j < p^n} U_{j,\mathbf{F}_p}.$$

As in 2.4, we have a homomorphism of group schemes

$$\tilde{\chi}_1 : G_{\mathbf{F}_p} = \left(\prod_{A/\mathbf{Z}} \mathbf{G}_{m,A} \right) \otimes_{\mathbf{Z}} \mathbf{F}_p \overset{\tilde{\chi}}{\xrightarrow{\sim}} \mathbf{G}_{m,\mathbf{F}_p} \times \prod_{\substack{1 \leq j < p^n \\ (j,p)=1}} U_{j,\mathbf{F}_p} \xrightarrow{\substack{\text{canonical} \\ \text{projection}}} U_{1,\mathbf{F}_p} = W_{n,\mathbf{F}_p}.$$

It is readily seen that $\tilde{\chi}_1(\gamma) = \mathbf{1} \in U_1(\mathbf{F}_p) = W_n(\mathbf{F}_p)$. Therefore we obtain a commutative diagram of group schemes over $\mathbf{F}_p$ with exact rows

$$\begin{tikzcd}
0 \arrow[r] & \Gamma \arrow[r] \arrow[d, "\wr"] & U(\Gamma)_{\mathbf{F}_p} \arrow[r] \arrow[d, "\tilde{\chi}_1\circ\xi"] & (U(\Gamma)/\Gamma)_{\mathbf{F}_p} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathbf{Z}/p^n\mathbf{Z} \arrow[r] & W_{n,\mathbf{F}_p} \arrow[r, "F-1"] & W_{n,\mathbf{F}_p} \arrow[r] & 0,
\end{tikzcd}$$

as is indicated by Serre [8, Ch.IV, 9].

3. Examples

Example 3.1. The case of $n = 1$. We have

$$E_p(X, 1; T) \equiv 1 + \binom{X}{1}T + \binom{X}{2}T^2 + \cdots + \binom{X}{p-1}T^{p-1} \mod T^p,$$

where

$$\binom{X}{j} = \frac{X(X-1)\dots(X-j+1)}{j!}.$$

Then we obtain equalities in $\mathbf{F}_p[X]$

$$\Psi_l(X) = \sum_{j=l}^{p-1}(-1)^{l+j}\binom{l}{j}\binom{X}{j} = 1 - (X-l)^{p-1}$$

for each $0 \leq l < p$.

For verification of the second equality, it is enough to remark the following two facts:

(1) For $l, N \in Z$ with $0 \leq l \leq N$, put

$$F(X) = \sum_{j=l}^{N}(-1)^{l+j}\binom{l}{j}\binom{X}{j} \in \mathbf{Q}[X].$$

Then we have

$$F(m) = \begin{cases} 1 & (m = l) \\ 0 & (m = 1, \dots, l-1, l+1, \dots, N), \end{cases}$$

which follows from the inversion formula for binomial coefficients:

$$\sum_{j=l}^{m}(-1)^{l+j}\binom{l}{j}\binom{m}{j} = \begin{cases} 1 & (m = l) \\ 0 & (m > l). \end{cases}$$

(2) For a prime number p and $l \in \mathbf{Z}$, put

$$F(X) = 1 - (X-l)^{p-1} \in \mathbf{F}_p[X].$$

Then we have

$$F(\alpha) = \begin{cases} 1 & (\alpha = l) \\ 0 & (\alpha \in \mathbf{F}_p, \alpha \neq l), \end{cases}$$

which follows from Fermat's theorem.

At last we obtain the following well known fact. Let R be an $\mathbf{F}_p$-algebra and S a cyclic unramified extension of R of degree p. Then there exists $a \in R$ such that S is isomorphic to $R[X]/(X^p - X - a)$. Let α denote the image X in S. Then the Galois group of S/R is generated by $\gamma : \alpha \mapsto \alpha + 1$. Moreover a normal basis of the cyclic extension S/R is generated by $\Psi_0(\alpha) = 1 - \alpha^{p-1}$.

Remark 3.2. In [9, Section 2] we first examined the sculpture and embedding problems for the Kummer theory, interpreting the Lagrange resolvant in the framework of group schemes. Next we examined the problems for the Kummer-Artin-Schreier theory, deforming the Lagrange resolvant. Last of all we obtained the result for the Artin-Schreier theory by modulo reduction from the Kummer-Artin-Schreier theory.

Example 3.3. The case of $p = 2$, $n = 2$. We have

$$E_2(X, 1; T) \equiv 1 + XT + (X + X^2)T^2 + (X + X^2)T^3 \mod(2, T^4),$$

and therefore

$$E_2(X_0, X_1, 1; T) \equiv 1 + X_0 T + (X_0 + X_0^2 + X_1)T^2 \\ + (X_0 + X_0^2 + X_0 X_1)T^3 \mod(2, T^4).$$

Hence we obtain

$$\Psi_0(X_0, X_1) = 1 + X_0 + X_1 + X_0 X_1 = (1 + X_0)(1 + X_1),$$

$$\Psi_1(X_0, X_1) = X_0^2 + X_0 X_1 = X_0(X_0 + X_1),$$

$$\Psi_2(X_0, X_1) = X_1 + X_0 X_1 = (1 + X_0)X_1,$$

$$\Psi_3(X_0, X_1) = X_0 + X_0^2 + X_0 X_1 = X_0(1 + X_0 + X_1).$$

On the other hand, the endomorphism

$$F - 1 : W_{2,\mathbf{F}_2} = \operatorname{Spec} \mathbf{F}_2[X_0, X_1] \to W_{2,\mathbf{F}_2} = \operatorname{Spec} \mathbf{F}_2[X_0, X_1]$$

is defined by

$$(X_0, X_1) \mapsto (X_0^2 + X_0, X_1^2 + X_1 + X_0^3 + X_0^2).$$

Let R be an $\mathbf{F}_2$-algebra and $a_0, a_1 \in R$. Put

$$S = R[X_0, X_1]/(X_0^2 + X_0 + a_0, X_1^2 + X_1 + X_0^3 + X_0^2 + a_1),$$

and let α_0 and α_1 denote the image of X_0 and X_1 in S, respectively. Then S/R is an unramified cyclic extension of degree 4. The Galois group of S/R is generared by

$$\gamma : (\alpha_0, \alpha_1) \mapsto (\alpha_0 + 1, \alpha_1 + \alpha_0).$$

Furthermore $\Psi_0(\alpha_0, \alpha_1) = (1 + \alpha_0)(1 + \alpha_1)$ generates a normal basis of S/R.

Example 3.4. The case of $p = 2$, $n = 3$. We have an equalilty in $\mathbf{F}_2[X, T]/(T^8)$

$$\begin{aligned} E_2(X, 1; T) = 1 &+ XT + (X + X^2)T^2 + (X + X^2)T^3 + (X^2 + X^3)T^4 \\ &+ (X + X^2 + X^3 + X^5)T^5 + (X + X^2)T^6 \\ &+ (X + X^3 + X^6 + X^7)T^7, \end{aligned}$$

and therefore an equality in $\mathbf{F}_2[X_0, X_1, X_2, T]/(T^8)$

$$\begin{aligned} E_2(X_0, X_1, X_2, 1; T) = 1 &+ X_0T + (X_0 + X_0^2 + X_1)T^2 + (X_0 + X_0^2 + X_0X_1)T^3 \\ &+ (X_0^2 + X_0^3 + X_1 + X_0X_1 + X_0^2X_1 + X_1^2 + X_2)T^4 \\ &+ (X_0 + X_0^2 + X_0^3 + X_0^5 + X_0^2X_1 + X_0X_1^2 + X_0X_2)T^5 \\ &+ (X_0 + X_0^2 + X_1 + X_0X_1 + X_0^3X_1 + X_1^2 + X_0X_1^2 \\ &\quad + X_0^2X_1^2 + X_0X_2 + X_0^2X_2 + X_1X_2)T^6 \\ &+ (X_0 + X_0^3 + X_0^6 + X_0^7 + X_0X_1 + X_0^3X_1 + X_0^5X_1 \\ &\quad + X_0^2X_1^2 + X_0X_2 + X_0^2X_2 + X_0X_1X_2)T^7. \end{aligned}$$

Hence we obtain

$$\begin{aligned} \Psi_0(\boldsymbol{X}) &= 1 + X_0^2 + X_0^3 + X_0^5 + X_0^6 + X_0^7 + X_1 + X_0^5X_1 + X_2 + X_0X_2 + X_1X_2 \\ &\quad + X_0X_1X_2, \\ \Psi_1(\boldsymbol{X}) &= X_0^5 + X_0^6 + X_0^7 + X_0^2X_1 + X_0^3X_1 + X_0^5X_1 + X_0X_1^2 + X_0^2X_1^2 + X_0^2X_2 \\ &\quad + X_0X_1X_2, \\ \Psi_2(\boldsymbol{X}) &= X_0^2 + X_0^3 + X_0^6 + X_0^7 + X_0X_1 + X_0^5X_1 + X_1^2 + X_0X_1^2 + X_1X_2 + X_0X_1X_2, \\ \Psi_3(\boldsymbol{X}) &= X_0^2 + X_0^3 + X_0^6 + X_0^7 + X_0^3X_1 + X_0^5X_1 + X_0^2X_1^2 + X_0X_2 + X_0^2X_2 \\ &\quad + X_0X_1X_2, \end{aligned}$$

$$\begin{aligned}\Psi_4(\boldsymbol{X}) &= X_0 + X_0^2 + X_0^3 + X_0^5 + X_0^6 + X_0^7 + X_0X_1 + X_0^5X_1 + X_2 + X_0X_2\\ &\quad + X_1X_2 + X_0X_1X_2,\\ \Psi_5(\boldsymbol{X}) &= X_0^2 + X_0^5 + X_0^6 + X_0^7 + X_0X_1 + X_0^2X_1 + X_0^3X_1 + X_0^5X_1 + X_0X_1^2\\ &\quad + X_0^2X_1^2 + X_0^2X_2 + X_0X_1X_2,\\ \Psi_6(\boldsymbol{X}) &= X_0^2 + X_0^3 + X_0^6 + X_0^7 + X_1 + X_0^5X_1 + X_1^2 + X_0X_1^2 + X_1X_2 + X_0X_1X_2,\\ \Psi_7(\boldsymbol{X}) &= X_0 + X_0^3 + X_0^6 + X_0^7 + X_0X_1 + X_0^3X_1 + X_0^5X_1 + X_0^2X_1^2 + X_0X_2\\ &\quad + X_0^2X_2 + X_0X_1X_2.\end{aligned}$$

On the other hand, the endomorphism

$$F - 1 : W_{3,\mathbf{F}_2} = \mathrm{Spec}\,\mathbf{F}_2[X_0, X_1, X_2] \to W_{3,\mathbf{F}_2} = \mathrm{Spec}\,\mathbf{F}_2[X_0, X_1, X_2]$$

is defined by

$$(X_0, X_1, X_2) \mapsto (\tilde{F}_0(X_0), \tilde{F}_1(X_0, X_1), \tilde{F}_2(X_0, X_1, X_2)),$$

where

$$\begin{aligned}\tilde{F}_0(X_0) &= X_0^2 + X_0,\\ \tilde{F}_1(X_0, X_1) &= X_1^2 + X_1 + X_0^3 + X_0^2,\\ \tilde{F}_2(X_0, X_1, X_2) &= X_2^2 + X_2 + X_1^3 + X_1^2X_0^3 + X_1^2X_0^2 + X_1^2 + X_1X_0^3\\ &\quad + X_1X_0^2 + X_0^7 + X_0^5.\end{aligned}$$

Let R be an $\mathbf{F}_2$-algebra and $a_0, a_1, a_2 \in R$. Put

$$S = R[X_0, X_1, X_2]/(\tilde{F}_0(X_0) + a_0, \tilde{F}_1(X_0, X_1) + a_1, \tilde{F}_2(X_0, X_1, X_2) + a_2),$$

and let α_0, α_1 and α_2 denote the image of X_0, X_1 and X_2 in S, respectively. Then S/R is an unramified cyclic extension of degree 8. The Galois group of S/R is generared by

$$\gamma : (\alpha_0, \alpha_1, \alpha_2) \mapsto (\alpha_0 + 1, \alpha_1 + \alpha_0, \alpha_2 + \alpha_1\alpha_0 + \alpha_0^3 + \alpha_0).$$

Furthermore $\Psi_0(\alpha_0, \alpha_1, \alpha_2)$ generates a normal basis of S/R.

Example 3.5. The case of $p = 3$, $n = 2$. We have an equality in $\mathbf{F}_3[X, T]/(T^9)$

$$\begin{aligned}E_3(X, 1; T) &= 1 + XT + (X + 2X^2)T^2 + (X^2 + 2X^3)T^3 + (2X + 2X^2 + 2X^3)T^4\\ &\quad + (2X + 2X^2 + 2X^3 + 2X^4 + X^5)T^5 + (X^2 + X^3 + X^4)T^6\\ &\quad + (X + 2X^2 + X^4 + X^5 + X^6)T^7 + (X + 2X^8)T^8,\end{aligned}$$

and therefore an equality in $\mathbf{F}_3[X_0, X_1, T]/(T^9)$

$$\begin{aligned}E_3(X_0, X_1, 1; T) = {} & 1 + X_0T + (X_0 + 2X_0^2)T^2 + (X_0 + X_0^2 + X_1)T^3 \\ & + (2X_0 + 2X_0^2 + 2X_0^3 + X_0X_1)T^4 \\ & + (2X_0 + 2X_0^2 + 2X_0^3 + 2X_0^4 + X_0^5 + X_0X_1 + 2X_0^2X_1)T^5 \\ & + (X_0^2 + X_0^3 + X_0^4 + X_1 + X_0X_1 + X_0^2X_1 + 2X_1^2)T^6 \\ & + (X_0 + 2X_0^2 + X_0^4 + X_0^5 + X_0^6 + 2X_0^2 + 2X_0^3X_1 + 2X_0X_1^2)T^7 \\ & + (X_0 + 2X_0^8 + X_0^2X_1 + 2X_0^3X_1 + 2X_0^4X_1 + X_0^5X_1 \\ & \quad + 2X_0X_1^2 + X_0^2X_1^2)T^8.\end{aligned}$$

Hence we obtain

$$\begin{aligned}\Psi_0(\boldsymbol{X}) = {} & 1 + 2X_0^3 + X_0^4 + X_0^5 + 2X_0^6 + 2X_0^8 + X_0^2X_1 + 2X_0^3X_1 + 2X_0^4X_1 + X_0^5X_1 \\ & + 2X_1^2 + X_0^2X_1^2, \\ \Psi_1(\boldsymbol{X}) = {} & 2X_0^3 + 2X_0^4 + X_0^6 + 2X_0^8 + X_0X_1 + X_0^2X_1 + X_0^3X_1 + 2X_0^4X_1 + X_0^5X_1 \\ & + X_0X_1^2 + X_0^2X_1^2, \\ \Psi_2(\boldsymbol{X}) = {} & X_0^3 + X_0^4 + 2X_0^5 + 2X_0^8 + 2X_0X_1 + 2X_0^2X_1 + 2X_0^3X_1 + 2X_0^4X_1 + X_0^5X_1 \\ & + 2X_0X_1^2 + X_0^2X_1^2, \\ \Psi_3(\boldsymbol{X}) = {} & 2X_0^4 + 2X_0^6 + 2X_0^8 + 2X_1 + 2X_0^2X_1 + 2X_0^3X_1 + 2X_0^4X_1 + X_0^5X_1 + 2X_1^2 \\ & + X_0^2X_1^2, \\ \Psi_4(\boldsymbol{X}) = {} & X_0^3 + 2X_0^5 + X_0^6 + 2X_0^8 + 2X_0X_1 + 2X_0^2X_1 + X_0^3X_1 + 2X_0^4X_1 + X_0^5X_1 \\ & + X_0X_1^2 + X_0^2X_1^2, \\ \Psi_5(\boldsymbol{X}) = {} & 2X_0^2 + 2X_0^3 + 2X_0^4 + X_0^5 + 2X_0^8 + X_0X_1 + 2X_0^3X_1 + 2X_0^4X_1 + X_0^5X_1 \\ & + 2X_0X_1^2 + X_0^2X_1^2, \\ \Psi_6(\boldsymbol{X}) = {} & 2X_0^2 + X_0^3 + 2X_0^5 + 2X_0^6 + 2X_0^8 + X_1 + 2X_0^3X_1 + 2X_0^4X_1 + X_0^5X_1 \\ & + 2X_1^2 + X_0^2X_1^2, \\ \Psi_7(\boldsymbol{X}) = {} & 2X_0 + 2X_0^2 + X_0^4 + X_0^5 + X_0^6 + 2X_0^8 + X_0^3X_1 + 2X_0^4X_1 + X_0^5X_1 \\ & + X_0X_1^2 + X_0^2X_1^2, \\ \Psi_8(\boldsymbol{X}) = {} & X_0 + 2X_0^8 + X_0^2X_1 + 2X_0^3X_1 + 2X_0^4X_1 + X_0^5X_1 + 2X_0X_1^2 + X_0^2X_1^2.\end{aligned}$$

On the other hand, the endomorphism

$$F-1 : W_{2,\mathbf{F}_3} = \operatorname{Spec} \mathbf{F}_3[X_0, X_1] \to W_{2,\mathbf{F}_3} = \operatorname{Spec} \mathbf{F}_3[X_0, X_1]$$

is defined by

$$(X_0, X_1) \mapsto (X_0^3 - X_0, X_1^3 - X_1 + X_0^7 - X_0^5).$$

Let R be an $\mathbf{F}_3$-algebra and $a_0, a_1 \in R$. Put

$$S = R[X_0, X_1]/(X_0^3 - X_0 - a_0, X_1^3 - X_1 + X_0^7 - X_0^5 - a_1),$$

and let α_0 and α_1 denote the image of X_0 and X_1 in S, respectively. Then S/R is an unramified cyclic extension of degree 9. The Galois group of S/R is generered by

$$\gamma : (\alpha_0, \alpha_1) \mapsto (\alpha_0 + 1, \alpha_1 - \alpha_0 - \alpha_0^2).$$

Furthermore $\Psi_0(\alpha_0, \alpha_1)$ generates a normal basis of S/R.

4. Remarks

4.1. Let Γ be a cyclic group of order p^n, and take a generator γ of Γ. Under the identification

$$U(\Gamma)_{\mathbf{F}_p} = \operatorname{Spec} \mathbf{F}_p\left[T_0, T_1, \dots, T_{p^n-1}, \frac{1}{T_0 + T_1 + \cdots + T_{p^n-1}}\right],$$

the right multiplication by γ on $U(\Gamma)_{\mathbf{F}_p}$ is defined by the cyclic permutation

$$T_0 \mapsto T_{p^n-1}, T_1 \mapsto T_0, T_2 \mapsto T_1, \dots, T_{p^n-1} \mapsto T_{p^n-2}.$$

Moreover we have

$$(U(\Gamma)/\Gamma)_{\mathbf{F}_p} = \operatorname{Spec} \mathbf{F}_p\left[T_0, T_1, \dots, T_{p^n-1}, \frac{1}{T_0 + T_1 + \cdots + T_{p^n-1}}\right]^{\Gamma},$$

where $\mathbf{F}_p[T_0, T_1, \dots, T_{p^n-1}, 1/(T_0 + T_1 + \cdots + T_{p^n-1})]^{\Gamma}$ denotes the subring of invariant rationals under the action by Γ on $\mathbf{F}_p[T_0, T_1, \dots, T_{p^n-1}, 1/(T_0 + T_1 + \cdots + T_{p^n-1})]$.

Now we have a commutative diagram of group schemes over $\mathbf{F}_p$ with exact rows

$$\begin{tikzcd}
0 \arrow[r] & \Gamma \arrow[r] \arrow[d, "\wr"] & U(\Gamma)_{\mathbf{F}_p} \arrow[r] \arrow[d, "\wr\,\chi^{(1)}\circ\xi"] & (U(\Gamma)/\Gamma)_{\mathbf{F}_p} \arrow[r] \arrow[d, "\wr"] & 0 \\
0 \arrow[r] & \mathbf{Z}/p^n\mathbf{Z} \arrow[r] & \mathbf{G}_{m,\mathbf{F}_p} \times \prod\limits_{\substack{1 \le j < p^n \\ (j,p)=1}} U_{j,\mathbf{F}_p} \arrow[r, "\Theta"] & \mathbf{G}_{m,\mathbf{F}_p} \times \prod\limits_{\substack{1 \le j < p^n \\ (j,p)=1}} U_{j,\mathbf{F}_p} \arrow[r] & 0,
\end{tikzcd}$$

where Θ is defined by the diagonal matrix with the entries $F-1 : W_{n,\mathbf{F}_p} \to W_{n,\mathbf{F}_p}$ for $j=1$ and the identity map for the others.

This observation allows us to write down in principle a generating family of the invariant subring $\mathbf{F}_p[T_0, T_1, \dots, T_{p^n-1}, 1/(T_0+T_1+\cdots+T_{p^n-1})]^{\Gamma}$.

For example, let $n=1$. Substituting

$$U_k = \sum_{j=k}^{p-1} \binom{j}{k} T_j$$

in

$$c_l(\boldsymbol{U}) = c_l\left(\frac{U_1}{U_0}, \frac{U_2}{U_0}, \dots, \frac{U_l}{U_0}\right) \in \mathbf{F}_p\left[\frac{U_1}{U_0}, \frac{U_2}{U_0}, \dots, \frac{U_l}{U_0}\right]$$

defined in 1.5, we obtain rationals

$$\begin{aligned}\tilde{c}_l(\boldsymbol{T}) &= \tilde{c}_l(T_0, T_1, \dots, T_{p-1})\\ &\in \mathbf{F}_p\left[T_0, T_1, \dots, T_{p-1}, \frac{1}{T_0+T_1+\cdots+T_{p-1}}\right] \qquad (0 \le l < p).\end{aligned}$$

More precisely, we have

$$\tilde{c}_0(\boldsymbol{T}) = \tilde{c}_0(T_0, T_1, \dots, T_{p-1}) = \sum_{j=0}^{p-1} T_j,$$

$$\tilde{c}_1(\boldsymbol{T}) = \tilde{c}_1(T_0, T_1, \dots, T_{p-1}) = \sum_{j=1}^{p-1} jT_j \Big/ \sum_{j=0}^{p-1} T_j$$

and, for $2 \le l < p$, $\tilde{c}_l(\boldsymbol{T}) = \tilde{c}_l(T_0, T_1, \dots, T_{p-1})$ is determined inductively by

$$\begin{aligned}&\sum_{\substack{\nu_1, \nu_2, \dots, \nu_{l-1} \ge 1\\ \nu_1+2\nu_2+\cdots+(l-1)\nu_{l-1}=l}} \binom{c_1(\boldsymbol{T})}{\nu_1}\binom{c_2(\boldsymbol{T})}{\nu_2}\cdots\binom{c_{l-1}(\boldsymbol{T})}{\nu_{l-1}} + c_l(\boldsymbol{T})\\ &\quad = \sum_{j=l}^{p-1}\binom{j}{l} T_j \Big/ \sum_{j=0}^{p-1} T_j.\end{aligned}$$

Then we obtain

$$\begin{aligned}&\mathbf{F}_p\left[T_0, T_1, \dots, T_{p-1}, \frac{1}{T_0+T_1+\cdots+T_{p-1}}\right]\\ &\quad = \mathbf{F}_p\left[\tilde{c}_0(\boldsymbol{T}), \tilde{c}_1(\boldsymbol{T}), \tilde{c}_2(\boldsymbol{T}), \dots, \tilde{c}_{p-1}(\boldsymbol{T}), \frac{1}{\tilde{c}_0(\boldsymbol{T})}\right]\end{aligned}$$

and

$$\begin{aligned}&\mathbf{F}_p\left[T_0, T_1, \dots, T_{p-1}, \frac{1}{T_0 + T_1 + \cdots + T_{p-1}}\right]^{\Gamma}\\&\quad = \mathbf{F}_p\left[\tilde{c}_0(\boldsymbol{T}), \tilde{c}_1(\boldsymbol{T})^p - \tilde{c}_1(\boldsymbol{T}), \tilde{c}_2(\boldsymbol{T}), \dots, \tilde{c}_{p-1}(\boldsymbol{T}), \frac{1}{\tilde{c}_0(\boldsymbol{T})}\right].\end{aligned}$$

It should be remarked that $\tilde{c}_0(\boldsymbol{T}) = T_0 + T_1 + \cdots + T_{p-1}$ is a group-like element of the Hopf algebra $\mathbf{F}_p[T_0, T_1, \dots, T_{p-1}, 1/(T_0 + T_1 + \cdots + T_{p-1})]$ and $\tilde{c}_1(\boldsymbol{T}), \tilde{c}_2(\boldsymbol{T}), \dots, \tilde{c}_{p-1}(\boldsymbol{T})$ are primitive elements.

In this manner we would be able to follow the path shown by Kuniyoshi [6].

Example 4.2. In the case of $p = 2$, we have

$$\tilde{c}_0(\boldsymbol{T}) = T_0 + T_1, \qquad \tilde{c}_1(\boldsymbol{T}) = \frac{T_1}{T_0 + T_1}$$

and

$$\tilde{c}_1(\boldsymbol{T})^2 - \tilde{c}_1(\boldsymbol{T}) = \frac{T_0 T_1}{T_0 + T_1}.$$

Example 4.3. In the case of $p = 3$, we have

$$\begin{aligned}&\tilde{c}_0(\boldsymbol{T}) = T_0 + T_1 + T_2, \qquad \tilde{c}_1(\boldsymbol{T}) = \frac{T_1 + 2T_2}{T_0 + T_1 + T_2},\\&\tilde{c}_2(\boldsymbol{T}) = -\frac{T_0 T_1 + T_1 T_2 + T_2 T_0}{(T_0 + T_1 + T_2)^2}\end{aligned}$$

and

$$\tilde{c}_1(\boldsymbol{T})^3 - \tilde{c}_1(\boldsymbol{T}) = \frac{(T_0 - T_1)(T_1 - T_2)(T_2 - T_0)}{(T_0 + T_1 + T_2)^3}.$$

Example 4.4. In the case of $p = 5$, we have

$$\begin{aligned}\tilde{c}_0(\boldsymbol{T}) &= T_0 + T_1 + T_2 + T_3 + T_4,\\ \tilde{c}_0(\boldsymbol{T})\tilde{c}_1(\boldsymbol{T}) &= T_1 + 2T_2 + 3T_3 + 4T_4,\\ \tilde{c}_0(\boldsymbol{T})^2\tilde{c}_2(\boldsymbol{T}) &= 3(T_0T_1 + T_1T_2 + T_2T_3 + T_3T_4 + T_4T_0)\\ &\quad + 2(T_0T_2 + T_1T_3 + T_2T_4 + T_3T_0 + T_4T_1),\end{aligned}$$

$$\begin{aligned}
\tilde{c}_0(\boldsymbol{T})^3\tilde{c}_3(\boldsymbol{T}) = {}& 3(T_0^2T_1 + T_1^2T_2 + T_2^2T_3 + T_3^2T_4 + T_4^2T_0) \\
&+ (T_0T_1^2 + T_1T_2^2 + T_2T_3^2 + T_3T_4^2 + T_4T_0^2) \\
&+ (T_0^2T_2 + T_1^2T_3 + T_2^2T_4 + T_3^2T_0 + T_4^2T_1) \\
&+ 2(T_0T_1T_2 + T_1T_2T_3 + T_2T_3T_4 + T_3T_4T_0 + T_4T_0T_1) \\
&+ 3(T_0T_1T_3 + T_1T_2T_4 + T_2T_3T_0 + T_3T_4T_1 + T_4T_0T_2),
\end{aligned}$$

$$\begin{aligned}
\tilde{c}_0(\boldsymbol{T})^3\tilde{c}_3(\boldsymbol{T}) = {}& 4(T_0^3T_1 + T_1^3T_2 + T_2^3T_3 + T_3^3T_4 + T_4^3T_0) \\
&+ 4(T_0^2T_1^2 + T_1^2T_2^2 + T_2^2T_3^2 + T_3^2T_4^2 + T_4^2T_0^2) \\
&+ 2(T_0T_1^3 + T_1T_2^3 + T_2T_3^3 + T_3T_4^3 + T_4T_0^3) \\
&+ 3(T_0^3T_2 + T_1^3T_3 + T_2^3T_4 + T_3^3T_0 + T_4^3T_1) \\
&+ 3(T_0^2T_2^2 + T_1^2T_3^2 + T_2^2T_4^2 + T_3^2T_0^2 + T_4^2T_1^2) \\
&+ 2(T_0T_2^3 + T_1T_3^3 + T_2T_4^3 + T_3T_0^3 + T_4T_1^3) \\
&+ 2(T_0^2T_1T_2 + T_1^2T_2T_3 + T_2^2T_3T_4 + T_3^2T_4T_0 + T_4^2T_0T_1) \\
&+ 3(T_0T_1^2T_2 + T_1T_2^2T_3 + T_2T_3^2T_4 + T_3T_4^2T_0 + T_4T_0^2T_1) \\
&+ 4(T_0T_1T_2^2 + T_1T_2T_3^2 + T_2T_3T_4^2 + T_4T_0T_1^2 + T_3T_4T_0^2) \\
&+ 3(T_0^2T_1T_3 + T_1^2T_2T_4 + T_2^2T_3T_0 + T_3^2T_4T_1 + T_4^2T_0T_2) \\
&+ 2(T_0T_1^2T_3 + T_1T_2^2T_4 + T_2T_3^2T_0 + T_3T_4^2T_1 + T_4T_0^2T_2) \\
&+ 4(T_0T_1T_3^2 + T_1T_2T_4^2 + T_2T_3T_0^2 + T_3T_4T_1^2 + T_4T_0T_2^2) \\
&+ 4(T_0T_1T_2T_3 + T_1T_2T_3T_4 + T_2T_3T_4T_0 + T_3T_4T_0T_2 + T_4T_0T_1T_2)
\end{aligned}$$

and

$$\begin{aligned}
&\tilde{c}_0(\boldsymbol{T})^4\{\tilde{c}_1(\boldsymbol{T})^5 - \tilde{c}_1(\boldsymbol{T})\} \\
&\quad = 4(T_0^4T_1 + T_1^4T_2 + T_2^4T_3 + T_3^4T_4 + T_4^4T_0) \\
&\qquad + (T_0^3T_1^2 + T_1^3T_2^2 + T_2^3T_3^2 + T_3^3T_4^2 + T_4^3T_0^2) \\
&\qquad + 4(T_0^2T_1^3 + T_1^2T_2^3 + T_2^2T_3^3 + T_3^2T_4^3 + T_4^2T_0^3) \\
&\qquad + (T_0T_1^4 + T_1T_2^4 + T_2T_3^4 + T_3T_4^4 + T_4T_0^4) \\
&\qquad + 3(T_0^4T_2 + T_1^4T_3 + T_2^4T_4 + T_3^4T_0 + T_4^4T_1)
\end{aligned}$$

$$
\begin{aligned}
&+2(T_0^3T_2^2+T_1^3T_3^2+T_2^3T_4^2+T_3^3T_0^2+T_4^3T_1^2)\\
&+3(T_0^2T_2^3+T_1^2T_3^3+T_2^2T_4^3+T_3^2T_0^3+T_4^2T_1^3)\\
&+2(T_0T_2^4+T_1T_3^4+T_2T_4^4+T_3T_0^4+T_4T_1^4)\\
&+3(T_0^3T_1T_2+T_1^3T_2T_3+T_2^3T_3T_4+T_3^3T_4T_0+T_4^3T_0T_1)\\
&+(T_0^2T_1^2T_2+T_1^2T_2^2T_3+T_2^2T_3^2T_4+T_3^2T_4^2T_0+T_4^2T_0^2T_1)\\
&+4(T_0T_1^2T_2^2+T_1T_2^2T_3^2+T_2T_3^2T_4^2+T_3T_4^2T_0^2+T_4T_0^2T_1^2)\\
&+2(T_0T_1T_2^3+T_1T_2T_3^3+T_2T_3T_4^3+T_3T_4T_0^3+T_4T_0T_1^3)\\
&+4(T_0^3T_1T_3+T_1^3T_2T_4+T_2^3T_3T_0+T_3^3T_4T_1+T_4^3T_0T_2)\\
&+3(T_0^2T_1T_3^2+T_1^2T_2T_4^2+T_2^2T_3T_0^2+T_3^2T_4T_1^2+T_4^2T_0T_2^2)\\
&+2(T_0T_1^2T_3^2+T_1T_2^2T_4^2+T_2T_3^2T_0^2+T_3T_4^2T_1^2+T_4T_0^2T_2^2)\\
&+(T_0T_1^3T_3+T_1T_2^3T_4+T_2T_3^3T_0+T_3T_4^3T_1+T_4T_0^3T_2)\\
&+3(T_0^2T_1T_2T_3+T_1^2T_2T_3T_4+T_2^2T_3T_4T_0+T_3^2T_4T_0T_1+T_4^2T_0T_1T_2)\\
&+(T_0T_1^2T_2T_3+T_1T_2^2T_3T_4+T_2T_3^2T_4T_0+T_3T_4^2T_0T_1+T_4T_0^2T_1T_2)\\
&+4(T_0T_1T_2^2T_3+T_1T_2T_3^2T_4+T_2T_3T_4^2T_0+T_3T_4T_0^2T_1+T_4T_0T_1^2T_2)\\
&+2(T_0T_1T_2T_3^2+T_1T_2T_3T_4^2+T_2T_3T_4T_0^2+T_3T_4T_0T_1^2+T_4T_0T_1T_2^2).
\end{aligned}
$$

Example 4.5. In the case of $p=2$, $n=2$, the isomorphism

$$
\begin{aligned}
\chi^{(1)}\circ\xi : U(\Gamma)_{\mathbf{F}_2} &= \operatorname{Spec}\mathbf{F}_2\left[T_0,T_1,T_2,T_3,\frac{1}{T_0+T_1+T_2+T_3}\right]\\
&\xrightarrow{\sim}\mathbf{G}_{m,\mathbf{F}_2}\times W_{2,\mathbf{F}_2}\times\mathbf{G}_{a,\mathbf{F}_2}=\operatorname{Spec}\mathbf{F}_2\left[X_0,X_1,X_2,X_3,\frac{1}{X_0}\right]
\end{aligned}
$$

is defined by

$$
X_0\mapsto\tilde{c}_0(\boldsymbol{T}),\qquad X_1\mapsto\tilde{c}_1(\boldsymbol{T}),\qquad X_2\mapsto\tilde{c}_2(\boldsymbol{T}),\qquad X_3\mapsto\tilde{c}_3(\boldsymbol{T}),
$$

where

$$
\begin{aligned}
&T_0+T_1(1+U)+T_2(1+U)^2+T_3(1+U)^3=\tilde{c}_0(\boldsymbol{T})\{1+\tilde{c}_3(\boldsymbol{T})U\}\\
&\{1+\tilde{c}_1(\boldsymbol{T})U+(\tilde{c}_1(\boldsymbol{T})+\tilde{c}_1(\boldsymbol{T})^2+\tilde{c}_2(\boldsymbol{T}))U^2+(\tilde{c}(\boldsymbol{T})+\tilde{c}_1(\boldsymbol{T})^2+\tilde{c}_1(\boldsymbol{T})\tilde{c}_2(\boldsymbol{T}))U^3\}
\end{aligned}
$$

in $\mathbf{F}_2[T_0,T_1,T_2,T_3][U]/(U^4)$. Hence we obtain

$$
\begin{aligned}
\tilde{c}_0(\boldsymbol{T}) &= T_0 + T_1 + T_2 + T_3, \\
\tilde{c}_0(\boldsymbol{T})\tilde{c}_1(\boldsymbol{T}) &= T_1 + T_3, \\
\tilde{c}_0(\boldsymbol{T})^2\tilde{c}_2(\boldsymbol{T}) &= T_2^2 + T_3^2 + T_0T_1 + T_0T_2 + T_1T_3 + T_2T_3, \\
\tilde{c}_0(\boldsymbol{T})^3\tilde{c}_3(\boldsymbol{T}) &= (T_0^2T_1 + T_1^2T_2 + T_2^2T_3 + T_3^2T_0) \\
&\quad + (T_0T_1T_2 + T_1T_2T_3 + T_2T_3T_0 + T_3T_0T_1).
\end{aligned}
$$

Furthermore we have

$$
\begin{aligned}
&\mathbf{F}_2\left[T_0, T_1, T_2, T_3, \frac{1}{T_0 + T_1 + T_2 + T_3}\right]^{\Gamma} \\
&= \mathbf{F}_2\left[\tilde{c}_0(\boldsymbol{T}), \tilde{c}_1(\boldsymbol{T})^2 + \tilde{c}_1(\boldsymbol{T}), \tilde{c}_2(\boldsymbol{T})^2 + \tilde{c}_2(\boldsymbol{T}) + \tilde{c}_1(\boldsymbol{T})^3 + \tilde{c}_1(\boldsymbol{T})^2, \tilde{c}_3(\boldsymbol{T}), \frac{1}{\tilde{c}_0(\boldsymbol{T})}\right].
\end{aligned}
$$

We have gotten

$$
\begin{aligned}
\tilde{c}_0(\boldsymbol{T})^2\{\tilde{c}_1(\boldsymbol{T})^2 + \tilde{c}_1(\boldsymbol{T})\} &= T_0T_1 + T_1T_2 + T_2T_3 + T_3T_0, \\
\tilde{c}_0(\boldsymbol{T})^4\{\tilde{c}_2(\boldsymbol{T})^2 + \tilde{c}_2(\boldsymbol{T}) + \tilde{c}_1(\boldsymbol{T})^3 + \tilde{c}_1(\boldsymbol{T})^2\}& \\
= (T_0^3T_1 + T_1^3T_2 + T_2^3T_3 + T_3^3T_0) &+ (T_0^3T_2 + T_1^3T_3 + T_2^3T_0 + T_3^3T_1) \\
+ (T_0T_1^2T_2 + T_1T_2^2T_3 + T_2T_3^2T_0 + T_3T_0^2T_1)& \\
+ (T_0T_1T_2^2 + T_1T_2T_3^2 + T_2T_3T_0^2 + T_3T_0T_1^2)&
\end{aligned}
$$

by a simple and honest calculation.

Remark 4.6. Let k be a field and Γ a finite group. Let K denote the rational function field $k(T_\gamma; \gamma \in \Gamma)$, and let Γ act on K by $(\gamma, T_{\gamma'}) \mapsto T_{\gamma\gamma'}$ or by $(\gamma, T_{\gamma'}) \mapsto T_{\gamma'\gamma^{-1}}$. Noether's problem asks if the fixed field K^Γ is purely transcendental over k or not. The argument of 4.1 gives an affirmative answer for Noether's problem in a more precise form when k is a field of characterisitic $p > 0$ and Γ is a cyclic group of order p^n.

It should be mentioned that Noether's problem is affirmative when k is a field of characterisitic $p > 0$ and Γ is a p-group. This fact is well known to experts, for example, stated as [1, Theorem 1.12] with a reference to Kuniyoshi [6].

4.7. We conclude the article by considering the sculpture and embedding problems for the Grothendieck resolution of a finite flat commutative group scheme. We refer to [11] for details, in particular concerning the relation with the Hopf-Galois theory.

Let S be a scheme and Γ an affine commutative group S-scheme such that $\mathcal{O}_\Gamma$ is a locally free $\mathcal{O}_S$-module of finite rank. Then the functor $\mathit{Hom}_{S-\mathrm{gr}}(\Gamma, \mathbf{G}_{m,S})$ is represented by a commutative group scheme $\Gamma^\vee$, called the Cartier dual of Γ. Indeed the $\mathcal{O}_S$-module $\mathcal{O}_\Gamma^\vee = \mathit{Hom}_{\mathcal{O}_S}(\mathcal{O}_\Gamma, \mathcal{O}_S)$ is also locally free of finite rank, and we have $\Gamma^\vee = \operatorname{Spec} \mathcal{O}_\Gamma^\vee$. The Cartier duality asserts that $\mathit{Hom}_{S-\mathrm{gr}}(\Gamma^\vee, \mathbf{G}_{m,S})$ is isomorphic to Γ.

Furthermore the functor $\mathit{Hom}_S(\Gamma^\vee, \mathbf{G}_{m,S})$ is nothing but the Weil restriction $\prod_{\Gamma^\vee/S} \mathbf{G}_{m,\Gamma^\vee}$, which is representable since $\mathcal{O}_{\Gamma^\vee}$ is a locally free $\mathcal{O}_S$-module of finite rank. Then we obtain an exact sequence of commutative group schemes

$$0 \to \Gamma \to \prod_{\Gamma^\vee/S} \mathbf{G}_{m,\Gamma^\vee} \to \left(\prod_{\Gamma^\vee/S} \mathbf{G}_{m,\Gamma^\vee}\right)\Big/\Gamma \to 0.$$

The Weil restriction $\prod_{\Gamma^\vee/S} \mathbf{G}_{m,\Gamma^\vee}$ is smooth over S since $\mathbf{G}_{m,\Gamma^\vee}$ is smooth over $\Gamma^\vee$, and therefore the quotient $\left(\prod_{\Gamma^\vee/S} \mathbf{G}_{m,\Gamma^\vee}\right)\Big/\Gamma$ is also smooth over S.

When Γ is a constant group scheme, the Grothendieck resolution

$$0 \to \Gamma \to \prod_{\Gamma^\vee/\mathbf{Z}} \mathbf{G}_{m,\Gamma^\vee} \to \left(\prod_{\Gamma^\vee/\mathbf{Z}} \mathbf{G}_{m,\Gamma^\vee}\right)\Big/\Gamma \to 0$$

is nothing but the exact sequence

$$0 \to \Gamma \to U(\Gamma) \to U(\Gamma)/\Gamma \to 0.$$

Example 4.8. Put ${}_1W_n = \operatorname{Ker}[F : W_{n,\mathbf{F}_p} \to W_{n,\mathbf{F}_p}]$. Then

$${}_1W_n = \operatorname{Spec} \mathbf{F}_p[T_0, T_1, \dots, T_{n-1}]/(T_0^p, T_1^p, \dots, T_{n-1}^p)$$

with the addition

$$\begin{aligned}&(T_0, T_1, \dots, T_{n-1})\\ &\qquad \mapsto (S_0(\boldsymbol{T} \otimes 1, 1 \otimes \boldsymbol{T}), S_1(\boldsymbol{T} \otimes 1, 1 \otimes \boldsymbol{T}), \dots, S_{n-1}(\boldsymbol{T} \otimes 1, 1 \otimes \boldsymbol{T})).\end{aligned}$$

As is known, the Cartier dual of ${}_1W_n$ is isomorphic to $\boldsymbol{\alpha}_{p^n} = \operatorname{Ker}[F^n : \mathbf{G}_{a,\mathbf{F}_p} \to \mathbf{G}_{a,\mathbf{F}_p}]$ (cf. [2, Ch.V. 4.4.7]). Therefore the Grothendieck resolution of the finite group scheme ${}_1W_n$ is written as

$$0 \to {}_1W_n \to \prod_{A/\mathbf{F}_p} \mathbf{G}_{m,A} \to \left(\prod_{A/\mathbf{F}_p} \mathbf{G}_{m,A}\right)\Big/{}_1W_n \to 0,$$

where $A = \mathbf{F}_p[T]/(T^{p^n})$. For an $\mathbf{F}_p$-algebra R, the injection

$${}_1W_n(R) \to \left(\prod_{A/\mathbf{F}_p} \mathbf{G}_{m,A}\right)(R) = (R[T]/(T^{p^n}))^\times$$

is given by

$$(a_0, a_1, \dots, a_{n-1}) \mapsto E_p(a_0T)E_p(a_1T^p)\dots E_p(a_{n-1}T^{p^{n-1}}).$$

Hence we obtain a commutative diagram of group schemes over $\mathbf{F}_p$ with exact rows

$$\begin{tikzcd}
0 \arrow[r] & {}_1W_n \arrow[r] \arrow[d, equal] & \prod_{A/\mathbf{F}_p} \mathbf{G}_{m,A} \arrow[r] \arrow[d, "\wr\, \chi^{(0)}"] & \left(\prod_{A/\mathbf{F}_p} \mathbf{G}_{m,A}\right)\Big/{}_1W_n \arrow[r] \arrow[d, "\wr"] & 0 \\
0 \arrow[r] & {}_1W_n \arrow[r] & \mathbf{G}_{m,\mathbf{F}_p} \times \prod_{\substack{1 \le j < p^n \\ (j,p)=1}} U_{j,\mathbf{F}_p} \arrow[r, "\Theta"] & \mathbf{G}_{m,\mathbf{F}_p} \times \prod_{\substack{1 \le j < p^n \\ (j,p)=1}} U_{j,\mathbf{F}_p} \arrow[r] & 0,
\end{tikzcd}$$

where Θ is defined by the diagonal matrix with the entries $F : W_{n,\mathbf{F}_p} \to W_{n,\mathbf{F}_p}$ for $j = 1$ and the identity map for the others.

Furthermore, taking the projection

$$\chi_1^{(0)} : \prod_{A/\mathbf{F}_p} \mathbf{G}_{m,A} \to U_{1,\mathbf{F}_p} = W_{n,\mathbf{F}_p}$$

and the injection

$$\sigma_1^{(0)} : U_{1,\mathbf{F}_p} = W_{n,\mathbf{F}_p} \to \prod_{A/\mathbf{F}_p} \mathbf{G}_{m,A},$$

we obtain commutative diagrams of group schemes over $\mathbf{F}_p$ with exact rows

$$\begin{tikzcd}
0 \arrow[r] & {}_1W_n \arrow[r] \arrow[d, equal] & \prod_{A/\mathbf{F}_p} \mathbf{G}_{m,A} \arrow[r] \arrow[d, "\chi_1^{(0)}"] & \left(\prod_{A/\mathbf{F}_p} \mathbf{G}_{m,A}\right)\Big/{}_1W_n \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & {}_1W_n \arrow[r] & W_{n,\mathbf{F}_p} \arrow[r, "F"] & W_{n,\mathbf{F}_p} \arrow[r] & 0
\end{tikzcd}$$

and

$$\begin{tikzcd}
0 \arrow[r] & {}_1W_n \arrow[r] \arrow[d, equal] & W_{n,\mathbf{F}_p} \arrow[r, "F"] \arrow[d, "\sigma_1^{(0)}"] & W_{n,\mathbf{F}_p} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & {}_1W_n \arrow[r] & \prod_{A/\mathbf{F}_p} \mathbf{G}_{m,A} \arrow[r] & \left(\prod_{A/\mathbf{F}_p} \mathbf{G}_{m,A}\right)\Big/{}_1W_n \arrow[r] & 0.
\end{tikzcd}$$

As a consequence, we arrive at the following assertion. Let R be an $\mathbf{F}_p$-algebra and S an R-algebra such that $\mathrm{Spec}\, S$ is a torsor under ${}_1W_n$. Then there exist morphisms $\mathrm{Spec}\, S \to W_{n,\mathbf{F}_p}$ and $\mathrm{Spec}\, R \to W_{n,\mathbf{F}_p}$ such that the diagram

$$\begin{tikzcd}
\mathrm{Spec}\, S \arrow[r] \arrow[d] & W_{n,\mathbf{F}_p} \arrow[d, "F"] \\
\mathrm{Spec}\, R \arrow[r] & W_{n,\mathbf{F}_p}
\end{tikzcd}$$

is cartesian. Moreover the Hopf-Galois extension S/R has a normal basis in the sense of Kreimer-Takeuchi [5, Definition 2.6].

Remark 4.9. Let R be an $\mathbf{F}_p$-algebra and $\lambda \in R$. Then the isogeny $F - [\lambda^{p-1}] : W_{n,R} \to W_{n,R}$ is finite and flat. Here $[\lambda^{p-1}] = (\lambda^{p-1}, 0, \dots, 0)$ denotes the Teichmüller representative of λ^{p-1} in $W_n(R)$. Put $N = \mathrm{Ker}[F - [\lambda^{p-1}] : W_{n,R} \to W_{n,R}]$.

Now we define an affine group R-scheme Γ by $\Gamma = \mathrm{Spec}\, R[T]/(T^{p^n})$ with
(a) the multiplication: $T \mapsto T \otimes 1 + 1 \otimes T + \lambda T \otimes T$;
(b) the unit: $T \mapsto 0$;
(c) the inverse: $T \mapsto -T/(1 + \lambda T)$.

It is deduced immeadiately from [7, Theorem 2.19.1] that the Cartier dual of Γ is isomorphic to N. More precisely, the correspondence

$$(a_0, a_1, \dots, a_{n-1}) \mapsto E_p(a_0, \lambda; T) E_p(a_1, \lambda^p; T^p) \dots E_p(a_{n-1}, \lambda^{p^{n-1}}; T^{p^{n-1}})$$

gives rise to a bijection

$$N(R) = \mathrm{Ker}[F - [\lambda^{p-1}] : W_n(R) \to W_n(R)] \xrightarrow{\sim} \mathrm{Hom}_{R\text{-gr}}(\Gamma, \mathbf{G}_{m,R}).$$

(Or we can reduce the verification to the case of $n = 1$, which is stated in [10, Theorem 2.7] in a different form, as is done in [12].)

Furthermore we obtain a commutative diagram of group schemes over R with exact rows

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r] \arrow[d, equal] & \prod_{A/R} \mathbf{G}_{m,A} \arrow[r] \arrow[d, "\wr\, \chi^{(\lambda)}"] & \left(\prod_{A/R} \mathbf{G}_{m,A}\right)\Big/ N \arrow[r] \arrow[d, "\wr"] & 0 \\
0 \arrow[r] & N \arrow[r] & \mathbf{G}_{m,R} \times \prod_{\substack{1 \le j < p^n \\ (j,p)=1}} U_{j,R} \arrow[r, "\Theta"] & \mathbf{G}_{m,R} \times \prod_{\substack{1 \le j < p^n \\ (j,p)=1}} U_{j,R} \arrow[r] & 0,
\end{tikzcd}$$

where $A = R[T]/(T^{p^n})$, and Θ is defined by the diagonal matrix with the entries $F - [\lambda^{p-1}] : W_{n,R} \to W_{n,R}$ for $j = 1$ and the identity map for the others.

Putting $\lambda = 0$ and $\lambda = 1$, we recover the diagrams in 4.8 and 4.1 respectively.

Example 4.10. Consider now the Grothendieck resolution of $\boldsymbol{\alpha}_{p^n} = \mathrm{Ker}[F^n : \mathbf{G}_{a,\mathbf{F}_p} \to \mathbf{G}_{a,\mathbf{F}_p}]$. As is recalled in 4.8, the Cartier dual of $\boldsymbol{\alpha}_{p^n}$ is isomorphic to ${}_1W_n = \mathrm{Ker}[F : W_{n,\mathbf{F}_p} \to W_{n,\mathbf{F}_p}]$. Hence the Grothendieck resolution of the finite group scheme $\boldsymbol{\alpha}_{p^n}$ is written as

$$0 \to \boldsymbol{\alpha}_{p^n} \to \prod_{A/\mathbf{F}_p} \mathbf{G}_{m,A} \to \left(\prod_{A/\mathbf{F}_p} \mathbf{G}_{m,A}\right) \Big/ \boldsymbol{\alpha}_{p^n} \to 0.$$

where $A = \mathbf{F}_p[T_0, T_1, \dots, T_{n-1}]/(T_0^p, T_1^p, \dots, T_{n-1}^p)$. For an $\mathbf{F}_p$-algebra R, the injection

$$\boldsymbol{\alpha}_{p^n}(R) \to \left(\prod_{A/\mathbf{F}_p} \mathbf{G}_{m,A}\right)(R) = (R[T_0, T_1, \dots, T_{n-1}]/(T_0^p, T_1^p, \dots, T_{n-1}^p))^\times$$

is given by

$$a \mapsto E_p(aT_0)E_p(a^pT_1)\dots E_p(a^{p^{n-1}}T_{n-1}).$$

Put now $A_0 = \mathbf{F}_p[T]/(T^p)$. Let R be an $\mathbf{F}_p$-algebra. Then the homomorphism of rings

$$\begin{aligned}&R[T_0, T_1, \dots, T_{n-1}]/(T_0^p, T_1^p, \dots, T_{n-1}^p) \\ &\qquad \to R[T]/(T^p) : T_0 \mapsto T, T_1 \mapsto 0, \dots, T_{n-1} \mapsto 0\end{aligned}$$

induces a homomorphism of multiplicative groups

$$\begin{aligned}\pi_R : \left(\prod_{A/\mathbf{F}_p} \mathbf{G}_{m,A}\right)(R) &= (R[T_0, T_1, \dots, T_{n-1}]/(T_0^p, T_1^p, \dots, T_{n-1}^p))^\times \\ &\to \left(\prod_{A_0/\mathbf{F}_p} \mathbf{G}_{m,A}\right)(R) = (R[T]/(T^p))^\times.\end{aligned}$$

It is readily seen that π_R is represented by a homomorphism of group schemes over $\mathbf{F}_p$

$$\pi : \prod_{A/\mathbf{F}_p} \mathbf{G}_{m,A} \to \prod_{A_0/\mathbf{F}_p} \mathbf{G}_{m,A}.$$

Put

$$\tilde{\chi} = \chi_1^{(0)} \circ \pi : \prod_{A/\mathbf{F}_p} \mathbf{G}_{m,A} \to \prod_{A_0/\mathbf{F}_p} \mathbf{G}_{m,A} \to U_1 = \mathbf{G}_{a,\mathbf{F}_p}.$$

Then we obtain a commutative diagram of group schemes over $\mathbf{F}_p$ with exact rows

$$\begin{tikzcd}
0 \arrow[r] & \boldsymbol{\alpha}_{p^n} \arrow[r] \arrow[d, equal] & \prod_{A/\mathbf{F}_p} \mathbf{G}_{m,A} \arrow[r] \arrow[d, "\tilde{\chi}"] & \left(\prod_{A/\mathbf{F}_p} \mathbf{G}_{m,A}\right)\Big/\boldsymbol{\alpha}_{p^n} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \boldsymbol{\alpha}_{p^n} \arrow[r] & \mathbf{G}_{a,\mathbf{F}_p} \arrow[r, "F^n"] & \mathbf{G}_{a,\mathbf{F}_p} \arrow[r] & 0.
\end{tikzcd}$$

On the other hand, for an $\mathbf{F}_p$-algebra R, we define a map

$$\imath_R : \mathbf{G}_a(R) = R \to \left(\prod_{A/\mathbf{F}_p} \mathbf{G}_{m,A}\right)(R) = (R[T_0, T_1, \ldots, T_{n-1}]/(T_0^p, T_1^p, \ldots, T_{n-1}^p))^\times$$

by

$$a \mapsto E_p(aT_0)E_p(a^pT_1)\ldots E_p(a^{p^{n-1}}T^{n-1}).$$

It is verified that $\imath_R$ is represented by a homomorphism of group schemes over $\mathbf{F}_p$

$$\imath : \mathbf{G}_{a,\mathbf{F}_p} \to \prod_{A/\mathbf{F}_p} \mathbf{G}_{m,A}.$$

Moreover we obtain a commutative diagram of group schemes over $\mathbf{F}_p$ with exact rows

$$\begin{tikzcd}
0 \arrow[r] & \boldsymbol{\alpha}_{p^n} \arrow[r] \arrow[d, equal] & \mathbf{G}_{a,\mathbf{F}_p} \arrow[r, "F^n"] \arrow[d, "\imath"] & \mathbf{G}_{a,\mathbf{F}_p} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \boldsymbol{\alpha}_{p^n} \arrow[r] & \prod_{A/\mathbf{F}_p} \mathbf{G}_{m,A} \arrow[r] & \left(\prod_{A/\mathbf{F}_p} \mathbf{G}_{m,A}\right)\Big/\boldsymbol{\alpha}_{p^n} \arrow[r] & 0.
\end{tikzcd}$$

As a consequence, we arrive at the following assertion. Let R be an $\mathbf{F}_p$-algebra and S an R-algebra such that Spec S is a torsor under $\boldsymbol{\alpha}_{p^n}$. Then there exist morphisms Spec $S \to \mathbf{G}_{a,\mathbf{F}_p}$ and Spec $R \to \mathbf{G}_{a,\mathbf{F}_p}$ such that the diagram

$$\begin{tikzcd}
\operatorname{Spec} S \arrow[r] \arrow[d] & \mathbf{G}_{a,\mathbf{F}_p} \arrow[d, "F^n"] \\
\operatorname{Spec} R \arrow[r] & \mathbf{G}_{a,\mathbf{F}_p}
\end{tikzcd}$$

is cartesian. Moreover the Hopf-Galois extension S/R is has a normal basis.

REMARK 4.11. Kreimer-Takeuchi [5] treats Example 4.8 and Example 4.10 as Example 4 and Example 3 respectively from a different aspect.

Acknowledgement

This article was written during the author's stay at Torre Archimede of Università degli studi di Padova. He would like to express his hearty thanks to its hospitality. In particular he is very grateful to Marco Garuti for his helpful advices and notices. He thanks also Boris Kunyavskii for his interest in this work.

References

[1] H. Chu, S. J. Hu, M. C. Kang, B. E. Kunyavskii, Noether's problem and the unramified Brauer group for groups of order 64, Int. Math. Res. Not. IMRN (2010) 2329–2366.

[2] M. Demazure, P. Gabriel, Groupes algébriques, Tome I, Masson & Cie, Editeur, Paris; North-Holland Publishing, Amsterdam, 1970.

[3] B. Dwork, On the rationality of the zeta function of an algebraic variety, Amer. J. Math. **82** (1960) 631–648.

[4] M. Hazewinkel, Formal groups and applications, Academic Press. New York, 1978.

[5] H. F. Kreimer, M. Takeuchi, Hopf algebras and Galois extensions of an algebra, Indiana Univ. Math. J. **30** (1981) 675–692.

[6] H. Kuniyoshi, On a problem of Chevalley, Nagoya Math. J. **8** (1955) 65–67.

[7] T. Sekiguchi, N. Suwa, A note on extensions of algebraic and formal groups IV, Tôhoku Math. J. **53** (2001) 203–240.

[8] J. P. Serre, Groupes algébriques et corps de classes, Hermann, Paris, 1959

[9] N. Suwa, Around Kummer theories, RIMS Kôkyûroku Bessatsu **B12** (2009) 115–148.

[10] Y. Tsuno, Degenerations of the Kummer sequence in characteristic $p > 0$, J. Théor. Nombres Bordeaux **22** (2010) 199–237.

[11] Y. Tsuno, Normal basis problem for torsors under a finite flat group scheme, RIMS Kôkyûroku Bessatsu **B25** (2009) 53–74.

[12] M. Amano, On the Cartier duality of certain finite group schemes of order p^n, Tokyo J. Math. **33** (2010) 117–127.

Noriyuki Suwa
Department of Mathematics
Chuo University
1-13-27 *Kasuga, Bunkyo-ku*
Tokyo 112-8551, *Japan*
E-mail: suwa@math.chuo-u.ac.jp