

Kummer-Artin-Schreier-Witt 理論の試み I

諏訪紀幸 (東京電機大学工学部)

1. 動機と主要な結果

1.1. K を体とする. K が標数 $\neq p$ で, K が 1 の p^n 乗根をすべて含むとき, K の p^n 次巡回拡大は K の元の p^n 乗根を添加することによって得られる (Kummer 理論). これは, 次の事実から導かれる.

(1) p が K で可逆なら, K の上の group scheme の完全列

$$0 \longrightarrow \mu_{p^n, K} \longrightarrow G_{m, K} \xrightarrow{p^n} G_{m, K} \longrightarrow 0$$

が $\text{Spec}K$ の上の étale 位相に対して完全. ($G_{m, K}$ は K の上の multiplicative group scheme);

(2) (Hilbert 90) $H_{\text{ét}}^1(K, G_{m, K}) = 0$

一方, K の標数が $p > 0$ のときは, K の p^n 次巡回拡大は Witt vector の方程式 $(t_0^p, t_1^p, \dots, t_{n-1}^p) - (t_0, t_1, \dots, t_{n-1}) = (a_0, a_1, \dots, a_{n-1})$ の根を添加することによって得られる (Artin-Schreier-Witt 理論). これは次の事実から導かれる.

(1) $\text{ch.}K = p > 0$ のとき, K の上の group scheme の完全列

$$0 \longrightarrow \mathbb{Z}/p^n \longrightarrow W_{n, K} \xrightarrow{F-1} W_{n, K} \longrightarrow 0$$

は $\text{Spec}K$ の上の étale 位相に対して完全. ($W_{n, K}$ は K の上の長さ n の Witt vector の group scheme);

(2) $H_{\text{ét}}^1(K, W_{n, K}) = 0$

1.2. 混標数の環の不分岐 p^n 次巡回拡大を記述する, Kummer 理論と Artin-Schreier-Witt 理論を統一する理論の存在は当然想起される問題であるが, Kummer の完全列と Artin-Schreier-Witt の完全列を結び付ける group scheme の完全列が $\mathbb{Z}_{(p)}[\mu_{p^n}]$ の上で存在する. 実際, $A = \mathbb{Z}_{(p)}[\mu_{p^n}]$ とすれば, A は $K = \mathbb{Q}(\mu_{p^n})$ を分数体とする離散付値環で, 剰余体は F_p に同型. このとき, A の上の smooth affine commutative group scheme の完全列

$$(\#_n) \quad 0 \longrightarrow \mathbb{Z}/p^n \longrightarrow W_{n, A} \xrightarrow{\Psi_n} U_{n, A} \longrightarrow 0$$

が存在して,

(1) $(\#_n)$ の generic fiber は完全列

$$0 \longrightarrow \mu_{p^n, K} \longrightarrow (G_{m, K})^n \xrightarrow{\Theta} (G_{m, K})^n \longrightarrow 0$$

に同型になる. ここで, $\Theta: (G_{m, Z})^n \rightarrow (G_{m, Z})^n$ は

$$(U_0, U_1, \dots, U_{n-1}) \mapsto (U_0^p, U_0^{-1}U_1^p, \dots, U_{n-1}^{-1}U_n^p) :$$

$$Z[U_0, \dots, U_{n-1}, U_0^{-1}, \dots, U_{n-1}^{-1}] \rightarrow Z[U_0, \dots, U_{n-1}, U_0^{-1}, \dots, U_{n-1}^{-1}]$$

によって定義される準同型;

(2) $(\#_n)$ の closed fiber は Artin-Schreier-Witt の完全列

$$0 \longrightarrow Z/p^n \longrightarrow W_{n, \mathbb{F}_p} \xrightarrow{F-1} W_{n, \mathbb{F}_p} \longrightarrow 0$$

に同型になる;

(3) (Hilbert 90) B が局所 A -代数なら, $H_{\text{et}}^1(B, W_{n, A}) = H_{\text{et}}^1(B, U_{n, A}) = 0$

註 1.3. $\Pi: (G_{m, Z})^n \rightarrow G_{m, Z}$ を

$$U \mapsto U_{n-1} : Z[U, U^{-1}] \rightarrow Z[U_0, \dots, U_{n-1}, U_0^{-1}, \dots, U_{n-1}^{-1}]$$

によって定義される準同型, $\mathcal{E}: (G_{m, Z})^n \rightarrow G_{m, Z}$ を

$$U \mapsto U_0 U_1^p \dots U_{n-1}^{p^{n-1}} : Z[U, U^{-1}] \rightarrow Z[U_0, \dots, U_{n-1}, U_0^{-1}, \dots, U_{n-1}^{-1}]$$

によって定義される準同型とすれば, 完全列の可換図式

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mu_{p^n, Z} & \longrightarrow & (G_{m, Z})^n & \xrightarrow{\Theta} & (G_{m, Z})^n \longrightarrow 0 \\ & & \parallel & & \downarrow \Pi & & \downarrow \mathcal{E} \\ 0 & \longrightarrow & \mu_{p^n, Z} & \longrightarrow & G_{m, Z} & \xrightarrow{p^n} & G_{m, Z} \longrightarrow 0 \end{array}$$

を得る.

1.4. $n=1$ の場合は Waterhouse [11] と関口 et al. [2] によって独立に定式化されたが, 理論の起源は Furtwängler の仕事に溯る. 一般の場合の理論の見通しをするために, ここで p 次の理論の概要を略述する.

A を整域, K を A の分数体とする. $\lambda \neq 0$ を A の可逆でない元とし, $A_0 = A/(\lambda)$ とする. A の上の smooth affine group scheme $\mathcal{G}^{(\lambda)}$ を

$$\mathcal{G}^{(\lambda)} = \text{Spec} A[T, 1/(\lambda T + 1)]$$

(1) (乗法) $T \mapsto \lambda T \otimes T + T \otimes 1 + 1 \otimes T;$

(2) (単位元) $T \mapsto 0$;

(3) (逆元) $T \mapsto -T/(\lambda T+1)$

で定義する. また, group scheme の準同型 $\alpha^{(\lambda)}: \mathcal{G}^{(\lambda)} = \text{Spec} A[T, 1/(\lambda T+1)] \rightarrow G_{m,A} = \text{Spec} A[U, U^{-1}]$ を

$$X \mapsto \lambda T+1 : A[U, U^{-1}] \rightarrow A[T, 1/(\lambda T+1)]$$

によつて定義する. このとき, $\alpha^{(\lambda)} \otimes_K: \mathcal{G}^{(\lambda)} \otimes_A K \rightarrow G_{m,K}$ は同型. また, $\mathcal{G}^{(\lambda)} \otimes_A A_0$ は G_{a,A_0} に他ならない.

(Hilbert 90) A が局所環なら,

$$H_{\text{ét}}^1(A, \mathcal{G}^{(\lambda)}) = 0$$

特に, $\zeta = e^{2\pi i/p}$, $\lambda = \zeta - 1$, $A = \mathbb{Z}[\zeta]$, $K = \mathbb{Q}(\zeta)$ とする. このとき, (λ) は A の prime ideal で, $(\lambda)^{p-1} = (p)$, $A/(\lambda) = \mathbb{F}_p$. 準同型 $\psi_1: \mathcal{G}^{(\lambda)} \rightarrow \mathcal{G}^{(\lambda^p)}$ を

$$T \mapsto \frac{(\lambda T+1)^{p-1}}{\lambda^p} : A[T, 1/(\lambda^p T+1)] \rightarrow A[T, 1/(\lambda T+1)]$$

によつて定義する. このとき, $\text{Ker} \psi_1 = \text{Spec} A[T, 1/(\lambda T+1)] / \left(\frac{(\lambda T+1)^{p-1}}{\lambda^p} \right)$ は constant group scheme \mathbb{Z}/p に同型. さらに,

group scheme の完全列の可換図式

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathbb{Z}/p & \longrightarrow & \mathcal{G}^{(\lambda)} & \xrightarrow{\psi_1} & \mathcal{G}^{(\lambda^p)} \longrightarrow 0 \\ & & \downarrow & & \downarrow \alpha^{(\lambda)} & & \downarrow \alpha^{(\lambda^p)} \\ 0 & \longrightarrow & \mu_{p,A} & \longrightarrow & G_{m,A} & \xrightarrow{p} & G_{m,A} \longrightarrow 0 \end{array}$$

を得る. このとき,

$$\begin{array}{ccccccc} [0 \longrightarrow \mathbb{Z}/p \longrightarrow \mathcal{G}^{(\lambda)} \xrightarrow{\psi_1} \mathcal{G}^{(\lambda^p)} \longrightarrow 0] \otimes_A K & & & & & & \\ & & \downarrow \zeta & & & & \\ [0 \longrightarrow \mu_{p,A} \longrightarrow G_{m,A} \xrightarrow{p} G_{m,A} \longrightarrow 0] \otimes_A K & & & & & & \end{array}$$

また,

$$[0 \longrightarrow \mathbb{Z}/p \longrightarrow \mathcal{G}^{(\lambda)} \xrightarrow{\psi_1} \mathcal{G}^{(\lambda^p)} \longrightarrow 0] \otimes_A \mathbb{F}_p$$

は Artin-Schreier の完全列

$$0 \longrightarrow \mathbb{Z}/p \longrightarrow G_{a,\mathbb{F}_p} \xrightarrow{F-1} G_{a,\mathbb{F}_p} \longrightarrow 0$$

に他ならない.

$$(\#_1) \quad 0 \longrightarrow Z/p \longrightarrow \mathcal{G}(\lambda) \xrightarrow{\psi_p} \mathcal{G}(\lambda^p) \longrightarrow 0$$

を Kummer-Artin-Schreier あるいは Furtwängler の完全列とよぶことにする.

Witt vector の formalism と両立するように $(\#_1)$ を積み重ねて $(\#_n)$ を構成する. 本稿では Witt vector について復習した後, $(\#_n)$ の構成の概略を述べる. II では Kummer-Artin-Schreier-Witt 理論に関する問題について説明する.

2. Witt vector

2.1. 各 $r \geq 0$ に対して

$$\Phi_r(T) = \Phi_r(T_0, T_1, \dots, T_r) = T_0^p + pT_1^{p-1} + \dots + p^r T_r \quad (\text{Witt 多項式})$$

と定義する. さらに,

$$S_r(X, Y) = S_r(X_0, X_1, \dots, X_r, Y_0, Y_1, \dots, Y_r),$$

$$P_r(X, Y) = P_r(X_0, X_1, \dots, X_r, Y_0, Y_1, \dots, Y_r)$$

をそれぞれ

$$\Phi_r(S_0, S_1, \dots, S_r) = \Phi_r(X_0, X_1, \dots, X_r) + \Phi_r(Y_0, Y_1, \dots, Y_r),$$

$$\Phi_r(P_0, P_1, \dots, P_r) = \Phi_r(X_0, X_1, \dots, X_r) \Phi_r(Y_0, Y_1, \dots, Y_r),$$

によって帰納的に定義する. このとき,

$$S_r(X, Y), P_r(X, Y) \in Z[X_0, X_1, \dots, X_r, Y_0, Y_1, \dots, Y_r]$$

例えば,

$$S_0(X_0, Y_0) = X_0 + Y_0, \quad S_1(X_0, X_1, Y_0, Y_1) = X_1 + Y_1 + \frac{X_0^p + Y_0^p - (X_0 + Y_0)^p}{p},$$

$$P_0(X_0, Y_0) = X_0 Y_0, \quad P_1(X_0, X_1, Y_0, Y_1) = X_0^p Y_1 + X_1 Y_0^p + p X_1 Y_1$$

$W_{n, Z} = \text{Spec} Z[T_0, T_1, \dots, T_{n-1}]$ に

$$\text{加法: } (T_0, T_1, \dots, T_{n-1}) \mapsto (S_0(X, Y), S_1(X, Y), \dots, S_{n-1}(X, Y)),$$

$$\text{乗法: } (T_0, T_1, \dots, T_{n-1}) \mapsto (P_0(X, Y), P_1(X, Y), \dots, P_{n-1}(X, Y))$$

によって環の構造を定義する. 零元は

$$(T_0, T_1, \dots, T_{n-1}) \mapsto (0, 0, \dots, 0)$$

で、単位元は

$$(T_0, T_1, \dots, T_{n-1}) \mapsto (1, 0, \dots, 0)$$

で与えられる.

さらに,

$$(T_0, T_1, \dots, T_{n-1}) \mapsto (T_0, T_1, \dots, T_{n-1}) : \\ Z[T_0, \dots, T_{n-1}] \rightarrow Z[T_0, \dots, T_{n-1}, T_n]$$

によつて環の準同型 $R: W_{n+1, Z} \rightarrow W_{n, Z}$ を,

$$(T_0, T_1, \dots, T_n) \mapsto (0, T_0, \dots, T_{n-1}) : \\ Z[T_0, \dots, T_{n-1}, T_n] \rightarrow Z[T_0, \dots, T_{n-1}]$$

によつて準同型 $V: W_{n, Z} \rightarrow W_{n+1, Z}$ を定義する. このとき, 群の完全列

$$(E_{m, n}) \quad 0 \rightarrow W_{n, Z} \xrightarrow{V^m} W_{n+m, Z} \xrightarrow{R^n} W_{m, Z} \rightarrow 0$$

を得る.

- (1) $\text{Ext}_Z^1(W_{m-1, Z}, W_{n, Z})$ において $[E_{m, n}]V = [E_{m-1, n}]$;
- (2) $\text{Ext}_Z^1(W_{m, Z}, W_{n-1, Z})$ において $R[E_{m, n}] = [E_{m, n-1}]$

$W_Z = \varprojlim W_{n, Z}$ とし, W_Z の部分関手 \hat{W}_Z を

$$\hat{W}(A) = \{ (a_r)_{r \geq 0} ; \text{各 } a_r \text{ は巾零, 有限個の } r \text{ を除いて } a_r = 0 \}$$

によつて定義する. このとき, \hat{W}_Z は W_Z の ideal.

$$2.2. \quad (T_0, T_1, \dots, T_{n-1}) \mapsto (T_0^p, T_1^p, \dots, T_{n-1}^p) :$$

$$F_p[T_0, T_1, \dots, T_{n-1}] \rightarrow F_p[T_0, T_1, \dots, T_{n-1}]$$

によつて環の準同型 $F: W_{n, F_p} \rightarrow W_{n, F_p}$ を定義する. このとき,

- (1) $FR = RF$;
- (2) $FV = VF$

A を F_p -代数とする. このとき, $\text{End}_{A\text{-gr}} G_{\alpha, A} = A[F]$. $\text{Ext}_A^1(W_{n, A}, G_{\alpha, A})$ は push-out によつて左 $A[F]$ -加群の構造を持つ.

補題 2.2.1. A を F_p -代数とする. このとき,

- (1) $\text{Ext}_A^1(W_{n,A}, G_{a,A})$ は $[E_{n,1}]$ を基底とする自由左 $A[F]$ -加群;
- (2) $V^*: \text{Ext}_A^1(W_{n,A}, G_{a,A}) \rightarrow \text{Ext}_A^1(W_{n-1,A}, G_{a,A})$ は左 $A[F]$ -加群の同型.

2.3. $E_p(U) = \exp\left(\sum_{r=0}^{\infty} \frac{U^{p^r}}{p^r}\right)$ (Artin-Hasse exponential)

とおく. このとき,

$$E_p(U) \in Z_{(p)}[[U]]$$

$U = (U_r)_{r \geq 0}$, $X = (X_r)_{r \geq 0}$ に対して

$$E_p(X, T) = \exp\left(\sum_{r=0}^{\infty} \frac{\Phi_r(X) \Phi_r(T)}{p^r}\right)$$

とおく. このとき,

$$E_p(X, T) E_p(Y, T) = E_p(S(X, Y), T),$$

$$E_p(X, T) E_p(X, U) = E_p(X, S(T, U))$$

さらに,

$$E_p(X; T_0, \dots, T_{n-1}) = E_p(X, (T_0, \dots, T_{n-1}, 0, \dots))$$

とおく. 例えば,

$$E_p(X; T) = \prod_{r=0}^{\infty} E_p(X_r T^{p^r})$$

A を F_p -代数とする. $a \in \hat{W}(A)$ なら, $E_p(a; T_0, \dots, T_{n-1}) \in A[T_0, \dots, T_{n-1}]$. さらに, $a \in {}_{F^n}\hat{W}(A)$ なら, $U \mapsto E_p(a; T_0, \dots, T_{n-1})$ によって $W_{n,A}$ から $G_{m,A}$ への準同型が定義される. $U \mapsto E_p(a; T_0, \dots, T_{n-1})$ は同型 ${}_{F^n}\hat{W}(A) \xrightarrow{\sim} \text{Hom}_{A\text{-gr}}(W_{n,A}, G_{m,A})$ を与える.

3. Kummer-Artin-Schreier-Witt 理論の構成

3.1. A を整域, K を A の分数体とする. $\lambda \neq 0$ を A の可逆でない元とし, $A_0 = A/(\lambda)$

とする。多項式の族 $F = (F_r(T))_{0 \leq r \leq n-1}$:

$$F_r(T) = F_r(T_0, T_1, \dots, T_{r-1}) \in A[T_0, T_1, \dots, T_{r-1}]$$

に対して

$$\alpha_0^F(T) = \alpha_r^F(T_0) = \lambda T_r + 1,$$

$$\alpha_r^F(T) = \alpha_r^F(T_0, \dots, T_r) = \lambda T_r + F_r(T_0, \dots, T_{r-1}) \quad (r \geq 1)$$

とおく。また,

$$\beta_r^F(U) = \beta_r^F(U_0, \dots, U_r) \in K[U_0, \dots, U_{r-1}],$$

$$\Lambda_r^F(X, Y) = \Lambda_r^F(X_0, \dots, X_r, Y_0, \dots, Y_r) \in K[X_0, \dots, X_r, Y_0, \dots, Y_r]$$

をそれぞれ帰納的に

$$\beta_r^F(U_0) = \frac{1}{\lambda} (U_0 - 1),$$

$$\beta_r^F(U_0, \dots, U_r) = \frac{1}{\lambda} [U_r - F_r(\beta_0^F(U), \beta_1^F(U), \dots, \beta_{r-1}^F(U))] \quad (r \geq 1)$$

あるいは,

$$\Lambda_0^F(X_0, Y_0) = \lambda X_0 Y_0 + X_0 + Y_0,$$

$$\Lambda_r^F(X_0, \dots, X_r, Y_0, \dots, Y_r) = \lambda X_r Y_r + X_r + Y_r$$

$$+ \frac{1}{\lambda} [F_r(X) F_r(Y) - F_r(\Lambda_0^F(X, Y), \dots, \Lambda_{r-1}^F(X, Y))] \quad (r \geq 1)$$

によって定義する。このとき,

$$(1) \alpha_r^F(\beta_0^F(U), \beta_1^F(U), \dots, \beta_r^F(U)) = U_r;$$

$$(2) \beta_r^F(\alpha_0^F(T), \alpha_1^F(T), \dots, \alpha_r^F(T)) = T_r;$$

$$(3) \alpha_r^F(\Lambda_0^F(X, Y), \Lambda_1^F(X, Y), \dots, \Lambda_r^F(X, Y)) = \alpha_r^F(X) \alpha_r^F(Y);$$

$$(4) \beta_r^F(X_0 Y_0, \dots, X_r Y_r) = \Lambda_r^F(\beta_0^F(X), \dots, \beta_r^F(X), \beta_0^F(Y), \dots, \beta_r^F(Y))$$

が成立する。

さらに, 各 r に対して $F_r(0) = F_r(0, \dots, 0) = 1$ なら,

$$(5) \alpha_r^F(0) = \alpha_r^F(0, \dots, 0) = 1;$$

$$(6) \beta_r^F(1) = \beta_r^F(1, \dots, 1) = 1;$$

$$(7) \Lambda_r^F(0, 0) = \Lambda_r^F(0, \dots, 0, 0, \dots, 0) = 0;$$

$$(8) \Lambda_r^F(\beta_0^F(X_0), \dots, \beta_r^F(X_0, \dots, X_r), \beta_0^F(X_0^{-1}), \dots, \beta_r^F(X_0^{-1}, \dots, X_r^{-1})) = 0;$$

$$(9) \Lambda_r^F(0, \dots, 0, X, 0, \dots, 0, Y) = \Lambda_0^F(X, Y) = \lambda XY + X + Y$$

が成立する。

命題 3.1.1. 各 $r \geq 0$ に対して

$$(0) F_r(0) = F_r(0, \dots, 0) = 1;$$

$$(1) F_r(X)F_r(Y) \equiv F_r(\Lambda_0^r(X, Y), \dots, \Lambda_{r-1}^r(X, Y)) \pmod{\lambda}$$

が成立すると仮定する. このとき,

$$(T_0, T_1, \dots, T_{n-1}) \mapsto (\Lambda_0^r(T \otimes 1, 1 \otimes T), \Lambda_1^r(T \otimes 1, 1 \otimes T), \dots, \Lambda_{n-1}^r(T \otimes 1, 1 \otimes T))$$

は

$$W_n^r = \text{Spec } A[T_0, T_1, \dots, T_{n-1}, \alpha_0^r(T)^{-1}, \alpha_1^r(T)^{-1}, \dots, \alpha_{n-1}^r(T)^{-1}]$$

の上に乗法を定義する. 単位元は

$$(T_0, T_1, \dots, T_{n-1}) \mapsto (0, 0, \dots, 0)$$

よって与えられる.

3.2. W_n^r は affine 空間 A^n の open subscheme なので, W_n^r は A の上に smooth. B を A -代数, $b = (b_0, b_1, \dots, b_{n-1}) \in B^n$ とする. このとき, b が $W_n^r(B)$ に属する $\Leftrightarrow \alpha_0^r(b), \alpha_1^r(b), \dots, \alpha_{n-1}^r(b)$ が B で可逆.

準同型 $\alpha^r: W_n^r \rightarrow (G_{m,A})^n$ を

$$\begin{aligned} (U_0, U_1, \dots, U_{n-1}) &\mapsto (\alpha_0^r(T), \alpha_1^r(T), \dots, \alpha_{n-1}^r(T)): \\ A[T_0, T_1, \dots, T_{n-1}, \alpha_0^r(T)^{-1}, \alpha_1^r(T)^{-1}, \dots, \alpha_{n-1}^r(T)^{-1}] &\rightarrow \\ A[U_0, \dots, U_{n-1}, U_0^{-1}, \dots, U_{n-1}^{-1}] & \end{aligned}$$

によって, 準同型 $\beta^r: (G_{m,K})^n \rightarrow W_{n,K}^r$ を

$$\begin{aligned} (T_0, T_1, \dots, T_{n-1}) &\mapsto (\beta_0^r(U), \beta_1^r(U), \dots, \beta_{n-1}^r(U)): \\ K[U_0, \dots, U_{n-1}, U_0^{-1}, \dots, U_{n-1}^{-1}] &\rightarrow \\ K[T_0, T_1, \dots, T_{n-1}, \alpha_0^r(T)^{-1}, \alpha_1^r(T)^{-1}, \dots, \alpha_{n-1}^r(T)^{-1}] & \end{aligned}$$

によって定義する. このとき, $\beta^r = (\alpha_K^r)^{-1}$, したがって, β^r は同型.

自然な単射 $(T_0, T_1, \dots, T_{n-2}) \mapsto (T_0, T_1, \dots, T_{n-2})$:

$$\begin{aligned} A[T_0, T_1, \dots, T_{n-2}, \alpha_0^r(T)^{-1}, \alpha_1^r(T)^{-1}, \dots, \alpha_{n-2}^r(T)^{-1}] &\rightarrow \\ A[T_0, T_1, \dots, T_{n-1}, \alpha_0^r(T)^{-1}, \alpha_1^r(T)^{-1}, \dots, \alpha_{n-1}^r(T)^{-1}] & \end{aligned}$$

によって群の準同型 $R: W_n^r \rightarrow W_{n-1}^r$ を定義する. このとき, R は全射で, $\text{Ker} R$ は $\mathcal{G}^{(\lambda)}$ に同型. A の上の group scheme の完全列

$$0 \rightarrow \mathcal{G}^{(\lambda)} \rightarrow W_n^F \xrightarrow{R} W_{n-1}^F \rightarrow 0$$

から, A_0 の上の group scheme の完全列

$$(E_{n-1,1}^F) \quad 0 \rightarrow G_{\alpha, A_0} \rightarrow W_{n, A_0}^F \xrightarrow{R} W_{n-1, A_0}^F \rightarrow 0$$

を得る. したがって, W_{n, A_0}^F は G_{α, A_0} の successive extension. 拡大 $(E_{n-1,1}^F)$ は 2-cocycle

$$\frac{1}{\lambda} [F_{n-1}(X)F_{n-1}(Y) - F_{n-1}(\Lambda_0^F(X, Y), \dots, \Lambda_{n-2}^F(X, Y))] \in Z_0^2(W_{n-2, A_0}^F, G_{\alpha, A_0})$$

によって定義される.

3.3. 以下, A は剰余体が標数 p の局所環で, $\lambda | p$ と仮定する.

各 r に対して $F_r(0, \dots, 0, T) \pmod{\lambda}$ が次数 $\leq p-1$ と仮定する. このとき, $\lambda | c_r^p$ を満たす $c_r \in A$ が存在して

$$F_r(0, \dots, 0, T) \equiv \sum_{i=0}^{p-1} \frac{(c_r T)^i}{i!} \pmod{\lambda}$$

となる.

命題 3.3.1. 各 r に対して

$$F_r(0, \dots, 0, T) \equiv \sum_{i=0}^{p-1} \frac{(c_r T)^i}{i!} \pmod{\lambda}$$

で, $\frac{c_r^p}{\lambda}$ が A_0 で可逆であると仮定する. このとき, 各 W_{r, A_0}^F は W_{r, A_0} に同型.

r に関する帰納法による. 拡大の同型

$$\begin{array}{ccccccc} 0 & \longrightarrow & G_{\alpha, A_0} & \xrightarrow{V^{r-1}} & W_{r, A_0}^F & \xrightarrow{R} & W_{r-1, A_0}^F \longrightarrow 0 \\ & & \downarrow a_r & & \downarrow \tilde{h}_r & & \downarrow \tilde{h}_{r-1} \\ 0 & \longrightarrow & G_{\alpha, A_0} & \xrightarrow{V^{r-1}} & W_{r, A_0} & \xrightarrow{R} & W_{r-1, A_0} \longrightarrow 0 \end{array}$$

a_r は A の可逆元,

が存在すると仮定する. $[E_{r,1}^F]$ を拡大

$$0 \rightarrow G_{\alpha, A_0} \rightarrow W_{r+1, A_0}^F \rightarrow W_{r, A_0}^F \rightarrow 0$$

の $\text{Ext}_{A_0}^1(W_{r, A_0}^F, G_{\alpha, A_0})$ における類とする. このとき, 仮定から A_0 で可逆な A の元 a_{r+1} が存在して $\text{Ext}_{A_0}^1(G_{\alpha, A_0}, G_{\alpha, A_0})$ において

$$[E_{r,1}^F] \tilde{h}_r^{-1} V^{r-1} = [E_{r,1}^F] V^{r-1} a_r^{-1} = a_{r+1}^{-1} [E_{1,1}]$$

となる。ここで、 $[E_{1,1}] = [E_{r,1}]V^{r-1}$ で、 $(V^{r-1})^* : \text{Ext}_{A_0}^1(W_{r,A_0}, G_{a,A_0}) \rightarrow \text{Ext}_{A_0}^1(G_{a,A_0}, G_{a,A_0})$ が双射なので、

$$[E_{r,1}^F] = a_{r+1}^{-1} [E_{r,1}] \tilde{h}_r$$

これから、拡大の同型

$$\begin{array}{ccccccc} 0 & \longrightarrow & G_{a,A_0} & \xrightarrow{V^r} & W_{r+1,A_0}^F & \xrightarrow{R} & W_{r,A_0}^F \longrightarrow 0 \\ & & \downarrow a_{r+1} & \downarrow V^r & \downarrow \tilde{h}_{r+1} & \downarrow R & \downarrow \tilde{h}_r \\ 0 & \longrightarrow & G_{a,A_0} & \longrightarrow & W_{r+1,A_0} & \xrightarrow{R} & W_{r,A_0} \longrightarrow 0 \end{array}$$

を得る。

以上の構成から、 $\tilde{h}_n : W_{n,A_0}^F \xrightarrow{\sim} W_{n,A_0}$ は

$$T_0 \mapsto h_0(T) = T_0,$$

$$T_j \mapsto h_r(T) = a_r(T_0, \dots, T_{r-1})T_r + b_r(T_0, \dots, T_{r-1}),$$

$$a_r(0) \equiv a_r \pmod{\lambda}, \quad b_r(0) \equiv 0 \pmod{\lambda} \quad (j \geq 1)$$

の形をしていることが従う。

3.4. $\zeta_k = e^{2\pi i/p^k}$ とおき、 $\tilde{A} = Z_{(p)}[\zeta_k; k > 0]$ とする。各 k に対して $\lambda_k = \zeta_k - 1$ とおく。特に、 $\lambda = \lambda_1 = \zeta_1 - 1$ とおく。 v を $v(p) = 1$ によって正規化された p 進付値とすれば、 $v(\lambda_k) = \frac{1}{(p-1)p^{k-1}}$

A を $Z[\zeta_1]$ を含む \tilde{A} の部分環、 K を A の分数体、 $A_0 = A/(\lambda)$ とする。

$i = \sum_{k=0}^{\infty} i_k p^k \in Z_p$ に対して

$$\zeta_{r+1}^i = \zeta_{r+1}^{i_0 + i_1 p + i_2 p^2 + \dots + i_r p^r}$$

と定義する。多項式の族 $F = (F_r(T))_{0 < r \leq n-1}$:

$$F_r(T) = F_r(T_0, T_1, \dots, T_{r-1}) \in A[T_0, T_1, \dots, T_{r-1}]$$

に対して

$$\omega_r^F(i) = \beta_r^F(\zeta_1^i, \dots, \zeta_r^i)$$

とおく。このとき、

$$(1) \quad \omega_r^F(i) = \omega_r^F(j) \Leftrightarrow i \equiv j \pmod{p^{r+1}};$$

$$(2) \quad \alpha_r^F(\omega_0^F(i), \omega_1^F(i), \dots, \omega_r^F(i)) = \zeta_{r+1}^i;$$

$$(3) A_r^F(\omega_0^F(i), \dots, \omega_r^F(i), \omega_0^F(i), \dots, \omega_r^F(i)) = \omega_r^F(i+j);$$

が成立する. さらに, 各 r に対して $F_r(0) = F_r(0, \dots, 0) = 1$ なら,

$$(4) \omega_r^F(0) = 0;$$

$$(5) \omega_r^F(p^r) = 1, \omega_r^F(p^m) = 0 \quad (m > r)$$

が成立する.

命題 3.4.1. 各 $r \geq 0$ に対して各 $r \geq 0$ に対して

$$(O) F_r(0) = F_r(0, \dots, 0) = 1;$$

$$(I) F_r(X)F_r(Y) \equiv F_r(A_0^F(X, Y), \dots, A_{r-1}^F(X, Y)) \pmod{\lambda}$$

$$(II) F_r(\omega_0^F(1), \omega_1^F(1), \dots, \omega_r^F(1)) \equiv \zeta_{r+1} \pmod{\lambda}$$

が成立すると仮定する. このとき, $i \mapsto (\omega_0^F(i), \omega_1^F(i), \dots, \omega_{n-1}^F(i))$ は単射 $\omega: Z/p^n \rightarrow W_n^F$ を誘導する. さらに, 各 $r \geq 0$ に対して

$$(III) F_r(0, \dots, 0, T) \pmod{\lambda} \text{ は次数 } \leq p-1$$

が成立すれば, 各 W_{r, A_0}^F は W_{r, A_0} に同型.

実際, $\lambda | c_r^p$ を満たす $c_r \in A$ が存在して

$$F_r(0, \dots, 0, T) \equiv \sum_{i=0}^{p-1} \frac{(c_r T)^i}{i!} \pmod{\lambda}$$

となる. ここで,

$$\begin{aligned} F_r(0, \dots, 0, 1) &= F_r(\omega_0^F(p^{r-1}), \dots, \omega_{r-2}^F(p^{r-1}), \omega_{r-1}^F(p^{r-1})) \\ &\equiv \zeta_{r+1}^{p^{r-1}} = \zeta_2 \pmod{\lambda} \end{aligned}$$

したがって,

$$c_r \equiv \zeta_2 - 1 \pmod{\lambda}$$

これから, $\frac{c_r^p}{\lambda}$ は A_0 で可逆.

さらに, $\tilde{h}_n: W_{n, A_0}^F \xrightarrow{\sim} W_{n, A_0}$ を 3.3.1 で構成した同型とする. 各 a_j を適宜取り替えることによつて,

$$T_0 \mapsto h_0(T) = T_0,$$

$$T_j \mapsto h_r(T) = a_r(T_0, \dots, T_{r-1})T_r + b_r(T_0, \dots, T_{r-1}),$$

$$a_r(0) \equiv a_r \pmod{\lambda}, \quad b_r(0) \equiv 0 \pmod{\lambda},$$

$$h_j(\omega^F(1)) \equiv 0 \pmod{\lambda} \quad (j \geq 1)$$

の形に構成できる.

実際,

$$h_1(\omega^F(1)) \equiv \dots \equiv h_{r-2}(\omega^F(1)) \equiv 0 \pmod{\lambda}$$

と仮定すれば, $W_r(A_0)$ において

$$\tilde{h}_r(\omega^F(1)) = (1, 0, \dots, 0, h_{r-1}(\omega^F(1)))$$

したがって, $\tilde{h}_r(\omega^F(1))$ は $W_r(A_0)$ において可逆. a_r を $\tilde{h}_r(\omega^F(1))^{-1}a_r$ で置き換えればよい.

定理 3.5. 多項式の族 $F = (F_r(T))_{r \geq 0}$:

$$F_r(T) = F_r(T_0, \dots, T_{r-1}) \in Z_{(p)}[\zeta_{r+1}][T_0, \dots, T_{r-1}]$$

が存在して, 各 r に対して

- (O) $F_r(0, \dots, 0) = 1$;
- (I) $F_r(X)F_r(Y) \equiv F_r(\Lambda_0^F(X, Y), \dots, \Lambda_{r-1}^F(X, Y)) \pmod{\lambda}$;
- (II) $F(\omega_0^F(1), \omega_1^F(1), \dots, \omega_r^F(1)) \equiv \zeta_{r+1} \pmod{\lambda}$;
- (III) $F_r(0, \dots, 0, T) \pmod{\lambda}$ は次数 $\leq p-1$

となる.

帰納的に $F_r(T) = F_r(T_0, \dots, T_{r-1})$ を定義する.

$L_p(1+U)$ を $E_p(U)$ の逆級数とし, 各 $r \geq 1$ に対して

$$\eta_r = L(\zeta_r) = L_p(1+\lambda_r) \in Z_p[\zeta_r]$$

とおく. このとき, $Z_p[\zeta_r]$ において $(\eta_r) = (\lambda_r)$, また, $E_p(\eta_r) = \zeta_r$. さらに,

- (1) $\lambda_{r+1}^p \equiv \lambda_r \pmod{p}$;
- (2) $\eta_{r+1}^p \equiv \lambda_1 \pmod{p}$

$F_1(T), F_2(T), \dots, F_{r-1}(T)$ を (O), (I), (II), (III) を満たす多項式の族とする.

このとき,

$$T_0 \mapsto h_0(T) = T_0,$$

$$T_j \mapsto h_j(T) = a_j(T_0, \dots, T_{j-1})T_j + b_j(T_0, \dots, T_{j-1}) \quad (j \geq 1),$$

$$a_j(0) \equiv a_j \pmod{\lambda}, \quad b_j(0) \equiv 0 \pmod{\lambda},$$

$$h_j(\omega^F(1)) \equiv 0 \pmod{\lambda} \quad (1 \leq j \leq r-1)$$

の形をしている同型 $\tilde{h}_r: W_{r, A_0}^F \xrightarrow{\sim} W_{r, A_0}$ が存在する.

$$\begin{aligned} \tilde{F}_r(T) &= \tilde{F}_r(T_0, T_1, \dots, T_{r-1}) = \\ &\prod_{j=0}^{r-1} E_p(\eta_{r+1}^{p^j} h_j(T)) \in Z_p[\zeta_{r+1}][[T_0, T_1, \dots, T_{r-1}]] \end{aligned}$$

とおき,

$$F_r(T) = F_r(T_0, T_1, \dots, T_{r-1}) \in Z_{(p)}[\zeta_{r+1}][[T_0, T_1, \dots, T_{r-1}]]$$

を

$$F_r(0) = 1;$$

$$F_r(T) \equiv \tilde{F}_r(T) \pmod{\lambda}$$

となるように選ぶ. このとき, $F = (F_1(T), F_2(T), \dots, F_r(T))$ は (I), (II), (III) を満たす.

(I)の証明

$\eta_{r+1}^{p^r} \equiv 0 \pmod{\lambda}$ なので, $U \mapsto \prod_{j=0}^{r-1} E_p(\eta_{r+1}^{p^j} T)$ は準同型 $W_{r, A_0} \rightarrow G_{m, A_0}$ を定義する. したがって, $U \mapsto F_r(T) = \prod_{j=0}^{r-1} E_p(\eta_{r+1}^{p^j} h_j(T))$ は準同型 $W_{r, A_0}^F \rightarrow G_{m, A_0}$ を定義する.

(II)の証明

$h_0(T) = T_0$ なので,

$$h_0(\omega^F(1)) = \omega_0^F(1) = 1$$

したがって,

$$E_p(\eta_{r+1} h_0(\omega^F(1))) = E_p(\eta_{r+1}) \equiv \zeta_{r+1} \pmod{\lambda}$$

さらに, $1 \leq j \leq r-1$ なら,

$$h_j(\omega^F(1)) \equiv 0 \pmod{\lambda}$$

なので,

$$E_p(\eta_{r+1}^{p^j} h_0(\omega^F(1))) \equiv E_p(0) = 1 \pmod{\lambda}$$

したがって,

$$\tilde{F}_r(\omega^F(1)) = \prod_{j=0}^{r-1} E_p(\eta_{r+1}^{p^j} h_j(\omega^F(1))) \equiv \zeta_{r+1} \pmod{\lambda}$$

したがって,

$$F_r(\omega^p(1)) \equiv \zeta_n \pmod{\lambda}$$

(III)の証明

$j \leq r-2$ なら,

$$h_j(0) \equiv 0 \pmod{\lambda}$$

なので,

$$E_p(\eta_{r+1}^{p^j} h_j(0)) \equiv 1 \pmod{\lambda}$$

一方,

$$h_{r-1}(0, \dots, 0, T) \equiv a_{r-1} T \pmod{\lambda},$$

なので,

$$E_p(\eta_{r+1}^{p^r} h_{r-1}(0)) \equiv \sum_{i=0}^{p-1} \frac{(\eta_{r+1}^{p^r} a_{r-1} T)^i}{i!} \pmod{\lambda}$$

3.6. $w_n = w_n^p$, $v_n = w_n / (Z/p^n)$ とおく. このとき, 多項式の族 $G = (G_r(T))_{r \geq 0}$:

$$G_r(T) = G_r(T_0, \dots, T_{r-1}) \in Z_{(p)}[\zeta_{r+1}][T_0, \dots, T_{r-1}]$$

が存在して,

$$v_n = \text{Spec } A[T_0, T_1, \dots, T_{n-1}, \alpha_0^G(T)^{-1}, \alpha_1^G(T)^{-1}, \dots, \alpha_{n-1}^G(T)^{-1}]$$

で,

$$(T_0, T_1, \dots, T_{r-1}) \mapsto (\Lambda_0^G(T \otimes 1, 1 \otimes T), \Lambda_1^G(T \otimes 1, 1 \otimes T), \dots, \Lambda_{n-1}^G(T \otimes 1, 1 \otimes T))$$

によって乗法が定義される. ここで,

$$\alpha_r^G(T) = \alpha_r^G(T_0, \dots, T_r) = \lambda^p T_r + G_r(T_0, \dots, T_{r-1})$$

とおき,

$$\Lambda_r^G(X, Y) = \Lambda_r^G(X_0, \dots, X_r, Y_0, \dots, Y_r) \in K[X_0, \dots, X_r, Y_0, \dots, Y_r]$$

を帰納的に

$$\Lambda_0^G(X_0, Y_0) = \lambda^p X_0 Y_0 + X_0 + Y_0,$$

$$\Lambda_r^G(X_0, \dots, X_r, Y_0, \dots, Y_r) = \lambda^p X_r Y_r + X_r + Y_r$$

$$+ \frac{1}{\lambda^p} [G_r(X) G_r(Y) - G_r(\Lambda_0^G(X, Y), \dots, \Lambda_{r-1}^G(X, Y))] \quad (r \geq 1)$$

によって定義する. 各 $r > 0$ に対して

$$G_r(X)G_r(Y) \equiv G_r(\Lambda_0^F(X,Y), \dots, \Lambda_{r-1}^F(X,Y)) \pmod{\lambda^p}$$

が成立する.

準同型 $\psi: W_n \rightarrow U_n$ は

$$(T_0, T_1, \dots, T_{n-1}) \mapsto (\psi_0(T), \psi_1(T), \dots, \psi_{n-1}(T))$$

によって定義される. ここで,

$$\lambda^p \psi_0(T_0) = (\lambda T_0 + 1)^p$$

を, また, 各 $r \geq 1$ に対して

$$\lambda^p \psi_r(T) + G_r(\psi_0(T), \psi_1(T), \dots, \psi_{r-1}(T)) = \left\{ \lambda T_{r-1} + F_{r-1}(T) \right\}^{-1} \left\{ \lambda T_r + F_r(T) \right\}^p$$

が成立する.

また, 準同型 $\alpha^G: U \rightarrow (G_{m,A})^n$ を

$$(U_0, U_1, \dots, U_{n-1}) \mapsto (\alpha_0^G(T), \alpha_1^G(T), \dots, \alpha_{n-1}^G(T)):$$

$$A[T_0, T_1, \dots, T_{n-1}, \alpha_0^G(T)^{-1}, \alpha_1^G(T)^{-1}, \dots, \alpha_{n-1}^G(T)^{-1}] \rightarrow$$

$$A[U_0, \dots, U_{n-1}, U_0^{-1}, \dots, U_{n-1}^{-1}],$$

$$\alpha_0^G(T) = \alpha_r^G(T_0) = \lambda^p T_r + 1,$$

$$\alpha_r^G(T) = \alpha_r^G(T_0, \dots, T_r) = \lambda^p T_r + G_r(T_0, \dots, T_{r-1}) \quad (r \geq 1)$$

によって定義すれば, $Z_{(p)}[\zeta_n]$ の上の group scheme の完全列の可換図式

$$\begin{array}{ccccccc} 0 & \longrightarrow & Z/p^n & \xrightarrow{\omega} & W & \xrightarrow{\psi_n} & U & \longrightarrow & 0 \\ & & \downarrow & & \downarrow \alpha^F & & \downarrow \alpha^G & & \\ 0 & \longrightarrow & \mu_{p^n, A} & \longrightarrow & (G_{m,A})^n & \xrightarrow{\oplus} & (G_{m,A})^n & \longrightarrow & 0 \end{array}$$

を得る.

3.7. (局所環に対する Kummer-Artin-Schreier-Witt 理論) B を局所 A -代数, C を B の不分岐 p^n 次巡回拡大とする. このとき, $U_{n,B}$ の B -有理点 $\text{Spec} B \rightarrow U_{n,B}$ が存在して

$$\begin{array}{ccc} \text{Spec} C & \longrightarrow & W_{n,B} \\ \downarrow & & \downarrow \psi_n \\ \text{Spec} B & \longrightarrow & U_{n,B} \end{array}$$

が cartesian となる. 別の言い方をすれば, $(a_0, a_1, \dots, a_{n-1}) \in U_n(B)$ が存在して $C = B[\xi_0, \xi_1, \dots, \xi_{n-1}]$ となる. ここで,

$$\psi_0(\xi_0) = a_0, \quad \psi_1(\xi_0, \xi_1) = a_1, \dots, \quad \psi_{n-1}(\xi_0, \xi_1, \dots, \xi_{n-1}) = a_{n-1}$$

さらに, $Z/p^n = \text{Gal}(C/B)$ は

$$(\xi_0, \xi_1, \dots, \xi_{n-1}) \mapsto$$

$$(\Lambda_0^G(\xi_0, 1), \Lambda_1^G(\xi_0, \xi_1, 1, 0), \dots, \Lambda_{n-1}^G(\xi_0, \xi_1, \dots, \xi_{n-1}, 1, 0, \dots, 0))$$

によって生成される.

例 3.8. p^2 次の場合

$$\lambda = \lambda_1 = \zeta_1 - 1,$$

$$\lambda_2 = \zeta_2 - 1,$$

$$\eta = \sum_{k=1}^{p-1} \frac{(-1)^{k-1}}{k} \lambda_2^k,$$

$$\tilde{\eta} = \frac{\lambda^{p-1}}{p} (p\eta - \lambda),$$

$$F_1(T) = F(T) = \sum_{k=1}^{p-1} \frac{(\eta T)^k}{k!},$$

$$G_1(T) = G(T) = \sum_{k=1}^{p-1} \frac{(\tilde{\eta} T)^k}{k!},$$

$$\Lambda_0^F(X_0, Y_0) = \lambda X_0 Y_0 + X_0 + Y_0,$$

$$\Lambda_1^F(X_0, X_1, Y_0, Y_1) = \lambda X_1 Y_1 + X_1 + Y_1 \\ + \frac{1}{\lambda} [F(X)F(Y) - F(\lambda X_1 Y_1 + X_1 + Y_1)],$$

$$\Lambda_0^G(X_0, Y_0) = \lambda^p X_0 Y_0 + X_0 + Y_0,$$

$$\Lambda_1^G(X_0, X_1, Y_0, Y_1) = \lambda^p X_1 Y_1 + X_1 + Y_1 \\ + \frac{1}{\lambda^p} [G(X)G(Y) - G(\lambda^p X_1 Y_1 + X_1 + Y_1)],$$

$$\psi_0(X) = \frac{(\lambda X + 1)^{p-1}}{\lambda^p},$$

$$\psi_1(X) = \frac{1}{\lambda^p} \left[\frac{\{\lambda T_1 + F(T_0)\}^p}{\lambda T_0 + 1} - G\left(\frac{(\lambda X + 1)^{p-1}}{\lambda^p}\right) \right],$$

$$W_2 = \text{Spec} A[T_0, T_1, 1/(\lambda T_0 + 1), 1/(\lambda T_1 + F(T_0))],$$

$$U_2 = \text{Spec} A[T_0, T_1, 1/(\lambda^p T_0 + 1), 1/(\lambda^p T_1 + G(T_0))]$$

註 3.9. 離散付値環の上の, 特に generic fiber が of multiplicative type で closed fiber が unipotent であるような, affine group scheme はそれ自体興味深い対象であるが, これについては Waterhouse, Weisfeiler による研究 [13], [12], および, 関口, 諏訪による研究 [1], [3], [4] がある。

References

- [1] T. Sekiguchi - On the deformation of Witt groups to tori II. J. Algebra 138 (1991) 273-297
- [2] T. Sekiguchi, F. Oort, N. Suwa - On the deformation of Artin-Schreier to Kummer. Ann. Scient. Ec. Normale Sup. 22 (1989) 345-375
- [3] T. Sekiguchi, N. Suwa - A case of extensions of group schemes over a discrete valuation ring - Tsukuba J. Math 14 (1990) 459-487
- [4] T. Sekiguchi, N. Suwa - Some cases of extensions of group schemes over a discrete valuation ring I. J. Fac. Sci. Univ. Tokyo 38 (1991) 1-45; II. Bull. Fac. Sci. Eng. Chuo Univ. 32 (1989) 17-35
- [5] T. Sekiguchi, N. Suwa - Théorie de Kummer-Artin-Schreier. C. R. Acad. Sci. Paris 312 (1991) 417-420
- [6] T. Sekiguchi, N. Suwa - Théories de Kummer-Artin-Schreier-Witt. C. R. Acad. Sci. Paris 319 (1994) 105-110
- [7] T. Sekiguchi, N. Suwa - On the unified Kummer-Artin-Schreier-Witt theory. Preprint Series Chuo University, Chuo Math 41 (1994)
- [8] T. Sekiguchi, N. Suwa - Théorie de Kummer-Artin et applications. (to appear in Proceedings of Journées

Arithmétiques Bordeaux 1993)

- [9] T. Sekiguchi, N. Suwa - On the structure of the group scheme $Z[Z/p^n]^\times$. *Compositio Math.* 97 (1995) 253-271
- [10] J. P. Serre - Groupes algébriques et corps de classes. Hermann, 1959
- [11] W. C. Waterhouse - A unified Kummer-Artin-Schreier sequence. *Math. Ann.* 277 (1987) 447-451
- [12] W. C. Waterhouse, B. Weisfeiler - One-dimensional affine group schemes. *J. Algebra* 66 (1980) 550-569
- [13] B. Weisfeiler - On a case of extensions of group schemes. *Trans. Amer. Math. Soc.* 248 (1979) 171-189
- [DM] M. Demazure, P. Gabriel - Groupes algébriques I. Masson-North Holland, 1970