The Artin-Hasse-Šafarevič function

By Koichi YAMAMOTO

(Received August 29, 1959)

Introduction.

Analysis of an algebraically closed complete field with a non-archimedean valuation is not fairly organized as yet. The present paper is an attempt to clarify some of analytic and algebraic aspects of these fields. Incidentally the paper bears a character of compilation of rather fragmentary results, centering around the Artin-Hasse function and its generalization by Šafarevič. Indeed §§ 1-3 deal with analysis of these fields, and some strange situations are presented. For instance in these fields the exponential function e^z is infinite multiple valent, whereas $\log z$ is univalent, quite on the opposite to the complex function theory. §§ 4-6, on the other hand, deal with an interrelation of the Witt vector and the Artin-Hasse-Šafarevič function. It seems that an important algorithm is hidden in Proposition 5. Although seemingly quite apart, these two directions have some common aim. The first determines the image of the group of principal units by the homomorphism $\log$, and the second does the same for the group of 'principal-unit formal power series'. They are stated as Propositions 2 and 7.

1. Analytic function over Ω .

Let p be a prime number, $\mathcal{Q}$ the field of rational p -adic numbers, where the valuation is normalized through $|p|=p^{-1}$. Denote by Ω the completion of an algebraic closure of $\mathcal{Q}$. If $\mathfrak{R}$ is a ring we denote by $\mathfrak{R}\langle X \rangle$ the ring of formal power series $\sum_{n=0}^{\infty} a_n X^n$ in an indeterminate X with coefficients $a_n \in \mathfrak{R}$.

If $f \in \Omega\langle X \rangle$, $f = \sum_{n=0}^{\infty} a_n X^n$, $x \in \Omega$, and if the sum $\sum_{n=0}^{\infty} a_n x^n$ is convergent, we say that $f(x)$ is *defined*, and we denote the sum by $f(x)$. If $f, g \in \Omega\langle X \rangle$ and $f(x)$, $g(x)$ are defined, then $(f \pm g)(x)$ and $(fg)(x)$ are defined and are equal to $f(x) \pm g(x)$ and $f(x)g(x)$ respectively.

It is well known that $f \in \Omega\langle X \rangle$ has the 'convergence radius' r_f , such that $f(x)$ is defined if $|x| < r_f$ and $f(x)$ is not defined if $|x| > r_f$. If $|x| = r_f$, then either $f(x)$ is defined for any x or for no x . An explicit value of r_f is determined by the Cauchy-Hadamard formula $r_f^{-1} = \limsup_{n \rightarrow \infty} |a_n|^{1/n}$.

LEMMA 1. *Let $f = \sum_{n=0}^{\infty} a_n X^n \in \Omega\langle X \rangle$. In order that $f(x)$ is defined and $|f(x)| \leq K$ for all x with $|x| \leq r$, it is necessary and sufficient that $|a_n| r^n \leq K$ for $n = 0, 1, \dots$*

Proof. We have only to prove the necessity part of the Lemma. Assume $|f(x)| \leq K$ for all x with $|x| \leq r$, but $|a_m| r^m > K$ for some m . Take a power s of p to a rational exponent and $\beta \in \Omega$ such that $|\beta| = s$, $s \leq r$, and s is sufficiently close to r . Then $|a_m \beta^m| > K$, $|f(\beta)| \leq K$. Suppose that the maximum of $|a_n \beta^n|$, $n = 0, 1, \dots$, is

attained at $n=n_1, \dots, n_t$. By putting $b_i = (a_{n_i} \beta^{n_i}) (a_{n_1} \beta^{n_1})^{-1}$ for $i=1, \dots, t$ we have $|b_i|=1$, $|\sum_{i=1}^t b_i| < 1$. We may replace β by $\beta\xi$ where ξ is an l th root of unity with $(l, p)=1$, resulting in $|\sum_{i=1}^t b_i \xi^{n_i}| < 1$. This implies that the polynomial $\sum_{i=1}^t b_i X^{n_i} \neq 0$ has infinitely many roots ξ in the residue class field of Ω , which of course is impossible.

The following Proposition is of crucial importance by 'substitution of analytic functions' over Ω .

PROPOSITION 1. *Let $f, g \in \Omega\langle X \rangle$, $f(0)=0$ and $h=g \circ f$ in $\Omega\langle X \rangle$. Suppose that $s \leq r_f$, and $|f(x)| < r_g$ for all x such that $|x| < s$. Then $h(x)$ is defined and is equal to $g(f(x))$ for $|x| < s$.*

Proof. Take an s_1 with $0 < s_1 < s$. Then since the 'analytic function' $f(x)$ is continuous over the compact domain $|x| \leq s_1$, it follows that $|f(x)|$ attains its supremum K , say, over $|x| \leq s_1$. Note that $K < r_g$. Now let $f = \sum_{n=1}^{\infty} a_n X^n$, $g = \sum_{n=0}^{\infty} b_n X^n$, $h = \sum_{n=0}^{\infty} c_n X^n$. Then $c_0 = b_0$ and

$$c_n = \sum_{m=1}^n b_m \sum_{n_1 + \dots + n_m = n} a_{n_1} \dots a_{n_m}$$

for $n \geq 1$. Let ρ be any positive number and determine N such that $N > \rho^{-1}$ and that $|a_n x^n| < \rho$ for $n > N$, where x is a fixed number with $|x| \leq s_1$. If $n > N^2$, then either some $n_i > N$ or else $m > N$. Hence by using Lemma 1,

$$|c_n x^n| \leq \max \left(\max_{m \leq n} (\rho |b_m| K^{m-1}), \max_{N < m \leq n} (|b_m| K^m) \right).$$

The last number becomes arbitrarily small by choosing ρ suitably. This means that $h(x)$ is defined. The fact that $h(x) = g(f(x))$ is easily proved by a standard argument.

REMARK. The equality $(g \circ f)(x) = g(f(x))$ does not follow from mere existence of the two numbers. This corresponds to a situation in complex function theory that the image of $|x| < s$ by a mapping f has not always a simply connected intersection with the disc $|x| < r_g$.

Denote by $\mathfrak{O}$ the ring of integers of Ω . Any $f \in \mathfrak{O}\langle X \rangle$ has convergence radius ≥ 1 . Moreover if $f \in \mathfrak{O}\langle X \rangle$, $|x| < 1$ then $|f(x)| \leq 1$. Conversely if $|f(x)| \leq 1$ as long as $|x| < 1$ for $f \in \Omega\langle X \rangle$, then $f \in \mathfrak{O}\langle X \rangle$. This is readily seen from Lemma 1. We state some further Lemmas in this context.

LEMMA 2. *If $f \in \mathfrak{O}\langle X \rangle$, $f \equiv vX \pmod{X^2 \mathfrak{O}\langle X \rangle}$ for a unit v , then the inverse power series f^{-1} of f belongs to $\mathfrak{O}\langle X \rangle$.*

LEMMA 3. *Let $f_n = \sum_{m=0}^{\infty} a_m^{(n)} X^m \in \mathfrak{O}\langle X \rangle$ for $n=1, 2, \dots$ and $\lim_{n \rightarrow \infty} a_m^{(n)} = a_m$ for $m=0, 1, \dots$. Then for $f = \sum_{m=0}^{\infty} a_m X^m$ and $|x| < 1$ we have $\lim_{n \rightarrow \infty} f_n(x) = f(x)$.*

These Lemmas are proved without difficulty and proofs are omitted.

2. Local exponential function.

The convergence radii of $\log(1+X) = \sum_{n=1}^{\infty} (-1)^{n-1} (X^n/n)$ and $\exp X = \sum_{n=0}^{\infty} (X^n/n!)$ are 1 and $p^{-1/(p-1)}$ respectively, as is well known. An element μ of Ω is called a *principal unit* if $|\mu-1| < 1$. The multiplicative group of all principal units of Ω will be denoted by $\mathbf{M}$. If $\mu \in \mathbf{M}$ then $\log \mu$ is defined, and $\log(\mu_1 \mu_2) = \log \mu_1 + \log \mu_2$.

for $\mu_1, \mu_2 \in \mathbf{M}$, since $\log(1 + (X_1 + X_2 + X_1 X_2)) = \log(1 + X_1) + \log(1 + X_2)$ for two indeterminates X_1, X_2 .

PROPOSITION 2. *By the homomorphism $\log$, the group $\mathbf{M}$ is mapped onto the additive group Ω^+ of Ω , and the kernel consists of roots of unity to p -power exponents.*

Proof. 1) If $|\mu - 1| < p^{-1/(p-1)}$ then $|\log \mu| = |\mu - 1|$, and if $|\beta| < p^{-1/(p-1)}$ then $|\exp \beta - 1| = |\beta|$. Since $\exp(\log(1 + X)) = 1 + X$, $\log(\exp X) = X$ in $\Omega\langle X \rangle$, it follows by Proposition 1 that

$$(1) \quad \exp(\log \mu) = \mu \quad \text{for } |\mu - 1| < p^{-\frac{1}{p-1}},$$

$$(2) \quad \log(\exp \beta) = \beta \quad \text{for } |\beta| < p^{-\frac{1}{p-1}}.$$

2) In particular (1) implies that $|\mu - 1| < p^{-1/(p-1)}$ and $\log \mu = 0$ entail $\mu = 1$. Now assume $\log \mu = 0$. We can find sufficiently large integer m such that $|\mu^{p^m} - 1| < p^{-1/(p-1)}$. Thus $\mu^{p^m} = 1$ by the above and μ is a p^m -th root of unity. This means that the kernel of the homomorphism $\log$ is the group $\mathbf{Z}$ of roots of unity to p -power exponents.

3) If $|\beta| < p^{-1/(p-1)}$ then $\beta = \log(\exp \beta) \in \log \mathbf{M}$, by (2). For an arbitrary $\beta \in \Omega$ we can find sufficiently large integer m such that $|p^m \beta| < p^{-1/(p-1)}$. Thus $p^m \beta = \log \mu$ for some $\mu \in \mathbf{M}$ by the above. Let $M = \sqrt[p^m]{\mu} \in \mathbf{M}$, then $\beta = \log M$. This implies that $\Omega^+ = \log \mathbf{M}$.

If we define e^β , for $\beta \in \Omega$, as any inverse image of β by the homomorphism $\log$, then e^β is an infinite multiple valent function of β . We may also define μ^β , for $\mu \in \mathbf{M}$, $\beta \in \Omega$, by $\mu^\beta = e^{\beta \log \mu}$. Then

$$(\mu_1 \mu_2)^\beta \equiv \mu_1^\beta \mu_2^\beta, \mu^{\beta_1 + \beta_2} \equiv \mu^{\beta_1} \mu^{\beta_2}, \mu^{\beta_1 \beta_2} \equiv (\mu^{\beta_1})^{\beta_2} \pmod{\mathbf{Z}}.$$

Over the field Ω , e^β is an infinite multiple valent function, whereas $\log \mu$ is univalent for $|\mu - 1| < 1$. The situation is quite opposite to the functions e^z and $\log z$ of complex variable, the complex number field being an analog of Ω for archimedean valuation.

3. The Artin-Hasse-Šafarevič function.

Denote by T the completion in Ω of the maximal unramified extension of $\mathbb{Q}$, and put $\mathbb{Q}_T = \mathbb{Q} \cap T$. The Artin-Hasse function $E(X)$ is defined by

$$E(X) = \exp\left(X + \frac{X^p}{p} + \frac{X^{p^2}}{p^2} + \dots\right) = \sum_{n=0}^{\infty} a_n X^n,$$

where $a_n = \tilde{a}_n/n!$, $\tilde{a}_n$ being the number of p -singular elements of the symmetric group $\mathfrak{S}_n$. According to a theorem of Frobenius ([10, p.44]) $\tilde{a}_n$ is divisible by the p -component of $n!$, and hence $a_n \in \mathbb{Q}_p = \mathbb{Q} \cap \mathbb{Q}_T$. Šafarevič's generalization $E(\alpha, X)$ of the Artin-Hasse function is defined for $\alpha \in T$ by

$$E(\alpha, X) = \exp\left(\alpha X + \frac{\alpha^P X^p}{p} + \frac{\alpha^{P^2} X^{p^2}}{p^2} + \dots\right),$$

where P is the Frobenius automorphism of $T/\mathbb{Q}$. If $\alpha \in \mathbb{Q}_T$, α can be written as α

$= \sum_{n=0}^{\infty} \alpha_n p^n$, α_n taken from the Teichmüller (multiplicative) representative system. Then $E(\alpha, X) = \prod_{n=0}^{\infty} (E(\alpha_n X))^{p^n}$ in $\Omega\langle X \rangle$, and $E(\alpha, X)$ has convergence radius ≥ 1 if $\alpha \in \mathfrak{O}_T$, as is seen by using Lemma 3.

PROPOSITION 3. *If $\alpha \in \mathfrak{O}_T$, $\alpha \neq 0$, then the convergence radius of $E(\alpha, X)$ is 1.*

Proof. Let $E(\alpha, X) = \sum_{n=0}^{\infty} b_n X^n$, $b_n \in \mathfrak{O}_T$. By logarithmic differentiation in $\Omega\langle X \rangle$ we see

$$X \frac{dE(\alpha, X)}{dX} = E(\alpha, X) \sum_{n=0}^{\infty} \alpha^n X^{p^n}.$$

Comparing coefficients of X^{p^λ} for $\lambda \geq 1$ we note that

$$p^\lambda b_{p^\lambda} = \alpha^{-1} b_{p^\lambda - 1} + \alpha^{-P} b_{p^\lambda - p} + \dots + \alpha^{-P^{\lambda-1}} b_{p^\lambda - p^{\lambda-1}} + \alpha^{-P} b_0.$$

Since $b_0 = 1$, and $\alpha^{-1}, \alpha^{-P}, \dots, \alpha^{-P^\lambda}$ have the same ordinal ≤ 0 in p , there exists at least one unit $b_{p^\lambda - p^\nu}$ with $1 \leq \nu \leq \lambda - 1$. Thus there are units b_m with $m \geq p^\lambda - p^{\lambda-1}$. Hence the convergence radius of $E(\alpha, X)$ is ≤ 1 .

Denote by $B(X)$ the inverse power series of $E(X) - 1$.

PROPOSITION 4. *The zero points of*

$$L(X) = X + \frac{X^p}{p} + \frac{X^{p^2}}{p^2} + \dots$$

are identical with $B(Z-1)$ for $Z \in \mathbf{Z}$.

Proof. In $\Omega\langle X \rangle$ we have $\log E(X) = L(X)$ and $|E(x) - 1| = |x|$ for $|x| < 1$. By Proposition 1 it follows that $\log(E(x)) = L(x)$. The last number is $= 0$ if and only if $E(x) \in \mathbf{Z}$, by Proposition 2, i.e., if and only if $x \in B(\mathbf{Z} - 1)$.

For instance a primitive p th root of unity $\zeta = E(\mathfrak{g})$, where $\mathfrak{g}$ is one of the 'smallest' roots of $L(X) = 0$.

4. The module $\log(1 + X\mathfrak{O}\langle X \rangle)$.

We have seen that $\log \mathbf{M} = \Omega^+$ in Proposition 2. Let us investigate the module of $\log f$ with $f \in 1 + X\mathfrak{O}\langle X \rangle$. The task is equivalent to find a necessary and sufficient condition for $\exp(\sum_{n=1}^{\infty} a_n X^n)$ to belong to $\mathfrak{O}\langle X \rangle$.

LEMMA 4. *In order for $f = \exp(\sum_{n=1}^{\infty} a_n X^n)$ to belong to $\mathfrak{O}\langle X \rangle$, it is necessary and sufficient that we have $\exp(\sum_{i=0}^{\infty} a_{mp^i} X^{mp^i}) \in \mathfrak{O}\langle X \rangle$ for all m with $(m, p) = 1$.*

Proof. If $f \in \mathfrak{O}\langle X \rangle$ and if l is prime to p then $f(\xi X) \in \mathfrak{O}\langle X \rangle$ for an l th root of unity ξ . The same is true for $\prod_{\xi} f(\xi X) = \exp(l \sum_{n=1}^{\infty} a_{ln} X^{ln})$, hence for $f_l = \exp(\sum_{n=1}^{\infty} a_{ln} X^{ln})$, by using the fact that $(1 + X)^{1/l} \in \mathfrak{O}\langle X \rangle$ for $(l, p) = 1$. Hence we have for $(m, p) = 1$ that $\prod_{(l, p)=1} f_{ml} = f_{ml}^{(\mu(l))} = \exp(\sum_{i=0}^{\infty} a_{mp^i} X^{mp^i})$, where $\mu(n)$ is the Möbius function. The converse is evident.

COROLLARY. *If $\exp(\sum_{n=1}^{\infty} a_n X^n) \in \mathfrak{O}\langle X \rangle$, then $na_n \in \mathfrak{O}$.*

Proof. In view of the Lemma it is sufficient to deal with the function of the type $g = \exp(\sum_{n=0}^{\infty} a_n X^{p^n})$. If $g \in \mathfrak{O}\langle X \rangle$, the same is true for $1/g$ and for dg/dX , hence also for the logarithmic differential $(X/g)(dg/dX) = \sum_{n=0}^{\infty} p^n a_n X^{p^n}$. This

means that $p^n a_n \in \mathfrak{O}$.

Note that the Artin-Hasse function corresponds to $p^n a_n = 1$ for all n , and the Safarevič generalization to $p^n a_n = \alpha p^n$.

The Corollary states only a necessary condition. A necessary and sufficient condition will be treated later (§ 6).

5. On the subcomponents of Witt vector.

Let k be a field of characteristic 0, and a be a Witt vector (based on the prime p) in k . We denote the components of a by $(\alpha_0, \alpha_1, \dots)$ and the subcomponents (*Nebenkomponenten*) of a by $(a_0, a_1, \dots)$, then $a_n = \alpha_0 p^n + p \alpha_1 p^{n-1} + \dots + p^n \alpha_n$ by definition. The sum, difference and product of two Witt vectors a, b are determined by subcomponents, which are sum, difference, and product of corresponding subcomponents of a, b .

PROPOSITION 5. Suppose that the subcomponents a_n of a Witt vector a in the field k satisfy the relations

$$a_n = z_0^{\theta^n} + p z_1^{\theta^{n-1}} + \dots + p^n z_n \quad (n=0, 1, \dots)$$

for a sequence $z_0, z_1, \dots$ of elements of k , where θ is an isomorphism of k into itself. Then components α_n of a can be written as a polynomial $\alpha_n = F_n(z) = F_n(z_0, z_1, \dots, z_n)$, with rational coefficients, which satisfies $F_0 = z_0$, and recurrent relation

$$F_n = z_n + \Delta_1 F_{n-1} + \dots + \Delta_n F_0 \quad (n \geq 1),$$

where $\Delta_s (s=1, 2, \dots)$ is an operator applying to elements x of k in such a way that

$$\Delta_s x = \frac{x^{\theta p^s - 1} - x^{p^s}}{p^s}.$$

Proof. We first note that

$$x^{\theta^n} - x^{p^n} = \sum_{i=1}^n p^i \Delta_i x^{\theta^{n-i}}.$$

Now the assertion is evident for $n=0$, since there is practically nothing to prove. Assume therefore $n \geq 1$ and the validity for lesser values of n . Since $a_n = \sum_{i=0}^n p^i \alpha_i p^{n-i} = \sum_{i=0}^n p^i z_i^{\theta^{n-i}}$, we have

$$p^n (\alpha_n - z_n) = \sum_{i=0}^{n-1} p^i (z_i^{\theta^{n-i}} - \alpha_i p^{n-i}) = \sum_{i=0}^{n-1} p^i (z_i^{\theta^{n-i}} - F_i^{\theta^{n-i}}).$$

Noticing that the isomorphism θ commutes with operators Δ_s we find for $0 \leq i \leq n-1$

$$z_i^{\theta^{n-i}} - F_i^{\theta^{n-i}} = (z_i - F_i)^{\theta^{n-i}} + F_i^{\theta^{n-i}} - F_i^{\theta^{n-i}} = - \sum_{j=1}^i \Delta_j F_i^{\theta^{n-i-j}} + \sum_{j=1}^{n-i} p^j \Delta_j F_i^{\theta^{n-i-j}}.$$

Thus

$$p^n (\alpha_n - z_n) = - \sum_{i=0}^{n-1} \sum_{j=1}^i p^i \Delta_j F_i^{\theta^{n-i-j}} + \sum_{i=0}^{n-1} \sum_{l=0}^{n-i} p^{i+l} \Delta_l F_i^{\theta^{n-i-l}} = p^n \sum_{j=1}^n \Delta_j F_{n-j}.$$

REMARK. It would be useful to display explicit forms of F_n for smaller n . $F_0 = z_0$, $F_1 = z_1 + \Delta z_0$, $F_2 = z_2 + \Delta(z_1 + \Delta z_0) + \Delta_2 z_0$, $F_3 = z_3 + \Delta(z_2 + \Delta(z_1 + \Delta z_0) + \Delta_2 z_0) + \Delta_2(z_1 + \Delta z_0) + \Delta_3 z_0, \dots$, with an obvious abbreviation $\Delta = \Delta_1$. It is to be noted that the operators does not obey distributive law with respect to addition.

EXAMPLE 1. Let $k = Q_0(\alpha_0, \alpha_1, \dots, \beta_0, \beta_1, \dots)$ where Q_0 is the rational number field, $\alpha_0, \alpha_1, \dots$ and $\beta_0, \beta_1, \dots$ are independent indeterminates. Define θ by putting $\alpha_n^\theta = \alpha_n^p$,

$\beta_n^p = \beta_n^p$, and let $z_n = \alpha_n + \beta_n$. Then the sum of two Witt vectors $a = (\alpha_0, \alpha_1, \dots)$ and $b = (\beta_0, \beta_1, \dots)$ is given by $\mathfrak{s} = (\sigma_0, \sigma_1, \dots)$ where $\sigma_n = F_n(z)$. Similarly for the difference and the product. We have only to consider $z_n = \alpha_n - \beta_n$ and $z_n = (\alpha_0 p^n \beta_0 + \alpha_n \beta_0 p^n) + p(\alpha_1 p^{n-1} \beta_n + \alpha_n \beta_1 p^{n-1}) + \dots + p^n \alpha_n \beta_n$, respectively.

If I denotes the integrity domain of rational integers, it is easy to see that $x \in I[\alpha_0, \alpha_1, \dots, \beta_0, \beta_1, \dots]$ entails $\Delta_s x \in I[\alpha_0, \alpha_1, \dots, \beta_0, \beta_1, \dots]$. This implies that the components of the sum, difference and product of two Witt vectors a, b are polynomials in $\alpha_0, \alpha_1, \dots, \beta_0, \beta_1, \dots$ with integral rational coefficients.

EXAMPLE 2. Let $k = Q_0(a_0, a_1, \dots)$ where $a_0, a_1, \dots$ are independent indeterminates. Define θ by putting $a_n^\theta = a_{n+1}$. Then components α_n of the Witt vector a with the subcomponents $(a_0, a_1, \dots)$ are given by $\alpha_n = F_n(a) = G_n(\Delta)a_0$, where $G_n(\Delta)$ is a non-commutative, non-distributive polynomial in $\Delta, \Delta^2, \dots$ such that $G_0(\Delta) = 1$, $G_n(\Delta) = \sum_{i=1}^n \Delta_i G_{n-i}(\Delta)$ for $n \geq 1$. Explicit forms of $G_n(\Delta)$ are: $G_1 = \Delta$, $G_2 = \Delta_2 + \Delta^2$, $G_3 = \Delta_3 + \Delta_2 \Delta + \Delta(\Delta_2 + \Delta^2)$, $G_4 = \Delta_4 + \Delta_3 \Delta + \Delta_2(\Delta_2 + \Delta^2) + \Delta(\Delta_3 + \Delta_2 \Delta + \Delta(\Delta_2 + \Delta^2))$, $\dots$

EXAMPLE 3. Let $k = T, \theta = P$ (Frobenius automorphism), $z_0 = \alpha, z_n = 0$ ($n \geq 1$) for $\alpha \in T$. Then $G_n(\Delta)\alpha$ is component of the Witt vector a with the subcomponents $(\alpha, \alpha^p, \alpha^{p^2}, \dots)$, where $G_n(\Delta)$ is just the same as in Example 2, but with different meaning of Δ . The algorithm corresponds to expand the Šafarevič function $E(\alpha, X)$ in terms of the proper Artin-Hasse function. Cf. § 6.

6. The Artin-Hasse-Šafarevič function and the Witt vector.

The following intimate relation between Witt vector and the Artin-Hasse function is remarkable.

PROPOSITION 6. In the ring $k\langle X \rangle$ of formal power series over a field k of characteristic 0, the relation

$$E(\alpha_0 X) E(\alpha_1 X^p) E(\alpha_2 X^{p^2}) \dots = \exp\left(a_0 X + \frac{a_1 X^p}{p} + \frac{a_2 X^{p^2}}{p^2} + \dots\right)$$

is equivalent to the statement that $(\alpha_0, \alpha_1, \alpha_2, \dots)$ is the component, and $(a_0, a_1, a_2, \dots)$ is the subcomponent, of the same Witt vector.

Proof. A straightforward calculation proves the Proposition.

We noted in Corollary to Lemma 4 that if $a_n \in \Omega$, then

$$\exp\left(\sum_{n=0}^{\infty} \frac{a_n X^{p^n}}{p^n}\right) \in \mathfrak{D}\langle X \rangle$$

only if $a_n \in \mathfrak{D}$. It follows, however, from Proposition 6:

COROLLARY. If $a_n \in \Omega$ then a necessary and sufficient condition for

$$\exp\left(\sum_{n=0}^{\infty} \frac{a_n X^{p^n}}{p^n}\right) \in \mathfrak{D}\langle X \rangle$$

is that all the components α_n of the Witt vector $a = (a_0, a_1, \dots)$, given by the subcomponents, are integral. The last condition is equivalent to $\Delta^n a_0 \in \mathfrak{D}$ ($n = 0, 1, \dots$) for the Δ of Example 2 above.

Indeed the condition $G_n(\Delta)a_0 \in \mathfrak{D}$ ($n = 0, 1, \dots$) is equivalent to $\Delta^n a_0 \in \mathfrak{D}$

($n=0, 1, \dots$), as is verified without much difficulty.

Matters are quite simple when we behave within the subfield T of Ω . Indeed we can expand $\exp(\sum_{n=0}^{\infty} a_n X^{p^n}/p^n)$ as a product of the Šafarevič function, instead of the proper Artin-Hasse function. It is readily verified that the relation

$$\exp\left(\sum_{n=0}^{\infty} \frac{a_n X^{p^n}}{p^n}\right) = \prod_{n=0}^{\infty} E(\beta_n, X^{p^n})$$

is equivalent to

$$a_n = \beta_0^{p^n} + p\beta_1^{p^{n-1}} + \dots + p^n \beta_n \quad (n=0, 1, \dots).$$

We may call numbers $(\beta_0, \beta_1, \dots)$ the Šafarevič components of the Witt vector $a = (a_0, a_1, \dots)$ written in subcomponents. We can solve the above equation in β_n very simply: $p^n \beta_n = a_n - a_{n-1}^p$ ($n=0, 1, \dots$), under the convention that $a_m = 0$ unless m is a non-negative integer. The Šafarevič component β_n is a homomorphism of the additive group of Witt vectors in T . Compare this with the tremendous complexity of the way to express components in terms of subcomponents (Example 2 above).

If $a_n \in T$ then $\exp(\sum_{n=0}^{\infty} a_n X^{p^n}/p^n) \in \mathfrak{D}_T\langle X \rangle$ if and only if the Šafarevič components $\beta_n = (1/p^n)(a_n - a_{n-1}^p)$ are all integers.

PROPOSITION 7. *In order that an element $f = \sum_{n=1}^{\infty} a_n X^n/n$ of $X\Omega\langle X \rangle$ belongs to $\log(1+X\mathfrak{D}\langle X \rangle)$, i.e., that $\exp(f(X)) \in \mathfrak{D}\langle X \rangle$, it is necessary and sufficient that the components of the Witt vector a_m given by the subcomponents $(a_m, a_{mp}, a_{mp^2}, \dots)$ are all integral for all m such that $(m, p) = 1$.*

In order that an element $f = \sum_{n=1}^{\infty} a_n X^n/n$ of $XT\langle X \rangle$ belongs to $\log(X\mathfrak{D}_T\langle X \rangle)$, i.e., that $\exp(f(X)) \in \mathfrak{D}_T\langle X \rangle$, it is necessary and sufficient that

$$a_n - a_{\frac{n}{p}}^p \in n\mathfrak{D}_T$$

for all n , under the convention that $a_n = 0$ unless n is a positive integer.

Proof. This follows from the above considerations together with Lemma 4.

Kyushu University.

References

- [1] Artin, E., und H. Hasse, Die beiden Ergänzungssätze zum Reziprozitätsgesetz der l^n -ten Potenzreste im Körper der l^n -ten Einheitswurzeln. Abh. Math. Sem. Hamburg. Univ. **6** (1928), 146–162.
- [2] Carlitz, L., Note on a paper of Dieudonné. Proc. Amer. Math. Soc. **9** (1958), 32–33.
- [3] Dieudonné, J., On the Artin-Hasse exponential series. Proc. Amer. Math. Soc. **8** (1957), 210–214.
- [4] Dwork, B., Norm residue symbol in local number fields. Abh. Math. Sem. Univ. Hamburg **22** (1958), 180–190.
- [5] Hasse, H., Die Gruppe der p^n -primären Zahlen für einen Primteiler p von p . Journ. Reine u. Angew. Math. **176** (1937), 174–183.
- [6] Hasse, H., Zahlentheorie. Berlin, 1949.
- [7] Hasse, H., Zur Arbeit von I. R. Šafarevič über das allgemeine Reziprozitätsgesetz. Math. Nachr. **5** (1951), 301–327.

- [8] Šafarevič, I. R., A general reciprocity law. Amer. Math. Soc. Transl., Ser. 2, 4 (1956), 73–106.
- [9] Shiratani, K., On potent functions in local number fields. Mem. Fac. Sci., Kyushu Univ., Ser. A, 13 (1956), 126–135.
- [10] Speiser, A., Die Theorie der Gruppen von endlicher Ordnung. 3. Aufl., Berlin, 1937.
- [11] Whaples, G., Generalized local class field theory, III. Second form of existence theorem. Structure of analytic groups. Duke Math. Journ. 21 (1954), 575–581.
- [12] Witt, E., Zyklische Körper und Algebren der Charakteristik p vom Grade p^n . Struktur diskret bewerteter perfekter Körper mit vollkommenen Restklassenkörper der Charakteristik p . Journ. Reine u. Angew. Math. 176 (1937), 126–140.