This proves the theorem.

The writer is indebted to Professor P. R. Garabedian for suggesting that a counterexample of this type must exist.

REFERENCE


Stanford University

ON THE ARTIN-HASSE EXPONENTIAL SERIES

JEAN DIEUDONNÉ

1. Professor G. Whaples has kindly drawn my attention to the very similar properties enjoyed by the series which I called the Witt hyperexponential in a recent paper [2], and a series which he had previously defined, using the Artin-Hasse exponential series [5]; the main fact is that both series define a homomorphism of the Witt group \( W \) onto the multiplicative group \( W^*_1 \). In answer to his questions, I propose in this note to clear up completely that relationship, by determining all formal power series which define such homomorphisms, in other words, what one might call the formal characters of the group \( W \); it turns out that the Artin-Hasse-Whaples series is the simplest member of that family, from which all others can be deduced by a simple transformation. I am indebted to Professor Whaples for several useful remarks and comments, as well as for pointing out a slight error in one of my original proofs.

2. Let \( (a_0, a_1, \cdots, a_i, \cdots) \) be an infinite sequence of rational numbers, and let us consider the power series in one indeterminate \( x \)

\[
\exp(a_0x + a_1x^p + a_2x^{p^2} + \cdots + a_ix^{p^i} + \cdots) = \sum_{n=0}^{\infty} c_n x^n
\]

where \( p \) is a prime number.

**Proposition 1.** In order that in the series (1) all coefficients \( c_n \) be \( p \)-adic integers, a necessary and sufficient condition is that, for each \( i \geq 0 \), one should have

Received by the editors April 12, 1956.
(2) \[ a_i = \frac{a_{i-1}}{p} + b_i \quad (a_{-1} = 0) \]

where each \( b_i \) is a \( p \)-adic integer.

To show conditions (2) are sufficient, we remark that the simplest solution of (2) is \( a_i = 1/p^i \) for \( i \geq 0 \); the corresponding series (1) is the inverse of the Artin-Hasse series (as defined, for instance, in [4]), in other words the series

\[ F_0(x) = \prod_{\mu(m)/m} (1 - x^m)^{-\mu(m)/m} \]

where \( \mu \) is the Möbius function; it is elementary to prove that its coefficients are \( p \)-adic integers (see [5, p. 576]). Now, in general, relations (2) imply

\[ a_i = \frac{b_0}{p^i} + \frac{b_1}{p^{i-1}} + \cdots + \frac{b_{i-1}}{p} + b_i; \]

therefore the series (1) can be written

(3) \[ (F_0(x))^{b_0} (F_0(x^p))^{b_1} \cdots (F_0(x^{p^k}))^{b_t} \cdots \]

and the same elementary argument shows that each of the factors has \( p \)-adic integers as coefficients (since the denominators of the \( b_i \) are prime to \( p \)).

Conversely, suppose the \( c_n \) are \( p \)-adic integers, and suppose we have proved (2) for \( i < h \); then the series obtained by multiplying (1) with the product

\[ ((F_0(x))^{b_0} (F_1(x^p))^{b_1} \cdots (F_0(x^{p^h}))^{b_h})^{-1} \]

has \( p \)-adic integers as coefficients; on the other hand, it can obviously be written

\[ \exp (d_{h+1} x^{p^{h+1}} + d_{h+2} x^{p^{h+2}} + \cdots) \]

with \( d_{h+1} = a_{h+1} - a_h/p \); writing that the coefficient of \( x^{p^{h+1}} \) is a \( p \)-adic integer proves (2) for \( i = h \), which concludes the proof of Proposition 1.¹

3. If we suppose conditions (2) verified, and if we replace in (1) each coefficient \( c_n \) by its class mod \( p \), we obtain a power series \( E(x) \) with coefficients in the prime field \( F_p \). For an indeterminate Witt vector \( x = (x_0, x_1, \ldots, x_n, \ldots) \), let us now define

¹ As observed by Professor Whaples, Proposition 1 and its proof are still valid if the \( a_i \) are supposed to be \( p \)-adic numbers.
(4) \[ E(x) = E(x_0, x_1, \ldots, x_i, \ldots) = \prod_{i=0}^{\infty} E(x_i) \]

each indeterminate \( x_i \) being considered as having weight \( p^i \); in particular, if we start from the power series \( F_0(x) \), the power series \( E_0(x) \) which we obtain in that way is the inverse of the Artin-Hasse-Whaples series \([5, \text{p. 576}].\)\(^2\)

Now, from the definition of the Witt additive group, it follows at once that

(5) \[ E_0(x)E_0(y) = E_0(x + y) \]

where \( y = (y_0, y_1, \ldots, y_n, \ldots) \) is a second indeterminate Witt vector, and \( x+y \) is the sum taken in the Witt group.

We are now going to obtain simple expressions of \( E(x) \) in terms of \( E_0(x) \). For an indeterminate \( z \), and a \( p \)-adic integer \( b = \sum_{h=0}^{\infty} \nu_h p^h \) \((0 \leq \nu_h \leq p-1)\), we define (see \([1, \text{p. 241}]\)) the power series \( (1+z)^b \) with coefficients in \( F_p \) as the product \( \prod_{h=0}^{\infty} (1+z^p)^{\nu_h} = \prod_{h=0}^{\infty} (1+z)^{\nu_h p^h} \). If \( c \) is a second \( p \)-adic integer such that \( b \equiv c \pmod{p^n} \), the terms in \( (1+z)^b \) and \( (1+z)^c \) have the same coefficient for all exponents \(<p^n\), from which remark the relation

\[ (1 + z)^{b+c} = (1 + z)^b(1 + z)^c \]

follows immediately by an obvious limiting process. In particular if \( b = r/s \) is a rational number, we have \( ((1+z)^b)^s = (1+z)^r \), hence in that case \( (1+z)^b \) can also be obtained by reducing \( b \pmod{p} \) the rational coefficients of the binomial series \( (1+z)^r/s \) (which are \( p \)-adic integers if \( b \) is a \( p \)-adic integer).

Using these elementary remarks and the fact that the coefficients of \( E_0(x) \) are in the prime field \( F_p \), it follows from the expression (3) of the series (1) that we have

(6) \[ E(x) = (E_0(x))^{b_0}E_0(x)^{b_1 p} \cdots (E_0(x))^{b_i p^i} \cdots = (E_0(x))^b \]

where \( b \) is the \( p \)-adic integer \( b_0 + b_1 p + \cdots + b_i p^i + \cdots \) (which of course is no more a rational number, in general). Hence, from definition (4), we also have

(7) \[ E(x) = (E_0(x))^b \]

for Witt vectors. Taking into account the multiplicative property \( (1+x)^b(1+y)^b = (1+x+y+xy)^b \), we deduce therefore from (4) and (7)

(8) \[ E(x)E(y) = E(x + y); \]

\(^2\) More precisely, this series is the one which would be written \( (E(x, 1))^{-1} \) in the notations of \([5, \text{p. 576}]\).
we observe that this gives a much simpler proof of Proposition 2 and its Corollary 2 in [2].

Let us now show that the expression (7) of $E(x)$ can also be transformed in the following:

$$E(x) = E_0(b \cdot x)$$

where the product $b \cdot x$ is understood in the following way: let us write $b = \beta_0 + \beta_1 p + \cdots + \beta_h p^h + \cdots$, where the $p$-adic integers $\beta_h$ belong to the set of Teichmüller representatives (in this case, the $(p-1)$th roots of unity in the $p$-adic field); if $\bar{\beta}_h$ is the class of $\beta_h$ in $\mathbb{F}_p$ and $\bar{\beta}$ is the Witt vector $(\bar{\beta}_0, \bar{\beta}_1, \cdots, \bar{\beta}_h, \cdots)$, $b \cdot x$ is by definition the Witt vector $\bar{\beta} \cdot x$, where the product is of course taken for the Witt multiplication. To prove (9), we observe that it follows at once from (5) that $E_0(b \cdot x) = (E_0(x))^b$ when $b$ is an ordinary integer, for then $b \cdot x$ is just the sum of $b$ vectors equal to $x$ [6, p. 133]. On the other hand, if two $p$-adic integers $b, c$ are such that $b \equiv c \pmod{p^n}$, it follows immediately from the preceding definitions that the terms of weight $< p^n$ are the same in the series $E_0(b \cdot x)$ and $E_0(c \cdot x)$, and the same is true for the two series $(E_0(x))^b$ and $(E_0(x))^c$, which ends the proof of (9).

4. We are now going to see that the expression (9) gives in fact the most general $\mathbb{F}_p$-homomorphism of the Witt group $W$ into the multiplicative group $W^\times$. More generally:

**Proposition 2.** If $K$ is a field of characteristic $p$, any formal $K$-homomorphism of $W$ into $W^\times$ is of the form $E_0(A \cdot x)$ where $A$ is a Witt vector with elements in $K$, and the product $A \cdot x$ is taken for the Witt multiplicative law.

Let the series $u(x)$ with coefficients in $K$, define a homomorphism of $W$ into $W^\times$, in other words be such that $u(x+y) = u(x) \cdot u(y)$. Suppose we have proved the existence of a Witt vector $A_h$ such that both series $u(x)$ and $E_0(A_h \cdot x)$ have the same terms of weight $\leq p^h$. It follows that we may write $u(x) = E_0(A_h \cdot x)v(x)$, where $v$ is another homomorphism; if $v = 1$, our proof is ended. If not, let $v(x) = 1 + P(x) + \cdots$, where $P$ is the sum of all nonconstant terms of smallest weight in $v$, and therefore an isobaric polynomial of weight $m > p^h$. Writing the relation $v(x+y) = v(x) \cdot v(y)$, and remembering that the Witt additive group law is isobaric, we obtain

$$P(x+y) = P(x) + P(y).$$

But it follows from the argument in [3, p. 432] that such a relation
implies that $P$ only contains $x_0$, and therefore is of the form $b x_0^k$ with $b \in K$ and $k > h$. Let $B = (0, \cdots, 0, b, 0, \cdots)$ be the Witt vector having all its components equal to 0 except the component of index $k$, equal to $b$; then $v(x)$ and $E_0(B \cdot x)$ have the same terms of weight $\leq p^k$, and therefore, if we put $A_h = A_h + B$, $u(x)$ and $E_0(A_h \cdot x)$ $= E_0(A_h \cdot x)E_0(B \cdot x)$ have the same terms of weight $\leq p^k$. The induction can thus proceed, and it is clear that the sequence $(A_h)$ of Witt vectors tends to a limit $A$ such that $A_h$ and $A$ have the same components of indices $\leq h$; hence $E_0(A \cdot x)$ and $E_0(A_h \cdot x)$ have the same terms of weight $\leq p^h$, and as $h$ is arbitrary, this ends the proof of Proposition 2.

Bibliography


Northwestern University