This proves the theorem.

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

Reference

1. Courant and Hilbert, *Methoden der mathematischen Physik*, vol. 2, 1937.

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

$$(1)\qquad \exp\left(a_0 x + a_1 x^p + a_2 x^{p^2} + \cdots + a_i x^{p^i} + \cdots\right) = \sum_{n=0}^{\infty} c_n x^n$$

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.

$$a_i = \frac{a_{i-1}}{p} + b_i \qquad (a_{-1} = 0) \tag{2}$$

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 $i \geqq 0$; the corresponding series (1) is the inverse of the Artin-Hasse series (as defined, for instance, in [**4**]), in other words the series

$$F_0(x) = \prod_{p \nmid m} (1 - x^m)^{-\mu(m)/m}$$

where μ 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

$$(F_0(x))^{b_0}(F_0(x^p))^{b_1} \cdots (F_0(x^{p^i}))^{b_i} \cdots \tag{3}$$

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 $\mathbf{x} = (x_0, x_1, \cdots, x_n, \cdots)$, 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.

$$E(\mathbf{x}) = E(x_0, x_1, \cdots, x_i, \cdots) = \prod_{i=0}^{\infty} E(x_i) \tag{4}$$

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 $E_0(\mathbf{x})$ which we obtain in that way is the inverse of the Artin-Hasse-Whaples series [5, p. 576].[2] Now, from the definition of the Witt additive group, it follows at once that

$$E_0(\mathbf{x})E_0(\mathbf{y}) = E_0(\mathbf{x} + \mathbf{y}) \tag{5}$$

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

We are now going to obtain simple expressions of $E(\mathbf{x})$ in terms of $E_0(\mathbf{x})$. For an indeterminate z, and a p-adic integer $b = \sum_{h=0}^{\infty} \nu_h p^h$ $(0 \leqq \nu_h \leqq p-1)$, we define (see [1, p. 241]) the power series $(1+z)^b$ with coefficients in $\boldsymbol{F}_p$ as the product $\prod_{h=0}^{\infty} (1+z^{p^h})^{\nu_h} = \prod_{h=0}^{\infty} (1+z)^{\nu_h p^h}$. 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 mod 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 $\boldsymbol{F}_p$, it follows from the expression (3) of the series (1) that we have

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

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

$$E(\mathbf{x}) = (E_0(\mathbf{x}))^b \tag{7}$$

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)

$$E(\mathbf{x})E(\mathbf{y}) = E(\mathbf{x} + \mathbf{y}); \tag{8}$$

[2] More precisely, this series is the one which would be written $(E(\mathbf{x}, 1))^{-1}$ in the notations of [5, 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 $E(\mathbf{x})$ can also be transformed in the following:

$$E(\mathbf{x}) = E_0(b\cdot \mathbf{x}) \tag{9}$$

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 β_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 β_h in $\boldsymbol{F}_p$ and $\bar{\beta}$ is the Witt vector $(\bar{\beta}_0, \bar{\beta}_1, \cdots, \bar{\beta}_h, \cdots)$, $b\cdot \mathbf{x}$ is by definition the Witt vector $\bar{\beta}\cdot \mathbf{x}$, where the product is of course taken for the Witt multiplication. To prove (9), we observe that it follows at once from (5) that $E_0(b\cdot \mathbf{x})=(E_0(\mathbf{x}))^b$ when b is an ordinary integer, for then $\bar{\beta}\cdot \mathbf{x}$ is just the sum of b vectors equal to $\mathbf{x}$ [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 $E_0(b\cdot \mathbf{x})$ and $E_0(c\cdot \mathbf{x})$, and the same is true for the two series $(E_0(\mathbf{x}))^b$ and $(E_0(\mathbf{x}))^c$, which ends the proof of (9).

4. We are now going to see that the expression (9) gives in fact the most general $\boldsymbol{F}_p$-homomorphism of the Witt group W into the multiplicative group W_1^*. More generally:

PROPOSITION 2. *If K is a field of characteristic p, any formal K-homomorphism of W into W_1^* is of the form $E_0(A\cdot \mathbf{x})$ where A is a Witt vector with elements in K, and the product $A\cdot \mathbf{x}$ is taken for the Witt multiplicative law.*

Let the series $u(\mathbf{x})$ with coefficients in K, define a homomorphism of W into W_1^*, in other words be such that $u(\mathbf{x}+\mathbf{y})=u(\mathbf{x})\cdot u(\mathbf{y})$. Suppose we have proved the existence of a Witt vector A_h such that both series $u(\mathbf{x})$ and $E_0(A_h\cdot \mathbf{x})$ have the same terms of weight $\leq p^h$. It follows that we may write $u(\mathbf{x})=E_0(A_h\cdot \mathbf{x})v(\mathbf{x})$, where v is another homomorphism; if $v=1$, our proof is ended. If not, let $v(\mathbf{x})=1+P(\mathbf{x}) + \cdots$, 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 $v(\mathbf{x}+\mathbf{y})=v(\mathbf{x})\cdot v(\mathbf{y})$, and remembering that the Witt additive group law is isobaric, we obtain

$$P(\mathbf{x} + \mathbf{y}) = P(\mathbf{x}) + P(\mathbf{y}).$$

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 $bx_0^{p^k}$ 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 $v(\mathbf{x})$ and $E_0(B \cdot \mathbf{x})$ have the same terms of weight $\leqq p^k$, and therefore, if we put $A_k = A_h + B$, $u(\mathbf{x})$ and $E_0(A_k \cdot \mathbf{x}) = E_0(A_h \cdot \mathbf{x}) E_0(B \cdot \mathbf{x})$ have the same terms of weight $\leqq p^k$. 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 $\leqq h$; hence $E_0(A \cdot \mathbf{x})$ and $E_0(A_h \cdot \mathbf{x})$ have the same terms of weight $\leqq p^h$, and as h is arbitrary, this ends the proof of Proposition 2.

Bibliography

1. J. Dieudonné, *Lie groups and Lie hyperalgebras over a field of characteristic* $p>0$ (II), Amer. J. Math. vol. 77 (1955) pp. 218–244.

2. ———, *Witt groups and hyperexponential groups*, Mathematika vol. 2 (1955) pp. 21–31.

3. ———, *Lie groups and Lie hyperalgebras over a field of characteristic* $p>0$ (IV), Amer. J. Math. vol. 77 (1955) pp. 429–452.

4. H. Hasse, *Die Gruppe der* p^n*-primären Zahlen für einen Primteiler* $\mathfrak{p}$ *von* p, J. Reine Angew. Math. vol. 176 (1936) pp. 174–183.

5. G. Whaples, *Generalized local class field theory* (III), Duke Math. J. vol. 21 (1954) pp. 575–581.

6. E. Witt, *Zyklische Körper und Algebren der Charakteristik* p *vom Grad* p^n, J. Reine Angew. Math. vol. 176 (1936) pp. 126–140.

Northwestern University