# ON WITT VECTORS AND PERIODIC GROUP-VARIETIES

BY

IACOPO BARSOTTI

**1.** Witt vectors were introduced in [11] (see bibliography at the end of the paper), and served the purpose of constructing unramified $p$-adic fields with preassigned residue fields; they entered the theory of analytic groups through the extensive use made of them in [7], [8], [9]; and they have now entered the field of algebraic geometry via analytic groups (see [3] or [4]), and also directly as in [10]; they play an essential role in some work still in progress (see introduction of [5]). The reason for the introduction of Witt vectors in algebraic geometry is in part the same which led to their discovery, namely the need of building a ring of characteristic zero from one of positive characteristic, but mainly the fact that truncated Witt vectors afford examples of periodic group-varieties, in the sense of [1]. Both reasons have a specious element in them, in that there is no a priori assurance that other, inequivalent, constructions would not accomplish the same purpose, or perhaps lead to more detailed results. A heuristic argument against this supposition is however offered by the fact that another construction, the hyperexponential vectors introduced in [6] for applications to the theory of analytic groups, turned out to be equivalent to Witt vectors, the specific transformation law being given in [8]. In this note we propose to show that any periodic group-variety of dimension $n$ and period $p^n$ is isogenous to a group-variety constructed by means of Witt vectors,[1] so that the use of these, for the purposes described above, will remain fully justified.

We recall briefly the definition and first properties of Witt vectors as given in [11]. Let $p$ be a prime number, and let $(x_0, x_1, \cdots)$ be an ordered set (*Witt vector*), either finite or countably infinite, of indeterminates; for each $i$, set

$$g_i(x) = \sum_{j=0}^{i} p^j x_j^{p^{i-j}} \in I[x_0, x_1, \cdots],$$

$I$ being the ring of integers. Then

$$x_i = f_i(g_0(x), \cdots, g_i(x)) \in R[g_0(x), g_1(x), \cdots],$$

$R$ being the field of rationals. If $(y_0, y_1, \cdots)$ is another Witt vector, of the same cardinality as $(x_0, x_1, \cdots)$, define

$$z_i' = f_i(g_0(x) + g_0(y), g_1(x) + g_1(y), \cdots);$$

Received May 15, 1957.

[1] I am informed by the referee that C. Chevalley, J-P. Serre, and M. Rosenlicht have found independent proofs of a generalization of this result, namely: *Any periodic group-variety is isogenous to a direct product of Witt varieties.* The *Appendix* to the present paper, which chronologically follows this footnote, contains my proof of a slightly more detailed result.

it is proved in [11] that

$$z_i' = \varphi_i'(x_0, \cdots, x_i; y_0, \cdots, y_i) \in I[x_0, x_1, \cdots; y_0, y_1, \cdots],$$

so that the image $\varphi_i$ of $\varphi_i'$, mod $pI[x; y]$, exists, and belongs to $C_p[x; y]$, $C_p$ being the prime field of characteristic $p$. We shall accordingly set

$$z_i = \varphi_i(x_0, \cdots, x_i; y_0, \cdots, y_i),$$

and

$$(x_0, x_1, \cdots) + (y_0, y_1, \cdots) = (z_0, z_1, \cdots).$$

This notation remains meaningful when the $x$'s and $y$'s are replaced by elements of an integral domain $K$ containing $C_p$ as a subfield; when this is done, it is proved in [11] that the Witt vectors of a given cardinality, with elements in $K$, form an abelian group with respect to the addition as defined above. The mappings $\boldsymbol{\pi}(x_0, \cdots, x_n) = (x_0^p, \cdots, x_n^p)$, $\mathbf{t}(x_0, \cdots, x_n) = (0, x_0, \cdots, x_n)$, $\boldsymbol{\rho}(x_0, \cdots, x_n) = (x_0, \cdots, x_{n-1})$ (which reduces to the identity if $n = \infty$) are respectively a group-isomorphism, a group-isomorphism, and a group-homomorphism. They commute with each other, and satisfy the relation

$$\boldsymbol{\pi}\mathbf{t}\boldsymbol{\rho} = p = \textit{multiplication by } p. \tag{1}$$

In order to introduce the hyperexponential vectors, we shall consider a countable infinity of indeterminates $z, u_0, u_1, \cdots$, and the power series (in $z$) $\exp \sum_{i=0}^{\infty} u_i z^{p^i}$; if $x_i$ is the coefficient of $z^{p^i}$ in this power series, the $x_i$ are algebraically independent over $R$, and, according to [6], there exist polynomials $e_j'(x_0, x_1, \cdots)$ ($j = 1, 2, \cdots$), with coefficients which are $p$-adic integers in $R$, such that $e_j'$ is the coefficient of $z^j$ in the above power series; moreover, $e_j' = x_i$ if $j = p^i$, while if $p^i < j < p^{i+1}$, $e_j'$ involves only the indeterminates $x_0, x_1, \cdots, x_i$. Denote by $e_j(x_0, x_1, \cdots)$ the image of $e_j'$ mod $pI_p[x]$, so that $e_j \in C_p[x]$; if now $(x_0, x_1, \cdots)$ and $(y_0, y_1, \cdots)$ are ordered sets (*hyperexponential vectors*) of the same cardinality, either finite or countable, of elements of an integral domain $K$ containing $C_p$ as a subfield, define $(x_0, x_1, \cdots)(y_0, y_1, \cdots) = (z_0, z_1, \cdots)$ by setting

$$z_i = x_i + y_i + \sum_{1}^{p^i-1}{}_j\, e_j(x)e_{p^i-j}(y). \tag{2}$$

The set of all the hyperexponential vectors, of a given cardinality, with elements in $K$ forms an abelian group with respect to the product as defined above. The operations $\boldsymbol{\pi}$, $\mathbf{t}$, $\boldsymbol{\rho}$ can be defined in the same manner as for Witt vectors, and (1) is satisfied. It is proved in [8] that this group is isomorphic to the group of Witt vectors.

**2.** In this note we depart from previous notations in that we use the symbol $+$ to denote the law of composition on a commutative group-variety. If $G$ is a commutative group-variety over the field $k$ of characteristic $p \neq 0$, and if $\{x_1, \cdots, x_n\}$ is a n.h.g.p. (nonhomogeneous general point) of $G$, there is a commutative group-variety $G^p$ over $k$ whose n.h.g.p. is $\{x_1^p, \cdots, x_n^p\}$; the natural homomorphism of $G$ onto $G^p$, previously denoted by $\delta_{1,G}$, will now be denoted by $\pi$; if $m$ is an integer, the endomorphism which maps any nondegenerate $P \in G$ onto $mP$, previously denoted by $m\delta_G$, will simply be denoted by $m$. For the meaning of "factor set", "crossed product", and of the symbols $\Gamma(G, V)$, $\Gamma_0(G, V)$, see [1].

(3) LEMMA. *Let $k$ be an algebraically closed field of characteristic $p \neq 0$; let $L$ be a 1-dimensional vector variety over $k$, and let $U$ be an $n$-dimensional periodic group-variety over $k$. Let $\varepsilon$ be a factor set of $L$ into $U$ ($\varepsilon \in \Gamma(L, U)$) such that, for a generic $P \in L$, $\varepsilon[P \times P_1] + \varepsilon[2P \times P_1] + \cdots + \varepsilon[(p-1)P \times P_1] = R$ is independent of $P$ ($P_1$ being the copy of $P$ on a copy $L_1$ of $L$). Then $\varepsilon \in \Gamma_0(L, U)$.*

*Proof.* Let $G$ be the crossed product $\{L, U, \varepsilon\}$, and let $\lambda$ be the rational mapping of $L$ into $G$ used in the definition of crossed product; namely, $\alpha\lambda P = P$ for a generic $P \in L$, if $\alpha$ is the natural homomorphism of $G$ onto $L = G/U$. We shall first of all replace $\lambda$ by $\lambda - \lambda E_L$ ($E_L$ being the identity of $L$); this implies the replacement of $\varepsilon$ by $\varepsilon - \lambda E_L$, which is associate to $\varepsilon$; we shall continue to denote $\lambda - \lambda E_L$ by $\lambda$, and $\varepsilon - \lambda E_L$ by $\varepsilon$. We have, for generic $P, Q \in L$: $\lambda P + \lambda Q = \lambda[P + Q] + \varepsilon[P \times Q_1]$, hence $p\lambda P = \lambda pP + \varepsilon[P \times P_1] + \varepsilon[2P \times P_1] + \cdots + \varepsilon[(p-1)P \times P_1] = \lambda pP + R = \lambda E_L + R = R$; for $P = E_L$ this gives $R = E_U = E_G$, so that $p\lambda L = E_G$. As $\lambda L$ is a 1-dimensional subvariety of $G$, this implies that it is a subvariety of the maximal vector subvariety $V$ of $G$; now, the maximal vector subvariety $Z$ of $U$ is a component of $V \cap U$, outside the degeneration locus; we can thus assert that $\varepsilon[P \times Q_1] = \lambda P + \lambda Q - \lambda[P + Q] \in Z$. Hence $\{L, Z, \varepsilon\}$ has a meaning, and the property of $\varepsilon$, when applied to $\{L, Z, \varepsilon\}$, shows that this group-variety has period $p$, and is therefore a vector variety, by Lemma 3.6 of [1]; but then $\varepsilon \in \Gamma_0(L, Z)$, and also $\varepsilon \in \Gamma_0(L, U)$, Q.E.D.

Let $\{x_0, \cdots, x_{n-1}\}$ be the n.h.g.p. of an $n$-dimensional projective space $G$ over a field $k$ of characteristic $p \neq 0$; let $G_1, G_2$ be copies of $G$, and let $\{y\}$, $\{z\}$ be the copies of $\{x\}$ in $k(G_1)$, $k(G_2)$ respectively; define a law of composition on $G$ by setting $(z_0, \cdots, z_{n-1}) = (x_0, \cdots, x_{n-1}) + (y_0, \cdots, y_{n-1})$, where the three vectors involved are Witt vectors. Then it is easily verified that $G$ becomes an $n$-dimensional periodic group-variety of period $p^n$, whose degeneration locus is the hyperplane at infinity for $\{x\}$; such $G$ will be called the $n$-dimensional *Witt variety over* $k$, and denoted by $W_n(k)$. The homomorphism $\pi$ becomes a purely inseparable endomorphism of degree $p^n$; $\mathfrak{t}$ becomes an isomorphism of $W_n(k)$ into $W_{n+1}(k)$; and $\varrho$ becomes a separable homomorphism of $W_n(k)$ onto $W_{n-1}(k)$; for $n = 1$, we shall identify $\varrho$ with the zero homomorphism. Also, $W_n(k)$ is a crossed product of $W_{n-1}(k)$ and $W_1(k)$, and $\varrho$ is the related natural homomorphism. Conversely, we have:

(4) LEMMA. *Let $G$ be a periodic group-variety of dimension $n > 0$ and period $p^n$ over the algebraically closed field $k$ of characteristic $p$; let $V$ be the maximal*

*vector subvariety of $G$, certainly of dimension* 1, *and set* $A = G/V$; *let* $\varrho$ *be the natural homomorphism of* $G$ *onto* $A$, *and set* $U = pG$. *Assume the existence of an isomorphism* $\zeta$ *of* $U$ *onto* $\zeta U$, *and of an isomorphism* $\mathbf{t}$ *of* $A$ *onto* $U$, *such that, for any nondegenerate* $P \in G$, $pP = \zeta^{-1}\pi\zeta\mathbf{t}\varrho P$. *Then* $G \cong W_n(k)$.

*Proof.* By Lemma 3.6 of [1], the result is true if $n = 1$; we can therefore apply a recursive argument on $n$.

*Part* 1. Assume $n > 1$; by the lemma just mentioned, $A$ has period $p^{n-1}$ and dimension $n - 1$; let $W$ be the maximal vector subvariety of $A$, and set $B = A/W$; let $\sigma$ be the natural homomorphism of $A$ onto $B$, and set $Z = pA$. Then the nondegenerate points of $Z$ are of the type $p\varrho P = \varrho pP$ for $P \in G$, so that $Z = \varrho U$; now, $V \subseteqq U$, so that $\varrho U \cong U/V \cong A/W = B$, or $Z \cong B$. For a nondegenerate $P \in G$ we have $p\varrho P = \varrho pP = \varrho\zeta^{-1}\pi\zeta\mathbf{t}\varrho P$, which is the same as $pQ = \varrho\zeta^{-1}\pi\zeta\mathbf{t}Q$ for a nondegenerate $Q \in A$; the relation $p = \zeta^{-1}\pi\zeta\mathbf{t}\varrho$ shows that $\pi\zeta U \cong \zeta U$, or that $\pi$ is an endomorphism of $\zeta U$; consequently, for any nondegenerate $Q \in A$, $\zeta^{-1}\pi\zeta\mathbf{t}Q = \mathbf{t}\eta^{-1}\pi\eta Q$, where $\eta = \zeta\mathbf{t}$, so that $pQ = \varrho\mathbf{t}\eta^{-1}\pi\eta Q$. Now, for a suitable isomorphism $\mathbf{s}$ of $B$ onto $Z$ we have $\varrho\mathbf{t}Q = \mathbf{s}\sigma Q$ for any nondegenerate $Q \in A$, so that $pQ = \mathbf{s}\sigma\eta^{-1}\pi\eta Q$. Since $\pi$ is an endomorphism of $\eta A$ onto itself, it is also an endomorphism of $\eta Z$ onto itself; therefore there exists an isomorphism $\mathbf{s}^*$ of $B$ onto $Z$ such that, for any nondegenerate $Q \in A$, $\mathbf{s}\sigma\eta^{-1}\pi\eta Q = \eta^{-1}\pi\eta\mathbf{s}^*\sigma Q$, or $pQ = \eta^{-1}\pi\eta\mathbf{s}^*\sigma Q$. This proves that $A$ satisfies the conditions stated in the lemma for $G$; by the recursive assumption, we conclude that $A \cong W_{n-1}(k)$.

*Part* 2. Having reached the result $A \cong W_{n-1}(k)$, there is no loss of generality in assuming $A = W_{n-1}(k)$. By Lemmas 3.2 and 3.6 of [1], we can write $G \cong \{L, A, \gamma\}$, and of course $G' = W_n(k) = \{L, A, \gamma'\}$, where $L$ is a 1-dimensional vector variety, and $\gamma, \gamma' \in \Gamma(L, A)$; on the other hand, we also have $G \cong \{A, L, \delta\}$, $G' \cong \{A, L, \delta'\}$, where $\delta, \delta' \in \Gamma(A, L)$, and $A = \{L, B, \theta\}$, $\theta \in \Gamma(L, B)$. All this implies the following: there are homomorphisms $\alpha$ of $G$ onto $L$ with kernel $U \cong A$, $\alpha'$ of $G'$ onto $L$ with kernel $U' \cong A$, $\varrho$ of $G$ onto $A$ with kernel $V \cong L$, $\varrho'$ of $G'$ onto $A$ with kernel $V' \cong L$, $\beta$ of $A$ onto $L$ with kernel $Z \cong B = W_{n-2}(k)$, and we may assume $\alpha = \beta\varrho$. There are also rational mappings $\lambda$ of $L$ into $G$, $\lambda'$ of $L$ into $G'$, $\mu$ of $A$ into $G$, $\mu'$ of $A$ into $G'$, $\nu$ of $L$ into $A$, such that $\alpha\lambda = \alpha'\lambda' = \varrho\mu = \varrho'\mu' = \beta\nu = 1$; and we may select $\lambda = \mu\nu$, $\lambda' = \mu'\nu$. Finally, there are isomorphisms $\mathbf{t}$ of $A$ onto $U$, $\mathbf{t}'$ of $A$ onto $U'$. A generic point of $G$ is of the type $R = \lambda P + \mathbf{t}Q$, where $P \in L$, $Q \in A$, so that $pR = p\lambda P + p\mathbf{t}Q = \lambda E_L + \mathbf{t}\gamma[P \times P_1] + \mathbf{t}\gamma[2P \times P_1] + \cdots + \mathbf{t}\gamma[(p-1)P \times P_1] + p\mathbf{t}Q$, $P_1$ being the copy of $P$ on a copy $L_1$ of $L$.

Having selected $A = W_{n-1}(k)$, we can also select, in the statement of the lemma, $\zeta = \eta\mathbf{t}^{-1}$, $\eta$ being an automorphism of $A$; then $pR = p\lambda P + p\mathbf{t}Q = t\eta^{-1}\pi\eta\varrho\lambda P + p\mathbf{t}Q = \mathbf{t}\eta^{-1}\pi\eta\varrho\mu\nu P + p\mathbf{t}Q = \mathbf{t}\eta^{-1}\pi\eta\nu P + p\mathbf{t}Q$. Hence,

$$
\begin{aligned}
(5)\qquad \gamma[P \times P_1] + \gamma[2P \times P_1] + \cdots + \gamma[(p-1)P \times P_1]& \\
= \mathbf{t}^{-1}(pR - \lambda E_L - p\mathbf{t}Q) &= \eta^{-1}\pi\eta\nu P - \mathbf{t}^{-1}\lambda E_L\,;
\end{aligned}
$$

likewise,

$$\begin{aligned}(6)\quad &\gamma'[P \times P_1] + \gamma'[2P \times P_1] + \cdots + \gamma'[(p-1)P \times P_1] \\ &\qquad = \pi\nu P - \mathfrak{t}'^{-1}\lambda' E_L ,\end{aligned}$$

since $\eta' = 1$ in this case. Now, there exists an automorphism $\varphi$ of $A$ such that, for a nondegenerate $S \in A$, $\varphi\eta^{-1}\pi\eta S = \pi S$; if we set $\gamma'' = \varphi\gamma$, we have $G \cong \{L, A, \gamma''\}$, and (5) becomes

$$\begin{aligned}(7)\quad &\gamma''[P \times P_1] + \gamma''[2P \times P_1] + \cdots + \gamma''[(p-1)P \times P_1] \\ &\qquad = \pi\nu P - \varphi\mathfrak{t}^{-1}\lambda E_L .\end{aligned}$$

Set $\varepsilon = \gamma'' - \gamma'$; then (6) and (7) give $\varepsilon[P \times P_1] + \varepsilon[2P \times P_1] + \cdots + \varepsilon[(p-1)P \times P_1] = \mathfrak{t}'^{-1}\lambda' E_L - \varphi\mathfrak{t}^{-1}\lambda E_L$, which is independent of $P$. Result (3) implies then $\varepsilon \in \Gamma_0(L, A)$, or $\gamma' \sim \gamma''$, so that $G \cong G' = W_n(k)$, Q.E.D.

**3.** It is now expedient to restate a particular case of (4), with some modifications, in a form which is independent of the language of algebraic geometry. Let $k$ be a field of characteristic $p \neq 0$, and let $g_i(x_0, \cdots, x_n; y_0, \cdots, y_n)$ $(i = 0, \cdots, n)$ be polynomials in the indeterminates $x_0, \cdots, y_n$, with coefficients in $k$; set $(x_0, \cdots, x_n) + (y_0, \cdots, y_n) = (g_0(x; y), \cdots, g_n(x; y))$. We say that $\{g_0, \cdots, g_n\}$ is a *commutative recursive group-law over* $k$ if the following conditions are satisfied:

(a) $g_i \in k[x_0, \cdots, x_i; y_0, \cdots, y_i]$;

(b) $g_i(x; y) = g_i(y; x)$;

(c) $(x_0, \cdots, x_n) + [(y_0, \cdots, y_n) + (z_0, \cdots, z_n)] = [(x_0, \cdots, x_n) + (y_0, \cdots, y_n)] + (z_0, \cdots, z_n)$, $\{z\}$ being another set of indeterminates;

(d) there exist polynomials $g'_i(x_0, \cdots, x_i)$, with coefficients in $k$, such that $g_i(x_0, \cdots, x_n; g'_0(x), \cdots, g'_n(x)) = 0$;

(e) $g_i(x_0, \cdots, x_n; 0, \cdots, 0) = x_i$;

(f) $g_i(0, x_0, \cdots, x_{n-1}; 0, y_0, \cdots, y_{n-1}) = g_{i-1}(x_0, \cdots, x_n; y_0, \cdots, y_n)$ if $i > 0$.

We have:

(8) THEOREM. *Let $k$ be a field of characteristic $p \neq 0$, and let $\{g_0, \cdots, g_n\}$ be a commutative recursive group-law over $k$; assume moreover that, in the previous notations, $p(x_0, \cdots, x_n) = (0, x_0^p, \cdots, x_{n-1}^p)$. Then there exist polynomials $\psi_i, \chi_i \in k[x_0, \cdots, x_i]$, $i = 0, \cdots, n$, such that*

$$\psi_i(\chi_0(x), \cdots, \chi_i(x)) = \chi_i(\psi_0(x), \cdots, \psi_i(x)) = x_i ,$$

*and that*

$$\begin{aligned}&(\psi_0(x), \cdots, \psi_n(x)) + (\psi_0(y), \cdots, \psi_n(y)) \\ &\quad = (\psi_0(g_0(x; y)), \psi_1(g_0(x; y), g_1(x; y)), \cdots, \psi_n(g_0(x; y), \cdots, g_n(x; y))),\end{aligned}$$

*the + denoting addition of Witt vectors.*

*Proof.* Let $G$ be a group-variety over $k$ with n.h.g.p. $\{x_0, \cdots, x_n\}$, and with the law of composition prescribed by $\{g_0, \cdots, g_n\}$. Then $\bar{G}$ (extension of $G$ over the algebraic closure $\bar{k}$ of $k$) is a periodic group-variety of dimension $n + 1$ and period $p^{n+1}$, endowed with all the properties requested for the applicability of (4). Hence, by (4), it is isomorphic to $W_{n+1}(\bar{k})$, and this proves the existence of $\psi_i, \chi_i \in \bar{k}(x_0, \cdots, x_i)$ with the properties expressed in the statement (see the remark at the end of this proof for the existence of the *endomorphism* $\pi$). Since $\bar{G}$ and $W_{n+1}(\bar{k})$ are normal varieties, and the birational correspondence of isomorphism is regular at finite distance, we also obtain that $\psi_i, \chi_i \in \bar{k}[x_0, \cdots, x_i]$. The stronger result according to which $\psi_i$ and $\chi_i$ can be selected in $k[x_0, \cdots, x_i]$ is proved by induction in the following manner: if $n = 0$, any $\chi_0$ must have the form $\chi_0(x_0) = ax_0 + b$, or $\psi_0(x_0) = a^{-1}(x_0 - b)$, where $a, b \in \bar{k}$ and $a \neq 0$; moreover, we can always select $a = 1$. We then have $g_0(x_0, y_0) = \chi_0(\psi_0(x_0) + \psi_0(y_0)) = x_0 + y_0 - b$, so that $b \in k$, since $\{g\}$ is a recursive law over $k$. We can then assume $\chi_i$, $\psi_i \in k[x]$ for $i < j \leqq n$, and prove the same for $i = j$; we shall do this for the particular case $j = n$, this being equivalent to the general case. Let $\chi_0, \cdots, \chi_{n-1}, \psi_0, \cdots, \psi_{n-1}$ be selected in $k[x]$, and let $\chi_n, \psi_n$ be any possible selection in $\bar{k}[x]$; we have $g_n(x; y) = x_n + y_n + h(x_0, \cdots, x_{n-1}; y_0, \cdots, y_{n-1})$, $h \in k[x; y]$; if for a Witt vector $(z_0, \cdots, z_n)$ and a polynomial $F$ we denote $F(z_0, \cdots, z_n)$ also by $F((z_0, \cdots, z_n))$, we must have

$$\begin{aligned}\chi_n((x_0, \cdots, x_n) &+ (y_0, \cdots, y_n)) \\ &= \chi_n(x) + \chi_n(y) + h(\chi_0(x), \cdots, \chi_{n-1}(x); \chi_0(y), \cdots, \chi_{n-1}(y)).\end{aligned}$$

If $k'$ is the smallest subfield of $\bar{k}$ over $k$ which contains all the coefficients of $\chi_n$, and if $b_1 = 1, b_2, \cdots, b_r$ is a $k$-basis for $k'$, write $\chi_n(x) = \sum_i F_i(x)b_i$, $F_i(x) \in k[x]$; then

$$\begin{aligned}\textstyle\sum_i [F_i((x_0, \cdots, x_n) + (y_0, \cdots, y_n)) - F_i(x) - F_i(y)]b_i& \\ = h(\chi(x); \chi(y)) \in k[x],&\end{aligned}$$

or

$$F_i((x) + (y)) - F_i(x) - F_i(y) = 0$$

for $i > 1$. This proves that for $i > 1$ the mapping $(x_0, \cdots, x_n) \rightarrow F_i(x)$ is a homomorphism of $W_{n+1}(k)$ into a 1-dimensional vector variety over $k$; thus, $F_i(x)$, for $i > 1$, belongs to $k[x_0]$. We can therefore change the selection of $\chi_n$ by taking $\chi_n(x) = F_1(x) \in k[x]$, with the assurance that $\psi_n(x)$ exists, and that the conditions expressed in the statement are fulfilled, Q.E.D.

*Remark.* Since, in the previous statement, the mapping $(x_0, \cdots, x_n) \rightarrow (0, x_0^p, \cdots, x_{n-1}^p)$ is a homomorphism, we must have

$$\begin{aligned}g_i(x_0^p, \cdots, x_i^p; y_0^p, \cdots, y_i^p) &= g_{i+1}(0, x_0^p, \cdots, x_i^p; 0, y_0^p, \cdots, y_i^p) \\ &= [g_i(x_0, \cdots, x_i; y_0, \cdots, y_i)]^p \quad \text{for} \quad i = 0, \cdots, n-1;\end{aligned}$$

hence, for these values of $i$, $g_i(x; y) \in C_p[x; y]$.

**4.** We recall that two commutative group-varieties are said to be isogenous if each is a homomorphic image of the other; we shall say that they are *inseparably isogenous* if each is the homomorphic image of the other in a purely inseparable homomorphism.

(9) THEOREM. *Let $G$ be a periodic group-variety of dimension $n$ over the algebraically closed field $k$ of characteristic $p$; then $G$ has period $p^n$ if and only if it is a homomorphic image of $W_n(k)$. And if this is the case, $G$ is inseparably isogenous to $W_n(k)$.*

*Proof.* If $G$ is a homomorphic image of $W_n(k)$, it certainly has period $p^n$. Conversely, let $G$ have period $p^n$; if $n = 1$, all the statements of the theorem are true; we shall accordingly proceed by induction on $n$. Consider the case in which $\dim G = n$, and let $A$, $U$, $V$, $L$ have the same meaning as in the proof of (4) (we recall that $L = G/U$); then $G \cong \{A, V, \delta\}$, for a suitable $\delta \in \Gamma(A, V)$. By the recurrence assumption, there exists a purely inseparable homomorphism $\beta$ such that $A = \beta W_{n-1}(k)$. The mapping $\delta'[P \times Q_1] = \delta[\beta P \times (\beta Q)_1]$, where $P$, $Q$ are generic points of $W_{n-1}(k)$, is a factor set of $W_{n-1}(k)$ into $V$, and obviously $G$ is a homomorphic image of $\{W_{n-1}(k), V, \delta'\}$ in a purely inseparable homomorphism. In order to prove that $G$ is a homomorphic image of $W_n(k)$, in a purely inseparable homomorphism, it is sufficient to prove that this is true of $\{W_{n-1}(k), V, \delta'\}$; we can, for this purpose, assume $A = W_{n-1}(k)$.

With this assumption, we shall denote by $\varrho$ the natural homomorphism of $G$ onto $A$, and by $\mu$ the rational mapping of $A$ into $G$ which defines a crossed product; then $p\mu$ is a homomorphism of $A$ onto $U$, certainly divisible by the endomorphism $\pi$ of $A$, since the homomorphism $p$ of $G$ is divisible by the homomorphism $\pi$ of $G$; we can thus write $p\mu = \mathbf{t}\pi$, $\mathbf{t}$ being a homomorphism of $A$ onto $U$. This gives $pR = \mathbf{t}\pi\varrho R$ for any nondegenerate $R \in G$; the latter is the same relation given in the statement of (4), with the difference that now $\mathbf{t}$ is a homomorphism rather than an isomorphism. As in part 2 of the proof of (4) we shall write $G = \{L, U, \gamma\} = \{A, V, \delta\}$, $A = \{L, B, \theta\}$, and denote by $\nu$ the rational mapping of $L$ into $A$ used in defining $\{L, B, \theta\}$; we shall also set $\lambda = \mu\nu$. A generic point of $G$ is of the type $R = \lambda P + Q$, with $P \in L$ and $Q \in U = \mathbf{t}A$, so that $pR = p\lambda P + pQ = \lambda E_L + \gamma[P \times P_1] + \gamma[2P \times P_1] + \cdots + \gamma[(p-1)P \times P_1] + pQ$. But $pR = \mathbf{t}\pi\varrho\mu\nu P + pQ = \mathbf{t}\pi\nu P + pQ$, so that $\gamma[P \times P_1] + \gamma[2P \times P_1] + \cdots + \gamma[(p-1)P \times P_1] = \mathbf{t}\pi\nu P - \lambda E_L$, which is the analogue of (5). On the other hand, if we write $W_n(k) = \{L, A, \gamma'\}$, we have, as in (6), $\gamma'[P \times P_1] + \gamma'[2P \times P_1] + \cdots + \gamma'[(p-1)P \times P_1] = \pi\nu P$, since $\lambda'$ can be so selected as to have $\lambda' E_L = E_{W_n(k)}$. If we now set $\gamma'' = \mathbf{t}\gamma'$, and $\varepsilon = \gamma'' - \gamma$, we have that $\varepsilon[P \times P_1] + \varepsilon[2P \times P_1] + \cdots + \varepsilon[(p-1)P \times P_1] = \lambda E_L$ is independent of $P$, so that, by (3), $\varepsilon \in \Gamma_0(L, U)$, and $\gamma \sim \gamma''$, $G = \{L, U, \gamma\} \cong \{L, U, \gamma''\}$; but $\{L, U, \gamma''\}$ is obviously a homomorphic image, in a purely inseparable homomorphism, of $\{L, A, \gamma'\} = W_n(k)$. It is thus proved that $G$ is a homomorphic image of $W_n(k)$ in a purely inseparable homomorphism. If we write, accordingly, $k(G) \subseteqq k(W_n(k))$, we have, for a suitable $r$, $(k(W_n(k)))^{p^r} \subseteqq k(G)$, so that $G$ is inseparably isogenous to $W_n(k)$, Q.E.D.

The existence of periodic group-varieties isogenous, but not isomorphic, to Witt varieties, is established, for instance, by the following example: $G$ is a 2-dimensional projective space with n.h.g.p. $\{x_0, x_1\}$ over a field of characteristic 2, with the law of composition given by $(x_0, x_1) + (y_0, y_1) = (x_0 + y_0, x_1 + y_1 + x_0^2 y_0^2)$.

A direct consequence of (9), and of a result of [11], is:

(10) Corollary. *Let $k$ be as in* (9), *and let $F$ be a field of characteristic zero, complete with respect to a normalized discrete valuation $v$ of rank* 1, *with residue field $k$, and such that $v(p) = 1$; if $R_v$, $\mathfrak{P}_v$ are respectively the valuation ring of $v$ and its prime ideal, and if $G$ is a periodic group-variety over $k$, of dimension $n$ and period $p^n$, the group of the nondegenerate points of $G$ is isomorphic to the additive group $R_v/\mathfrak{P}_v^n \cong \mathfrak{P}_v^{-n}/R_v$.*

It may not be superfluous to note specifically that from the construction used in the proof of (9) follows that for any $n$-dimensional periodic group-variety $G$ over $k$, of period $p^n$, there exist $(n + 1)$-dimensional group-varieties $G'$ and $G''$ over $k$, of period $p^{n+1}$, of which $G$ is, respectively, a homomorphic image (in a separable homomorphism) and a group-subvariety. The projective and injective limits of chains of the type $G, G', \cdots$, or $G, G'', \cdots$ yield, respectively, an infinite abelian torsion-free group, and an infinite abelian torsion group. These are isomorphic to, respectively, $R_v$ and $F/R_v$.

**5.** According to (6) of [2], each periodic group-variety over the algebraically closed field $k$ of characteristic $p$ is isomorphic to a Vessiot variety; this must be true, in particular, of $W_n(k)$; now, according to (8), or also by Corollary 1 §8 of [8], $W_n(k)$ is isomorphic to a group-variety $G$ with a general point $\{x_0, \cdots, x_{n-1}\}$, whose law of composition is the recursive group law (2) of hyperexponential vectors; namely, if for a nondegenerate $P \in G$ we denote by $x_i(P)$ the value of $x_i$ at $P$, we have $x_i(P + Q) = x_i(P) + x_i(Q) + \sum_j e_j(x(P))e_{p^i-j}(x(Q))$. Let then $M = (m_{ij})$ $(i, j = 0, \cdots, p^{n-1})$ be the square matrix of order $p^{n-1} + 1$ such that: $m_{ij} = 0$ if $j > i$; $m_{ii} = 1$; $m_{ij} = e_{i-j}(x)$ if $j < i$; since, in the notations of (2), $e_r(z) = e_r(x) + e_r(y) + \sum_{j=1}^{r-1} e_j(x)e_{r-j}(y)$, it is easily verified that $M(P + Q) = M(P)M(Q)$, so that $M$ provides an explicit representation of $W_n(k)$ as a Vessiot variety.

Periodic group-varieties are rational, that is, birationally equivalent to projective spaces; Witt varieties, in addition, are actually projective spaces, with a hyperplane as degeneration locus, and a group of Cremona transformations as group of "translations"; we shall prove that this property is common to all periodic group-varieties of the type studied in this note (the relation of this property to Fano's theorem on regular group-varieties is not investigated here):

(11) THEOREM. *Let $A$ be a periodic group-variety of dimension $n$ and period $p^n$ over the algebraically closed field $k$ of characteristic $p \neq 0$; then $A$ is isomorphic to a group-variety $G$ over $k$, with degeneration locus $F$, such that $G$ is a projective space; and a n.h.g.p. $\{x_0, \cdots, x_{n-1}\}$ of $G$ can be selected in such a way that $F$ is the hyperplane at infinity for $\{x\}$, and that the law of composition on $G$ is (a Cremona transformation) given by*

$$x_i(P + Q) = x_i(P) + x_i(Q) + f_i(x_0(P), \cdots, x_{i-1}(P); x_0(Q), \cdots, x_{i-1}(Q)),$$

*$f_i$ being a polynomial with coefficients in $k$.*

*Proof.* The theorem is true for $n = 1$; we shall therefore proceed by induction on $n$. Given $A$, of dimension $n$, we have, by (9), $A = \alpha W_n(k)$, $\alpha$ being a purely inseparable homomorphism; we shall accordingly assume $k(A) \subseteqq k(W_n(k))$ as prescribed by $\alpha$. There is a natural homomorphism $\varrho$ of $W_n(k)$ onto $W_{n-1}(k)$, and a natural homomorphism $\sigma$ of $A$ onto an $(n - 1)$-dimensional periodic group-variety $B$ over $k$, of dimension $n - 1$ and period $p^{n-1}$; we shall assume, accordingly, $k(W_{n-1}(k)) \subset k(W_n(k))$, $k(B) \subset k(A)$. Since $\dim B = n - 1$, by the recurrence assumption we may assume $B$ to have the property claimed for $G$, and denote by $\{x_0, \cdots, x_{n-2}\}$ a n.h.g.p. of $B$ having the properties stated in the theorem. Furthermore, the previous embeddings are such that $k(B) \subseteqq k(W_{n-1}(k))$; this generates a homomorphism $\beta$ of $W_{n-1}(k)$ onto $B$. There are rational mappings $\lambda$ of $W_{n-1}(k)$ into $W_n(k)$, and $\mu$ of $B$ into $A$, such that $\varrho\lambda = \sigma\mu = 1$. Since the rational mapping $\sigma\alpha\lambda$ of $W_{n-1}(k)$ into $B$ coincides with $\beta$, we can select $\mu$ to be such that $\mu\beta = \alpha\lambda$; then, for a nondegenerate $P \in B$, say $P = \beta Q$ where $Q \in W_{n-1}(k)$ is nondegenerate, we have $\mu[P] = \alpha\lambda[Q]$; since, by the nature of $\lambda$, $\lambda[Q]$ is a nondegenerate point of $W_n(k)$, $\mu[P]$ is a nondegenerate point of $A$. But then there exists a factor set $\gamma$ of $B$ into a 1-dimensional vector variety $V$ over $k$, such that $A \cong \{B, V, \gamma\}$, and such that $\gamma[P \times Q_1] = \mu[P] + \mu[Q] - \mu[P + Q]$ is a nondegenerate point of $V$ for each pair of nondegenerate points $P$, $Q$ of $B$. If $x_{n-1}$ is a canonical coordinate on $V$, namely one for which $x_{n-1}(P + Q) = x_{n-1}(P) + x_{n-1}(Q)$, this means that

$$x_{n-1}(\gamma[P \times Q_1]) = f_{n-1}(x_0(P), \cdots, x_{n-2}(P); x_0(Q), \cdots, x_{n-2}(Q)),$$

$f_{n-1}$ being a polynomial with coefficients in $k$. Thus $A$ is isomorphic to the projective space $G$ with n.h.g.p. $\{x_0, \cdots, x_{n-1}\}$, and has the required degeneration locus and the required law of composition, Q.E.D.

## Appendix

In this appendix, all varieties are over an algebraically closed field $k$ of characteristic $p \neq 0$. Those group-varieties which are isogenous to Witt varieties will be called *of Witt type*.

(12) LEMMA. *Let $V$, $W$ be varieties of Witt type, $V$ being 1-dimensional. If $\{V, W, \gamma\}$ is a homomorphic image of $V \times W$, then $\gamma \in \Gamma_0(V, W)$.*

*Proof.* If $\dim W = 1$, the lemma is true, since in this case $\{V, W, \gamma\}$ is a vector variety, hence isomorphic to $V \times W$. If $\dim W = n > 1$, and the lemma is accepted when $\dim W < n$, then either $\gamma$ operates on the $(n - 1)$-dimensional irreducible group-subvariety $U$ of $W$, certainly of Witt type by (9), and in this case the result is true by the recurrence assumption; or else, if $\beta$ is the natural homomorphism of $W$ onto $L = W/U$, $\{V, L, \beta\gamma\}$ is a homomorphic image of $V \times L$, so that $\beta\gamma \in \Gamma_0(V, L)$, $\gamma$ is associate to a $\gamma'$ which operates on $U$, and the previous case gives $\gamma' \in \Gamma_0(V, W)$, Q.E.D.

(13) LEMMA. *$V$ and $W$ having the same meaning as in* (12), *any given $\{V, W, \gamma\}$ is either of Witt type, or isomorphic to $V \times W$.*

*Proof.* The lemma will be proved by recurrence on $n = \dim W$, since the result is true if $\dim W = 1$, by (9). If $\{V, W, \gamma\}$ is not of Witt type, then, by (9), it has period $p^n$, so that $p^{n-1}\sum_{i=1}^{p-1} \gamma[iP \times P_1] = \sum_{i=1}^{p^n-1} \gamma[iP \times P_1] = E_W$ for a generic $P \in V$. Then $\sum_{i=1}^{p-1} \gamma[iP \times P_1]$ belongs to the irreducible $(n - 1)$-dimensional group-subvariety $U$ of $W$; if $\alpha$ is the natural homomorphism of $W$ onto $W/U$, we have $\sum_{i=1}^{p-1} \alpha\gamma[iP \times P_1] = E_{\alpha W}$, hence

$$\alpha\gamma \in \Gamma_0(V, \alpha W)$$

by (3), and $\gamma$ is associate to a $\gamma'$ which operates on $U$. We shall consequently assume $\gamma$ to operate on $U$ from the beginning; if

$$\{V, U, \gamma\} \cong V \times U,$$

$\gamma$ belongs to $\Gamma_0(V, W)$, as claimed. Otherwise, by recurrence, $\{V, U, \gamma\}$ is of Witt type, and is therefore a homomorphic image of $W \cong \{V, U, \delta\}$, by (9); but then $\{V, W, \gamma\}$ is a homomorphic image of $\{V, W, \delta\}$, and this is isomorphic to $V \times W$ since $\delta \in \Gamma_0(V, W)$. The result now descends from (12), Q.E.D.

(14) THEOREM. *Let $A$ be a periodic group-variety of period $p^n$; then $A$ is isomorphic to the direct product of varieties of Witt type. In particular, $A$ possesses $n$-dimensional group-subvarieties of Witt type, and any one of these is a direct factor of $A$.*

*Proof.* The first statement is a consequence of the second; the two parts of the second statement will be proved by recurrence on $\dim A$. If $X = pA$, $X$ has the period $p^{n-1}$; if $X$ is not of Witt type, by the recurrence assumption we have $X \cong Y \times Z$, where $Y$ is of Witt type and dimension $n - 1$, and $\dim Z > 0$; after setting $W = p^{-1}Y \subset A$, $W$ has the period $p^n$, hence it possesses an irreducible $n$-dimensional group-subvariety of Witt type; it follows that $A$ has the same property. If instead $X$ is of Witt type, $L = A/X$ has period $p$, and is therefore isomorphic to a direct product $V_1 \times \cdots \times V_r$ of 1-dimensional vector varieties; but then

$$A \cong \{V_1 \times \cdots \times V_r, X, \gamma_1 + \cdots + \gamma_r\}$$

(by Lemma 3.3 of [1]), where $\gamma_i \in \Gamma(V_i, X)$, and $\gamma_i \notin \Gamma_0(V_i, X)$ for at least one value of $i$, say $i = 1$ (otherwise $A \cong L \times X$ would have period $p^{n-1}$). Thus $\{V_1, X, \gamma_1\}$ is a group-subvariety of $A$, of dimension $n$, and it is of Witt type by (13).

Having now established that $A$ possesses an $n$-dimensional group-subvariety of Witt type, if $\dim A > n$ let $B$ be an irreducible group-subvariety of $A$, containing $W$, and having dimension equal to $\dim A - 1$. Then, by the recurrence assumption, $B \cong W \times C$, and $A \cong \{V, W \times C, \delta_0 + \delta_1\}$, where $V$ is a 1-dimensional vector variety, $\delta_0 \in \Gamma(V, W)$, and $\delta_1 \in \Gamma(V, C)$; now, $\{V, W, \delta_0\} \cong A/C$ has period $p^n$, so that, by (13), $\delta_0 \in \Gamma_0(V, W)$, and $A \cong \{V, C, \delta_1\} \times W$, Q.E.D.

*Remark.* If $W$ is a group-subvariety of $A$, of Witt type and dimension $<n$, in general $W$ is not a direct factor of $A$, not even in the case in which $W$ is not a proper group-subvariety of any group-subvariety of Witt type of $A$. For instance, if $A$ has n.h.g.p. $\{x, y, z\}$ and law of composition

$$(x, y, z) + (x', y', z') = (x + x', y + y' + f(x, x'), z + z'),$$

where $f(x, x') = -\sum_{i=1}^{p-1}(i!)^{-1}[(p - i)!]^{-1}x^i x'^{p-i}$, the vector group-subvariety $W$ given by $x = 0$, $z = y^p$ is not properly contained in any group-subvariety of Witt type of $A$, since no point of $W$, with the exception of $E_W$, is of the type $pP$ with $P \in A$. However, $W$ is not a direct factor of $A$; in fact, $V = A/W$ has n.h.g.p. $\{\xi, \eta\}$ and the law of composition $(\xi, \eta) + (\xi', \eta') = (\xi + \xi', \eta + \eta' + f(\xi, \xi')^p)$, and the natural homomorphism of $A$ onto $V$ is given by $\xi = x$, $\eta = y^p - z$. We have $A = \{V, W, \delta\}$, where $\delta$ is determined by the function $g\big((\xi, \eta), (\xi', \eta')\big) = f(\xi, \xi')$. Were $W$ a direct factor of $A$, $\delta$ would belong to $\Gamma_0(V, W)$, and it would be possible to find an $h(\xi, \eta) \in k(\xi, \eta)$ such that

$$f(\xi, \xi') = h(\xi, \eta) + h(\xi', \eta') - h\big(\xi + \xi', \eta + \eta' + f(\xi, \xi')^p\big).$$

Set here $\eta = \eta' = 0$, derivate with respect to $\xi'$, and set $\xi' = 0$; one obtains $\xi^{p-1} + dh(\xi, 0)/d\xi \in k$, which is impossible.

## Bibliography


1. I. Barsotti, *Structure theorems for group-varieties*, Ann. Mat. Pura Appl. (4), vol. 38 (1955), pp. 77–119.
2. ———, *Un teorema di struttura per le varietà gruppali*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat. (8), vol. 18 (1955), pp. 43–50.
3. ———, *Abelian varieties over fields of positive characteristic*, Rend. Circ. Mat. Palermo (2), vol. 5 (1956), pp. 145–169.
4. ———, *Gli endomorfismi delle varietà abeliane su corpi di caratteristica positiva*, Ann. Scuola Norm. Sup. Pisa (3), vol. 10 (1956), pp. 1–24.
5. ———, *Repartitions on abelian varieties*, Illinois J. Math., vol. 2 (1958), pp. 43-70.
6. J. Dieudonné, *Sur les groupes de Lie algêbriques sur un corps de caractêristique* $p > 0$, Rend. Circ. Mat. Palermo (2), vol. 1 (1952), pp. 380–402.
7. ———, *Groupes de Lie et hyperalgèbres de Lie sur un corps de caractêristique* $p > 0$. *III*, Math. Zeit., vol. 63 (1955), pp. 53–75.

8. ———, *Witt groups and hyperexponential groups*, Mathematika, vol. 2 (1955), pp. 21–31.
9. ———, *Lie groups and Lie hyperalgebras over a field of characteristic $p > 0$ (IV)*, Amer. J. Math., vol. 77 (1955), pp. 429–452.
10. J-P. SERRE, *Sur la topologie des variétés algébriques en caractéristique p*, mimeographed notes of the Symposium of Algebraic Topology, Mexico, Summer 1956.
11. E. WITT, *Zyklische Körper und Algebren der Charakteristik p vom Grad $p^m$. Struktur diskret bewerteter perfekter Körper mit volkommenem Restklassenkörper der Charakteristik p*, J. Reine Angew. Math., vol. 176 (1937), pp. 126–140.

UNIVERSITY OF PITTSBURGH
PITTSBURGH, PENNSYLVANIA