Polynomial sequences in groups

A. Leibman

Department of Mathematics
The Ohio State University
Columbus, OH43210, USA
e-mail: leibman@math.ohio-state.edu

Abstract

Given a group G with lower central series $G = G_1 \supseteq G_2 \supseteq G_3 \supseteq \ldots$, we say that a sequence $g\colon \mathbb{Z} \longrightarrow G$ is *polynomial* if for any k there is d such that the sequence obtained from g by applying the difference operator $Dg(n) = g(n)^{-1}g(n+1)$ d times takes its values in G_k. We introduce the notion of *the degree of a polynomial sequence* and prove that polynomial sequences of degrees not exceeding a given one form a group. As an application we obtain the following extension of the Hall-Petresco theorem:

Theorem. *Let $G = G_1 \supseteq G_2 \supseteq G_3 \supseteq \ldots$ be the lower central series of a group G. Let $x \in G_k$, $y \in G_l$ and let p, q be polynomials $\mathbb{Z} \longrightarrow \mathbb{Z}$ of degrees k and l respectively. Then there is a sequence $z_0 \in G$, $z_i \in G_i$ for $i \in \mathbb{N}$, such that $x^{p(n)}y^{q(n)} = z_0^{\binom{n}{0}} z_1^{\binom{n}{1}} \ldots z_n^{\binom{n}{n}}$ for all $n \in \mathbb{N}$.*

0. Introduction

The intention of this paper is to provide an answer to a question related to the following Hall-Petresco theorem:

Theorem HP. (See, for example, [P].) *Let $G = G_1 \supseteq G_2 \supseteq G_3 \supseteq \ldots$ be the lower central series of a group G and let $x, y \in G$. There exists a sequence $z_i \in G_i$ for $i \in \mathbb{N}$, such that*

$$x^n y^n = z_1^{\binom{n}{1}} z_2^{\binom{n}{2}} \ldots z_n^{\binom{n}{n}} \tag{0.1}$$

for all $n \in \mathbb{N}$.

The question was: *does the conclusion of Theorem HP remain true if one replaces* (0.1) *by*

$$x^{\binom{n}{k}} y^{\binom{n}{l}} = z_l^{\binom{n}{l}} z_{l+1}^{\binom{n}{l+1}} \ldots z_n^{\binom{n}{n}}$$

under the assumption that $x \in G_k$, $y \in G_l$ and $k \geq l$?

We answer this question positively, using the technique of what we call *polynomial sequences.* The element-wise product gh of two homomorphisms $g, h\colon \mathbb{Z} \longrightarrow G$, that is of two "linear" sequences $g(n)=x^n$ and $h(n)=y^n$ in G, is not, generally speaking, a homomorphism. However, gh is a homomorphism modulo the commutator subgroup $G_2=[G,G]$ of G: $gh(n)=(xy)^n r(n)$ with $r(n)\in G_2$ for all $n\in\mathbb{Z}$. It is seen from Theorem HP that for any $k\in\mathbb{N}$, the sequence $gh(n)$ can be written as a polynomial expression modulo G_{k+1}: $gh(n)=z_1^{\binom{n}{1}}z_2^{\binom{n}{2}}\ldots z_k^{\binom{n}{k}}r(n)$ with $r(n)\in G_{k+1}$ for all $n\in\mathbb{N}$, where $\binom{n}{l}=\frac{n(n-1)\ldots(n-l+1)}{l!}$ is a polynomial of degree l with respect to n.

The sequence $gh(n)=x^n y^n$ is an example of *a polynomial sequence of degree* $\leq(1,2,3,\ldots)$ in G. One could define a general polynomial sequence as a mapping $g\colon\mathbb{Z}\longrightarrow G$ such that for every $k\in\mathbb{N}$ there are $z_1,\ldots,z_t\in G$ and polynomials $p_1,\ldots,p_t\colon\mathbb{Z}\longrightarrow\mathbb{Z}$ for which $g(n)\Big(z_1^{p_1(n)}\ldots z_t^{p_t(n)}\Big)^{-1}\in G_{k+1}$ for $n\in\mathbb{Z}$. We have preferred a different approach, based on the following property of ordinary polynomials: they vanish after finitely many applications of the difference operator $Dp(n)=p(n+1)-p(n)$. We call a mapping $g\colon\mathbb{Z}\longrightarrow G$ *a polynomial sequence in* G if for every $k\in\mathbb{N}$ the sequence obtained from g by applying the operator $Dg(n)=g(n)^{-1}g(n+1)$ finitely many times takes its values in G_{k+1}. *The degree* of a polynomial sequence g is the sequence $(d_1,d_2,d_3,\ldots)$ of integers where $d_k=\min\{d: D^{d+1}g(n)\in G_{k+1}\text{ for all } n\}$.

We show that polynomial sequences form a group with respect to element-wise multiplication. This is not surprising and follows from the well known fact that multiplication in a nilpotent group is polynomial (see subsection 2.9). What is more important, for every sequence $\bar{d}=(d_1,d_2,d_3,\ldots)$ with the property $d_{i+j}\geq d_i+d_j$ for all $i,j\in\mathbb{N}$, the polynomial sequences whose degrees do not exceed $\bar{d}$ also form a group. An example is given by the group of polynomial sequences of degrees $\leq(1,2,3,\ldots)$; we denote it by $\wp_{(1,2,3,\ldots)}G$. This group contains all homomorphisms $\mathbb{Z}\longrightarrow G$, $n\mapsto x^n$, as well as all sequences of the form $x^{p(n)}$ with $x\in G_k$ and p being a polynomial of degree $\leq k$ for some $k\in\mathbb{N}$. We prove that the polynomial sequences $z^{\binom{n}{k}}$ with $z\in G_k$ form a sort of basis for $\wp_{(1,2,3,\ldots)}G$: for any sequence $g\in\wp_{(1,2,3,\ldots)}G$ there are $z_0\in G$ and $z_k\in G_k$ for $k\in\mathbb{N}$, such that for every $k\in\mathbb{N}$ one has $g(n)=z_1^{\binom{n}{1}}\ldots z_k^{\binom{n}{k}}r_k(n)$ with $r_k(n)\in G_{k+1}$ for all $n\in\mathbb{Z}$. It gives an alternative proof of Theorem HP and answers the foregoing question.

After this paper was written, it was brought to our attention that similar questions were treated in [L]. In (a part of) his work, M. Lazard used the Lie algebra associated to a group G to study the group of sequences in G of the form $x_1^{p_1(n)}\ldots x_s^{p_s(n)}$, where $x_j\in G_j$ and p_j is a polynomial of degree $\leq j$ (the group $\wp_{(1,2,3,\ldots)}G$ in our notation). In particular, a version of Proposition 3.1 is proved there. Though it seems clear enough that the methods of [L] can be utilized to obtain the other results of our paper, we feel that our approach has advantages of its own and may lead to new interesting developments. For instance, instead of polynomial sequences $\mathbb{Z}\longrightarrow G$, one can consider *polynomial mappings* $H\longrightarrow G$, where H is a general abelian group; most of the results of this paper can be extended to this case. (See also Remark 3.4.)

Acknowledgment. I thank H. Furstenberg for bringing this problem to my attention. I am thankful to Vitaly Bergelson for his advise and permanent support. In fact, the subject of this paper is closely related to our joint research on generalized polynomiality (see [BL1]). I thank Ron Karidi for his comments on the preliminary version of this paper.

I also thank the referee for many useful remarks and suggestions.

1. Groups of polynomial sequences

1.1. We define $Z_+ = \{0, 1, 2, \ldots\}$, $Z_* = \{-\infty, 0, 1, 2, \ldots\}$. We will always assume that $-\infty + (-\infty) = -\infty$, and that $-\infty < t$ and $-\infty \pm t = -\infty$ for all $t \in \mathbb{Z}_+$.

We also define $d \dot{-} t$ for $d \in \mathbb{Z}_*$ and $t \in \mathbb{Z}_+$ by

$$d \dot{-} t = \begin{cases} d - t, & \text{if } \ d \geq t \\ -\infty, & \text{if } \ d < t. \end{cases}$$

Note that $(d \dot{-} t_1) \dot{-} t_2 = d \dot{-} (t_1 + t_2)$.

Let $\bar{d} = (d_k)_{k \in \mathbb{N}}$ where $d_k \in \mathbb{Z}_*$ for $k \in \mathbb{N}$, and let $t \in \mathbb{Z}_+$. We define $\bar{d} \dot{-} t = (d_k \dot{-} t)_{k \in \mathbb{N}}$.

Given $\bar{d} = (d_k)_{k \in \mathbb{N}}$ and $\bar{c} = (c_k)_{k \in \mathbb{N}}$ with $d_k, c_k \in \mathbb{Z}_*$ for $k \in \mathbb{N}$, we will write $\bar{d} \leq \bar{c}$ if $d_k \leq c_k$ for all $k \in \mathbb{N}$. Clearly, $\bar{d} \dot{-} t_1 \leq \bar{d} \dot{-} t_2$ for $t_1 \geq t_2$.

1.2. Let G be a group. For $x, y \in G$, *the commutator of* x *and* y is $[x, y] = x^{-1}y^{-1}xy$; the identity $xy = yx[x, y]$ will be frequently used in the sequel. For $A, B \subseteq G$, $[A, B]$ is the group generated by $\Big\{[x, y] \ \Big| \ x \in A, \ y \in B\Big\}$.

Let $G = G_1 \supseteq G_2 \supseteq G_3 \supseteq \ldots$ be *the lower central series* of G, that is $G_1 = G$, $G_{k+1} = [G, G_k]$ for $k = 1, 2, \ldots$. It is known (and not hard to verify) that $[G_i, G_j] \subseteq G_{i+j}$ for any $i, j \in \mathbb{N}$.

1.3. Given a (two-sided) sequence $g\colon \mathbb{Z} \longrightarrow G$, its *derivative* Dg is the sequence defined by $Dg(n) = g(n)^{-1}g(n+1)$. Every sequence g in G is uniquely defined by its derivative Dg and one of its values, say $g(0)$:

Lemma. *Let g and h be two sequences in G with $Dg = Dh$ and $g(0) = h(0)$. Then $g(n) = h(n)$ for all $n \in \mathbb{Z}$.*

Proof. By induction on n. ■

1.4. The derivation D is a mapping from the set $G^{\mathbb{Z}}$ of sequences in G into itself; let $D^1 = D$, $D^{l+1} = D \circ D^l$ for $l = 1, 2, \ldots$, and $D^{-\infty} = D^0 = \mathrm{id}_{G^{\mathbb{Z}}}$.

Let $\bar{d} = (d_1, d_2, \ldots)$ where $d_k \in \mathbb{Z}_*$ for $k \in \mathbb{N}$. A sequence $g \in G^{\mathbb{Z}}$ is said to be *polynomial of degree* $\leq \bar{d}$ if for every $k \in \mathbb{N}$, $D^{d_k+1}g$ takes its values in G_{k+1}: $D^{d_k+1}g(n) \in G_{k+1}$ for all $n \in \mathbb{Z}$. In particular, $d_k = -\infty$ implies $g(n) \in G_{k+1}$ for all $n \in \mathbb{Z}$.

1.5. Let H be a subgroup of G, let $H = H_1 \supseteq H_2 \supseteq H_3 \supseteq \ldots$ be its lower central series and let g be a sequence in H. Since $H_k \subseteq G_k$ for all $k \in \mathbb{N}$, if g is polynomial in H then it is also polynomial in G.

1.6. Examples.

1.6.1. Let $x \in G$, let $p \in \mathbb{Z}[n]$ be a polynomial of degree $\leq d$. Then the sequence $g(n) = x^{p(n)}$ is polynomial of degree $\leq (d, d, d, \ldots)$: we have $Dg(n) = x^{p(n+1)-p(n)}$ and

$p(n+1)-p(n)$ is a polynomial of degree $\leq d-1$, so $D^{d+1}g \equiv \mathbf{1}_G$. We say that g is of *absolute degree* $\leq d$.

If, in addition, $x \in G_k$, then g is polynomial of degree $\leq (\underset{1}{-\infty}, \ldots, \underset{k-1}{-\infty}, d, d, \ldots)$.

1.6.2. Let $G = \left\{x, y, z \mid [x,y]=z,\ [x,z]=[y,z]=\mathbf{1}_g\right\}$ (G is isomorphic to the smallest Heisenberg group, the group of 3×3 upper triangular matrices over $\mathbb{Z}$ with unit main diagonal). Let $g(n)=x^n y^n$. Then

$$\begin{aligned}
&Dg(n) = y^{-n}x^{-n}x^{n+1}y^{n+1} = y^{-n}xy^{n+1} = y^{-n}y^{n+1}x[x,y^{n+1}] = yxz^{n+1}\\
&D^2g(n) = z^{-n}(yx)^{-1}yxz^{n+1} = z \in G_2\\
&D^3g(n) = z^{-1}z = \mathbf{1}_G
\end{aligned}$$

Hence, g is a polynomial sequence of degree $\leq (1,2,2,\ldots)$.

1.6.3. Let G be a nilpotent group of class $\leq l$, that is let $G_{l+1}=\{\mathbf{1}_G\}$. Then a sequence g in G is polynomial if and only if $D^{d+1}g(n) \in G_{l+1}$ for some $d \in \mathbb{Z}_+$, that is $D^{d+1}g \equiv \mathbf{1}_G$. If this is the case, g is of degree $\leq (d,d,d,\ldots)$ (that is of absolute degree $\leq d$).

Note that when we deal with nilpotent (in particular, abelian) groups the degree of a polynomial sequence is actually represented by a finite sequence: if G is of class $\leq l$ then any polynomial sequence in G is of degree $\leq (d_1,d_2,\ldots)$ with $d_l = d_{l+1} = d_{l+2} = \ldots$. In such case we will say that the polynomial sequence is of degree $\leq (d_1,\ldots,d_l)$.

1.6.4. Let g be a polynomial sequence of degree $\leq (\underset{1}{0}, \ldots, \underset{k}{0}, d_{k+1}, \ldots)$. Then $Dg(n) = g(n)^{-1}g(n+1) \in G_{k+1}$, so $g(n)G_{k+1} = g(n+1)G_{k+1}$ for $n \in \mathbb{Z}$. This means that g is constant on G/G_{k+1}: $g(n)G_{k+1} = g(0)G_{k+1}$ for all $n \in \mathbb{Z}$.

The following two elementary propositions will be used many times in the sequel; we omit proofs.

1.7. Proposition. *If g is a polynomial sequence of degree $\leq \bar{d}$, then Dg is a polynomial sequence of degree $\leq \bar{d} \dot{-} 1$. If Dg is a polynomial sequence of degree $\leq (c_k)$, then g is a polynomial sequence of degree $\leq (b_k)$, where $b_k = c_k+1$ if $c_k \geq 0$ and $b_k = 0$ if $c_k = -\infty$.*

1.8. Proposition. *If $g(n)$ is a polynomial sequence of degree $\leq \bar{d}$, then for any fixed $m \in \mathbb{Z}$ the sequence $g(n+m)$ is also polynomial of degree $\leq \bar{d}$.*

1.9. A sequence $\bar{d} = (d_k)_{k\in\mathbb{N}}$ with $d_k \in \mathbb{Z}_*$ is said to be *superadditive* if it is nondecreasing and satisfies $d_i + d_j \leq d_{i+j}$ for all $i,j \in \mathbb{N}$.

Examples. $(1,2,3,\ldots,)$, $(-\infty,-\infty,0,1,2,\ldots)$, $(3,6,9,\ldots)$ and $(1,2,4,\ldots)$ are superadditive sequences, $(2,3,4,\ldots)$ is not.

1.10. The following lemma is obvious.

Lemma. *If $t \in \mathbb{Z}_+$ and $\bar{d}$ is a superadditive sequence, then $\bar{d} \dot{-} t$ is also a superadditive sequence.*

Note also that for every sequence $\bar{c} = (c_k)_{k\in\mathbb{N}}$ with $c_k \in \mathbb{Z}_*$ there is a superadditive sequence $\bar{d}$ dominating $\bar{c}$: $\bar{c} \leq \bar{d}$.

1.11. Remark. Given $\bar{d} = (d_k)_{k\in\mathbb{N}}$ and $\bar{c} = (c_k)_{k\in\mathbb{N}}$ with $d_k, c_k \in \mathbb{Z}_*$, define $\bar{d} * \bar{c} = (a_k)_{k\in\mathbb{N}}$ by $a_1 = -\infty$, $a_k = \max\{d_i + c_j \mid i + j = k\}$ for $k = 2, 3, \ldots$. The operation "$*$" preserves the set of superadditive sequences: if $\bar{d}$ and $\bar{c}$ are both superadditive then $\bar{d} * \bar{c}$ is. Moreover, if $\bar{d}$ is superadditive, we have $(\bar{d} \dotdiv t_1) * (\bar{d} \dotdiv t_2) \leq \bar{d} \dotdiv (t_1 + t_2)$ for any $t_1, t_2 \in \mathbb{Z}_+$. This property of superadditive sequences will be implicitly used in the proof of Proposition 1.14 below.

1.12. The following theorem is the main result of this paper.

Theorem. *Let $\bar{d}$ be a superadditive sequence. Then polynomial sequences of degree $\leq \bar{d}$ form a group (with respect to element-wise multiplication).*

1.13. Corollary. *The set of polynomial sequences in G is a group.*

1.14. Theorem 1.12 is a corollary of the following proposition:

Proposition. *Let $\bar{d} = (d_k)_{k\in\mathbb{N}}$ be a superadditive sequence, let $t, t_1, t_2 \in \mathbb{Z}_+$.*

(a) If g, h are polynomial sequences of degree $\leq \bar{d} \dotdiv t$, then gh is a polynomial sequence of degree $\leq \bar{d} \dotdiv t$ as well.

(b) If g is a polynomial sequence of degree $\leq \bar{d} \dotdiv t_1$ and h is a polynomial sequence of degree $\leq \bar{d} \dotdiv t_2$, then $[g, h]$ is a polynomial sequence of degree $\leq \bar{d} \dotdiv (t_1 + t_2)$.

(c) If g is a polynomial sequence of degree $\leq \bar{d} \dotdiv t$, then so is g^{-1}.

The proof of this proposition in the paper published in ETDS contains a mistake; below is a corrected proof.

Proof. First of all, we may reduce the problem to the case where G is a nilpotent group. Indeed, to prove that a sequence f in G (of the form gh, $[g, h]$ or g^{-1}) is polynomial of degree $\leq \bar{d} \dotdiv t$ one has to show that for any k,

$$D^{d_k \dotdiv t+1} f \subset G_{k+1}. \tag{1.1}$$

(We will write $f \subset H$ if $f(n) \in H$ for all n.) Fix an $l \in \mathbb{N}$; if we prove Proposition 1.14 for $f \bmod G_{l+1}$ in G/G_{l+1} we will have (1.1) for all $k \leq l$. Thus, we replace G by G/G_{l+1} and assume from now on that $G_{l+1} = \{1\}$.

We will first prove (a) and (b). We will use the following commutator identities that hold for any sequences g, h in G:

$$D(gh)(n) = Dg(n)Dh(n)\big[Dg(n), h(n+1)\big] \tag{1.2}$$

and

$$\begin{aligned} D[g,h](n) = {} & [g(n), Dh(n)]\big[Dh(n), [h(n), g(n)]\big]\cdot \\ & \Big[[g(n), Dh(n)]\big[Dh(n), [h(n), g(n)]\big], [g(n), h(n)]\Big]\cdot \\ & \big[[g(n), h(n+1)], Dg(n)\big]\big[Dg(n), h(n+1)\big]. \end{aligned} \tag{1.3}$$

We will be proving a statement more general than Proposition 1.14. Let us say that a sequence f in G is a *cp-sequence* (commutator-polynomial sequence) if f can be constructed from polynomial sequences of degree $\leq \bar{d} \div t$, $t \in \mathbb{Z}_+$, by multiplying them and taking their commutators. More exactly, f is a cp-sequence if f is a polynomial sequence of degree $\leq \bar{d} \div t$ for some $t \in \mathbb{Z}_+$, or $f = gh$ where g, h are cp-sequences, or $f = [g, h]$ where g, h are cp-sequences. We note that if f is a cp-sequence then $f(n+1)$ is also a cp-sequence.

We define an integer parameter w on the set of cp-sequences in the following way: if f is a polynomial sequence of degree $\leq \bar{d} \div t$ for some $t \in \mathbb{Z}_+$ then we write $w(f) \geq t$; if $f = gh$ where g, h are cp-sequences with $w(g), w(h) \geq t$, then $w(f) \geq t$; if $f = [g, h]$ where g, h are cp-sequences with $w(g) \geq r$ and $w(h) \geq s$, then $w(f) \geq r + s$.

Lemma C1. *If f is a cp-sequence with $w(f) \geq t$ then Df is a cp-sequence with $w(Df) \geq t + 1$.*

Proof. We use induction on the construction of f. If f is a polynomial sequence of degree $\leq \bar{d} \div t$, $t \in \mathbb{Z}_+$, the assertion of the lemma is trivial. If $f = gh$ where g, h are cp-sequences with $w(g), w(h) \geq t$ and for which the assertion of the lemma already holds, then Df is a cp-sequence with $w(Dq) \geq t+1$ by formula (1.2). If $f = [g, h]$ where g, h are cp-sequences with $w(g) \geq r$ and $w(h) \geq t - r$ and for which the assertion of the lemma holds, then Df is a cp-sequence with $w(Df) \geq t + 1$ by formula (1.3). ■

Lemma C2. *If f is a cp-sequence and $w(f) \geq d_k + 1$ for some $k \in \mathbb{N}$ then $f \subset G_{k+1}$. In particular, if $w(f) \geq d_l + 1$ then $f \equiv 1$.*

Proof. Again, we use induction on the construction of f. If f is a polynomial sequence of degree $\leq \bar{d} \div (d_k + 1)$ then $f \subset G_{k+1}$ by definition. If $f = gh$ with $w(g), w(h) \geq d_k + 1$, then by induction $g, h \subset G_{k+1}$, so $f \subset G_{k+1}$. If $f = [g, h]$ with $w(g) \geq r$ and $w(h) \geq s$ such that $r + s = d_k + 1$, let $m < k$ be such that $d_m + 1 \leq r \leq d_{m+1}$; then

$$s = d_k + 1 - r \geq d_{m+1} + d_{k-m-1} + 1 - r \geq d_{k-m-1} + 1.$$

By induction $g \subset G_{m+1}$ and $h \subset G_{k-m}$, thus $f \subset G_{k+1}$. ■

Now, parts (a) and (b) of Proposition 1.14 are very special cases of the following statement:

Lemma C3. *If f is a cp-sequence with $w(f) \geq t$ then f is a polynomial sequence of degree $\leq \bar{d} \div t$.*

Proof. We will use a descending induction on t; for $t \geq d_l + 1$ the assertion trivially holds by Lemma C2. By Lemma C1, if f is a cp-sequence with $w(f) \geq t$ then Df is a cp-sequence with $w(Df) \geq t + 1$, thus by induction hypothesis Df is a polynomial sequence of degree $\leq \bar{d} \div (t + 1)$. By Proposition 1.7, f is a polynomial sequence of degree $\leq \bar{b}$ where $b_k = d_k - t$ if $d_k \geq t$. It remains to check that $f \subset G_{k+1}$ if $d_k < t$, but this is again given by Lemma C2. ■

To prove part (c) of Proposition 1.14 we use the following identity:

$$D(g^{-1})(n) = Dg(n)^{-1}[g(n), Dg(n)^{-1}]\big[g(n), [g(n), Dg(n)^{-1}]\big] \ldots \\ \big[g(n), \ldots, [g(n), Dg(n)^{-1}] \ldots\big],$$

where the last commutator has l brackets. By a descending induction on t, $(Dg)^{-1}$ is a polynomial sequence of degree $\leq \bar{d} \dot{-} t$, thus by Lemma C3, $D(g^{-1})$ is a polynomial sequence of degree $\leq \bar{d} \dot{-} t$, and by Proposition 1.7, g^{-1} is a polynomial sequence of degree $\leq \bar{b}$ where $b_k = d_k - t$ if $d_k \geq t$. It remains to check that $g^{-1} \subset G_{k+1}$ if $d_k < t$; but this is obvious because $g \subset G_{k+1}$ in this case. ■

Remark. The proof of Proposition 1.14 is based on the fact the product xy is linear on G_k/G_{k+1}, and the commutator $[x, y]$ is a bilinear mapping $(G_k/G_{k+1}) \times (G_l/G_{l+1}) \longrightarrow G_{k+l}/G_{k+l+1}$ for any $k, l \in \mathbb{N}$.

1.15. For completeness, let us bring one more theorem of the same type; we will not use it.

Theorem. *Let $\bar{d} = (d_k)_{k\in\mathbb{N}}$ be a superadditive sequence, let g be a polynomial sequence of degree $\leq \bar{d}$ and let p be a polynomial taking on integer values on the integers with $\deg p = c$. Then the sequence $h(n) = g(n)^{p(n)}$ for $n \in \mathbb{Z}$ is polynomial of degree $\leq (d_k + kc)_{k\in\mathbb{N}}$.*

Proof. We will use induction on increasing c and on decreasing $t \in \mathbb{Z}_+$ to prove that if $g(n)$ is a polynomial sequence of degree $\leq \bar{d} \dot{-} t$, then $g(n)^{p(n)}$ is a polynomial sequence of degree $\leq (d_k \dot{-} t + kc)_{k\in\mathbb{N}}$. If $c = 0$ the polynomial p is constant, and the statement is a corollary of Theorem 1.12.

Let $c \geq 1$. The base of induction on t is established by passing to factors G/G_{k+1} for $k \in \mathbb{N}$, as in the proof of Proposition 1.14. Write

$$\begin{aligned} D\Big(g(n)^{p(n)}\Big) = g(n)^{-p(n)}g(n+1)^{p(n+1)} = g(n)^{-p(n)}g(n)^{p(n+1)}g(n)^{-p(n+1)}g(n+1)^{p(n+1)} \\ = g(n)^{p(n+1)-p(n)}(Dg(n))^{p(n+1)}. \end{aligned}$$

$p(n+1) - p(n)$ is a polynomial of degree $c-1$, so by the induction hypothesis the sequence $g(n)^{p(n+1)-p(n)}$ is polynomial of degree $\leq (d_k \dot{-} t + k(c-1))_{k\in\mathbb{N}} \leq (d_k \dot{-} t + kc - 1)_{k\in\mathbb{N}}$. $Dg(n)$ is a polynomial sequence of degree $\leq \bar{d} \dot{-} (t+1)$, so by the induction hypothesis $(Dg(n))^{p(n+1)}$ is a polynomial sequence of degree $\leq (d_k \dot{-} (t+1) + kc)_{k\in\mathbb{N}} \leq (d_k \dot{-} t + kc - 1)_{k\in\mathbb{N}}$. By Theorem 1.12 their product $D(g(n)^{p(n)})$ is also polynomial of degree $\leq (d_k \dot{-} t + kc - 1)_{k\in\mathbb{N}}$, and by Proposition 1.7 the sequence $g(n)^{p(n)}$ is polynomial of degree $\leq (d_k \dot{-} t + kc)_{k\in\mathbb{N}}$. ■

1.16. Remark. Theorems 1.12 and 1.15 hold true if we substitute $\mathbb{Z}$ for an arbitrary abelian group H and consider *polynomial mappings* $H \longrightarrow G$ instead of polynomial sequences $\mathbb{Z} \longrightarrow G$.

2. Representation by infinite series

2.1. We keep the notation of Section 1. We will denote the group of polynomial sequences in G by $\wp G$. For a $\mathbb{Z}_*$-valued superadditive sequence $\bar{d}$, we will denote the group of polynomial sequences of degree $\leq \bar{d}$ by $\wp_{\bar{d}} G$. The goal of this section is to represent polynomial sequences in the form of infinite products of elements of G raised to polynomial exponents.

2.2. Introduce on G the $\{G_k\}_{k\in\mathbb{N}}$-adic topology: in this topology the groups G_k for $k \in \mathbb{N}$ form a basis of neighbourhoods of $\mathbf{1}_G$. Now, a sequence (x_i) in G converges to $x \in G$, $x_i \underset{i\to\infty}{\longrightarrow} x$ or $\lim_{i\to\infty} x_i = x$, if for any $k \in \mathbb{N}$ there is l such that $x^{-1}x_i \in G_k$ for all $i > l$.

Given a sequence $(x_i)_{i=1}^{\infty}$ in G, we define $\prod_{i=1}^{\infty} x_i = \lim_{l\to\infty} \prod_{i=1}^{l} x_i$ if the limit exists.

Note that $\prod_{i=1}^{\infty} x_i$ may exist only if $x_i \to \mathbf{1}_G$; the converse is not true generally speaking. Besides, if the nilpotent residue $\bigcap_{k=1}^{\infty} G_k$ is nontrivial, the product $\prod_{i=1}^{\infty} x_i$ is not uniquely defined (the introduced topology is not Hausdorff in this case). One could avoid these troubles by passing to the completion of G, $G_* = \varprojlim G/G_k$: for any sequence (x_i) in G_* converging to $\mathbf{1}_{G_*}$, the product $\prod_{i=1}^{\infty} x_i$ exists and is unique. We however prefer to remain in G.

2.3. We define *an integral polynomial* as a polynomial with rational coefficients taking on integer values on the integers. The binomial coefficients $b_k(n) = \binom{n}{k} = \frac{n(n-1)\ldots(n-k+1)}{k(k-1)\ldots 1}$ for $k \in \mathbb{Z}_+$ form a natural basis for the module (over $\mathbb{Z}$) of integral polynomials: $b_k(n)$ is (the only) integral polynomial of degree k satisfying $b_k(0) = \ldots = b_k(k-1) = 0$, $b_k(k) = 1$. Every integral polynomial $p(n)$ of degree $\leq d$ is uniquely determined by its values at any $d+1$ distinct points; we have, consequently,

$$\begin{aligned} &p(n) = c_0 b_0(n) + c_1 b_1(n) + \ldots + c_d b_d(n), \\ &\qquad\text{where } c_0 = p(0),\ c_k = p(k) - \Big(c_0 b_0(k) + \ldots + c_{k-1} b_{k-1}(k)\Big) \text{ for } k = 1, \ldots, d. \end{aligned} \tag{2.1}$$

The difference operator $Dp(n) = p(n+1) - p(n)$ maps the group of integral polynomials onto itself: the "primitive" P of an integral polynomial p, defined by $DP = p$ and say $P(0) = 0$, is an integral polynomial as well. Indeed, $b_k = Db_{k+1}$ for all $k \in \mathbb{Z}_+$ (to check this note that $Db_{k+1}(0) = 0$ for $n = 0, \ldots, k-1$ and $Db_{k+1}(k) = 1$).

2.4. We will now show that polynomial sequences in G are exactly (infinite) products of elements raised to integral polynomial exponents.

Theorem. *Let $\bar{d} = (d_k)_{k\in\mathbb{N}}$ be a superadditive sequence, let a sequence g in G be given by a (converging) product*

$$g(n) = \prod_{i=1}^{\infty} x_i^{p_i(n)} \text{ for } n \in \mathbb{Z},$$

where, for $i \in \mathbb{N}$, $x_i \in G_{k_i}$ and p_i is an integral polynomial of degree $\leq d_{k_i}$. Then $g \in \wp_{\bar{d}} G$.

Proof. We have to show that, for every $k \in \mathbb{N}$, $D^{d_k+1} g(n) \in G_{k+1}$ for all $n \in \mathbb{Z}$. To do it, we may pass to G/G_{k+1}, that is assume that $G_{k+1} = \{\mathbf{1}_G\}$. Since $x_i \underset{i\to\infty}{\longrightarrow} \mathbf{1}_G$, g is then given by a finite product $g(n) = \prod_{i=1}^{l} x_i^{p_i(n)}$ for $n \in \mathbb{Z}$, and by 1.6.1, $x_i^{p_i(n)}$ is a polynomial sequence of degree $\leq (\underset{1}{-\infty}, \ldots, \underset{k_i-1}{-\infty}, d_{k_i}, d_{k_i}, \ldots) \leq \bar{d}$ for every $i = 1, \ldots, l$. By Theorem 1.12, g is polynomial of degree $\leq \bar{d}$. ■

2.5. The converse theorem holds as well.

Theorem. *Let $\bar{d} = (d_k)_{k\in\mathbb{N}}$ be a superadditive sequence, let $g \in \wp_{\bar{d}}G$. Then there exist a sequence $(x_i)_{i=1}^{\infty}$ with $x_i \in G_{k_i}$, and a sequence of integral polynomials $(p_i)_{i=1}^{\infty}$ with $\deg p_i \leq d_{k_i}$ such that $g(n) = \prod_{i=1}^{\infty} x_i^{p_i(n)}$ for all $n \in \mathbb{Z}$. Moreover, if X is a subset of G such that for every $k \in \mathbb{N}$ the elements of X lying in G_k generate G_k/G_{k+1}, then x_i for all $i \in \mathbb{N}$ can be chosen from X.*

Proof. We have to find elements $x_1, x_2, \ldots \in X$ and integral polynomials $p_1, p_2, \ldots$ such that for every $k \in \mathbb{N}$ there is $l \in \mathbb{N}$ such that $x_i \in G_{k+1}$ for $i > l$, $\deg p_i \leq d_k$ for $i \leq l$ and

$$\Big(\prod_{i=1}^{l} x_i^{p_i(n)}\Big)^{-1} g(n) \in G_{k+1} \text{ for all } n \in \mathbb{Z}. \tag{2.2}$$

We will do it using induction on k.

Assume that we have found elements $x_i \in X \cap G_{k_i}$ and polynomials p_i with $\deg p_i \leq d_{k_i}$ for $i = 1, \ldots, j$ such that

$$g'(n) = \Big(\prod_{i=1}^{j} x_i^{p_i(n)}\Big)^{-1} g(n) \in G_k \text{ for all } n \in \mathbb{Z}.$$

By Theorem 1.12, $g'(n)$ is a polynomial sequence of degree $\leq \bar{d}$, thus $D^{d_k+1}g'(n) \in G_{k+1}$ for all $n \in \mathbb{Z}$. Assume now that we can find $x_{j+1}, \ldots x_l \in X \cap G_k$ and integral polynomials $p_{j+1}, \ldots, p_l$ with $\deg p_i \leq d_k$ for $i = j+1, \ldots, l$, such that $g'(n) \cdot G_{k+1} = \prod_{i=j+1}^{l} x_i^{p_i(n)} \cdot G_{k+1}$ for all $n \in \mathbb{Z}$. Then we will have (2.2).

2.6. It follows that we may confine ourselves to the case of an abelian group, that is, it suffices to prove the following proposition:

Proposition. *Let H be an abelian group, let a set $X \subseteq H$ generate H and let h be a sequence in H satisfying $D^{d+1}h(n) = \mathbf{1}_H$ for some $d \in \mathbb{Z}$, $d \geq -1$. Then h can be represented in the form*

$$h(n) = \prod_{i=1}^{s} y_i^{q_i(n)} \text{ for } n \in \mathbb{Z},$$

where $y_1, \ldots, y_s \in X$ and $q_1, \ldots, q_s$ are integral polynomials of degree $\leq d$.

Indeed, applying this proposition to the abelian group $H = G_k/G_{k+1}$ and the sequence $h(n) = g'(n) \cdot G_{k+1}$ in H we will find the required $x_{j+1}, \ldots, x_l$ and $p_{j+1}, \ldots, p_l$. ■

Proof of Proposition. We will use induction on d. For $d = -1$ the statement is trivial; assume that it holds for $d-1$. Find $y_1, \ldots, y_t \in X$ and integral polynomials $q'_1, \ldots, q'_t$ of degree $\leq d-1$ such that $Dh(n) = \prod_{i=1}^{t} y_1^{q'_i(n)}$ for $n \in \mathbb{Z}$. Let $q_1, \ldots, q_t$ be integral polynomials with $q_i(n+1) - q_i(n) = q'_i(n)$ for $n \in \mathbb{Z}$ (they exist, see 2.3). We may also assume that $q_i(0) = 0$ for $i = 1, \ldots, t$. Represent $h(0) = y_{t+1} \ldots y_s$ with $y_{t+1}, \ldots, y_s \in X$. Define

$$h'(n) = \prod_{i=1}^{t} y_i^{q_i(n)} \prod_{i=t+1}^{s} y_i \text{ for } n \in \mathbb{Z}. \tag{2.3}$$

Then $h'(0) = h(0)$ and

$$Dh'(n) = h'(n)^{-1}h'(n+1) = \Big(\prod_{i=1}^{t} y_i^{q_i(n)} \prod_{i=t+1}^{s} y_i\Big)^{-1} \prod_{i=1}^{t} y_i^{q_i(n+1)} \prod_{i=t+1}^{s} y_i$$
$$= \prod_{i=1}^{t} y_i^{q_i(n+1)-q_i(n)} = \prod_{i=1}^{t} y_i^{q_i'(n)} = Dh(n) \text{ for } n \in \mathbb{Z}.$$

By Lemma 1.3, $h = h'$ and so (2.3) is the desired representation of h. ■

2.7. In the proof of Theorem 2.5 the elements $x_1, x_2, x_3, \ldots$, participating in the product $g(n) = \prod_{i=1}^{\infty} x_i^{p_i(n)}$, are picked from successive members of the lower central series of G: say, $x_1, \ldots, x_{t_1} \in G_1$, $x_{t_1+1}, \ldots, x_{t_2} \in G_2$, and so on. This is not however necessary, since the proof works as well if one requires that x_i for $i \in \mathbb{N}$ occur in this product in accordance with any a priori chosen ordering.

Let us define such a product in the following way. Let S be a linearly ordered set, let $\{x_s\}_{s\in S}$ be a subset of G indexed by S. If S is finite, $S = (s_1, s_2, \ldots, s_t)$, we put $\prod_{s\in S} x_s = x_{s_1}x_{s_2}\ldots x_{s_t}$. If S is such that $S_k = \{s \in S \mid x_s \notin G_{k+1}\}$ is finite for all $k \in \mathbb{N}$, we define $\prod_{s\in S} x_s = \lim_{k\to\infty} \prod_{s\in S_k} x_s$ if this limit exists.

Examples. If $S = (1, 2, \ldots)$, then $\prod_{s\in S} x_s = \prod_{i=1}^{\infty} x_i$; both parts have sense only if $x_i \underset{i\to\infty}{\longrightarrow} \mathbf{1}_G$. If $S = (\ldots, -2, -1)$, then $\prod_{s\in S} x_s = \prod_{-\infty}^{i=-1} x_i$. If $S = (1, 2, \ldots, -1, -2, \ldots)$, then $\prod_{s\in S} x_s = \prod_{i=1}^{\infty} x_i \prod_{i=1}^{\infty} x_{-i}$ (if these products are defined).

2.8. Now we can generalize Theorems 2.4 and 2.5.

Theorem. *Let $\bar{d} = (d_k)_{k\in\mathbb{N}}$ be a superadditive sequence.*

a) Let S be a linearly ordered subset of G, for every $x \in S$ let $k_x \in \mathbb{N}$ be such that $x \in G_{k_x}$, let $\{p_x\}_{x\in S}$ be a family of integral polynomials with $\deg p_x \le d_{k_x}$ for $x \in S$, and let a sequence $g(n)$ in G be given by $g(n) = \prod_{x\in S} x^{p_x(n)}$ for $n \in \mathbb{Z}$. Then $g \in \wp_{\bar{d}}G$.

b) Let $g \in \wp_{\bar{d}}G$, let X be a linearly ordered subset of G such that for every $k \in \mathbb{N}$, $X \cap G_k$ generates G_k/G_{k+1}. Then there is $S \subseteq X$ and a family $\{p_x\}_{x\in S}$ of integral polynomials with $\deg p_x \le d_{k_x}$ for $x \in S$ (where again, $k_x \in \mathbb{N}$ is such that $x \in G_{k_x}$) such that $g(n) = \prod_{x\in S} x^{p_x(n)}$ for all $n \in \mathbb{Z}$.

Proof. a) Fix $k \in \mathbb{N}$, let $S_k = S \setminus G_k$. S_k must be finite (otherwise $g(n) = \prod_{x\in S} x^{p_x(n)}$ has no sense), thus in G_k/G_{k+1} the sequence $g(n) \cdot G_{k+1}$ is represented by the finite product $\prod_{x\in S_k} x^{p_x(n)}$, which belongs to $\wp_{\bar{d}}(G/G_{k+1})$ by Theorem 1.12. So, $D^{d_k+1}g(n) \cdot G_{k+1} = \mathbf{1}_{G/G_{k+1}}$, that is $D^{d_k+1}g(n) \in G_{k+1}$ for all $n \in \mathbb{Z}$.

b) We use induction on $k \in \mathbb{N}$ to find a sequence of sets $R_k \subseteq X \cap G_k$ and families of integral polynomials $\{p_x\}_{x\in R_k}$ with $\deg p_x \le d_k$ for $x \in R_k$, such that for $S_k = R_1 \cup \ldots \cup R_k$ one has

$$\Big(\prod_{x\in S_k} x^{p_x(n)}\Big)^{-1} g(n) \in G_{k+1} \text{ for } n \in \mathbb{Z}. \tag{2.4}$$

Then, for $S=\bigcup_{k=1}^\infty R_k$, we will have $g(n)=\prod_{x\in S}x^{p_x(n)}$ for all $n\in\mathbb{Z}$.

Assume that $R_1,\ldots,R_{k-1}$ and $\{p_x\}_{x\in R_1},\ldots,\{p_x\}_{x\in R_{k-1}}$ have been found: for $S_{k-1}=R_1\cup\ldots\cup R_{k-1}$ we have $g'(n)=\Big(\prod_{x\in S_{k-1}}x^{p_x(n)}\Big)^{-1}g(n)\in G_k$ for $n\in\mathbb{Z}$. By Theorem 1.12, $g'\in\wp_{\bar{d}}G$, so $D^{d_k+1}g'(n)\in G_{k+1}$, that is $D^{d_k+1}g'(n)\cdot G_{k+1}=\mathbf{1}_{G/G_{k+1}}$ for all $n\in\mathbb{Z}$. By Proposition 2.6, applied to the sequence $g'(n)\cdot G_{k+1}$ in the abelian group G_k/G_{k+1}, there are $x_1,\ldots,x_t\in X\cap G_k$ and integral polynomials $p_{x_1},\ldots,p_{x_t}$ of degree $\le d_k$ such that

$$g'(n)\cdot G_{k+1}=\prod_{i=1}^t x_i^{p_{x_i}(n)}\cdot G_{k+1}\text{ for }n\in\mathbb{Z}.$$

Put $R_k=\{x_1,\ldots,x_t\}$, $S_k=S_{k-1}\cup R_k$. Since G_k/G_{k+1} is in the center of G/G_{k+1}, we have

$$\prod_{x\in S_k}x^{p_x(n)}\cdot G_{k+1}=\prod_{x\in S_{k-1}}x^{p_x(n)}\prod_{x\in R_k}x^{p_x(n)}\cdot G_{k+1}\text{ for }n\in\mathbb{Z},$$

thus

$$\begin{aligned}\Big(\prod_{x\in S_k}x^{p_x(n)}\Big)^{-1}g(n)\cdot G_{k+1}&=\Big(\prod_{x\in R_k}x^{p_x(n)}\Big)^{-1}\Big(\prod_{x\in S_{k-1}}x^{p_x(n)}\Big)^{-1}g(n)\cdot G_{k+1}\\&=\Big(\prod_{x\in R_k}x^{p_x(n)}\Big)^{-1}g'(n)\cdot G_{k+1}=\mathbf{1}_{G/G_{k+1}}\text{ for }n\in\mathbb{Z}.\end{aligned}$$

It gives (2.4). ■

2.9. As an application, let us derive from Theorem 2.8 the fact that "the multiplication in a nilpotent group is polynomial". Namely, let G be a finitely generated torsion-free nilpotent group of class $\le l$ (that is, let $G_{l+1}=\{\mathbf{1}_G\}$). All factors G_k/G_{k+1} for $k=1,\ldots,l$ are then finitely generated free abelian groups (see, for example, [KM]). Let $X=(x_1,\ldots,x_t)$ be a linearly ordered subset of G such that $X\cap(G_k\setminus G_{k+1})$ is a basis for G_k/G_{k+1} for all $k=1,\ldots,l$. Then every element $y\in G$ can be uniquely written in the form $y=\prod_{i=1}^t x_i^{a_i}$, where $a_i\in\mathbb{Z}$ for $i=1,\ldots,t$. Indeed, let it be so in G/G_l by induction: $y\cdot G_l=\prod_{x_i\notin G_l}x_i^{a_i}\cdot G_l$. Represent $y'=\Big(\prod_{x_i\notin G_l}x_i^{a_i}\Big)^{-1}y\in G_l$ as $y'=\prod_{x_j\in G_l}x_j^{a_j}$. Then $y=\Big(\prod_{x_i\notin G_l}x_i^{a_i}\Big)\Big(\prod_{x_j\in G_l}x_j^{a_j}\Big)$, and since G_l is in the center of G, $y=\prod_{i=1}^t x_i^{a_i}$.

Proposition. *Under the assumption above*

(a) There are polynomials $P_1,\ldots,P_t$ of $2t$ variables such that for any $y,z\in G$, if $y=\prod_{i=1}^t x_i^{a_i}$, $z=\prod_{i=1}^t x_i^{b_i}$ and $yz=\prod_{i=1}^t x_i^{c_i}$, then $c_i=P_i(a_1,\ldots,a_t,b_1,\ldots,b_t)$ for $i=1,\ldots,t$.

(b) There are polynomials $Q_1,\ldots,Q_t$ of $t+1$ variables such that for any $y\in G$ and any $b\in\mathbb{Z}$, if $y=\prod_{i=1}^t x_i^{a_i}$ and $y^b=\prod_{i=1}^t x_i^{c_i}$, then $c_i=Q_i(a_1,\ldots,a_t,b)$ for $i=1,\ldots,t$.

Proof. (a) The product $yz=\prod_{i=1}^t x_i^{a_i}\prod_{i=1}^t x_i^{b_i}$ is a polynomial sequence of degree $\le(1,2,\ldots,l)$ with respect to any of variables $a_1,\ldots,b_t$ if the rest are fixed. By Theorem 2.8, in the unique representation $yz=\prod_{i=1}^t x_i^{c_i}$ the exponents $c_1,\ldots,c_t$ are polynomials of degree $\le l$ with respect to any of these variables. It remains to use the following fact:

Lemma. *Let $F(u_1,\ldots,u_s)$ be a function on $\mathbb{Z}^s$ such that F is a polynomial of degree $\le l$ of every of its variables if the rest are fixed. Then F is a polynomial.*

(Note that the lemma does not hold if the degrees of the polynomials are not assumed to be uniformly bounded.)

(b) Similarly, $y^b = \left(\prod_{i=1}^t x_i^{a_i}\right)^b$ is a polynomial sequence of degree $\le (1,2,\ldots,l)$ with respect to any of the variables $a_1,\ldots,a_t,b$ if the rest are fixed. So by Theorem 2.8, in the (unique) representation $y^b = \prod_{i=1}^t x_i^{c_i}$ the exponents $c_1,\ldots,c_t$ are polynomials of degree $\le l$ with respect to any of these variables. By the above lemma $c_1,\ldots,c_t$ are polynomials. ■

3. The group of polynomial sequences of degree $\le (1,2,3\ldots)$

Let us turn now to a concrete group of polynomial sequences, the group $\wp_{(1,2,3,\ldots)}G$. By definition, $\wp_{(1,2,3,\ldots)}G$ consists of sequences g in G satisfying $D^{k+1}g(n) \in G_{k+1}$ for all $n \in \mathbb{Z}$ and $k \in \mathbb{N}$.

3.1. Proposition. (See also [L]. *Let S denote $\{0,1,2,\ldots\}$ with any linear ordering on it. Every $g \in \wp_{(1,2,3,\ldots)}G$ can be uniquely written in the form $g(n) = \prod_{k\in S} z_k^{\binom{n}{k}}$ with $z_0 \in G$ and $z_k \in G_k$ for $k \in \mathbb{N}$.*

If, in addition, $g(0) = g(1) = \ldots = g(l) = \mathbf{1}_G$, then $z_0 = z_1 = \ldots = z_l = \mathbf{1}_G$.

3.2. We need the following simple fact:

Lemma. *Let H be a group, let g be "a polynomial sequence in H of absolute degree $\le d$", that is let $D^{d+1}h(n) \equiv \mathbf{1}_H$. Then h is completely defined by its values in $0,1,\ldots,d$: if h' is another sequence in H with $D^{d+1}h(n) \equiv \mathbf{1}_H$ and $h'(n) = h(n)$ for $n = 0,1,\ldots,d$, then $h'(n) = h(n)$ for all $n \in \mathbb{Z}$.*

Proof. We use induction on d. For $d = -1$ the statement is trivial; let it be true for $d-1$, $d \ge 0$. Then we can apply it to $Dh'(n)$ and $Dh(n)$: $Dh'(n) = h'(n)^{-1}h'(n+1) = h(n)^{-1}h(n+1) = Dh(n)$ for $n = 0,1,\ldots,d-1$, hence Dh' coincides with Dh. Since, in addition, $h'(0) = h(0)$, h' and h coincide by Lemma 1.3. ■

Proof of Proposition 3.1. We define elements z_k for $k \in \mathbb{Z}_+$ recurrently: $z_0 = g(0)$ and z_k is such that $g(k) = \prod_{i=0}^k z_i^{\binom{k}{i}}$ for $k = 1,2,\ldots$ (since $\binom{k}{k} = 1$, z_k is uniquely defined; cf. (2.1)). We have only to check that

$$g_k(n) = \Big(\prod_{\substack{i\in S\\ 0\le i\le k}} z_i^{\binom{n}{i}}\Big)^{-1} g(n) \in G_{k+1} \text{ for } n \in \mathbb{Z} \tag{3.1}$$

for all k ("$\le$" is used in the usual sense). Then, in particular,

$$\prod_{\substack{i\in S\\ 0\le i\le k}} z_i^{\binom{k+1}{i}} \cdot G_{k+1} = g(k+1)\cdot G_{k+1} = \prod_{\substack{i\in S\\ 0\le i\le k+1}} z_i^{\binom{k+1}{i}} \cdot G_{k+1},$$

so $z_{k+1} \in G_{k+1}$, and $g(n) = \lim_{k\to\infty} \prod_{\substack{i\in S\\ 0\le i\le k}} z_i^{\binom{n}{i}} = \prod_{i\in S} z_i^{\binom{n}{i}}$ for $n \in \mathbb{Z}$. The second statement of the proposition follows immediately.

We use induction on k. The statement is trivial for $k = 0$; fix $k \in \mathbb{N}$ and assume that $z_i \in G_i$ for $i \le k$. Then $g_k \in \wp_{(1,2,3,\dots)}G$ by Theorem 1.12, thus $D^{k+1}g_k(n) \in G_{k+1}$ for $n \in \mathbb{Z}$. But $g_k(0) = g_k(1) = \ldots = g_k(k) = \mathbf{1}_G$ by construction, so by Lemma 3.2, applied to the sequence $g_k(n)\cdot G_{k+1}$, it is trivial in the group G/G_{k+1}: $g_k(n)\cdot G_{k+1} = \mathbf{1}_{G/G_{k+1}}$ for all $n \in \mathbb{Z}$. This gives (3.1). ■

3.3. We are now in position to obtain the promised generalization of Hall-Petresco's theorem.

Corollary. *Let $x_1, \ldots, x_s$ be elements of G where $x_j \in G_{k_j}$, and let $p_1, \ldots, p_s$ be integral polynomials with $\deg p_j \le k_j$ for $j = 1, \ldots, s$. Let S be the set of nonnegative integers with a fixed linear ordering. Then there are $z_0 \in G$ and $z_k \in G_k$ for $k = 1, 2, \ldots$ such that*

$$\prod_{j=1}^{s} x_j^{p_j(n)} = \prod_{\substack{k\in S\\ 0\le k\le n}} z_k^{\binom{n}{k}}$$

for all $n \in \mathbb{Z}_+$. (If the ordering of S is standard, the last product is $\prod_{k=0}^{n} z_k^{\binom{n}{k}}$.)

If, in addition, $p_j(0) = \ldots = p_j(l) = 0$ for all $j = 1, \ldots, s$, then

$$\prod_{j=1}^{s} x_j^{p_j(n)} = \prod_{\substack{k\in S\\ l+1\le k\le n}} z_k^{\binom{n}{k}}$$

for all $n \in \mathbb{Z}_+$.

Proof. Indeed, $g(n) = \prod_{j=1}^{s} x_j^{p_j(n)} \in \wp_{(1,2,3,\dots)}G$, so $g(n) = \prod_{k\in S} z_k^{\binom{n}{k}}$ for all $n \in \mathbb{Z}$ for suitable $z_0, z_1, \ldots$. But for $n \ge 0$ one has $\binom{n}{k} \ne 0$ only for $k = 0, \ldots, n$.

If $p_j(0) = \ldots = p_j(l) = 0$ for $j = 1, \ldots, s$, then $g(0) = \ldots = g(l) = \mathbf{1}_G$ and thus $z_0 = \ldots = z_l = \mathbf{1}_G$. ■

3.4. Remark. Considering *polynomial mappings* $\mathbb{Z}^r \longrightarrow G$ instead of polynomial sequences $\mathbb{Z} \longrightarrow G$, we easily obtain a generalization of the Dark theorem (see, for example, [P]):

Theorem. *Let $x_1, \ldots, x_s$ be elements of G where $x_j \in G_{k_j}$, and let $p_1, \ldots, p_s$ be polynomials $\mathbb{Z}^r \longrightarrow \mathbb{Z}$ with $\deg p_j \le k_j$ for $j = 1, \ldots, s$. Fix a linear ordering on the set $(\mathbb{Z}_+)^r$. Then for every $(l_1, \ldots, l_r) \in (\mathbb{Z}_+)^r$ there exists $z_{l_1,\ldots,l_r} \in G_{l_1+\ldots+l_r}$ such that*

$$\prod_{j=1}^{s} x_j^{p_j(n_1,\ldots,n_r)} = \prod_{I} z_{l_1,\ldots,l_r}^{\binom{n_1}{l_1}\cdots\binom{n_r}{l_r}} \tag{3.2}$$

for all $(n_1, \ldots, n_r) \in \mathbb{Z}_+^r$, where $I = \{0 \le l_1 \le n_1\} \times \ldots \times \{0 \le l_r \le n_r\}$, and the factors in the product on the right hand side of (3.2) *are multiplied in accordance with the ordering induced on I from $(\mathbb{Z}_+)^r$.*

(In Dark's theorem, $[x^{n_1},y^{n_2}]=\prod_{\substack{1\le l_1\le n_1\\ 1\le l_2\le n_2}} z_{l_1,l_2}^{\binom{n_1}{l_1}\binom{n_2}{l_2}}$, where the factors in the product are ordered first according to n_1+n_2 and then according to n_1.)

Scetch of the proof for $r=2$. Fix $l_1,l_2\in\mathbb{Z}_+$, let $l=l_1+l_2$. Since $\binom{l_1}{l_1}\binom{l_2}{l_2}=1$, the element z_{l_1,l_2} is uniquely defined by (3.2). It is only to check that $z_{l_1,l_2}\in G_l$. Assume by induction that $z_{k_1,k_2}\in G_{k_1+k_2}$ for all $(k_1,k_2)\in(\mathbb{Z}_+)^2$ with $k_1+k_2<l$. Then the polynomial mapping $g\colon\mathbb{Z}^2\longrightarrow G$ defined by

$$g(n_1,n_2)=\Bigl(\prod_{j=1}^{s}x_j^{p_j(n_1,n_2)}\Bigr)^{-1}\prod_{\substack{(k_1,k_2)\in(\mathbb{Z}_+)^2\\ k_1+k_2<l}} z_{k_1,k_2}^{\binom{n_1}{k_1}\binom{n_2}{k_2}}$$

is of degree $\le(1,2,3,\ldots)$. So, $g(n_1,n_2)\cdot G_l$ is a polynomial mapping $\mathbb{Z}^2\longrightarrow G/G_l$ of *absolute degree* $\le l-1$, and thus it is determined by its values at the points $(n_1,n_2)\in\mathbb{Z}^2$ with $n_1,n_2\ge 0$, $n_1+n_2<l$. Since $\binom{n_1}{k_1}\binom{n_2}{k_2}=0$ if either $k_1>n_1$ or $k_2>n_2$, by definition of z_{k_1,k_2} we have $g(n_1,n_2)=\mathbf{1}_G$ for all such (n_1,n_2). Hence, $g(n_1,n_2)\in G_l$ for all $n_1,n_2\in\mathbb{Z}^2$; it implies $z_{l_1,l_2}\in G_l$. ∎

References

[**BL1**] V. Bergelson and A. Leibman, Set-polynomials and Polynomial Extension of Hales-Jewett Theorem, *submitted* .

[**KM**] M. Kargapolov and Ju. Merzljakov, *Fundamentals of the Theory of Groups*, Springer Verlag, New York, Heidelberg, Berlin, 1979.

[**L**] M. Lazard, Sur les groupes nilpotents et les anneaux de Lie, *Ann. Sci. Ecole Norm. Sup. (3)* **71** (1954), 101–190.

[**P**] D. S. Passman, *The Algebraic Structure of Group Rings*, Wiley, New York, 1977.