Generating integer polynomials using function composition

Sebastian Kreinecker, Erhard Aichinger

Institute for Algebra

June, 2017

Supported by the Austrian Science Fund (FWF): P29931

JOHANNES KEPLER
UNIVERSITY LINZ

How we can build new polynomials from other polynomials

We use function composition $\circ$ and $+, -$. Let us start with x^2.

How we can build new polynomials from other polynomials

We use function composition $\circ$ and $+, -$. Let us start with x^2.

$$\begin{aligned} x^2 \circ x^2 &= x^4 \\ x^2 \circ x^4 &= x^8 \\ x^2 \circ x^8 &= x^{16} \\ &\dots \end{aligned}$$

How we can build new polynomials from other polynomials

We use function composition $\circ$ and $+, -$. Let us start with x^2.

$$\begin{aligned} x^2 \circ x^2 &= x^4 \\ x^2 \circ x^4 &= x^8 \\ x^2 \circ x^8 &= x^{16} \end{aligned}$$

$$\dots$$

$$\begin{aligned} x^2 \circ (x^2 + x^4) &= x^4 + 2x^6 + x^8 \\ x^4 + 2x^6 + x^8 - x^4 - x^8 &= 2x^6 \\ x^2 \circ (x^2 + x^8) &= x^4 + 2x^{10} + x^{16} \\ x^4 + 2x^{10} + x^{16} - x^4 - x^{16} &= 2x^{10} \end{aligned}$$

$$\dots$$

Which polynomials do we get and which not?

- We do not get any monomial with odd degree:

$$x^2 \circ (ax^j + bx^i) = a^2x^{2j} + 2abx^{i+j} + b^2x^{2i}.$$

Which polynomials do we get and which not?

- We do not get any monomial with odd degree:

$$x^2 \circ (ax^j + bx^i) = a^2x^{2j} + 2abx^{i+j} + b^2x^{2i}.$$

- Do we get all $\sum_{i=0}^{\infty} c_i x^{2i}$?

Which polynomials do we get and which not?

- We do not get any monomial with odd degree:

$$x^2 \circ (ax^j + bx^i) = a^2x^{2j} + 2abx^{i+j} + b^2x^{2i}.$$

- Do we get all $\sum_{i=0}^{\infty} c_i x^{2i}$?
- Answer: No.

Which polynomials do we get and which not?

- We do not get any monomial with odd degree:

$$x^2 \circ (ax^j + bx^i) = a^2x^{2j} + 2abx^{i+j} + b^2x^{2i}.$$

- Do we get all $\sum_{i=0}^{\infty} c_i x^{2i}$?
- Answer: No.
- We cannot produce 1 as leading coefficient for all degrees.

Which polynomials do we get and which not?

- We do not get any monomial with odd degree:

$$x^2 \circ (ax^j + bx^i) = a^2x^{2j} + 2abx^{i+j} + b^2x^{2i}.$$

- Do we get all $\sum_{i=0}^{\infty} c_i x^{2i}$?
- Answer: No.
- We cannot produce 1 as leading coefficient for all degrees.
- Which condition do the coefficients c_i have to satisfy?

Which polynomials do we get and which not?

- We do not get any monomial with odd degree:

$$x^2 \circ (ax^j + bx^i) = a^2x^{2j} + 2abx^{i+j} + b^2x^{2i}.$$

- Do we get all $\sum_{i=0}^{\infty} c_i x^{2i}$?
- Answer: No.
- We cannot produce 1 as leading coefficient for all degrees.
- Which condition do the coefficients c_i have to satisfy?
- How can we generalize this question?

Nearrings

Definition

Let N be a nonempty set and $+, \circ$ two binary operations on N. $(N, +, \circ)$ is a nearring if $(N, +)$ is a group, $(N, \circ)$ is a semigroup and for all $x, y, z \in N$, it holds that $(x + y) \circ z = (x \circ z) + (y \circ z)$.

Nearrings

Definition

Let N be a nonempty set and $+, \circ$ two binary operations on N. $(N, +, \circ)$ is a nearring if $(N, +)$ is a group, $(N, \circ)$ is a semigroup and for all $x, y, z \in N$, it holds that $(x + y) \circ z = (x \circ z) + (y \circ z)$.

Definition

Let $(N, +, \circ)$ be a nearring. If $M \subseteq N$ and $(M, +, \circ)$ is a nearring, then $(M, +, \circ)$ is a subnearring of $(N, +, \circ)$.

Nearrings

Definition

Let N be a nonempty set and $+, \circ$ two binary operations on N. $(N, +, \circ)$ is a nearring if $(N, +)$ is a group, $(N, \circ)$ is a semigroup and for all $x, y, z \in N$, it holds that $(x + y) \circ z = (x \circ z) + (y \circ z)$.

Definition

Let $(N, +, \circ)$ be a nearring. If $M \subseteq N$ and $(M, +, \circ)$ is a nearring, then $(M, +, \circ)$ is a subnearring of $(N, +, \circ)$.

Definition

Let $(N, +, \circ)$ be a nearring and $F \subseteq N$. The subnearring of $(N, +, \circ)$ which is generated by F is defined by

$$\langle F \rangle := \bigcap \{M \mid F \subseteq M,\ (M, +, \circ) \text{ is a subnearring of } (N, +, \circ)\}.$$

Starting question in the language of nearrings

What do the polynomials of the subnearring of $(\mathbb{Z}[x], +, \circ)$ generated by $\{x^2\}$ look like?

Starting question in the language of nearrings

What do the polynomials of the subnearring of $(\mathbb{Z}[x], +, \circ)$ generated by $\{x^2\}$ look like?

Let $p(x) = \sum_{i=1}^{\infty} c_i x^i \in \langle\{x^2\}\rangle$. Which conditions do we have on the coefficients c_i?

Starting question in the language of nearrings

What do the polynomials of the subnearring of $(\mathbb{Z}[x], +, \circ)$ generated by $\{x^2\}$ look like?

Let $p(x) = \sum_{i=1}^{\infty} c_i x^i \in \langle\{x^2\}\rangle$. Which conditions do we have on the coefficients c_i?

If we have a guess, how can we prove it?

Generation Lemma

Lemma (Lemma 2.1 of [Aichinger, 2013])

Let $(N, +, \circ)$ be a nearring, and let F and M be non-empty subsets of N. We assume that the following conditions hold:

- $F \subseteq M$.
- $M \subseteq \langle F \rangle$.
- M *is closed under* $+$ *and* $-$.
- $F \circ M \subseteq M$.

Then $M = \langle F \rangle$.

Proof.

[Aichinger, 2013]. □

The subnearring generated by $\{x^2\}$

We denote by $s_b(a)$ the digit sum of the number a in base b.

Theorem

A polynomial $p = \sum_{i=1}^{n} c_i x^i \in \mathbb{Z}[x]$ lies in the subnearring of $(\mathbb{Z}[x], +, \circ)$ that is generated by $\{x^2\}$ if and only if for all $i \in \mathbb{N}$, $2^{s_2(2i)-1}$ divides c_{2i} and $c_{2i+1} = 0$.

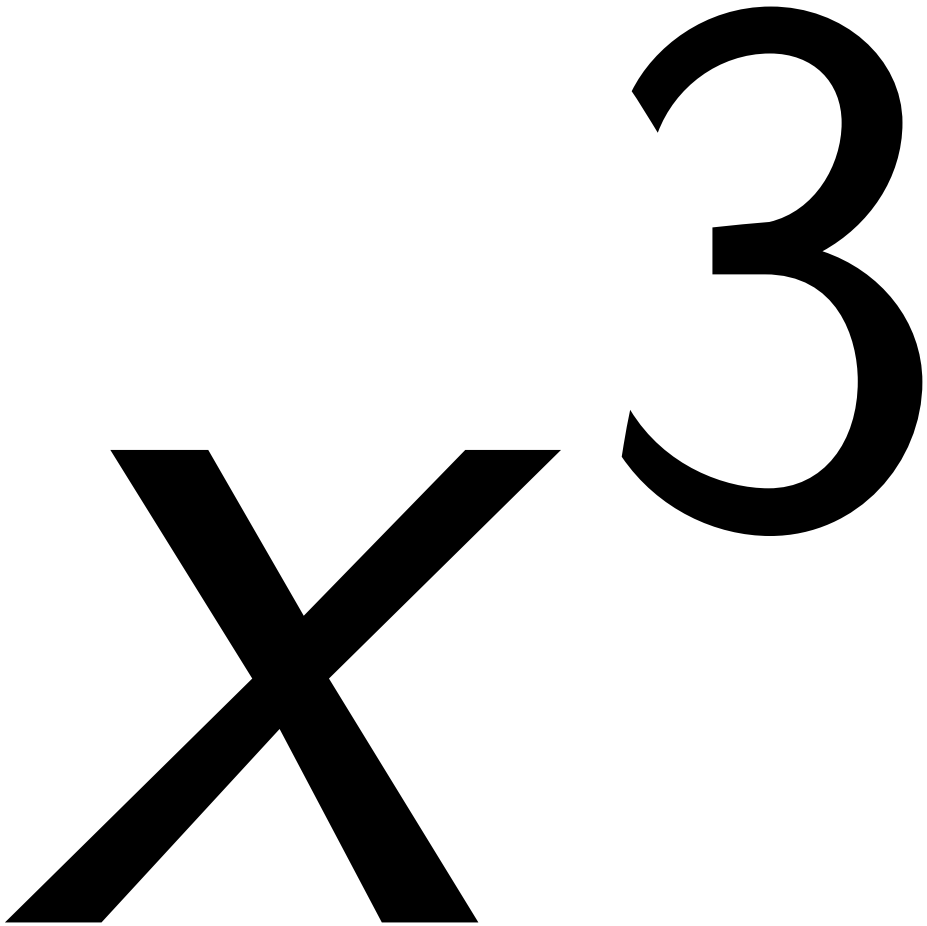
Proof of $\langle\{x^2\}\rangle$

Proof. We define $F := \{x^2\}$ and

$$M := \left\{ \sum_{i=1}^{n} c_i x^i \mid n \in \mathbb{N}, \forall i \in \mathbb{N}_0 : 2^{s_2(2i)-1} \mid c_{2i} \text{ and } c_{2i+1} = 0 \right\}.$$

By the Generation Lemma we have to check the following conditions:

- $F \subseteq M$.
- $M \subseteq \langle F \rangle$.
- M is closed under $+$ and $-$.
- $F \circ M \subseteq M$.


x3

The subnearring generated by $\{x^3\}$

Definition

Let $i, j \in \mathbb{N}$ and $y_1, \ldots, y_j \in \mathbb{N}_0$. We denote by $[\equiv_i;\ y_1, \ldots, y_j]$ the set $\{x \in \mathbb{N}_0 \mid \exists k \in \{1, \ldots, j\} :\ x \equiv_i y_k\}$.

The subnearring generated by $\{x^3\}$

Definition

Let $i, j \in \mathbb{N}$ and $y_1, \ldots, y_j \in \mathbb{N}_0$. We denote by $[\equiv_i;\ y_1, \ldots, y_j]$ the set $\{x \in \mathbb{N}_0 \mid \exists k \in \{1, \ldots, j\} :\ x \equiv_i y_k\}$.

Theorem

A polynomial $p = \sum_{i=0}^{n} c_i x^i \in \mathbb{Z}[x]$ *lies in the subnearring of* $(\mathbb{Z}[x], +, \circ)$ *that is generated by* $\{x^3\}$ *if and only if for all* $i \in \mathbb{N}_0$*:*

- *If* $i \notin [\equiv_6;\ 3]$ *then* $c_i = 0$.
- *If* $i \in [\equiv_6;\ 3]$ *then* $3^{\frac{s_3(i)-1}{2}}$ *divides* c_i.
- 2 *divides* $\sum_{j \in [\equiv_{24};\ 15,21]} c_j$.
- 2 *divides* $\sum_{\substack{j \in [\equiv_{72};\ 3,33,45,51,57,63] \\ j \neq 3}} c_j$.

Difficulty of the case $\{x^3\}$

We have (only) the following rules to construct polynomials:
If $p(x) \in \langle\{x^3\}\rangle$ then for all $a \in \mathbb{N}$ we have

- $x^{3^a} \in \langle\{x^3\}\rangle$,
- $3p(x)^2x^{3^a} + 3p(x)x^{2\cdot 3^a} \in \langle\{x^3\}\rangle$,
- $6p(x)^2x^{3^a} \in \langle\{x^3\}\rangle$ and
- $6p(x)x^{2\cdot 3^a} \in \langle\{x^3\}\rangle$.

Difficulty of the case $\{x^3\}$

We have (only) the following rules to construct polynomials:
If $p(x) \in \langle\{x^3\}\rangle$ then for all $a \in \mathbb{N}$ we have

- $x^{3^a} \in \langle\{x^3\}\rangle$,
- $3p(x)^2x^{3^a} + 3p(x)x^{2\cdot 3^a} \in \langle\{x^3\}\rangle$,
- $6p(x)^2x^{3^a} \in \langle\{x^3\}\rangle$ and
- $6p(x)x^{2\cdot 3^a} \in \langle\{x^3\}\rangle$.

$$(x^{3^a} + p(x))^3 - x^{3^{a+1}} - p(x)^3 = 3p(x)^2x^{3^a} + 3p(x)x^{2\cdot 3^a} \in \langle\{x^3\}\rangle.$$

Difficulty of the case $\{x^3\}$

We have (only) the following rules to construct polynomials:
If $p(x) \in \langle\{x^3\}\rangle$ then for all $a \in \mathbb{N}$ we have

- $x^{3^a} \in \langle\{x^3\}\rangle$,
- $3p(x)^2x^{3^a} + 3p(x)x^{2\cdot 3^a} \in \langle\{x^3\}\rangle$,
- $6p(x)^2x^{3^a} \in \langle\{x^3\}\rangle$ and
- $6p(x)x^{2\cdot 3^a} \in \langle\{x^3\}\rangle$.

$$(x^{3^a} + p(x))^3 - x^{3^{a+1}} - p(x)^3 = 3p(x)^2x^{3^a} + 3p(x)x^{2\cdot 3^a} \in \langle\{x^3\}\rangle.$$

$$-p(x) \in \langle F\rangle \Rightarrow 6p(x)^2x^{3^a}, 6p(x)x^{2\cdot 3^a} \in \langle\{x^3\}\rangle.$$

Difficulty of the case $\{x^3\}$

We have (only) the following rules to construct polynomials:
If $p(x) \in \langle\{x^3\}\rangle$ then for all $a \in \mathbb{N}$ we have

- $x^{3^a} \in \langle\{x^3\}\rangle$,
- $3p(x)^2x^{3^a} + 3p(x)x^{2\cdot 3^a} \in \langle\{x^3\}\rangle$,
- $6p(x)^2x^{3^a} \in \langle\{x^3\}\rangle$ and
- $6p(x)x^{2\cdot 3^a} \in \langle\{x^3\}\rangle$.

$$(x^{3^a} + p(x))^3 - x^{3^{a+1}} - p(x)^3 = 3p(x)^2x^{3^a} + 3p(x)x^{2\cdot 3^a} \in \langle\{x^3\}\rangle.$$

$$-p(x) \in \langle F\rangle \Rightarrow 6p(x)^2x^{3^a}, 6p(x)x^{2\cdot 3^a} \in \langle\{x^3\}\rangle.$$

Setting $p(x) = x^3$, $a = 1$ we get $3x^{15} + 3x^{21} \in \langle\{x^3\}\rangle$, also $6x^{15}$ and $6x^{21}$ lie in $\langle\{x^3\}\rangle$. But we cannot construct the polynomial $3x^{15}$. Therefore we get these additional conditions.

General questions

Let N be a subnearring of $(\mathbb{Z}[x], +, \circ)$.

- Is N always finitely generated?
- Are there uncountable many subnearrings of $(\mathbb{Z}[x], +, \circ)$?

Infinite independent subset of $(\mathbb{Z}[x], +, \circ)$

For $i \in \mathbb{N}$, let $p_i := x^{2^{i+1}-2}$. For each $j \in \mathbb{N}$,

$$\langle \{ p_i \mid i \in \mathbb{N} \setminus \{j\} \} \rangle$$

is an independent subset of $(\mathbb{Z}[x], +, \circ)$.

We have to show that,

$$p_j \notin \langle \{ p_i \mid i \in \mathbb{N} \setminus \{j\} \} \rangle, \ \forall j \in \mathbb{N}.$$

Such an independent subset yields:
The mapping that associates with each $M \subseteq \mathbb{N}$ the nearring generated by $\{p_i \mid i \in M\}$ is an order embedding of the power set $(\mathcal{P}(\mathbb{N}), \subseteq)$ of the natural numbers into the set of subnearrings of $(\mathbb{Z}[x], +, \circ)$, ordered by inclusion.
This means, we have:

- *Infinite ascending chains*, i.e., subsets order isomorphic to $(\mathbb{N}, \leq)$.
- *Infinite descending chains*, i.e., subsets order isomorphic to $(\{z \in \mathbb{Z} \mid z < 0\}, \leq)$.
- *Uncountable linearly ordered subsets that are order isomorphic to* $(\mathbb{R}, \leq)$.
- *Uncountable antichains*, i.e., subsets order isomorphic to $(\mathbb{R}, =)$.

Proof of the Theorem

Preliminaries from elementary number theory:

Lemma (Corollary 32.1 of [Singmaster, 1980])

Let $p \in \mathbb{P}$, let $n, s \in \mathbb{N}$, let $j \in \{1, \ldots, n\}$, and let $k, k_1, \ldots, k_n \in \mathbb{N}_0$ be such that $k = k_1 + \ldots + k_n$. If p^s divides k and $\gcd(k_j, p) = 1$, then p^s divides $\binom{k}{k_1, \ldots, k_n}$.

Proof of the Theorem

Preliminaries from elementary number theory:

Lemma (Corollary 32.1 of [Singmaster, 1980])

Let $p \in \mathbb{P}$, let $n, s \in \mathbb{N}$, let $j \in \{1, \ldots, n\}$, and let $k, k_1, \ldots, k_n \in \mathbb{N}_0$ be such that $k = k_1 + \ldots + k_n$. If p^s divides k and $\gcd(k_j, p) = 1$, then p^s divides $\binom{k}{k_1, \ldots, k_n}$.

Lemma

Let $n, m \in \mathbb{N}$, and let $l_1, \ldots l_n, k_1, \ldots, k_n, k \in \mathbb{N}_0$ be such that $k = k_1 + \ldots + k_n$, $k \equiv_2 0$, and for all $i \in \{1, \ldots, n\}$, $l_i \equiv_2 0$. We assume that $2^{m+1} - 2 = l_1 k_1 + \ldots + l_n k_n$. Then 2 divides $\binom{k}{k_1, \ldots, k_n}$.

Proof of the Lemma

Proof.

We assume, that $\binom{k}{k_1,\ldots,k_n}$ is odd.

Proof of the Lemma

Proof.

We assume, that $\binom{k}{k_1,\ldots,k_n}$ is odd.

Then we get from the previous Lemma that k is odd, or for all $j \leq n$ we have that $\gcd(k_j, 2) \neq 1$.

Proof of the Lemma

Proof.

We assume, that $\binom{k}{k_1,\ldots,k_n}$ is odd.

Then we get from the previous Lemma that k is odd, or for all $j \leq n$ we have that $\gcd(k_j, 2) \neq 1$.

Since k is even by assumption, we have that all k_j are even.
By assumption all l_i are even.

$$\Rightarrow 4 \mid l_1 k_1 + \ldots + l_n k_n.$$

Proof of the Lemma

Proof.

We assume, that $\binom{k}{k_1,\ldots,k_n}$ is odd.

Then we get from the previous Lemma that k is odd, or for all $j \leq n$ we have that $\gcd(k_j, 2) \neq 1$.

Since k is even by assumption, we have that all k_j are even.
By assumption all l_i are even.

$$\Rightarrow 4 \mid l_1 k_1 + \ldots + l_n k_n.$$

Contradiction to

$$2^{m+1} - 2 = l_1 k_1 + \ldots + l_n k_n.$$

Now we are able to prove:

Theorem

For $i \in \mathbb{N}$, let $p_i := x^{2^{i+1}-2}$, let S be the set of all subnearrings of $(\mathbb{Z}[x], +, \circ)$ and let $\Phi : P(\mathbb{N}) \to S$, where for each $A \subseteq \mathbb{N}$, $\Phi(A)$ is the subnearring of $\mathbb{Z}[x]$ that is generated by $\{p_i \mid i \in A\}$. Then we have:

- *For each $j \in \mathbb{N}$, p_j is not an element of the nearring $\Phi(\mathbb{N} \setminus \{j\})$.*
- *For all $A, B \in P(\mathbb{N})$ we have $\Phi(A) \subseteq \Phi(B)$ if and only if $A \subseteq B$. In particular, Φ is injective and hence $|S| = 2^{\aleph_0}$.*
- *$(S, \subseteq)$ contains a subset that is order isomorphic to $(P(\mathbb{N}), \subseteq)$.*

Examples of a descending and an ascending chain

Theorem

Let $(N_i)_{i\in\mathbb{N}_0}$ *where* $N_i := \langle\{x^{2^{2^i}}\}\rangle$. *Then* $(N_i)_{i\in\mathbb{N}_0}$ *is a descending chain of subnearrings of* $(\mathbb{Z}[x], +, \circ)$.

Examples of a descending and an ascending chain

Theorem

Let $(N_i)_{i\in\mathbb{N}_0}$ *where* $N_i := \langle\{x^{2^{2^i}}\}\rangle$. *Then* $(N_i)_{i\in\mathbb{N}_0}$ *is a descending chain of subnearrings of* $(\mathbb{Z}[x], +, \circ)$.

Theorem

Let $(N_i)_{i\in\mathbb{N}}$ *where* $N_i := \langle\{x^{2^{k+1}-2} \mid k \in \mathbb{N}, k \leq i\}\rangle$. *Then* $(N_i)_{i\in\mathbb{N}}$ *is an ascending chain of subnearrings of* $(\mathbb{Z}[x], +, \circ)$.

Nearring which is not finitely generated

$$\langle \{ x^{2^{k+1}-2} \mid k \in \mathbb{N} \} \rangle$$


Aichinger, E. (2013).
Generating polynomials using function composition.
Quaest. Math., 36(1):39–46.


Singmaster, D. (1980).
Divisibility of binomial and multinomial coefficients by primes and prime powers.
In *A collection of manuscripts related to the Fibonacci sequence*, pages 98–113. Fibonacci Assoc., Santa Clara, Calif.