Split absolutely irreducible integer-valued polynomials over discrete valuation domains

Sarah Nakato

(joint work with Sophie Frisch and Roswitha Rissner)

Conference on Rings and Factorizations 2023

July 13, 2023

Der Wissenschaftsfonds.

Outline

- Preliminaries on integer-valued polynomials
- Absolute irreducibility
- Split absolutely irreducible integer-valued polynomials

Int(**D**)

Definition 1

Let D be a domain with quotient field K. The ring of integer-valued polynomials on D is

$$\mathrm{Int}(D) = \{F \in K[x] \mid \forall\ a \in D, F(a) \in D\} \subseteq K[x]$$

$\Longrightarrow F = \frac{g}{b}$ is in $\mathrm{Int}(D)$ if and only if $b \mid g(a)$ for all $a \in D$.

Example

1. $D[x] \subseteq \mathrm{Int}(D)$
2. $\frac{x(x-1)}{2} \in \mathrm{Int}(\mathbb{Z})$; $\frac{x^p - x}{p} \in \mathrm{Int}(\mathbb{Z}) \Longleftarrow a^p \equiv a \pmod{p}\ \forall\ a \in \mathbb{Z}$

Non-unique factorizations in Int(D)

- Int(D) in general is not a unique factorization domain e.g., in Int($\mathbb{Z}$),

$$\begin{aligned}\frac{x(x-1)(x-3)}{2} &= \frac{x(x-1)}{2}\cdot(x-3)\\ &= \frac{x(x-3)}{2}\cdot(x-1)\end{aligned}$$

(Frisch, N., Rissner, 2019) Given any finite multi-set of integers greater than one, say $\{2,4,5,5\}$, there exists $H \in \text{Int}(D)$ such that

$$\begin{aligned}H &= h_1 \cdot h_2\\ &= f_1 \cdot f_2 \cdot f_3 \cdot f_4\\ &= g_1 \cdot g_2 \cdot g_3 \cdot g_4 \cdot g_5\\ &= \ell_1 \cdot \ell_2 \cdot \ell_3 \cdot \ell_4 \cdot \ell_5\end{aligned}$$

Absolute irreducibility

Definition 2

Let R be a commutative ring with identity.

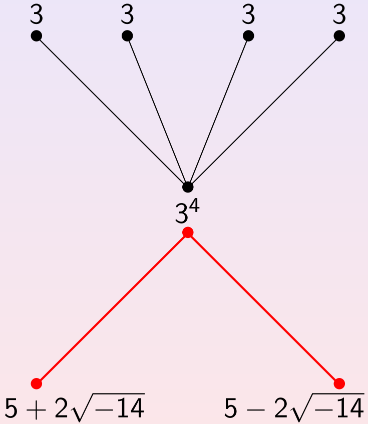
1. A non-zero non-unit $r \in R$ is said to be **irreducible** in R if whenever $r = ab$, then either a or b is a unit.

2. An irreducible element $r \in R$ is called **absolutely irreducible** if for all natural numbers n, every factorization of r^n is essentially the same as $r^n = r \cdots r$, e.g., in $\mathrm{Int}(\mathbb{Z})$, $\binom{x}{n} = \frac{x(x-1)(x-2)\cdots(x-n+1)}{n!}$ (Rissner, Windisch, 2021)

3. If r is irreducible but there exists a natural number $n > 1$ such that r^n has other factorizations essentially different from $r^n = r \cdots r$, then r is called **non-absolutely irreducible**.

Examples of non-absolutely irreducible elements

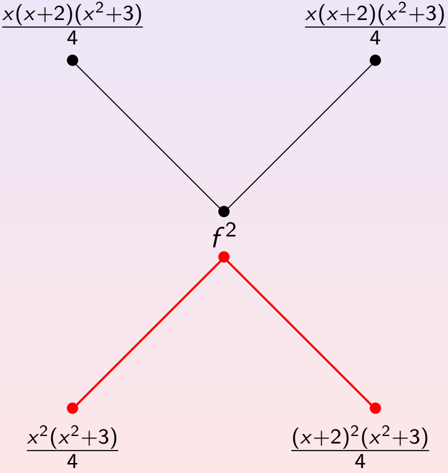
In $\mathbb{Z}[\sqrt{-14}]$



Every irreducible element of $\mathcal{O}_K$ is absolutely irreducible if and only if $\mathcal{O}_K$ is a UFD. (Chapman and Krause, 2012)

Non-absolutely irreducible elements in $\mathrm{Int}(\mathbb{Z})$

Consider $f = \frac{x(x+2)(x^2+3)}{4} \in \mathrm{Int}(\mathbb{Z})$.



- **See (N, 2020) for general constructions of non-absolutely irreducibles in $\mathrm{Int}(\mathbb{Z})$.**

Chapman-Krause Criterion

Lemma 1 (Chapman and Krause, 2012)

Let D be an integral domain and $c \in D$ an irreducible element. Then the following are equivalent:

1. c is absolutely irreducible.
2. For every irreducible b which is not associated to c there exists a prime ideal P of D such that $b \in P$ and $c \notin P$.

Split absolutely irreducibles

Goal:

Let (R, M) be a discrete valuation domain (DVR) with quotient field K and finite residue field. Let

$$f = \frac{\prod_{s \in S}(x - s)^{m_s}}{c} \in \mathrm{Int}(R) \qquad (\star)$$

where $\emptyset \neq S \subseteq R$, each m_s is a positive integer, and $c \in R \setminus \{0\}$. We characterize the absolutely irreducible elements of the form $(\star)$.

Posh set of a polynomial

Definition 1

The **posh set** of a polynomial $F \in K[x]$ is,

$$\mathcal{P}(F) = \left\{ r \in R \mid v(F(r)) > \min_{t \in R} v(F(t)) \right\}.$$

If $F \in \mathrm{Int}(R)$, then $\min_{t \in R} v(F(t)) = v(\mathrm{d}_F)$.

Recall: the **fixed divisor** of $F \in \mathrm{Int}(R)$ is the ideal

$$\mathrm{d}_F = \gcd[F(a) \mid a \in R].$$

$\Rightarrow a \in \mathcal{P}(F)$ iff $F \in M_a$ where $M_a = \{G \in \mathrm{Int}(R) : v(G(a)) > 0\}\}$.

Balanced sets

Definition 2

Let (R, M) be a DVR and $S \subseteq R$ a finite set. An **M-adic partition $\mathcal{C}$ of R** is a finite partition of R into residue classes of powers of M. That is

$$\mathcal{C} = \{s + M^{n_s} \mid s \in S\}$$

such that $R = \bigcup_{s \in S}(s + M^{n_s})$ and $(s + M^{n_s}) \cap (t + M^{n_t}) = \emptyset$ for $s \neq t$. We say that the set S is a set of representatives of $\mathcal{C}$.

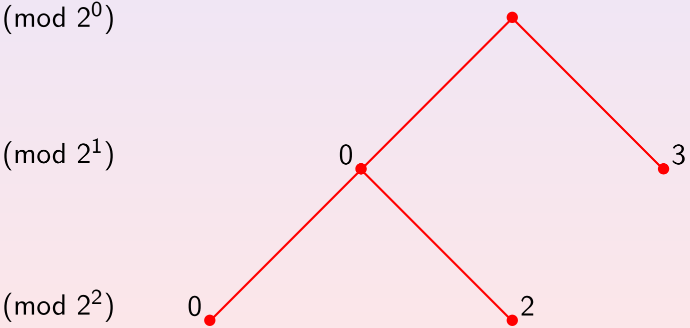
Definition 3

Let (R, M) be a DVR. We call $S \subseteq R$ **balanced** if, when we take for each $s \in S$ the minimal n_s such that $s + M^{n_s}$ contains no other element of S, the resulting M-adic neighborhoods $s + M^{n_s}$ cover R.

Balanced sets cont'd

Example 1

Let $R = \mathbb{Z}_{(2)}$. Then $S = \{0, 2, 3\}$ is a balanced set with partition $\mathcal{C} = \{0 + (4),\ 2 + (4),\ 3 + (2)\}$.



The M-adic partition associated to a finite set

Lemma 4

Let $S \subseteq R$ be a finite set. Then there exists a uniquely determined M-adic partition

$$\mathcal{C}_S = \{s + M^{n_s} \mid s \in S\}$$

of R such that every residue class $s + M^{n_s}$ that occurs as a block of $\mathcal{C}_S$ contains both a residue class of M^{n_s+1} intersecting S and a residue class of M^{n_s+1} disjoint from S.

The partition $\mathcal{C}_S$ of R is called the **partition associated to S**.

Example 2

Let $R = \mathbb{Z}_{(2)}$ and $S = \{0, 2, 3\}$. Then

$$\mathcal{C}_S = \{0 + (4),\ 2 + (4),\ 3 + (2)\}$$

- $0 + (4) = 0 + (8) \ \cup \ 4 + (8)$
- $2 + (4) = 2 + (8) \ \cup \ 6 + (8)$
- $3 + (2) = 3 + (4) \ \cup \ 1 + (4)$

Rich neighborhoods and poor neighborhoods

Definition 5

Let $S \subseteq R$ be a finite set and $\mathcal{C}_S = \{s + M^{n_s} \mid s \in S\}$ the partition associated to it;

1. An ***S-rich neighborhood*** is a residue class $s + M^{n_s+1}$ with $s \in S$.
2. An ***S-poor neighborhood*** is a residue class of the form $r + M^{n_s+1}$ disjoint from S where $r \in (s + M^{n_s})$ for some $s \in S$.
3. The **rich set of S**, denoted by $\mathcal{R}(S)$, is the union of the rich neighborhoods, that is,

$$\mathcal{R}(S) = \bigcup_{s \in S} s + M^{n_s+1}$$

4. For $F \in K[x]$ that splits over R, the **rich set of F**, denoted by $\mathcal{R}(F)$, is the rich set of the set of its roots S.

The partition matrix

Lemma 6

Let $S \subseteq R$ be a finite set and $g = \prod_{s \in S}(x-s)^{m_s}$ with $m_s \in \mathbb{N}$ for $s \in S$. Then $\mathcal{R}(g) \subseteq \mathcal{P}(g)$.

Definition 7

Let S be a set of representatives of the $M-$adic partition

$$\mathcal{C} = \{s + M^{n_s} \mid s \in S\}.$$

The **partition matrix of $\mathcal{C}$** is
$A_{\mathcal{C}} = (a_{s,t})_{s,t \in S}$ where

$$a_{s,t} = \begin{cases} n_s & s = t \\ v(s-t) & s \neq t \end{cases}.$$

The equalizing polynomial of a balanced set

Definition 8

Let $S \subseteq R$ be a balanced set and A the partition matrix of the partition associated to S. We define the **equalizing polynomial of S** as

$$g = \prod_{s \in S} (x - s)^{m_s},$$

where $(m_s)_{s \in S}$ is the uniquely determined solution to $A\bar{x} = \bar{e}$ with $\bar{x} = (x_s \mid s \in S)^\intercal$ and $\bar{e} = (e, e, \ldots, e)^\intercal$.

Lemma 9

Let $S \subseteq R$ be a balanced set and g the equalizing polynomial of S. Then $\mathcal{R}(g) = \mathcal{P}(g)$.

The equalizing polynomial of a balanced set

Example 3

For $R = \mathbb{Z}_{(2)}$, $S = \{0, 2, 3\}$ and $\mathcal{C} = \{0 + (4),\ 2 + (4),\ 3 + (2)\}$.

$$\begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} e \\ e \\ e \end{pmatrix}$$

Gives $x_0 = x_2 = 1$ and $x_3 = 3$, thus the equalizing polynomial of S is

$$g = x(x-2)(x-3)^3.$$

The resulting polynomial $\frac{g}{2^e} = \frac{x(x-2)(x-3)^3}{2^3}$ is absolutely irreducible in $\mathrm{Int}(\mathbb{Z}_{(2)})$.

Main results

Theorem 2

Let $S \subseteq R$ be a balanced set, g the equalizing polynomial of S, and $c = \mathrm{d}(g)$. Then $F = \frac{g}{c}$ is absolutely irreducible in $\mathrm{Int}(R)$.

Theorem 3

Let $S \subseteq R$ be a finite set and for each $s \in S$, $m_s \in \mathbb{N}$. Let

$$g = \prod_{s \in S} (x - s)^{m_s} \quad \text{and} \quad F = \frac{g}{c}$$

Then F is absolutely irreducible in $\mathrm{Int}(R)$ if and only if

1. S is balanced.
2. g is the equalizing polynomial of S.
3. c is a generator of the fixed divisor of g.

The bijection

Corollary 1

Let R be a DVR. The absolutely irreducible polynomials of $\mathrm{Int}(R)$ of the form

$$F = \frac{\prod_{s \in S}(x-s)^{m_s}}{c}$$

correspond bijectively to balanced sets $S \subseteq R$, that is,

- given an absolutely irreducible polynomial $F = \frac{\prod_{s \in S}(x-s)^{m_s}}{c}$, map F to its set of roots S.
- Conversely, given a balanced finite set $S \subseteq R$, let g be its equalizing polynomial and $c \in R$ a generator of the fixed divisor of g, and map S to $F = \frac{g}{c}$.

References

1. Paul-Jean Cahen and Jean-Luc Chabert. **Integer-valued polynomials**. Vol. 48. Mathematical Surveys and Monographs. American Mathematical Society, Providence, RI,1997.

2. Alfred Geroldinger and Franz Halter-Koch. **Non-unique factorizations.** Vol. 278. Pure and Applied Mathematics (Boca Raton). Algebraic, combinatorial and analytic theory. Chapman & Hall/CRC, Boca Raton, FL, 2006.

3. Sophie Frisch. **A construction of integer-valued polynomials with prescribed sets of lengths of factorizations.** Monatsh. Math. 171.3-4 (2013).

4. Sophie Frisch, Sarah Nakato, and Roswitha Rissner. **Sets of lengths of factorizations of integer-valued polynomials on Dedekind domains with finite residue fields**. *J. Algebra* 528 (2019).

References

5. Scott T. Chapman and Ulrich Krause. **A closer look at non-unique factorization via atomic decay and strong atoms**. *Progress in commutative algebra 2*. Walter de Gruyter, Berlin, 2012.

6. Sarah Nakato. **Non-absolutely irreducible elements in the ring of integer-valued polynomials.** Communications in Algebra 48.4 (2020).

7. **Sophie Frisch, Sarah Nakato, and Roswitha Rissner. Split absolutely irreducible integer-valued polynomials over discrete valuation domains. *J. Algebra* 602 (2022).**

8. Roswitha Rissner and Daniel Windisch. **Absolute irreducibility of the binomial polynomials.** *Journal of Algebra* 578 (2021).