τ-factorization and τ-elasticity

Richard Hasenauer Bethany Kubik

[1]Northeastern State University
[2]University of Minnesota Duluth

22 March 2019

Definition

Let R be a PID (commutative with identity) and I be an ideal of R.

For any nonzero non-unit $a \in R$, we say

$$a = \lambda b_1 \cdots b_n$$

is a τ_I*-factorization of* a if λ is a unit, $b_1, \ldots, b_n$ are nonzero non-units, and $b_1 \equiv \cdots \equiv b_n \pmod{I}$.

Example

Let $R = \mathbb{Z}$ and $I = (2)$.
Then

$$20 = 2 \cdot 10$$

is a τ_I-factorization since $2 \equiv 10 \pmod 2$.

Example

Let $R = \mathbb{Z}$ and $I = (2)$.
Then

$$20 = 2 \cdot 10$$

is a τ_I-factorization since $2 \equiv 10 \pmod 2$.
However,

$$20 = 4 \cdot 5$$

is **not** a τ_I-factorization since $4 \not\equiv 5 \pmod 2$.

Example

Let $R = \mathbb{Z}$ and $I = (7)$.
Then

$$\begin{aligned} 30 &= 2 \cdot 3 \cdot 5 \\ &= 6 \cdot 5 \\ &= 2 \cdot 15 \\ &= 3 \cdot 10. \end{aligned}$$

The only valid τ_I-factorization of the above list is $3 \cdot 10$ since $3 \equiv 10 \pmod 7$.

Definition

We say $a \in R$ is a τ_l-*atom* if, for any τ_l-factorization $a = bc$, either b or c is a unit.

Definition

We say $a \in R$ is a τ_l-*atom* if, for any τ_l-factorization $a = bc$, either b or c is a unit.

Definition

We say R is τ_l-*atomic* if every nonzero non-unit element has a τ_l-factorization into a finite product of τ_l-atoms.

Definition

We say $a \in R$ is a τ_I-*atom* if, for any τ_I-factorization $a = bc$, either b or c is a unit.

Definition

We say R is τ_I-*atomic* if every nonzero non-unit element has a τ_I-factorization into a finite product of τ_I-atoms.

Example

Let $R = \mathbb{Z}$ and $I = (1) = \mathbb{Z}$. Then R is τ_I-atomic.

Example

Let $R = \mathbb{Z}$ and $I = (7)$.
Then

$$44 = 4 \cdot 11$$

is a τ_I-factorization since $4 \equiv 11 \pmod 7$.

Example

Let $R = \mathbb{Z}$ and $I = (7)$.
Then

$$44 = 4 \cdot 11$$

is a τ_I-factorization since $4 \equiv 11 \pmod 7$.
Also,

$$4 = 2 \cdot 2$$

is a τ_I-factorization.

Example

Let $R = \mathbb{Z}$ and $I = (7)$.
Then

$$44 = 4 \cdot 11$$

is a τ_I-factorization since $4 \equiv 11 \pmod 7$.
Also,

$$4 = 2 \cdot 2$$

is a τ_I-factorization.
However,

$$44 = 2 \cdot 2 \cdot 11$$

is not a τ_I-factorization.

Example

Let $R = \mathbb{Z}$ and $I = (7)$.
Then

$$44 = 4 \cdot 11$$

is a τ_I-factorization since $4 \equiv 11 \pmod 7$.
Also,

$$4 = 2 \cdot 2$$

is a τ_I-factorization.
However,

$$44 = 2 \cdot 2 \cdot 11$$

is not a τ_I-factorization.

Since 44 does not factor into a product of τ_I-atoms, it follows that R is not τ_I-atomic.

Question: What effect (if any) does the size of R/I have on τ_I-factorization?

Question: What effect (if any) does the size of R/I have on τ_I-factorization?

Fact

If $|R/I| = 2$ *or* 3*, then* R *is always* τ_I*-atomic.*

Question: What effect (if any) does the size of R/I have on τ_I-factorization?

Fact

If $|R/I| = 2$ *or* 3*, then* R *is always* τ_I*-atomic.*

The first interesting cases occur when $|R/I| = 4$.

Question: What effect (if any) does the size of R/I have on τ_I-factorization?

Fact

If $|R/I| = 2$ *or* 3*, then* R *is always* τ_I*-atomic.*

The first interesting cases occur when $|R/I| = 4$.

Commutative rings with identity and four elements:

$$\mathbb{Z}_4, \quad \mathbb{F}_4, \quad \mathbb{Z}_2[x]/(x^2 + x), \quad \mathbb{Z}_2[x]/(x^2 + 1).$$

We assume R is a PID throughout.

We assume R is a PID throughout.

Fact

R/I is a domain if and only if I is prime.

We assume R is a PID throughout.

Fact

R/I is a domain if and only if I is prime.
In other words, R/I is not a domain if and only if I is not prime.

We assume R is a PID throughout.

Fact

R/I is a domain if and only if I is prime.
In other words, R/I is not a domain if and only if I is not prime.

Remark

When R/I is not a domain, I is not prime. Since R is a PID, we have $I = (a)$ for some non prime $a \in R$.
Thus there is no prime p with $p \equiv 0 \pmod{I}$.

Lemma

Let R be a PID and I an ideal of R. If $R/I \cong \mathbb{Z}_4$, then R is τ_I-atomic.

Lemma

Let R be a PID and I an ideal of R. If $R/I \cong \mathbb{Z}_4$, then R is τ_I-atomic.

Since $R/I \cong \mathbb{Z}_4$, primes must be equivalent to $1, 2$, or $3 \pmod{I}$.

Lemma

Let R be a PID and I an ideal of R. If $R/I \cong \mathbb{Z}_4$, then R is τ_I-atomic.

Since $R/I \cong \mathbb{Z}_4$, primes must be equivalent to $1, 2$, or $3 \pmod{I}$.

Let $a \in R$. Factor a into a unique product of primes

$$a = p_1 \cdots p_k q_1 \cdots q_l r_1 \cdots r_s$$

where $p_i \equiv 1 \pmod{I}$, $q_i \equiv 2 \pmod{I}$, and $r_i \equiv 3 \pmod{I}$.

Case 1: When $a \equiv 0$ or $2 \pmod{l}$, write

$$a = q_1 \cdots q_{l-1}(q_l p_1 \cdots p_k r_1 \cdots r_s)$$

for the τ_l-atomic factorization of a.

Case 1: When $a \equiv 0$ or $2 \pmod{l}$, write

$$a = q_1 \cdots q_{l-1}(q_l p_1 \cdots p_k r_1 \cdots r_s)$$

for the τ_l-atomic factorization of a.

Case 2: When $a \equiv 1$ or $3 \pmod{l}$, write

$$a = p_1 \cdots p_k r_1 \cdots r_s = (-1)^s p_1 \cdots p_k (-r_1) \cdots (-r_s)$$

for the τ_l-atomic factorization of a.

Lemma

Let R be a PID and I an ideal of R. If $R/I \cong \mathbb{Z}_2[x]/(x^2 + x)$, then R is τ_I-atomic.

Lemma

Let R be a PID and I an ideal of R. If $R/I \cong \mathbb{Z}_2[x]/(x^2 + 1)$, then R is τ_I-atomic.

Remark

$\mathbb{F}_4$ is the least well behaved with respect to τ_l-atomicity.

Remark

$\mathbb{F}_4$ is the least well behaved with respect to τ_l-atomicity.

We have τ_l-atomicity, but not under all conditions.

Remark

$\mathbb{F}_4$ is the least well behaved with respect to τ_I-atomicity.

We have τ_I-atomicity, but not under all conditions.

Theorem

Let R be a PID and I be an ideal such that R/I has a unit in every class. Then R is τ_I-atomic.

Since R is a PID, there is some prime $p \in R$ such that $I = (p)$.

Since R is a PID, there is some prime $p \in R$ such that $I = (p)$.

Case 1: Assume $a \equiv 0 \pmod{I}$.

Then $a = p^k m$ for some $k \in \mathbb{N}$ and some $m \notin I$ and

$$a = p \cdots p(pm)$$

is a τ_I-atomic factorization.

Since R is a PID, there is some prime $p \in R$ such that $I = (p)$.

Case 1: Assume $a \equiv 0 \pmod{I}$.

Then $a = p^k m$ for some $k \in \mathbb{N}$ and some $m \notin I$ and

$$a = p \cdots p(pm)$$

is a τ_I-atomic factorization.

Case 2: Assume $a \not\equiv 0 \pmod{I}$.

Assume $a = p_1 p_2$ is a product of primes where $p_i \not\equiv 0 \pmod{l}$.

Assume $a = p_1 p_2$ is a product of primes where $p_i \not\equiv 0 \pmod{I}$.

Since there is a unit in every class, there is some λ with

$$\lambda \equiv p_1 p_2^{-1} \pmod{I}.$$

Assume $a = p_1 p_2$ is a product of primes where $p_i \not\equiv 0 \pmod{I}$.

Since there is a unit in every class, there is some λ with

$$\lambda \equiv p_1 p_2^{-1} \pmod{I}.$$

Then

$$a = p_1 p_2 = \lambda^{-1} p_1 (\lambda p_2)$$

is a τ_I-atomic factorization of a where

$$\lambda p_2 \equiv p_1 p_2^{-1} p_2 \equiv p_1 \pmod{I}.$$

We write $a = p_1 \cdots p_k$ where each p_i is a prime and us the same method to obtain

$$a = (\lambda_2^{-1} \cdots \lambda_k^{-1}) p_1 (\lambda_2 p_2) \cdots (\lambda_k p_k).$$

We write $a = p_1 \cdots p_k$ where each p_i is a prime and us the same method to obtain

$$a = (\lambda_2^{-1} \cdots \lambda_k^{-1}) p_1 (\lambda_2 p_2) \cdots (\lambda_k p_k).$$

Thus a has a τ_l-atomic factorization and R is τ_l-atomic.

Example

Let $R = \mathbb{Z}[\alpha]$ where $\alpha = \frac{1+\sqrt{5}}{2}$ and let $I = 2\mathbb{Z}[\alpha]$.
Then

$$R/I = \mathbb{Z}[\alpha]/2\mathbb{Z}[\alpha] = \{\overline{a} + \overline{b}\alpha : \overline{a}, \overline{b} \in \mathbb{Z}_2\} \cong \mathbb{F}_4.$$

Example

Let $R = \mathbb{Z}[\alpha]$ where $\alpha = \frac{1+\sqrt{5}}{2}$ and let $I = 2\mathbb{Z}[\alpha]$.
Then

$$R/I = \mathbb{Z}[\alpha]/2\mathbb{Z}[\alpha] = \{\overline{a} + \overline{b}\alpha : \overline{a}, \overline{b} \in \mathbb{Z}_2\} \cong \mathbb{F}_4.$$

Then -1, α and α^{-1} are all units in R with each one in a different nonzero class.

Lemma

Let R be a PID and I an ideal of R such that R/I has a prime in every class. If $R/I \cong \mathbb{F}_4$ and R does not have a unit in every nonzero class of R/I, then R is not τ_I-atomic.

Lemma

Let R be a PID and I an ideal of R such that R/I has a prime in every class. If $R/I \cong \mathbb{F}_4$ and R does not have a unit in every nonzero class of R/I, then R is not τ_I-atomic.

Label the four elements of $\mathbb{F}_4$ as $0, 1, a, b$ and create the Cayley table.

	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a

	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a

Since there exists at least one prime in every class, there exists primes p and q with $p \equiv a \pmod{l}$ and $q \equiv b \pmod{l}$.
Then

$$p^2q = (p^2)(q)$$

has only one τ_l-factorization, but p^2 is not a τ_l-atom since $p^2 = (p)(p)$.

	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a

Since there exists at least one prime in every class, there exists primes p and q with $p \equiv a \pmod{I}$ and $q \equiv b \pmod{I}$.
Then

$$p^2 q = (p^2)(q)$$

has only one τ_I-factorization, but p^2 is not a τ_I-atom since $p^2 = (p)(p)$.
Hence R is not τ_I-atomic.

The assumption that there is a prime in every class is necessary.

Example

Let $R = \mathbb{F}_4[[x]]$ and $I = (x)$. Then $R/I \cong \mathbb{F}_4$. Recall that any power series with a nonzero constant term is a unit.

The assumption that there is a prime in every class is necessary.

Example

Let $R = \mathbb{F}_4[[x]]$ and $I = (x)$. Then $R/I \cong \mathbb{F}_4$. Recall that any power series with a nonzero constant term is a unit.

Let $f \in R$. Then $f = x^n g$ where g has a nonzero constant term.

The assumption that there is a prime in every class is necessary.

Example

Let $R = \mathbb{F}_4[[x]]$ and $I = (x)$. Then $R/I \cong \mathbb{F}_4$. Recall that any power series with a nonzero constant term is a unit.

Let $f \in R$. Then $f = x^n g$ where g has a nonzero constant term.

This is always a τ_I-atomic factorization and hence R is τ_I-atomic.

Theorem

Let R be a PID with a prime in every class and I an ideal of R such that $|R/I| = 4$. Then R is τ_I-atomic if and only if $R/I \ncong \mathbb{F}_4$ and R does not contain a unit in every nonzero class.

Question: Let $R = \mathbb{Z}$ and $I = (n)$ for some $n \in \mathbb{Z}$. Can we determine the τ_I-elasticity of R for a given n?

Question: Let $R = \mathbb{Z}$ and $I = (n)$ for some $n \in \mathbb{Z}$. Can we determine the τ_I-elasticity of R for a given n?

Definition

Let $a \in R$. The τ_I-elasticity of a, denoted $\rho_\tau(a)$, is the ratio of the longest τ_I-atomic factorization over the shortest τ_I-atomic factorization. The τ_I-elasticity of R is $\rho_\tau(R) = sup\{\rho_\tau(a) | a \in R\}$.

Recall that if α and $2\alpha + 1$ are both primes, we say α is a *Germain* prime and $2\alpha + 1$ is a *safe* prime.

Recall that if α and $2\alpha + 1$ are both primes, we say α is a *Germain* prime and $2\alpha + 1$ is a *safe* prime.

Lemma

Let $n = 2\alpha + 1$ be a safe prime. Let p, q and r be primes such that $p^k(qr)$ is a τ_n-factorization. If $p \equiv \pm 1 \pmod{n}$, then there exists no other τ_n-factorization of $p^k(qr)$.

Recall that if α and $2\alpha + 1$ are both primes, we say α is a *Germain* prime and $2\alpha + 1$ is a *safe* prime.

Lemma

Let $n = 2\alpha + 1$ be a safe prime. Let p, q and r be primes such that $p^k(qr)$ is a τ_n-factorization. If $p \equiv \pm 1 \pmod{n}$, then there exists no other τ_n-factorization of $p^k(qr)$.

If there existed a second τ_n-factorization it would be of the form

$$(p^s q)(p^{k-s} r).$$

Recall that if α and $2\alpha + 1$ are both primes, we say α is a *Germain* prime and $2\alpha + 1$ is a *safe* prime.

Lemma

Let $n = 2\alpha + 1$ be a safe prime. Let p, q and r be primes such that $p^k(qr)$ is a τ_n-factorization. If $p \equiv \pm 1 \pmod{n}$, then there exists no other τ_n-factorization of $p^k(qr)$.

If there existed a second τ_n-factorization it would be of the form

$$(p^s q)(p^{k-s} r).$$

Since $p \equiv \pm 1 \pmod{n}$, this would imply $q \equiv \pm r \pmod{n}$. But (qr) cannot be factored since $p^k(qr)$ is a τ_n-factorization.

Theorem

Let $n = 2\alpha + 1$ be a safe prime. Let p be a prime and r be an integer such that r is not equal to ± 1. Then $p^k r$ is not a τ_n-atom for $k \geqslant \alpha$.

Theorem

Let $n = 2\alpha + 1$ be a safe prime. Then for any integer m we have

$$\rho_\tau(m) \leqslant \alpha - 1.$$

Thank you!