On Monoids and Domains From Gauss's Lemma

Victor Gonzalez and Ishan Panpaliya

Summer Workshop for the Intrepid Mathematician (SWIM 2024)

Aug 19, 2024

Table of Contents

Our Notation

Notation Adopted Here:

- $\mathbb{P}$ - The set of prime numbers.
- $\mathbb{F}_q$ - The field on q elements.
- $[[1, n]]$ - The discrete interval between 1 and n.

Monoids and Groups (Recap)

Definition: A monoid $M = (M, \cdot)$ is a set M equipped with an associative binary operation $(\cdot)$ which contains an identity element.

Definitions: A Puiseux monoid is a monoid that is a subset of $\mathbb{Q}_{\geq 0}$. A numerical monoid is a monoid M such that $M \subseteq \mathbb{N}_0$ and $|\mathbb{N}_0 \backslash M| < \infty$.

Remark: We denote the set of units of a monoid M as $M^\times$.

Definition: A group is a monoid in which every element is a unit.

We will adopt as convention the following 2 properties:

- Commutativity: For any $a, b \in M$, $a \cdot b = b \cdot a$.
- Cancellativity: For any $a, b, c \in M$, the fact that $a \cdot b = a \cdot c$ implies that $b = c$.

Definition: A monoid M is torsion-free if for any elements $a, b \in M \backslash M^\times$, the equality $a^n = b^n$ implies that $a = b$.

Atoms and Primes

Definition: Let M be a monoid. An element $a \in M \backslash M^{\times}$ is an atom if when $a = b \cdot c$, where $b, c \in M$, then either $b \in M^{\times}$ or $c \in M^{\times}$. The set of atoms of M is denoted by $\mathcal{A}(M)$.

Definition: Let M be a monoid. An element $p \in M \backslash M^{\times}$ is a prime if when $p \mid_M bc$, for some $b, c \in M$, then either $p \mid_M b$ or $p \mid_M c$.

Definition: A monoid with no atoms is antimatter.

Remark:

- In a monoid M, every prime element is an atom.

The converse is not true in general as the following example shows:

- Set $M := (\mathbb{N}_0 \setminus \{1\}, +)$.
- In the monoid M, $3 \in \mathcal{A}(M)$ and $3 \mid_M 2 + 4$. However, $3 \nmid_M 2$ and $3 \nmid_M 4$.

Integral Domains and Fields (Recap)

Definition: An integral domain $D = (D, +, \cdot)$ is a set equipped with 2 binary operations $(+)$ and $(\cdot)$ that has the following properties:

- $(D, +)$ is a group, with identity denoted by 0.
- $(D \backslash \{0\}, \cdot)$ is a monoid with identity denoted by 1. This is the multiplicative monoid of D.
- For any $a, b, c \in D$, $a \cdot (b + c) = a \cdot b + a \cdot c$.
- For any $a, b \in D$, if $a, b \neq 0$, then $a \cdot b \neq 0$.

Definition: Let R be an integral domain. The polynomial extension of R, denoted by $R[X]$, is the integral domain consisting of all polynomials with coefficients in R.

Examples: $\mathbb{Z}, \mathbb{Z}[X]$.

Definition: An integral domain D is a field if $(D, \cdot)$ is a group.

Examples: $\mathbb{Q}, \mathbb{R}$.

Monoid Algebras Pt.1

Definition:
Let R be an integral domain, and let M be a torsion-free monoid with strict total order $(<)$.

$$R[x;M] := \left\{ \sum_{i=1}^{n} r_i x^{b_i} : r_1, \ldots, r_n \in R\backslash\{0\} \text{ and } b_1, \ldots, b_n \in M \right\}$$

Where $\mathrm{b}_1 < b_2 < \cdots < b_n$.

We call $R[x;M]$ the monoid algebra of M over R and we write $R[M]$ for the sake of simplicity from now on. It is well known that if M is a (cancellative) torsion-free monoid, then $R[M]$ is an integral domain.

Examples:

- The monoid algebra $R[\mathbb{N}_0]$ is just the polynomial extension of R.
- $R[\mathbb{Z}]$ is the set of Laurent polynomials with coefficients in R.

Monoid Algebras Pt.2

Definitions:

Let R be a integral domain and M a torsion-free monoid with strict total order $(<)$. Let

$$f = \sum_{i=1}^{n} r_i x^{m_i} \in R[M].$$

- We define the support of f as $\text{supp}(f) := \{m_i : i \in [[1, n]]\}$.
- We define the degree of f as $\deg(f) := \max(\text{supp}(f))$.
- We define the order of f as $\text{ord}(f) := \min(\text{supp}(f))$.

Unique Factorization Monoids/Domains

Definition: A unique factorization monoid (UFM) is a monoid in which every element can be expressed uniquely as a product of atoms (up to order and associates). A unique factorization domain (UFD) is an integral domain whose multiplicative monoid is a UFM.

Examples: $(\mathbb{N}_0, +)$, $(\mathbb{Z}, \cdot)$.

Non-Example:

1. Let $P = (p_n)_{n \geq 1}$ be the set of odd primes.
2. Define the Grams' monoid $G := \left\langle \frac{1}{2^{n-1} \cdot p_n} \middle| n \geq 1 \right\rangle$. One can prove that the defining generators are precisely the atoms.
3. Since $1 = 3(\frac{1}{3}) = 10(\frac{1}{10})$, G is not a UFM.

GCD Domains

Definition: Given a monoid M and a finite subset $S \subseteq M$, an element $d \in M$ is a greatest common divisor (gcd) of S if d divides every element of S and for every common divisor d' of S, $d'|_M\, d$.

Definition: An integral domain D is a GCD domain if any finite subset of $D \backslash \{0\}$ has a greatest common divisor.

Remark: If the only common divisors of a set S are units, then we write $\gcd(S) = 1$.

Examples:

- $\mathbb{Z}, \mathbb{Q}[\mathbb{Q}_{\geq 0}]$.

Non-Example:

- Let $R := \mathbb{Z}[\sqrt{-5}]$ defined as $R = \left\{a + b\sqrt{-5} : a, b \in \mathbb{Z}\right\}$.
- One can check that R is an integral domain.
- $\{2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}\} \subset \mathcal{A}(R)$.
- Observe that $6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \cdot 3$.

AP Domains

Definition: An AP domain is an integral domain in which every atom is a prime.

Examples:

- $\mathbb{R}[X]$.
- $\mathbb{Q}$ (antimatter).

UFD $\subsetneq$ GCD domain $\subsetneq$ AP domain.

First Motivating Question: IDF Ascent

Question

Given that D is an IDF domain, is $D[X]$ also IDF? If not, can we classify for which classes of integral domains the IDF property ascends?

Introducing the IDF Property

Definition: A monoid M satisfies the Irreducible Divisor Finite (IDF) property if each element of M is divisible by finitely many atoms (up to associates). An integral domain is IDF if its multiplicative monoid is IDF.

Examples:

- $(\mathbb{N}, \cdot)$: Each number is divisible by finitely many primes (i.e. the primes in its factorization).
- In general, all UFDs are IDF.

Non-Example:

- Set $Q := (\{0\} \cup \mathbb{Q}_{\geq 1}, +)$.
- $\mathcal{A}(Q) = [1, 2) \cap \mathbb{Q}$. Any atom divides 3, so Q is not IDF.

Ascent of IDF Property (AP)

Lemma (Malcolmson and Okoh, 2009)

Every (countable) domain can be embedded in an antimatter domain R_∞ such that the polynomial extension $R_\infty[T]$ is not IDF.

Observations:

- An antimatter domain is (vacuously) AP.
- An antimatter domain has 0 atoms and hence is an IDF domain.

Putting these observations together, along with Malcolmson and Okoh's embedding lemma, one arrives at the following theorem:

Theorem (Malcolmson and Okoh, 2009)

There exists an IDF AP domain D such that $D[X]$ is not IDF.

Con: Complicated construction.

Ascent of IDF Property (PSP/GCD)

Theorem (Malcolmson and Okoh, 2009)

The IDF property ascends in the class of GCD domains.

Theorem (Gotti and Zafrullah, 2022)

The IDF property ascends in the class of PSP domains.

Remark: The class of PSP domains is a strict subset of the domains in which every atom is a prime.

UFDs $\subsetneq$ GCD domains $\subsetneq$ PSP domains $\subsetneq$ AP domains.

Today's Main Course: GL-Domains

Definition: A polynomial is primitive if the gcd of its coefficients is 1.

Examples: In $\mathbb{Z}[X]$, $2x^2 + 3x + 5$ and $x + 4$ are primitive.

Non-example: In $\mathbb{Z}[X]$, $2x^2 + 12x + 14$ is not primitive as $2|_{\mathbb{Z}}\ 2, 12, 14$.

Gauss's Lemma

In $\mathbb{Z}[X]$, the product of 2 primitive polynomials is again primitive.

Definition: An integral domain that satisfies the statement of Gauss's Lemma is a GL-domain.

UFDs $\subsetneq$ GCD domains $\subsetneq$ PSP domains $\subsetneq$ GL-domains $\subsetneq$ AP domains.

Question

Does the IDF property ascend in the class of GL-domains?

Ascent of IDF Property Classification Diagram

Current Picture:

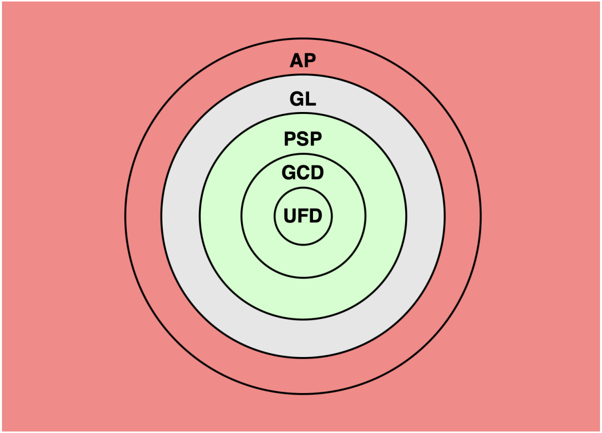

Figure: Current Classification of IDF Ascent.

CrowdMath 2024 1st Main Result

In CrowdMath 2024, we proved the following theorem:

Theorem (CrowdMath, 2024)

The IDF property does not ascend in the class of GL-domains.

Remarks:

- Construction of counterexample using monoid algebras.
- Proved by reframing Gauss's Lemma in terms of ideal theory.

In CrowdMath 2024, we also improved upon past results for AP domains:

Construction (CrowdMath, 2024)

A relatively simple monoid domain which is IDF but whose polynomial extension is not IDF.

The GL-Property in The Setting of Integral Domains

Anderson and Quintero provided the following characterization of GL-domain:

Proposition (Anderson and Quintero, 1997)

For an integral domain R the following are equivalent.

1. R is a GL-domain.
2. Whenever $a, b, c \in R$ such that $\gcd(a, b) = \gcd(a, c) = 1$, then $\gcd(a, bc) = 1$.

Examples:

- $\mathbb{Q}[x]$ and $\mathbb{R}[x]$.
- In general, every UFD is a GL-domain.
- For every field F, the monoid algebra $F[\mathbb{Q}_{\geq 0}]$ is a GL-domain that is not a UFD.

The GL-Property in the Setting of Monoids

Definition: Let M be a monoid. We say that M is a GL-monoid if whenever $a, b, c \in M$ such that $\gcd(a, b) = \gcd(a, c) = 1$, then $\gcd(a, bc) = 1$.

Examples:

- The only numerical monoid having the GL-property is $\mathbb{N}_0$.
- The Puiseux monoid

$$M := \left\langle \frac{1}{2^n} : n \in \mathbb{N}_0 \right\rangle$$

  is a GL-monoid.

The Prime-Like Property

In CrowdMath 2024, we generalized the notion of a primal element (introduced by Cohn in 1968) as follows:

Definition: Let M be a monoid. An element $d \in M \setminus M^{\times}$ is prime-like if whenever $d \mid_M bc$, for some $b, c \in M$, then there exists a non-unit divisor $d' \in M$ of d that divides either b or c.

Examples:

- Every non-unit element in $(\mathbb{N}, \cdot)$ is prime-like.
- In general, every non-unit element of a UFM is prime-like.
- Every non-zero element in $M := \left\langle \frac{1}{3^n} \mid n \in \mathbb{N}_0 \right\rangle$ is prime-like.

GL-Property = Prime-Like

Proposition (CrowdMath, 2024)

Let M be a monoid. The following conditions are equivalent:

1. M is a GL-monoid.
2. Every nonunit element of M is prime-like.

The D-Property in the Setting of Monoids

Definition: Let M be a monoid:

- We say that M satisfies the D-property if whenever a, b and c are elements of M such that $\gcd(a, b) = 1$ and $a \mid_M bc$, then $a \mid_M c$.
- An integral domain satisfies the D-property if its multiplicative monoid satisfies the D-property.

Examples:

- $(\mathbb{N}, \cdot)$ has the D-property.
- In general, every GCD monoid has the D-property.

Non-example:

- Let $R := \mathbb{Z}[\sqrt{-5}]$. Note that R does not have the D-property. Indeed, note that $2 \mid_R (1 - \sqrt{-5})(1 + \sqrt{-5}), \gcd(2, 1 - \sqrt{-5}) = 1$, and $2 \nmid_R 1 + \sqrt{-5}$.

The GL-property and the D-property

Proposition (CrowdMath, 2024; Anderson and Quintero, 1997)

1. Every monoid that satisfies the D-property is a GL-monoid.
2. Every GL-monoid satisfies the AP-property.

UFD $\subsetneq$ GCD $\subsetneq$ PSP $\subseteq$ D $\subsetneq$ GL $\subsetneq$ AP.

1. - Let $a, b, c \in M$ with $\gcd(a, b) = \gcd(a, c) = 1$.
   - If $d \in CD(a, bc)$, then $\gcd(d, b) = 1$.
   - M satisfies the D-property and so $d \in CD(a, c)$, which implies that d is a unit.
2. - Let $a \in \mathcal{A}(M)$, where M is a GL-monoid.
   - Then a is a prime-like element and every non-unit divisor of a is associate with a.
   - Therefore a is prime.

The GL-Property and the Pre-Schreier Property

Definition: Let M be a monoid. For $a \in M$, we say that

- a is primal if whenever $a \mid_M bc$ for some $b, c \in M$, we can write $a = b'c'$ for some $b', c' \in M$ such that $b' \mid_M b$ and $c' \mid_M c$.
- M is pre-Schreier if every (nonunit) of M is primal.
- An integral domain is pre-Schreier if its multiplicative monoid is pre-Schreier.

  UFD $\subsetneq$ GCD $\subsetneq$ pre-Schreier $\subsetneq$ PSP $\subseteq$ D $\subsetneq$ GL $\subsetneq$ AP.

Examples:

- $(\mathbb{N}, \cdot)$ is pre-Schreier.

  Note that $6 \mid_{\mathbb{N}} 150 = 10 \cdot 15$. Also, $6 = 2 \cdot 3$, where $2 \mid_{\mathbb{N}} 10$ and $3 \mid_{\mathbb{N}} 15$.
- Generally, every GCD domain is pre-Schreier.

It follows directly from the definition that every pre-Schreier monoid is a GL-monoid.

Rank 1 GL-Monoid That is not Pre-Schreier

Example: The Puiseux monoid $M := \mathbb{Z}\left[\frac{1}{2}\right]_{\geq 0} \cup \mathbb{Z}\left[\frac{1}{2}, \frac{1}{3}\right]_{\geq 1}$ is a GL-monoid but not a pre-Schreier monoid.

1. Let p be a prime and n a rational. We denote by $v_p(n)$ the p-adic valuation of n.
2. For each $q \in M \setminus \{0\}$, there exists a large enough $n \in \mathbb{N}_0$ such that $\frac{1}{2^n} \mid_M q$.
3. Take $q \mid_M b + c$ and n large enough such that $\frac{1}{2^n} \in CD(q, b, c)$.
4. We have that $1 \mid_M \frac{4}{3} + \frac{4}{3}$.
5. Take $b, c \in M$ such that $1 = b + c$ and $b, c \mid_M \frac{4}{3}$.
6. Note that the 3-adic valuations $v_3(b)$ and $v_3(c)$ are nonnegative.
7. Since $b \mid_M \frac{4}{3}$, $b < \frac{1}{3}$ as otherwise $v_3(\frac{4}{3} - b) \geq 0$ would implies that $v_3(b) < 0$. The same applies to c.

GL-Domain That is not Pre-Schreier

Example: The domain $R := \mathbb{Z} + x\mathbb{R}[x]$ is a GL-domain that is not a pre-Schreier domain.

1. Fix $d(x) \in R\backslash\{0\}$, and suppose that $d(x) \mid_R b(x)c(x)$ for some $b(x), c(x) \in R$.
2. If ord $d(x) \geq 1$, then 2 is a non-unit divisor of $d(x)$ that divides either $b(x)$ or $c(x)$.
3. If ord $d(x) = 0$ and $d(0) \notin \{\pm 1\}$, for some $p \in \mathbb{P}$, we know that $p \mid_R d(x)$ and then, either $p \mid_R b(x)$ or $p \mid_R c(x)$.

GL-Domain That is not Pre-Schreier

1. If ord $d(x) = 0$ and $d(0) \in \{\pm 1\}$, we can consider that $b(0) = 1$ and $c(0) = 1$.
2. We can conclude that there exists some $a(x) \in \mathcal{A}(R)$, $a(x) \mid_R d(x)$ such that either $a(x) \mid_R b(x)$ or $a(x) \mid_R c(x)$.
3. The element $\sqrt{2}x$ is not primal. Note that $\sqrt{2}x \mid_R (\sqrt{3}x)(\sqrt{\frac{2}{3}}x)$.
4. The only way of decomposing $\sqrt{2}x$ as a product of two elements in R is $\sqrt{2}x = n \cdot \frac{\sqrt{2}}{n}x$.
5. Note that $\frac{\sqrt{2}}{n}x \nmid_R \sqrt{3}x$ because $\sqrt{\frac{3}{2}} \notin \mathbb{Q}$ while $\frac{\sqrt{2}}{n}x \nmid_R \sqrt{\frac{2}{3}}x$ because $\sqrt{3} \notin \mathbb{Q}$.

Introducing MCD-Monoids

Definitions:

- Let M be a monoid. We say that $d \in M$ is a maximal common divisor (mcd) of $A \subset M$ if d divides every element of A and there does not exist a non-unit d' such that $d \cdot d'$ also divides every element of A.
- We denote the set of maximal common divisors of A by $\mathrm{MCD}(A)$.
- M is a 2-MCD monoid if the maximal common divisor of every two elements exists.

Examples:

- In the numerical monoid $M := \{0\} \cup \mathbb{N}_{\geq 3}$, $4 \in \mathrm{MCD}(7, 8)$, but also $3 \in \mathrm{MCD}(7, 8)$.
- In the multiplicative monoid $(\mathbb{R}[x] \setminus \{0\}, \cdot)$, $x + 1$ is an mcd of $x^2 - 1$ and $x^3 + 1$.

MCD-Monoids Cont.

Examples:

- If the gcd of two elements exists, then the elements have an mcd, namely their gcd, which is unique up to associates.
- Let $M := \langle 2, 3 \rangle$. Note that $\gcd(5, 6)$ does not exist because $2, 3 \in CD(5, 6)$ and neither $2 \mid_M 3$ nor $3 \mid_M 2$. However, we have that $2, 3 \in \mathrm{MCD}(5, 6)$.
- Let $P := \langle \frac{1}{p^n} : p \in \mathbb{P}_{>3}, n \in \mathbb{N}_0 \rangle$ and consider the additive monoid $M := P \cup \mathbb{Q}_{\geq 1}$.
  - First, note that $1 \nmid_M \frac{4}{3}$.
  - For every $r \in M \setminus \{0\}$, we can always find a large enough m such that $r - \frac{1}{p^m} \in M$.
  - Let $d \in CD(1, \frac{4}{3})$. Then, we can write $1 = d + a$, $\frac{4}{3} = d + b$ for some $a, b \in M$.
  - Let $m \in \mathbb{N}$ large enough such that $a - \frac{1}{p^m}, b - \frac{1}{p^m} \in M$.
  - Therefore $d + \frac{1}{p^m} \in CD(1, \frac{4}{3})$.

The GL-Property in 2-MCD Monoids

Theorem (CrowdMath, 2024)

Let M be a 2-MCD monoid. Then M is pre-Schreier if and only if M has the GL-property.

The Ascent of the GL-Property

Theorem (Arnold and Sheldon, 1975)

There exists a GL-domain R such that the integral domain $R[x]$ is not GL.

Theorem (CrowdMath, 2024)

There exists a GL-monoid M such that the monoid algebra $\mathbb{F}_2[M]$ is not a GL-domain.

Construction of Counterexample to GL Ascent

1. Let $M := \mathbb{Z}\left[\frac{1}{2}\right]_{\geq 0} \cup \mathbb{Z}\left[\frac{1}{2}, \frac{1}{3}\right]_{\geq 1}$ and consider the monoid algebra $\mathbb{F}_2[M]$.
2. We have that
$$(x+1) \mid_{\mathbb{F}_2[M]} \left(x^{\frac{4}{3}}+1\right)\left(x^{\frac{8}{3}}+x^{\frac{4}{3}}+1\right).$$
3. Every divisor of $x+1$ in $\mathbb{F}_2[M]$ is of the form $(x^{\frac{1}{2^k}}+1)^{\ell}$ for some $k, \ell \in \mathbb{N}_0$.
4. No element of the form $(x^{\frac{1}{2^k}}+1)$ with $k \in \mathbb{N}_0$ divides either $\left(x^{\frac{4}{3}}+1\right)$ or $\left(x^{\frac{8}{3}}+x^{\frac{4}{3}}+1\right)$.
5. The binomial $x+1$ is not a prime-like element in $\mathbb{F}_2[M]$.

Presenting the Ongoing CrowdMath Project

Definitions: Let M be a monoid.

- M is nearly atomic if there exists an element $b \in M$ such that $b \cdot c$ is atomic for every non-unit element $c \in M$.
- An integral domain is nearly atomic if its multiplicative monoid is nearly atomic.

Remark: Every atomic monoid/domain is nearly atomic.

Examples:

- The Puiseux monoid $M_q := \langle q^n \mid n \in \mathbb{N}_0 \rangle$, where $q \in \mathbb{Q} \cap (0, 1)$ and $q^{-1} \notin \mathbb{N}_0$ is atomic.
- Let $\phi : \mathbb{Q}_{\geq 0} \to \mathbb{P}$ be an injective function and α an irrational number. Then the monoid $M := \left\langle q, \frac{\alpha+q}{\phi(q)} \middle| q \in \mathbb{Q}_{\geq 0} \right\rangle$ is a nearly atomic monoid which is not atomic.

Presenting the Ongoing CrowdMath Project

Theorem (CrowdMath, 2024)

There exists a nearly atomic Puiseux monoid M such that the monoid algebra $\mathbb{F}_2[M]$ is not nearly atomic.

Theorem [under review] (CrowdMath, 2024)

There exists an atomic Puiseux monoid M such that $\mathbb{Q}[M]$ is not nearly atomic.

References

D. D. Anderson, R. O. Quintero, *Some generalizations of GCD-domains*. In: Factorization in Integral Domains (Ed. D. D. Anderson) pp. 189–195, Lectures in Pure and Applied Mathematics, Marcel Dekker, New York 1997.

D. D. Anderson and M. Zafrullah, *The schreier property and Gauss' Lemma*, Bollettino dell' Unione Matematica Italiana, Series 8, **10-B** (2027) 43–62.

J. T. Arnold and P. B. Sheldon, *Integral domains that satisfy Gauss's lemma*, Michigan Math. J. **22** (1975) 39–51.

P. M. Cohn, *Bezout rings and their subrings*, Proc. Cambridge Philos. Soc. **64** (1968) 251–264.

W. Dicks and E. D. Sontag, *Sylvester domains*, J. Pure Appl. Algebra **13** (1978) 243–275.

References Pg.2

- S. Eftekhari and M. R. Khorsandi, *MCD-finite domains and ascent of IDF-property in polynomial extensions*, Comm. Algebra **46** (2018) 3865–3872.
- F. Gotti, *Hereditary atomicity and ACCP in abelian groups*. Submitted. Preprint on arXiv: https://arxiv.org/abs/2303.01039
- F. Gotti and M. Gotti, *On the molecules of numerical semigroups, Puiseux monoids, and Puiseux algebras*. In: Numerical Semigroups (Eds. V. Barucci, S. T. Chapman, M. D'Anna, and R. Fröberg) pp. 141–161, Springer INdAM Series, vol. **40**, Springer Nature, Switzerland, 2020.
- S. McAdam and D. E. Rush, *Schreier rings*, Bull. London Math. Soc. **10** (1978) 77–80.
- H. T. Tang, *Gauss' lemma*, Proc. Amer. Math. Soc. **35** (1972) 372–376.

References Pg.3

M. Zafrullah, *On a property of pre-Schreier domains*, Comm. Algebra **15** (1987) 1895–1920.

M. Zafrullah, *Well behaved prime t-ideals*, J. Pure Appl. Algebra **65** (1990) 199–207.

THANK YOU!!!