Factorizations of Algebraic Integers, Block Monoids, and Additive Number Theory

Scott Chapman

January 25, 2021

Prologue

This talk is based the paper:

[1] P. Baginski and S. T. Chapman, Factorizations of Algebraic Integers, Block Monoids and Additive Number Theory, *Amer. Math. Monthly* **118**(10), 901-920.

More information and background on this area can be found in:

[2] S. T. Chapman, On the Davenport constant, the cross number and their application in factorization theory, *Lecture Notes in Pure and Applied Mathematics*, Marcel Dekker, **171**(1995), 167-190.

[3] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations. Algebraic, Combinatorial and Analytic Theory*, Chapman & Hall/CRC, 2006.

Prologue

This talk is based the paper:

[1] P. Baginski and S. T. Chapman, Factorizations of Algebraic Integers, Block Monoids and Additive Number Theory, *Amer. Math. Monthly* **118**(10), 901-920.

More information and background on this area can be found in:

[2] S. T. Chapman, On the Davenport constant, the cross number and their application in factorization theory, *Lecture Notes in Pure and Applied Mathematics*, Marcel Dekker, **171**(1995), 167-190.

[3] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations. Algebraic, Combinatorial and Analytic Theory*, Chapman & Hall/CRC, 2006.

Prologue

This talk is based the paper:

[1] P. Baginski and S. T. Chapman, Factorizations of Algebraic Integers, Block Monoids and Additive Number Theory, *Amer. Math. Monthly* **118**(10), 901-920.

More information and background on this area can be found in:

[2] S. T. Chapman, On the Davenport constant, the cross number and their application in factorization theory, *Lecture Notes in Pure and Applied Mathematics*, Marcel Dekker, **171**(1995), 167-190.

[3] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations. Algebraic, Combinatorial and Analytic Theory*, Chapman & Hall/CRC, 2006.

Motivation

Let $K = \mathbb{Q}(\alpha)$ be a finite extension of the rationals.

Let $\mathcal{O}_K = \{\alpha \in K \mid f(\alpha) = 0 \text{ for some monic } f(X) \in \mathbb{Z}[X]\}$ be the ring of integers of K.

Let $\mathcal{I}(\mathcal{O}_K)$ represent the set of nonzero ideals of $\mathcal{O}_K$ and $\mathcal{P}(\mathcal{O}_K)$ its associated subset of nonzero principal ideals.

Fundamental Question

If $\alpha \in \mathcal{O}_K$, then how does α factor into irreducible elements of $\mathcal{O}_K$? When do the elements of $\mathcal{O}_K$ have unique factorization like in $\mathbb{Z}$?

Answer: The factorizations of α depend on the factorization of the ideal (α) into the prime ideals of $\mathcal{I}(\mathcal{O}_K)$. $\mathcal{O}_K$ is a unique factorization domain exactly when $\mathcal{I}(\mathcal{O}_K) = \mathcal{P}(\mathcal{O}_K)$.

Motivation

Let $K = \mathbb{Q}(\alpha)$ be a finite extension of the rationals.

Let $\mathcal{O}_K = \{\alpha \in K \mid f(\alpha) = 0 \text{ for some monic } f(X) \in \mathbb{Z}[X]\}$ be the ring of integers of K.

Let $\mathcal{I}(\mathcal{O}_K)$ represent the set of nonzero ideals of $\mathcal{O}_K$ and $\mathcal{P}(\mathcal{O}_K)$ its associated subset of nonzero principal ideals.

Fundamental Question

If $\alpha \in \mathcal{O}_K$, then how does α factor into irreducible elements of $\mathcal{O}_K$? When do the elements of $\mathcal{O}_K$ have unique factorization like in $\mathbb{Z}$?

Answer: The factorizations of α depend on the factorization of the ideal (α) into the prime ideals of $\mathcal{I}(\mathcal{O}_K)$. $\mathcal{O}_K$ is a unique factorization domain exactly when $\mathcal{I}(\mathcal{O}_K) = \mathcal{P}(\mathcal{O}_K)$.

Motivation

Let $K = \mathbb{Q}(\alpha)$ be a finite extension of the rationals.

Let $\mathcal{O}_K = \{\alpha \in K \mid f(\alpha) = 0 \text{ for some monic } f(X) \in \mathbb{Z}[X]\}$ be the ring of integers of K.

Let $\mathcal{I}(\mathcal{O}_K)$ represent the set of nonzero ideals of $\mathcal{O}_K$ and $\mathcal{P}(\mathcal{O}_K)$ its associated subset of nonzero principal ideals.

Fundamental Question

If $\alpha \in \mathcal{O}_K$, then how does α factor into irreducible elements of $\mathcal{O}_K$? When do the elements of $\mathcal{O}_K$ have unique factorization like in $\mathbb{Z}$?

Answer: The factorizations of α depend on the factorization of the ideal (α) into the prime ideals of $\mathcal{I}(\mathcal{O}_K)$. $\mathcal{O}_K$ is a unique factorization domain exactly when $\mathcal{I}(\mathcal{O}_K) = \mathcal{P}(\mathcal{O}_K)$.

Motivation

Let $K = \mathbb{Q}(\alpha)$ be a finite extension of the rationals.

Let $\mathcal{O}_K = \{\alpha \in K \mid f(\alpha) = 0 \text{ for some monic } f(X) \in \mathbb{Z}[X]\}$ be the ring of integers of K.

Let $\mathcal{I}(\mathcal{O}_K)$ represent the set of nonzero ideals of $\mathcal{O}_K$ and $\mathcal{P}(\mathcal{O}_K)$ its associated subset of nonzero principal ideals.

Fundamental Question

If $\alpha \in \mathcal{O}_K$, then how does α factor into irreducible elements of $\mathcal{O}_K$? When do the elements of $\mathcal{O}_K$ have unique factorization like in $\mathbb{Z}$?

Answer: The factorizations of α depend on the factorization of the ideal (α) into the prime ideals of $\mathcal{I}(\mathcal{O}_K)$. $\mathcal{O}_K$ is a unique factorization domain exactly when $\mathcal{I}(\mathcal{O}_K) = \mathcal{P}(\mathcal{O}_K)$.

Motivation

Let $K = \mathbb{Q}(\alpha)$ be a finite extension of the rationals.

Let $\mathcal{O}_K = \{\alpha \in K \mid f(\alpha) = 0 \text{ for some monic } f(X) \in \mathbb{Z}[X]\}$ be the ring of integers of K.

Let $\mathcal{I}(\mathcal{O}_K)$ represent the set of nonzero ideals of $\mathcal{O}_K$ and $\mathcal{P}(\mathcal{O}_K)$ its associated subset of nonzero principal ideals.

Fundamental Question

If $\alpha \in \mathcal{O}_K$, then how does α factor into irreducible elements of $\mathcal{O}_K$? When do the elements of $\mathcal{O}_K$ have unique factorization like in $\mathbb{Z}$?

Answer: The factorizations of α depend on the factorization of the ideal (α) into the prime ideals of $\mathcal{I}(\mathcal{O}_K)$. $\mathcal{O}_K$ is a unique factorization domain exactly when $\mathcal{I}(\mathcal{O}_K) = \mathcal{P}(\mathcal{O}_K)$.

More Motivation

The usual example used in an undergraduate Abstract Algebra Textbook to demonstrate that the Fundamental Theorem of Arithmetic can fail in an integral domain is:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \tag{1}$$

in the algebraic number ring $\mathbb{Z}[\sqrt{-5}]$.

The actual argument to complete this observation involves showing two things:

(i) $2, 3, 1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are all irreducible, and

(ii) 2 (resp. 3) is neither an associate of $(1 + \sqrt{-5})$ nor of $(1 - \sqrt{-5})$ (this is clear once ± 1 are established as the only units of $\mathbb{Z}[\sqrt{-5}]$).

More Motivation

The usual example used in an undergraduate Abstract Algebra Textbook to demonstrate that the Fundamental Theorem of Arithmetic can fail in an integral domain is:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \tag{1}$$

in the algebraic number ring $\mathbb{Z}[\sqrt{-5}]$.

The actual argument to complete this observation involves showing two things:

(i) $2, 3, 1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are all irreducible, and

(ii) 2 (resp. 3) is neither an associate of $(1 + \sqrt{-5})$ nor of $(1 - \sqrt{-5})$ (this is clear once ± 1 are established as the only units of $\mathbb{Z}[\sqrt{-5}]$).

More Motivation

The usual example used in an undergraduate Abstract Algebra Textbook to demonstrate that the Fundamental Theorem of Arithmetic can fail in an integral domain is:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \tag{1}$$

in the algebraic number ring $\mathbb{Z}[\sqrt{-5}]$.

The actual argument to complete this observation involves showing two things:

(i) $2, 3, 1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are all irreducible, and

(ii) 2 (resp. 3) is neither an associate of $(1 + \sqrt{-5})$ nor of $(1 - \sqrt{-5})$ (this is clear once ± 1 are established as the only units of $\mathbb{Z}[\sqrt{-5}]$).

Motivation

Most books fail to point out to the readers that while $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, it does have a rather nice factorization property.

Specifically, if $\alpha_1, \ldots \alpha_n, \beta_1, \ldots, \beta_m$ are irreducible elements of $\mathbb{Z}[\sqrt{-5}]$ with

$$\alpha_1 \cdots \alpha_n = \beta_1 \cdots \beta_m, \tag{2}$$

then $n = m$.

In general, an integral domain with this property is known as a *half-factorial domain* (HFD).

Motivation

Most books fail to point out to the readers that while $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, it does have a rather nice factorization property.

Specifically, if $\alpha_1, \ldots \alpha_n, \beta_1, \ldots, \beta_m$ are irreducible elements of $\mathbb{Z}[\sqrt{-5}]$ with

$$\alpha_1 \cdots \alpha_n = \beta_1 \cdots \beta_m, \tag{2}$$

then $n = m$.

In general, an integral domain with this property is known as a *half-factorial domain* (HFD).

Motivation

Most books fail to point out to the readers that while $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, it does have a rather nice factorization property.

Specifically, if $\alpha_1, \dots \alpha_n, \beta_1, \dots, \beta_m$ are irreducible elements of $\mathbb{Z}[\sqrt{-5}]$ with

$$\alpha_1 \cdots \alpha_n = \beta_1 \cdots \beta_m, \tag{2}$$

then $n = m$.

In general, an integral domain with this property is known as a *half-factorial domain* (HFD).

Goals

Using the ideal class group (and, more generally, the class number), one can construct a very simple proof of this fact for $\mathbb{Z}[\sqrt{-5}]$.

Carlitz first illustrated this argument in *PAMS* 11(1960), 391-392.

His proof (while short) leads to a deeper understanding of how elements factor in an algebraic ring of integers.

Goals

Using the ideal class group (and, more generally, the class number), one can construct a very simple proof of this fact for $\mathbb{Z}[\sqrt{-5}]$.

Carlitz first illustrated this argument in *PAMS* 11(1960), 391-392.

His proof (while short) leads to a deeper understanding of how elements factor in an algebraic ring of integers.

Goals

Using the ideal class group (and, more generally, the class number), one can construct a very simple proof of this fact for $\mathbb{Z}[\sqrt{-5}]$.

Carlitz first illustrated this argument in *PAMS* 11(1960), 391-392.

His proof (while short) leads to a deeper understanding of how elements factor in an algebraic ring of integers.

Goals

The purpose of this talk is to develop this understanding by using a structure, known as a *block monoid*, that is associated to the class group.

In fact, block monoids have greater utility and we shall show that they can be used in a similar line of analysis in more general classes of integral domains, such as Dedekind domains and Krull domains.

Our work will involve a close study of the combinatorial properties of block monoids and lead to an examination of an actively researched concept from Additive Number Theory known as *Davenport's constant*.

Goals

The purpose of this talk is to develop this understanding by using a structure, known as a *block monoid*, that is associated to the class group.

In fact, block monoids have greater utility and we shall show that they can be used in a similar line of analysis in more general classes of integral domains, such as Dedekind domains and Krull domains.

Our work will involve a close study of the combinatorial properties of block monoids and lead to an examination of an actively researched concept from Additive Number Theory known as *Davenport's constant*.

Goals

The purpose of this talk is to develop this understanding by using a structure, known as a *block monoid*, that is associated to the class group.

In fact, block monoids have greater utility and we shall show that they can be used in a similar line of analysis in more general classes of integral domains, such as Dedekind domains and Krull domains.

Our work will involve a close study of the combinatorial properties of block monoids and lead to an examination of an actively researched concept from Additive Number Theory known as *Davenport's constant*.

Definitions

Proposition

Let I be an ideal of $\mathcal{O}_K$ and $\mathcal{I}(\mathcal{O}_K)$ and $\mathcal{P}(\mathcal{O}_K)$ be as above.

1. *$\mathcal{O}_K$ is a Dedekind domain. Moreover, there exists elements α and β in $\mathcal{O}_K$ such that $I = (\alpha, \beta)$.*
2. *The factor monoid $\mathcal{C}(\mathcal{O}_K) = \mathcal{I}(\mathcal{O}_K)/\mathcal{P}(\mathcal{O}_K)$ forms a finite abelian group.*
3. *Let $[I]$ represent the image of the ideal I in $\mathcal{C}(\mathcal{O}_K)$. Then, for each $g \in \mathcal{C}(\mathcal{O}_K)$ there exists a prime ideal P of $\mathcal{O}_K$ such that $[P] = g$.*

A Classic Theorem

The group $\mathcal{C}(\mathcal{O}_K)$ is known as the *class group* of $\mathcal{O}_K$ and its order $|\mathcal{C}(\mathcal{O}_K)|$ is the *class number* of $\mathcal{O}_K$.

The class number gives a classic answer to the question of when a ring of algebraic integers admits unique factorization.

Theorem

The ring of integers $\mathcal{O}_K$ in an algebraic number field K is a unique factorization domain if and only if the class number of $\mathcal{O}_K$ is 1.

In fact, the size of the class group of $\mathcal{O}_K$ was generally assumed to be a measure of how far a ring of integers was from being a UFD.

A Classic Theorem

The group $\mathcal{C}(\mathcal{O}_K)$ is known as the *class group* of $\mathcal{O}_K$ and its order $|\mathcal{C}(\mathcal{O}_K)|$ is the *class number* of $\mathcal{O}_K$.

The class number gives a classic answer to the question of when a ring of algebraic integers admits unique factorization.

Theorem

The ring of integers $\mathcal{O}_K$ in an algebraic number field K is a unique factorization domain if and only if the class number of $\mathcal{O}_K$ is 1.

In fact, the size of the class group of $\mathcal{O}_K$ was generally assumed to be a measure of how far a ring of integers was from being a UFD.

The Connection Between Ideals and Factorizations

Proposition

Let D be a Dedekind domain and $x \in D$ a nonzero nonunit. Suppose in D that

$$(x) = P_1 \cdots P_k$$

where $k \geq 1$ and the $P_1, \cdots P_k$ are not necessarily distinct prime ideals of D. Then

1. *In $\mathcal{C}(D)$, $[P_1] + \cdots + [P_k] = 0$.*
2. *The element x is prime in D if and only if $k = 1$.*
3. *The element x is irreducible in D if and only if for every nonempty proper subset $T \subset \{1, \ldots, k\}$, $\sum_{i \in T} [P_i] \neq 0$.*

Proof of (3)

Proof.

We prove (3) by contrapositive. ($\Rightarrow$) Suppose for some proper subset T that $\sum_{i\in T}[P_i] = 0$. Then $\prod_{i\in T} P_i = (y)$ for some nonzero nonunit $y \in D$. By (1) we have $[P_1] + \cdots + [P_k] = 0$, so $\sum_{i\in \overline{T}}[P_i] = 0$ also. Thus, $\prod_{i\in \overline{T}} P_i = (z)$ for some nonzero nonunit $z \in D$. Hence $(x) = (y)(z)$ implies that $x = uyz$ where u is a unit of D and so x is reducible. ($\Leftarrow$) Suppose that x is reducible in D, i.e. $x = yz$ for nonunits y and z in D. By the Fundamental Theorem, there is a proper nonempty subset $T \subset \{1, \ldots, k\}$ such that $(y) = \prod_{i\in T} P_i$. By (1), in $\mathcal{C}(D)$, $\sum_{i\in T}[P_i] = 0$. □

An Application

What happened in $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$?

The only units of $\mathcal{O}_K$ are ± 1 and it is well known that the class number of $\mathcal{O}_K$ is 2 (hence $\mathcal{C}(\mathcal{O}_K) \cong \mathbb{Z}_2$).

Let's reconsider

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \tag{3}$$

in $\mathbb{Z}[\sqrt{-5}]$.

The prime ideal decompositions of (2) and (3) in $\mathbb{Z}[\sqrt{-5}]$ are

$$(2) = (2, 1 + \sqrt{-5})^2 \text{ and } (3) = (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}).$$

An Application

What happened in $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$?

The only units of $\mathcal{O}_K$ are ± 1 and it is well known that the class number of $\mathcal{O}_K$ is 2 (hence $\mathcal{C}(\mathcal{O}_K) \cong \mathbb{Z}_2$).

Let's reconsider

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \quad (3)$$

in $\mathbb{Z}[\sqrt{-5}]$.

The prime ideal decompositions of (2) and (3) in $\mathbb{Z}[\sqrt{-5}]$ are

$$(2) = (2, 1 + \sqrt{-5})^2 \text{ and } (3) = (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}).$$

An Application

What happened in $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$?

The only units of $\mathcal{O}_K$ are ± 1 and it is well known that the class number of $\mathcal{O}_K$ is 2 (hence $\mathcal{C}(\mathcal{O}_K) \cong \mathbb{Z}_2$).

Let's reconsider

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \tag{3}$$

in $\mathbb{Z}[\sqrt{-5}]$.

The prime ideal decompositions of (2) and (3) in $\mathbb{Z}[\sqrt{-5}]$ are

$$(2) = (2, 1 + \sqrt{-5})^2 \text{ and } (3) = (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}).$$

An Application

What happened in $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$?

The only units of $\mathcal{O}_K$ are ± 1 and it is well known that the class number of $\mathcal{O}_K$ is 2 (hence $\mathcal{C}(\mathcal{O}_K) \cong \mathbb{Z}_2$).

Let's reconsider

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \tag{3}$$

in $\mathbb{Z}[\sqrt{-5}]$.

The prime ideal decompositions of (2) and (3) in $\mathbb{Z}[\sqrt{-5}]$ are

$$(2) = (2, 1 + \sqrt{-5})^2 \text{ and } (3) = (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}).$$

An Application

Hence,

$$(6) = (2)(3) = (2, 1+\sqrt{-5})^2(3, 1+\sqrt{-5})(3, 1-\sqrt{-5}). \qquad (4)$$

The second factorization in Eq. 3 is obtained by rearranging the product in Eq. 4,

$$(6) = (2)(3) = (2, 1+\sqrt{-5})^2(3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$$
$$= (2, 1+\sqrt{-5})(3, 1+\sqrt{-5})(2, 1+\sqrt{-5})(3, 1-\sqrt{-5}) = (1+\sqrt{-5})(1-\sqrt{-5}).$$

Moreover, since the class group of $\mathbb{Z}[\sqrt{-5}]$ requires a product of two nonprincipal prime ideals to obtain a principal ideal, these are the only two factorizations of 6 in $\mathbb{Z}[\sqrt{-5}]$ up to associates.

An Application

Hence,

$$(6) = (2)(3) = (2, 1+\sqrt{-5})^2(3, 1+\sqrt{-5})(3, 1-\sqrt{-5}). \qquad (4)$$

The second factorization in Eq. 3 is obtained by rearranging the product in Eq. 4,

$$(6) = (2)(3) = (2, 1+\sqrt{-5})^2(3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$$
$$= (2, 1+\sqrt{-5})(3, 1+\sqrt{-5})(2, 1+\sqrt{-5})(3, 1-\sqrt{-5}) = (1+\sqrt{-5})(1-\sqrt{-5}).$$

Moreover, since the class group of $\mathbb{Z}[\sqrt{-5}]$ requires a product of two nonprincipal prime ideals to obtain a principal ideal, these are the only two factorizations of 6 in $\mathbb{Z}[\sqrt{-5}]$ up to associates.

An Application

Hence,

$$(6) = (2)(3) = (2, 1+\sqrt{-5})^2(3, 1+\sqrt{-5})(3, 1-\sqrt{-5}). \tag{4}$$

The second factorization in Eq. 3 is obtained by rearranging the product in Eq. 4,

$$\begin{aligned}(6) &= (2)(3) = (2, 1+\sqrt{-5})^2(3, 1+\sqrt{-5})(3, 1-\sqrt{-5}) \\ &= (2, 1+\sqrt{-5})(3, 1+\sqrt{-5})(2, 1+\sqrt{-5})(3, 1-\sqrt{-5}) = (1+\sqrt{-5})(1-\sqrt{-5}).\end{aligned}$$

Moreover, since the class group of $\mathbb{Z}[\sqrt{-5}]$ requires a product of two nonprincipal prime ideals to obtain a principal ideal, these are the only two factorizations of 6 in $\mathbb{Z}[\sqrt{-5}]$ up to associates.

Block Monoids

Let G be an abelian group. If $A \subseteq G$, then let $\langle A \rangle$ represent the subgroup generated by A.

Further, let $\mathcal{F}(G)$ represent the free abelian monoid on G. We write the elements of $\mathcal{F}(G)$ as $C = \prod_{g \in G} g^{v_g(C)}$ where $v_g(C)$ is a nonnegative integer.

Definition

Let G be an abelian group. The set

$$\mathcal{B}(G) = \left\{ C \;\middle|\; C = \prod_{g \in G} g^{v_g(C)} \text{ with } \sum_{g \in G} v_g(C) g = 0 \right\}$$

forms a submonoid of $\mathcal{F}(G)$ known as the *block monoid of* G.

Block Monoids

Let G be an abelian group. If $A \subseteq G$, then let $\langle A \rangle$ represent the subgroup generated by A.

Further, let $\mathcal{F}(G)$ represent the free abelian monoid on G. We write the elements of $\mathcal{F}(G)$ as $C = \prod_{g \in G} g^{v_g(C)}$ where $v_g(C)$ is a nonnegative integer.

Definition

Let G be an abelian group. The set

$$\mathcal{B}(G) = \left\{ C \,\middle|\, C = \prod_{g \in G} g^{v_g(C)} \text{ with } \sum_{g \in G} v_g(C) g = 0 \right\}$$

forms a submonoid of $\mathcal{F}(G)$ known as the *block monoid of* G.

Block Moniods

Definition

If S is a nonempty subset of G, then the set

$$\mathcal{B}(G,S) = \left\{ C \;\middle|\; C = \prod_{g \in G} g^{v_g(C)} \text{ with } \sum_{g \in G} v_g(C)g = 0 \text{ and } v_g(C) = 0 \text{ if } g \notin S \right\}$$

is a submonoid of $\mathcal{B}(G)$ known as the *block monoid of* G *restricted to* S.

We call the identity of $\mathcal{B}(G,S)$, $E = \prod_{g \in G} g^0$, the *empty block*.

A block B divides a block C, denoted $B \mid C$ if there is a block T such that $C = BT$.

Block Moniods

Definition

If S is a nonempty subset of G, then the set

$$\mathcal{B}(G,S) = \left\{ C \;\middle|\; C = \prod_{g\in G} g^{v_g(C)} \text{ with } \sum_{g\in G} v_g(C)g = 0 \text{ and } v_g(C) = 0 \text{ if } g \notin S \right\}$$

is a submonoid of $\mathcal{B}(G)$ known as the *block monoid of* G *restricted to* S.

We call the identity of $\mathcal{B}(G,S)$, $E = \prod_{g\in G} g^0$, the *empty block*.

A block B divides a block C, denoted $B \mid C$ if there is a block T such that $C = BT$.

Block Monoids

A block $B \neq E$ is *irreducible* if $B = CT$ for C, T in $\mathcal{B}(G, S)$ implies that either $C = E$ or $T = E$.

A block $B \neq E$ is *prime* if whenever $B \mid CT$ then either $B \mid C$ or $B \mid T$.

As with the usual theory of factorization in an integral domain, a prime block B is irreducible, but not conversely.

For the block $C = \prod_{g \in G} g^{v_g(C)}$, we set $|C| = \sum_{g \in G} v_g(C)$ to be the *size* of C.

Block Monoids

A block $B \neq E$ is *irreducible* if $B = CT$ for C, T in $\mathcal{B}(G,S)$ implies that either $C = E$ or $T = E$.

A block $B \neq E$ is *prime* if whenever $B \mid CT$ then either $B \mid C$ or $B \mid T$.

As with the usual theory of factorization in an integral domain, a prime block B is irreducible, but not conversely.

For the block $C = \prod_{g \in G} g^{v_g(C)}$, we set $|C| = \sum_{g \in G} v_g(C)$ to be the *size* of C.

Block Monoids

A block $B \neq E$ is *irreducible* if $B = CT$ for C, T in $\mathcal{B}(G,S)$ implies that either $C = E$ or $T = E$.

A block $B \neq E$ is *prime* if whenever $B \mid CT$ then either $B \mid C$ or $B \mid T$.

As with the usual theory of factorization in an integral domain, a prime block B is irreducible, but not conversely.

For the block $C = \prod_{g \in G} g^{v_g(C)}$, we set $|C| = \sum_{g \in G} v_g(C)$ to be the *size* of C.

Block Monoids

A block $B \neq E$ is *irreducible* if $B = CT$ for C, T in $\mathcal{B}(G, S)$ implies that either $C = E$ or $T = E$.

A block $B \neq E$ is *prime* if whenever $B \mid CT$ then either $B \mid C$ or $B \mid T$.

As with the usual theory of factorization in an integral domain, a prime block B is irreducible, but not conversely.

For the block $C = \prod_{g \in G} g^{v_g(C)}$, we set $|C| = \sum_{g \in G} v_g(C)$ to be the *size* of C.

Basic Facts About Block Monoids

We compile a few facts about block monoids.

Proposition

Let G be an abelian group and S a nonempty subset of G.

1. *The block $B = \prod_{g \in S} g^{v_g(B)} \neq E$ is irreducible in $\mathcal{B}(G, S)$ if and only if for each nonempty subset T of S we have $\sum_{g \in T} v'_g(B)g \neq 0$ for any integers $v'_g(B)$ with $0 \leq v'_g(B) \leq v_g(B)$ where at least one $v'_g(B) \neq 0$ and at least one $v'_g(B) < v_g(B)$.*
2. *If $B \neq E$ in $\mathcal{B}(G, S)$, then B can be written as a product of irreducible blocks in $\mathcal{B}(G, S)$.*
3. *If $0 \in S$, then the block 0^1 is prime in $\mathcal{B}(G, S)$.*
4. *If G is finite, then $\mathcal{B}(G, S)$ contains finitely many irreducible blocks.*

Basic Facts About Block Monoids

We compile a few facts about block monoids.

Proposition

Let G be an abelian group and S a nonempty subset of G.

1. *The block $B = \prod_{g \in S} g^{v_g(B)} \neq E$ is irreducible in $\mathcal{B}(G,S)$ if and only if for each nonempty subset T of S we have $\sum_{g \in T} v'_g(B)g \neq 0$ for any integers $v'_g(B)$ with $0 \leq v'_g(B) \leq v_g(B)$ where at least one $v'_g(B) \neq 0$ and at least one $v'_g(B) < v_g(B)$.*
2. *If $B \neq E$ in $\mathcal{B}(G,S)$, then B can be written as a product of irreducible blocks in $\mathcal{B}(G,S)$.*
3. *If $0 \in S$, then the block 0^1 is prime in $\mathcal{B}(G,S)$.*
4. *If G is finite, then $\mathcal{B}(G,S)$ contains finitely many irreducible blocks.*

SH

An Example

Example

Let $G = \mathbb{Z}_4$. Here

$$\mathcal{B}(\mathbb{Z}_4) = \{\overline{0}^{x_0}\overline{1}^{x_1}\overline{2}^{x_2}\overline{3}^{x_3} \mid \text{each } x_i \geq 0 \text{ and } x_1 + 2x_2 + 3x_3 \equiv 0 \pmod 4\}.$$

Notice that the non-prime irreducible blocks of $\mathcal{B}(\mathbb{Z}_4)$ are as follows:

$$\overline{1}^4, \overline{2}^2, \overline{3}^4, \overline{1}^2\overline{2}^1, \overline{1}^1\overline{3}^1, \text{ and } \overline{2}^1\overline{3}^2.$$

In this monoid it is easy to produce factorizations of blocks into irreducible blocks which differ in length. For instance

$$B = (\overline{1}^4)(\overline{3}^4) = (\overline{1}^1\overline{3}^1)^4$$

is a factorization of B into 2 and 4 irreducible blocks respectfully.

An Example

Example

Let $G = \mathbb{Z}_4$. Here

$$\mathcal{B}(\mathbb{Z}_4) = \{\overline{0}^{x_0}\overline{1}^{x_1}\overline{2}^{x_2}\overline{3}^{x_3} \mid \text{each } x_i \geq 0 \text{ and } x_1 + 2x_2 + 3x_3 \equiv 0 \pmod 4\}.$$

Notice that the non-prime irreducible blocks of $\mathcal{B}(\mathbb{Z}_4)$ are as follows:

$$\overline{1}^4, \overline{2}^2, \overline{3}^4, \overline{1}^2\overline{2}^1, \overline{1}^1\overline{3}^1, \text{ and } \overline{2}^1\overline{3}^2.$$

In this monoid it is easy to produce factorizations of blocks into irreducible blocks which differ in length. For instance

$$B = (\overline{1}^4)(\overline{3}^4) = (\overline{1}^1\overline{3}^1)^4$$

is a factorization of B into 2 and 4 irreducible blocks respectfully.

An Example

Example

Let $G = \mathbb{Z}_4$. Here

$$\mathcal{B}(\mathbb{Z}_4) = \{\overline{0}^{x_0}\overline{1}^{x_1}\overline{2}^{x_2}\overline{3}^{x_3} \mid \text{each } x_i \geq 0 \text{ and } x_1 + 2x_2 + 3x_3 \equiv 0 \pmod 4\}.$$

Notice that the non-prime irreducible blocks of $\mathcal{B}(\mathbb{Z}_4)$ are as follows:

$$\overline{1}^4, \overline{2}^2, \overline{3}^4, \overline{1}^2\overline{2}^1, \overline{1}^1\overline{3}^1, \text{ and } \overline{2}^1\overline{3}^2.$$

In this monoid it is easy to produce factorizations of blocks into irreducible blocks which differ in length. For instance

$$B = (\overline{1}^4)(\overline{3}^4) = (\overline{1}^1\overline{3}^1)^4$$

is a factorization of B into 2 and 4 irreducible blocks respectfully.

An Example

Example

Let $G = \mathbb{Z}_4$. Here

$$\mathcal{B}(\mathbb{Z}_4) = \{\overline{0}^{x_0}\overline{1}^{x_1}\overline{2}^{x_2}\overline{3}^{x_3} \mid \text{each } x_i \geq 0 \text{ and } x_1 + 2x_2 + 3x_3 \equiv 0 \pmod 4\}.$$

Notice that the non-prime irreducible blocks of $\mathcal{B}(\mathbb{Z}_4)$ are as follows:

$$\overline{1}^4, \overline{2}^2, \overline{3}^4, \overline{1}^2\overline{2}^1, \overline{1}^1\overline{3}^1, \text{ and } \overline{2}^1\overline{3}^2.$$

In this monoid it is easy to produce factorizations of blocks into irreducible blocks which differ in length. For instance

$$B = (\overline{1}^4)(\overline{3}^4) = (\overline{1}^1\overline{3}^1)^4$$

is a factorization of B into 2 and 4 irreducible blocks respectfully.

Factorial vs. Half-Factorial

Proposition

Let G be an abelian group. The following statements are equivalent.

1. $\mathcal{B}(G)$ *is factorial.*
2. $\mathcal{B}(G)$ *is half-factorial.*
3. $|G| \leq 2$.

Proof.

(2) $\Rightarrow$ (3) Suppose $\mathcal{B}(G)$ is half-factorial and that $|G| > 3$. Then G has two distinct nonzero elements g_1 and g_2 with $g_3 = g_1 + g_2 \neq 0$ and $g_3 \neq g_1, g_2$. The blocks $A_1 = (-g_3)^1 g_1^1 g_2^1$, $A_2 = g_3^1(-g_1)^1(-g_2)^1$, $B_1 = g_1^1(-g_1)^1$, $B_2 = g_2^1(-g_2)^1$ and $B_3 = g_3^1(-g_3)^1$ are all irreducibles of $\mathcal{B}(G)$. But $A_1A_2 = B_1B_2B_3$, so $B(G)$ is not half factorial, a contradiction. Hence $|G| \leq 3$. If $|G| = 3$, then $G \cong \mathbb{Z}_3$. If $A = \overline{1}^3$, $B = \overline{2}^3$ and $C = \overline{1}^1\overline{2}^1$, then $AB = C^3$ and $\mathcal{B}(\mathbb{Z}_3)$ is not half-factorial. Hence, we conclude that $|G| \leq 2$. □

Factorial vs. Half-Factorial

Proposition

Let G be an abelian group. The following statements are equivalent.

1. *$\mathcal{B}(G)$ is factorial.*
2. *$\mathcal{B}(G)$ is half-factorial.*
3. *$|G| \leq 2$.*

[redacted]

(2) $\Rightarrow$ (3) Suppose $\mathcal{B}(G)$ is half-factorial and that $|G| > 3$. Then G has two distinct nonzero elements g_1 and g_2 with $g_3 = g_1 + g_2 \neq 0$ and $g_3 \neq g_1, g_2$. The blocks $A_1 = (-g_3)^1 g_1^1 g_2^1$, $A_2 = g_3^1(-g_1)^1(-g_2)^1$, $B_1 = g_1^1(-g_1)^1$, $B_2 = g_2^1(-g_2)^1$ and $B_3 = g_3^1(-g_3)^1$ are all irreducibles of $\mathcal{B}(G)$. But $A_1 A_2 = B_1 B_2 B_3$, so $B(G)$ is not half factorial, a contradiction. Hence $|G| \leq 3$. If $|G| = 3$, then $G \cong \mathbb{Z}_3$. If $A = \overline{1}^3$, $B = \overline{2}^3$ and $C = \overline{1}^1\overline{2}^1$, then $AB = C^3$ and $\mathcal{B}(\mathbb{Z}_3)$ is not half-factorial. Hence, we conclude that $|G| \leq 2$. □

A Little Additive Number Theory

Definition

Let G be an abelian group. The *Davenport constant* of G is defined as

$$D(G) = \sup\{\, |B| \mid B \text{ is an irreducible element of } \mathcal{B}(G)\}.$$

If S is a nonempty subset of G, then

$$D(G, S) = \sup\{\, |B| \mid B \text{ is an irreducible element of } \mathcal{B}(G, S)\}$$

is known as the Davenport constant of G relative to S.

No closed formula for the computation of the Davenport constant is known.

Davenport's constant arises in several unexpected areas. Alford, Granville and Pomerance used the bound $D(G) \leq \exp(G)(1 + \log(|G|/\exp(G))$ to prove there are infinitely many Carmichael numbers.

A Little Additive Number Theory

Definition

Let G be an abelian group. The *Davenport constant* of G is defined as

$$D(G) = \sup\{\, |B| \mid B \text{ is an irreducible element of } \mathcal{B}(G)\}.$$

If S is a nonempty subset of G, then

$$D(G,S) = \sup\{\, |B| \mid B \text{ is an irreducible element of } \mathcal{B}(G,S)\}$$

is known as the Davenport constant of G relative to S.

No closed formula for the computation of the Davenport constant is known.

Davenport's constant arises in several unexpected areas. Alford, Granville and Pomerance used the bound $D(G) \leq \exp(G)(1 + \log(|G|/\exp(G))$ to prove there are infinitely many Carmichael numbers.

A Little Additive Number Theory

If $G = \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ is a finite abelian group with $n_i \mid n_{i+1}$ for each $1 \leq i < k$, then set

$$M(G) = [\sum_{i+1}^{k}(n_i - 1)] + 1.$$

Proposition

Let G be an abelian group.

1. *If $|G| = \infty$, then $D(G) = \infty$.*
2. *If $|G| < \infty$, then $M(G) \leq D(G) \leq |G|$.*

A Little Additive Number Theory

If $G = \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ is a finite abelian group with $n_i \mid n_{i+1}$ for each $1 \leq i < k$, then set

$$M(G) = [\sum_{i+1}^{k} (n_i - 1)] + 1.$$

Proposition

Let G be an abelian group.

1. *If $|G| = \infty$, then $D(G) = \infty$.*
2. *If $|G| < \infty$, then $M(G) \leq D(G) \leq |G|$.*

Davenport Facts

It is possible for the upper inequality in Proposition 9 (2) to be strict.

Erdős conjectured in the mid-sixties that $D(G) = M(G)$. It was not until 1969 that this conjecture was disproved.

The group of smallest order that is a counterexample is

$$G_1 = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6.$$

If G is of rank less than or equal to 2, then $D(G) = M(G)$.

It is unknown whether there is a counterexample of rank 3, and this, in fact, is an active area of research.

Davenport Facts

It is possible for the upper inequality in Proposition 9 (2) to be strict. Erdős conjectured in the mid-sixties that $D(G) = M(G)$. It was not until 1969 that this conjecture was disproved.

The group of smallest order that is a counterexample is

$$G_1 = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6.$$

If G is of rank less than or equal to 2, then $D(G) = M(G)$.

It is unknown whether there is a counterexample of rank 3, and this, in fact, is an active area of research.

Davenport Facts

It is possible for the upper inequality in Proposition 9 (2) to be strict. Erdős conjectured in the mid-sixties that $D(G) = M(G)$. It was not until 1969 that this conjecture was disproved.

The group of smallest order that is a counterexample is

$$G_1 = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6.$$

If G is of rank less than or equal to 2, then $D(G) = M(G)$.

It is unknown whether there is a counterexample of rank 3, and this, in fact, is an active area of research.

Davenport Facts

It is possible for the upper inequality in Proposition 9 (2) to be strict. Erdős conjectured in the mid-sixties that $D(G) = M(G)$. It was not until 1969 that this conjecture was disproved.

The group of smallest order that is a counterexample is

$$G_1 = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6.$$

If G is of rank less than or equal to 2, then $D(G) = M(G)$.

It is unknown whether there is a counterexample of rank 3, and this, in fact, is an active area of research.

Davenport Facts

It is possible for the upper inequality in Proposition 9 (2) to be strict. Erdős conjectured in the mid-sixties that $D(G) = M(G)$. It was not until 1969 that this conjecture was disproved.
The group of smallest order that is a counterexample is

$$G_1 = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6.$$

If G is of rank less than or equal to 2, then $D(G) = M(G)$.
It is unknown whether there is a counterexample of rank 3, and this, in fact, is an active area of research.

A Little More Terminology

Let M be a commutative cancellative monoid in which each nonunit can be written as product of irreducible elements (such a monoid is called *atomic*).

Let $\mathcal{A}(M)$ represent the set of irreducible elements of M and $M^\times$ its set of units.
For $x \in M \backslash M^\times$, set

$$\mathcal{L}(x) = \{n \mid n \in \mathbb{N} \text{ and there exist } x_1, \ldots, x_n \in \mathcal{A}(M) \text{ with } x = x_1 \cdots x_n\}.$$

We will refer to $\mathcal{L}(x)$ as the *set of lengths of* x in M.

A Little More Terminology

Let M be a commutative cancellative monoid in which each nonunit can be written as product of irreducible elements (such a monoid is called *atomic*).

Let $\mathcal{A}(M)$ represent the set of irreducible elements of M and $M^\times$ its set of units.

For $x \in M \backslash M^\times$, set

$$\mathcal{L}(x) = \{n \mid n \in \mathbb{N} \text{ and there exist } x_1, \ldots, x_n \in \mathcal{A}(M) \text{ with } x = x_1 \cdots x_n\}.$$

We will refer to $\mathcal{L}(x)$ as the *set of lengths of* x in M.

A Little More Terminology

Let M be a commutative cancellative monoid in which each nonunit can be written as product of irreducible elements (such a monoid is called *atomic*).

Let $\mathcal{A}(M)$ represent the set of irreducible elements of M and $M^\times$ its set of units.
For $x \in M \backslash M^\times$, set

$$\mathcal{L}(x) = \{n \mid n \in \mathbb{N} \text{ and there exist } x_1, \ldots, x_n \in \mathcal{A}(M) \text{ with } x = x_1 \cdots x_n\}.$$

We will refer to $\mathcal{L}(x)$ as the *set of lengths of* x in M.

A Little More Terminology

Let M be a commutative cancellative monoid in which each nonunit can be written as product of irreducible elements (such a monoid is called *atomic*).

Let $\mathcal{A}(M)$ represent the set of irreducible elements of M and $M^\times$ its set of units.
For $x \in M \backslash M^\times$, set

$$\mathcal{L}(x) = \{n \mid n \in \mathbb{N} \text{ and there exist } x_1, \ldots, x_n \in \mathcal{A}(M) \text{ with } x = x_1 \cdots x_n\}.$$

We will refer to $\mathcal{L}(x)$ as the *set of lengths of* x in M.

A Little More Terminology

We can extend $\mathcal{L}(x)$ to a global descriptor by setting

$$\mathcal{L}(M) = \{\mathcal{L}(x) \mid x \in M \backslash M^{\times}\}.$$

We will refer to $\mathcal{L}(M)$ as the *set of lengths of* M.

There is another popular invariant which describes the variance in length of the factorizations of an element.

For $x \in M \backslash M^{\times}$ set

$$L(x) = \sup\{n \mid \text{there are } x_1, \ldots, x_n \in \mathcal{A}(M) \text{ such that } x = x_1 \cdots x_n\}$$

and

$$l(x) = \inf\{n \mid \text{there are } x_1, \ldots, x_n \in \mathcal{A}(M) \text{ such that } x = x_1 \cdots x_n\}.$$

A Little More Terminology

We can extend $\mathcal{L}(x)$ to a global descriptor by setting

$$\mathcal{L}(M) = \{\mathcal{L}(x) \mid x \in M \backslash M^{\times}\}.$$

We will refer to $\mathcal{L}(M)$ as the *set of lengths of* M.

There is another popular invariant which describes the variance in length of the factorizations of an element.

For $x \in M \backslash M^{\times}$ set

$$L(x) = \sup\{n \mid \text{there are } x_1, \ldots, x_n \in \mathcal{A}(M) \text{ such that } x = x_1 \cdots x_n\}$$

and

$$l(x) = \inf\{n \mid \text{there are } x_1, \ldots, x_n \in \mathcal{A}(M) \text{ such that } x = x_1 \cdots x_n\}.$$

A Little More Terminology

We can extend $\mathcal{L}(x)$ to a global descriptor by setting

$$\mathcal{L}(M) = \{\mathcal{L}(x) \mid x \in M \backslash M^{\times}\}.$$

We will refer to $\mathcal{L}(M)$ as the *set of lengths of* M.

There is another popular invariant which describes the variance in length of the factorizations of an element.

For $x \in M \backslash M^{\times}$ set

$$L(x) = \sup\{n \mid \text{there are } x_1, \ldots, x_n \in \mathcal{A}(M) \text{ such that } x = x_1 \cdots x_n\}$$

and

$$l(x) = \inf\{n \mid \text{there are } x_1, \ldots, x_n \in \mathcal{A}(M) \text{ such that } x = x_1 \cdots x_n\}.$$

A Little More Terminology

We can extend $\mathcal{L}(x)$ to a global descriptor by setting

$$\mathcal{L}(M) = \{\mathcal{L}(x) \mid x \in M \backslash M^{\times}\}.$$

We will refer to $\mathcal{L}(M)$ as the *set of lengths of* M.

There is another popular invariant which describes the variance in length of the factorizations of an element.

For $x \in M \backslash M^{\times}$ set

$$L(x) = \sup\{n \mid \text{there are } x_1, \ldots, x_n \in \mathcal{A}(M) \text{ such that } x = x_1 \cdots x_n\}$$

and

$$l(x) = \inf\{n \mid \text{there are } x_1, \ldots, x_n \in \mathcal{A}(M) \text{ such that } x = x_1 \cdots x_n\}.$$

A Little More Terminology

We can extend $\mathcal{L}(x)$ to a global descriptor by setting

$$\mathcal{L}(M) = \{\mathcal{L}(x) \mid x \in M \backslash M^{\times}\}.$$

We will refer to $\mathcal{L}(M)$ as the *set of lengths of* M.

There is another popular invariant which describes the variance in length of the factorizations of an element.

For $x \in M \backslash M^{\times}$ set

$$L(x) = \sup\{n \mid \text{there are } x_1, \ldots, x_n \in \mathcal{A}(M) \text{ such that } x = x_1 \cdots x_n\}$$

and

$$l(x) = \inf\{n \mid \text{there are } x_1, \ldots, x_n \in \mathcal{A}(M) \text{ such that } x = x_1 \cdots x_n\}.$$

A Little More Terminology

The *elasticity of* x is defined as

$$\rho(x) = \frac{L(x)}{l(x)}.$$

We can again extend this definition to all of M by setting

$$\rho(M) = \sup\{\rho(x) \mid x \in M \backslash M^{\times}\}$$

and call $\rho(M)$ the *elasticity of* M.

A Little More Terminology

The *elasticity of* x is defined as

$$\rho(x) = \frac{L(x)}{l(x)}.$$

We can again extend this definition to all of M by setting

$$\rho(M) = \sup\{\rho(x) \mid x \in M \backslash M^{\times}\}$$

and call $\rho(M)$ the *elasticity of* M.

Questions

Obvious Questions:

(1) Which rings of algebraic integers $\mathcal{O}_K$ are half-factorial?

(2) What is the elasticity of a given ring $\mathcal{O}_K$ of integers?

HARDER QUESTIONS:

(3) What Dedekind domains are half-factorial?

(4) What is the elasticity of a given Dedekind domain?

Questions

Obvious Questions:

(1) Which rings of algebraic integers $\mathcal{O}_K$ are half-factorial?

(2) What is the elasticity of a given ring $\mathcal{O}_K$ of integers?

HARDER QUESTIONS:

(3) What Dedekind domains are half-factorial?

(4) What is the elasticity of a given Dedekind domain?

Questions

Obvious Questions:

(1) Which rings of algebraic integers $\mathcal{O}_K$ are half-factorial?

(2) What is the elasticity of a given ring $\mathcal{O}_K$ of integers?

HARDER QUESTIONS:

(3) What Dedekind domains are half-factorial?

(4) What is the elasticity of a given Dedekind domain?

Questions

Obvious Questions:

(1) Which rings of algebraic integers $\mathcal{O}_K$ are half-factorial?

(2) What is the elasticity of a given ring $\mathcal{O}_K$ of integers?

HARDER QUESTIONS:

(3) What Dedekind domains are half-factorial?

(4) What is the elasticity of a given Dedekind domain?

Questions

Obvious Questions:

(1) Which rings of algebraic integers $\mathcal{O}_K$ are half-factorial?

(2) What is the elasticity of a given ring $\mathcal{O}_K$ of integers?

HARDER QUESTIONS:

(3) What Dedekind domains are half-factorial?

(4) What is the elasticity of a given Dedekind domain?

An Example

Example

To illustrate the above ideas, we can compute the sets of length for the block monoid $\mathcal{B}(\mathbb{Z}_3)$.

If $B = \overline{0}^{x_1}\overline{1}^{x_2}\overline{2}^{x_3}$ is in $\mathcal{B}(G)$, then $x_2 + 2x_3 \equiv 0 \pmod 3$, so $x_2 \equiv x_3 \pmod 3$.

Write $x_2 = 3q_2 + r$ and $x_3 = 3q_3 + r$, where $0 \leq r < 3$.

A calculation involving the irreducible blocks yields

$$\mathcal{L}(B) = \{x_1 + q_2 + q_3 + r + k \mid 0 \leq k \leq \min\{q_2, q_3\}\}$$

and so $\rho(B) = 1 + \min\{q_2, q_3\}/(x_1 + q_2 + q_3 + r)$.

This formula is maximized when $q_2 = q_3$ and $x_1 = r = 0$, so that $\rho(\mathcal{B}(\mathbb{Z}_3)) = 3/2$.

An Example

Example

To illustrate the above ideas, we can compute the sets of length for the block monoid $\mathcal{B}(\mathbb{Z}_3)$.

If $B = \overline{0}^{x_1}\overline{1}^{x_2}\overline{2}^{x_3}$ is in $\mathcal{B}(G)$, then $x_2 + 2x_3 \equiv 0 \pmod 3$, so $x_2 \equiv x_3 \pmod 3$.

Write $x_2 = 3q_2 + r$ and $x_3 = 3q_3 + r$, where $0 \leq r < 3$.

A calculation involving the irreducible blocks yields

$$\mathcal{L}(B) = \{x_1 + q_2 + q_3 + r + k \mid 0 \leq k \leq \min\{q_2, q_3\}\}$$

and so $\rho(B) = 1 + \min\{q_2, q_3\}/(x_1 + q_2 + q_3 + r)$.

This formula is maximized when $q_2 = q_3$ and $x_1 = r = 0$, so that $\rho(\mathcal{B}(\mathbb{Z}_3)) = 3/2$.

An Example

Example

To illustrate the above ideas, we can compute the sets of length for the block monoid $\mathcal{B}(\mathbb{Z}_3)$.

If $B = \overline{0}^{x_1}\overline{1}^{x_2}\overline{2}^{x_3}$ is in $\mathcal{B}(G)$, then $x_2 + 2x_3 \equiv 0 \pmod 3$, so $x_2 \equiv x_3 \pmod 3$.

Write $x_2 = 3q_2 + r$ and $x_3 = 3q_3 + r$, where $0 \leq r < 3$.

A calculation involving the irreducible blocks yields

$$\mathcal{L}(B) = \{x_1 + q_2 + q_3 + r + k \mid 0 \leq k \leq \min\{q_2, q_3\}\}$$

and so $\rho(B) = 1 + \min\{q_2, q_3\}/(x_1 + q_2 + q_3 + r)$.

This formula is maximized when $q_2 = q_3$ and $x_1 = r = 0$, so that $\rho(\mathcal{B}(\mathbb{Z}_3)) = 3/2$.

An Example

Example

To illustrate the above ideas, we can compute the sets of length for the block monoid $\mathcal{B}(\mathbb{Z}_3)$.

If $B = \overline{0}^{x_1}\overline{1}^{x_2}\overline{2}^{x_3}$ is in $\mathcal{B}(G)$, then $x_2 + 2x_3 \equiv 0 \pmod 3$, so $x_2 \equiv x_3 \pmod 3$.

Write $x_2 = 3q_2 + r$ and $x_3 = 3q_3 + r$, where $0 \leq r < 3$.

A calculation involving the irreducible blocks yields

$$\mathcal{L}(B) = \{x_1 + q_2 + q_3 + r + k \mid 0 \leq k \leq \min\{q_2, q_3\}\}$$

and so $\rho(B) = 1 + \min\{q_2, q_3\}/(x_1 + q_2 + q_3 + r)$.

This formula is maximized when $q_2 = q_3$ and $x_1 = r = 0$, so that $\rho(\mathcal{B}(\mathbb{Z}_3)) = 3/2$.

An Example

Example

To illustrate the above ideas, we can compute the sets of length for the block monoid $\mathcal{B}(\mathbb{Z}_3)$.

If $B = \overline{0}^{x_1}\overline{1}^{x_2}\overline{2}^{x_3}$ is in $\mathcal{B}(G)$, then $x_2 + 2x_3 \equiv 0 \pmod 3$, so $x_2 \equiv x_3 \pmod 3$.

Write $x_2 = 3q_2 + r$ and $x_3 = 3q_3 + r$, where $0 \le r < 3$.

A calculation involving the irreducible blocks yields

$$\mathcal{L}(B) = \{x_1 + q_2 + q_3 + r + k \mid 0 \le k \le \min\{q_2, q_3\}\}$$

and so $\rho(B) = 1 + \min\{q_2, q_3\}/(x_1 + q_2 + q_3 + r)$.

This formula is maximized when $q_2 = q_3$ and $x_1 = r = 0$, so that $\rho(\mathcal{B}(\mathbb{Z}_3)) = 3/2$.

How To Compute Elasticities of Dededkind Domains

Geroldinger's Theorem

Let D be a Dedekind domain with divisor class group $G = \mathcal{C}(D)$, D^* the multiplicative monoid of D and S be the set of divisor classes of $\mathcal{C}(D)$ containing prime ideals. Suppose further that for $x \in D^*$, we have $(x) = P_1 \cdots P_k$ for not necessary distinct prime ideals $P_1, \ldots, P_k$ of D. The function

$$\varphi : D^* \to \mathcal{B}(G, S)$$

defined by

$$\varphi(x) = [P_1] \cdots [P_k]$$

is a well-defined monoid homomorphism that is surjective and preserves lengths of factorizations into irreducibles (i.e., $\mathcal{L}(x) = \mathcal{L}(\varphi(x))$ for each $x \in D^*$). Hence

$$\mathcal{L}(D) = \mathcal{L}(\mathcal{B}(G, S)).$$

Implications of Geroldinger's Theorem

Geroldinger's Theorem can be extended to include the more general class of *Krull domains*.

When $D = \mathcal{O}_K$ is the ring of integers of a finite extension K of the rationals, we earlier established that $S = G$, so Geroldinger's Theorem establishes a correspondence between $\mathcal{O}_K$ and the full block monoid $\mathcal{B}(G)$ over the class group. The following well-known theorem of Carlitz now follows as a corollary to Geroldinger's Theorem.

Carlitz's Theorem

Let $\mathcal{O}_K$ be the ring of integers in a finite extension of the rationals. Then $\mathcal{O}_K$ is half-factorial if and only if the class number of $\mathcal{O}_K$ is less than or equal to 2. Equivalently, $\mathcal{O}_K$ is half-factorial if and only if $|\mathcal{C}(\mathcal{O}_K)| \leq 2$.

Implications of Geroldinger's Theorem

Geroldinger's Theorem can be extended to include the more general class of *Krull domains*.

When $D = \mathcal{O}_K$ is the ring of integers of a finite extension K of the rationals, we earlier established that $S = G$, so Geroldinger's Theorem establishes a correspondence between $\mathcal{O}_K$ and the full block monoid $\mathcal{B}(G)$ over the class group. The following well-known theorem of Carlitz now follows as a corollary to Geroldinger's Theorem.

Carlitz's Theorem

Let $\mathcal{O}_K$ be the ring of integers in a finite extension of the rationals. Then $\mathcal{O}_K$ is half-factorial if and only if the class number of $\mathcal{O}_K$ is less than or equal to 2. Equivalently, $\mathcal{O}_K$ is half-factorial if and only if $|\mathcal{C}(\mathcal{O}_K)| \leq 2$.

Implications of Geroldinger's Theorem

Geroldinger's Theorem can be extended to include the more general class of *Krull domains*.

When $D = \mathcal{O}_K$ is the ring of integers of a finite extension K of the rationals, we earlier established that $S = G$, so Geroldinger's Theorem establishes a correspondence between $\mathcal{O}_K$ and the full block monoid $\mathcal{B}(G)$ over the class group. The following well-known theorem of Carlitz now follows as a corollary to Geroldinger's Theorem.

Carlitz's Theorem

Let $\mathcal{O}_K$ be the ring of integers in a finite extension of the rationals. Then $\mathcal{O}_K$ is half-factorial if and only if the class number of $\mathcal{O}_K$ is less than or equal to 2. Equivalently, $\mathcal{O}_K$ is half-factorial if and only if $|\mathcal{C}(\mathcal{O}_K)| \leq 2$.

On Elasticity

Proposition

Let D be a Dedekind domain with class group G and S defined as above. Assume further that $\mid G \mid < \infty$ and $G \neq \{0\}$.

1. *If $S \neq \{0\}$, then $\rho(D) \leq \frac{D(G,S)}{2}$.*
2. *If $G = S$, then $\rho(D) = \frac{D(G)}{2}$. Moreover, in this case there is an $x \in D^*$ with $\rho(x) = \rho(D)$.*

Sketch of Proof: By Geroldinger's Theorem, we can pass to $\mathcal{B}(G, S)$.
If $B \in \mathcal{B}(G, S)$, then write it as $B = g_1 \cdots g_n$.
The shortest factorization of B is greater than $n/D(G, S)$ and the longest less than $n/2$.
Hence, $\rho(\mathcal{B}(G, S)) \leq \frac{n/2}{n/D(G,S)} = \frac{D(G,S)}{2}$.

On Elasticity

Proposition

Let D be a Dedekind domain with class group G and S defined as above. Assume further that $|G| < \infty$ and $G \neq \{0\}$.

1. *If $S \neq \{0\}$, then $\rho(D) \leq \frac{D(G,S)}{2}$.*
2. *If $G = S$, then $\rho(D) = \frac{D(G)}{2}$. Moreover, in this case there is an $x \in D^*$ with $\rho(x) = \rho(D)$.*

Sketch of Proof: By Geroldinger's Theorem, we can pass to $\mathcal{B}(G, S)$.

If $B \in \mathcal{B}(G, S)$, then write it as $B = g_1 \cdots g_n$.

The shortest factorization of B is greater than $n/D(G, S)$ and the longest less than $n/2$.

Hence, $\rho(\mathcal{B}(G, S)) \leq \frac{n/2}{n/D(G,S)} = \frac{D(G,S)}{2}$.

On Elasticity

Proposition

Let D be a Dedekind domain with class group G and S defined as above. Assume further that $|G| < \infty$ and $G \neq \{0\}$.

1. *If $S \neq \{0\}$, then $\rho(D) \leq \frac{D(G,S)}{2}$.*
2. *If $G = S$, then $\rho(D) = \frac{D(G)}{2}$. Moreover, in this case there is an $x \in D^*$ with $\rho(x) = \rho(D)$.*

Sketch of Proof: By Geroldinger's Theorem, we can pass to $\mathcal{B}(G, S)$. If $B \in \mathcal{B}(G, S)$, then write it as $B = g_1 \cdots g_n$.

The shortest factorization of B is greater than $n/D(G, S)$ and the longest less than $n/2$.

Hence, $\rho(\mathcal{B}(G, S)) \leq \frac{n/2}{n/D(G,S)} = \frac{D(G,S)}{2}$.

On Elasticity

Proposition

Let D be a Dedekind domain with class group G and S defined as above. Assume further that $\mid G \mid < \infty$ and $G \neq \{0\}$.

1. *If $S \neq \{0\}$, then $\rho(D) \leq \frac{D(G,S)}{2}$.*
2. *If $G = S$, then $\rho(D) = \frac{D(G)}{2}$. Moreover, in this case there is an $x \in D^*$ with $\rho(x) = \rho(D)$.*

Sketch of Proof: By Geroldinger's Theorem, we can pass to $\mathcal{B}(G, S)$.
If $B \in \mathcal{B}(G, S)$, then write it as $B = g_1 \cdots g_n$.
The shortest factorization of B is greater than $n/D(G, S)$ and the longest less than $n/2$.
Hence, $\rho(\mathcal{B}(G, S)) \leq \frac{n/2}{n/D(G,S)} = \frac{D(G,S)}{2}$.

On Elasticity

Proposition

Let D be a Dedekind domain with class group G and S defined as above. Assume further that $\mid G \mid < \infty$ and $G \neq \{0\}$.

1. *If $S \neq \{0\}$, then $\rho(D) \leq \frac{D(G,S)}{2}$.*
2. *If $G = S$, then $\rho(D) = \frac{D(G)}{2}$. Moreover, in this case there is an $x \in D^*$ with $\rho(x) = \rho(D)$.*

Sketch of Proof: By Geroldinger's Theorem, we can pass to $\mathcal{B}(G, S)$.
If $B \in \mathcal{B}(G, S)$, then write it as $B = g_1 \cdots g_n$.
The shortest factorization of B is greater than $n/D(G, S)$ and the longest less than $n/2$.
Hence, $\rho(\mathcal{B}(G, S)) \leq \frac{n/2}{n/D(G,S)} = \frac{D(G,S)}{2}$.

Valenza's Theorem

The last result leads to an easy proof of a well-known extension of Carlitz's Theorem by Valenza.

Valenza's Theorem

Let $\mathcal{O}_K$ be the ring of integers in a finite extension of the rationals. Then

$$\rho(\mathcal{O}_K) = \frac{D(\mathcal{C}(\mathcal{O}_K))}{2}.$$

Valenza's Theorem

The last result leads to an easy proof of a well-known extension of Carlitz's Theorem by Valenza.

Valenza's Theorem

Let $\mathcal{O}_K$ be the ring of integers in a finite extension of the rationals. Then

$$\rho(\mathcal{O}_K) = \frac{D(\mathcal{C}(\mathcal{O}_K))}{2}.$$