

Monoids and Combinatorics III

Paul Baginski

University of California, Berkeley

The Art of Factorization in Multiplicative Structures

Trinity University, San Antonio, Texas

24 May 2007

Transfer Homomorphisms

Definition

A monoid homomorphism $\phi : M \rightarrow N$ is a *transfer homomorphism* if 1) every element of N is associate to an element of $\phi(M)$, and 2) whenever $\phi(x) = ab$ then there are $y, z \in M$ such that $yz = x$ and $\phi(y)$ is associate to a and $\phi(z)$ is associate to b .

Krull Monoid

Definition

M is a *Krull monoid* if there exists a free abelian monoid D and a homomorphism $\delta : M \rightarrow D$ such that:

- 1 $x|y$ in M if $\delta(x)|\delta(y)$ in D , and
- 2 every $\beta \in D$ is the gcd of some finite set of elements in $\delta(M)$.

In this case, $D/\delta(M)$ forms a group, known as the *class group* of M .

Krull Monoid

Definition

M is a *Krull monoid* if there exists a free abelian monoid D and a homomorphism $\delta : M \rightarrow D$ such that:

- 1 $x|y$ in M if $\delta(x)|\delta(y)$ in D , and
- 2 every $\beta \in D$ is the gcd of some finite set of elements in $\delta(M)$.

In this case, $D/\delta(M)$ forms a group, known as the *class group* of M .

Why is it called the class group?

Analogy with Number Theory

Can think of M lying inside D , which is free abelian so factorial.
That means every atom of D is prime in D .

Analogy with Number Theory

Can think of M lying inside D , which is free abelian so factorial. That means every atom of D is prime in D . Every element of M is a unique product of these primes of D . So this allows us to define:

For every $p \in D$ prime, consider

$$P_p = \{x \in M : p|x\}$$

This is an ideal of M which is not principal unless $p \in M$.

Analogy with Number Theory

Can think of M lying inside D , which is free abelian so factorial. That means every atom of D is prime in D . Every element of M is a unique product of these primes of D . So this allows us to define:

For every $p \in D$ prime, consider

$$P_p = \{x \in M : p|x\}$$

This is an ideal of M which is not principal unless $p \in M$.

These ideals have a natural multiplication and every ideal I of M can be decomposed uniquely as a product of these ideals, using the gcd. D factorial ensures that $\gcd(P_{p_1} \cdots P_{p_k}) = p_1 \cdots p_k$.

Analogy continued

We are interested when the products of the P_p yield principal ideals (m) for $m \in M$. This corresponds exactly to when the product of the primes p lands in M .

Analogy continued

We are interested when the products of the P_p yield principal ideals (m) for $m \in M$. This corresponds exactly to when the product of the primes p lands in M .

So the monoid of ideals P_p under multiplication, has the submonoid of principal ideals (m) of M . Relate ideals $I \sim J$ iff $(m)I = (m')J$ and quotient out to get a class group construction analogous to number theory. But this quotient is just D/M .

Classic Example

Consider \mathcal{O}_K , the ring of integers of an algebraic number field. Then D is the class of all ideals of \mathcal{O}_K , G is the usual class group, and so factorization in \mathcal{O}_K corresponds to factoring corresponding blocks in $\mathcal{B}(G)$.

General Picture for Krull Monoids

M is a Krull monoid, D its monoid of divisors and G is the class group.

$$M \hookrightarrow D = D^\times \times \mathcal{F}(P)$$

and $M \rightarrow \mathcal{B}(G)$ is a transfer homomorphism.

General Picture for Krull Monoids

M is a Krull monoid, D its monoid of divisors and G is the class group.

$$\begin{array}{ccc} M & \hookrightarrow & D = D^\times \times \mathcal{F}(P) \\ \downarrow & & \downarrow \\ \mathcal{B}(G) & \hookrightarrow & D^\times \times \mathcal{F}(G) \end{array}$$

and $M \rightarrow \mathcal{B}(G)$ is a transfer homomorphism.

Can quotient out units (M^\times and D^\times) from this picture.

Motivating Scenario for C-monoids

R is a Noetherian domain with integral closure \hat{R} . D is the monoid of ideals generated by all height 1 prime ideals of R , which is abelian. So

$$D \cong \coprod_{\mathfrak{p} \text{ height } 1} R_{\mathfrak{p}}/R_{\mathfrak{p}}^{\times}$$

Goal is to show that D has large factorial part.

Motivating Scenario for C-monoids

R is a Noetherian domain with integral closure \hat{R} . D is the monoid of ideals generated by all height 1 prime ideals of R , which is abelian. So

$$D \cong \coprod_{\mathfrak{p} \text{ height } 1} R_{\mathfrak{p}}/R_{\mathfrak{p}}^{\times}$$

Goal is to show that D has large factorial part.

We also want $\mathfrak{f} = (R : \hat{R})$ nontrivial, so that some prime ideals of R split in \hat{R} .

Localizations

If $\mathfrak{p} \not\supseteq \mathfrak{f}$, then \mathfrak{p} has exactly one prime ideal \mathfrak{q} above it in \hat{R} (and \mathfrak{q} is height 1 in \hat{R}). So $\hat{R}_{\mathfrak{q}}$ is a DVR, and $R_{\mathfrak{p}}$ embeds inside it, so is also a DVR. Any DVR quotiented out by its units has multiplicative structure isomorphic to $(\mathbb{N}_0, +)$.

Localizations

If $\mathfrak{p} \not\supseteq \mathfrak{f}$, then \mathfrak{p} has exactly one prime ideal \mathfrak{q} above it in \hat{R} (and \mathfrak{q} is height 1 in \hat{R}). So $\hat{R}_{\mathfrak{q}}$ is a DVR, and $R_{\mathfrak{p}}$ embeds inside it, so is also a DVR. Any DVR quotiented out by its units has multiplicative structure isomorphic to $(\mathbb{N}_0, +)$.

So if $P = \{\mathfrak{p} \mid \mathfrak{p} \not\supseteq \mathfrak{f}\}$ and $\bar{P} = \{\mathfrak{p} \mid \mathfrak{p} \supseteq \mathfrak{f}\}$, then

$$D \cong \prod_{\mathfrak{p} \text{ height } 1} R_{\mathfrak{p}}/R_{\mathfrak{p}}^{\times} = \mathcal{F}(P) \times \prod_{\mathfrak{p} \in \bar{P}} R_{\mathfrak{p}}/R_{\mathfrak{p}}^{\times} = \mathcal{F}(P) \times \prod_{\mathfrak{p} \in \bar{P}} R_{\mathfrak{p}}/R_{\mathfrak{p}}^{\times}$$

General Picture

R is a (reduced) monoid, D its monoid of divisors and G is the class semigroup. We set $T = \prod_{p \in \bar{P}} R_p / R_p^\times$.

$$\begin{array}{ccc}
 R & \hookrightarrow & \mathcal{F}(P) \times T \\
 \downarrow & & \downarrow \\
 & \hookrightarrow &
 \end{array}$$

and $M \rightarrow$ is a transfer homomorphism.

General Picture

R is a (reduced) monoid, D its monoid of divisors and G is the class semigroup. We set $T = \prod_{p \in \bar{P}} R_p / R_p^\times$.

$$\begin{array}{ccc}
 R & \hookrightarrow & \mathcal{F}(P) \times T \\
 \downarrow & & \downarrow \\
 & \hookrightarrow & \mathcal{F}(G) \times T
 \end{array}$$

and $M \rightarrow$ is a transfer homomorphism.

General Picture

R is a (reduced) monoid, D its monoid of divisors and G is the class semigroup. We set $T = \prod_{p \in \bar{P}} R_p / R_p^\times$.

$$\begin{array}{ccc} R & \hookrightarrow & \mathcal{F}(P) \times T \\ \downarrow & & \downarrow \\ \mathcal{B}(G, T, \iota) & \hookrightarrow & \mathcal{F}(G) \times T \end{array}$$

and $M \rightarrow \mathcal{B}(G, T, \iota)$ is a transfer homomorphism.

Here $\mathcal{B}(G, T, \iota)$ is defined as:

$$\left\{ s_1 \cdots s_k t \mid s_i \in G, t \in T, \sum_{i=1}^k s_i + \sum_{p \in \bar{P}} \iota(t_p) = 0 \right\}$$

$$\mathbb{Z}[\sqrt{-7}]$$

Let's consider $R = \mathbb{Z}[\sqrt{-7}]$. Its field of fractions is $\mathbb{Q}(\sqrt{-7})$, whose ring of algebraic integers is

$$\hat{R} = \mathbb{Z} \left[\frac{1 + \sqrt{-7}}{2} \right]$$

What are the factorization properties of R ? E.g. elasticity, catenary degree?

Conductor

$$\mathfrak{f} = (R : \hat{R}) = \{r \in R \mid r\hat{R} \subseteq R\}$$

So we need $(a + b\sqrt{-7})(\frac{c}{2} + \frac{d}{2}\sqrt{-7}) \in R$ for every $c, d \in \mathbb{Z}$ of the same parity.

Conductor

$$\mathfrak{f} = (R : \hat{R}) = \{r \in R \mid r\hat{R} \subseteq R\}$$

So we need $(a + b\sqrt{-7})(\frac{c}{2} + \frac{d}{2}\sqrt{-7}) \in R$ for every $c, d \in \mathbb{Z}$ of the same parity.

Clearly if $2|a$ and $2|b$, then this happens, so $\mathfrak{f} \supseteq (2)$. By a norm argument, (2) is maximal in $\mathbb{Z}[\sqrt{-7}]$, so we have equality.

Conductor

$$\mathfrak{f} = (R : \hat{R}) = \{r \in R \mid r\hat{R} \subseteq R\}$$

So we need $(a + b\sqrt{-7})(\frac{c}{2} + \frac{d}{2}\sqrt{-7}) \in R$ for every $c, d \in \mathbb{Z}$ of the same parity.

Clearly if $2|a$ and $2|b$, then this happens, so $\mathfrak{f} \supseteq (2)$. By a norm argument, (2) is maximal in $\mathbb{Z}[\sqrt{-7}]$, so we have equality.

Since $\mathfrak{f} = (2)$ is maximal in R , we see $\bar{P} = \{(2)\}$. In \hat{R} , (2) splits as $(2) = (\omega)(\bar{\omega})$, where

$$\omega = \frac{1 + \sqrt{-7}}{2}, \quad \bar{\omega} = \frac{1 - \sqrt{-7}}{2}$$

Plugging In

$$\begin{array}{ccc}
 R = \mathbb{Z}[\sqrt{-7}] & \hookrightarrow & \mathcal{F}(P) \times R_{(2)}/R_{(2)}^{\times} \\
 \downarrow & & \downarrow \\
 \mathcal{B}(G, T, \iota) & \hookrightarrow & \mathcal{F}(G) \times R_{(2)}/R_{(2)}^{\times}
 \end{array}$$

Class group

It turns out that $G = \{0\}$. So

$$\mathcal{B}(G, T, \iota) = \left\{ s_1 \cdots s_k t \mid s_i \in G, t \in T, \sum_{i=1}^k s_i + \sum_{p \in \bar{P}} \iota(t_p) = 0 \right\}$$

Class group

It turns out that $G = \{0\}$. So

$$\begin{aligned} \mathcal{B}(G, T, \iota) &= \left\{ s_1 \cdots s_k t \mid s_i \in G, t \in T, \sum_{i=1}^k s_i + \sum_{p \in \bar{P}} \iota(t_p) = 0 \right\} \\ &= \mathcal{F}(G) \times R_{(2)}/R_{(2)}^{\times} \\ &\cong \mathbb{N}_0 \times R_{(2)}/R_{(2)}^{\times} \end{aligned}$$

Full Picture

$$\begin{array}{ccc} R = \mathbb{Z}[\sqrt{-7}] & \hookrightarrow & \mathcal{F}(P) \times R_{(2)}/R_{(2)}^{\times} \\ \downarrow & & \downarrow \\ \mathbb{N}_0 \times R_{(2)}/R_{(2)}^{\times} & = & \mathbb{N}_0 \times R_{(2)}/R_{(2)}^{\times} \end{array}$$

Monoid Incognito!

Need to understand $\mathbb{N}_0 \times R_{(2)}/R_{(2)}^x$.

Monoid Incognito!

Need to understand $\mathbb{N}_0 \times R_{(2)}/R_{(2)}^\times$.

Every element of $R_{(2)}$ is either a unit, or else a unit times $\omega^v \bar{\omega}^w$ for some $v, w \geq 1$. This representation is unique.

Monoid Incognito!

Need to understand $\mathbb{N}_0 \times R_{(2)}/R_{(2)}^x$.

Every element of $R_{(2)}$ is either a unit, or else a unit times $\omega^v \bar{\omega}^w$ for some $v, w \geq 1$. This representation is unique.

So $R_{(2)}/R_{(2)}^x \cong (\mathbb{N}^2 \cup \{(0, 0)\}, +)$.

Properties

In $M = \mathbb{N}^2 \cup \{(0, 0)\}$, all the irreducibles are precisely elements of the form $(n, 1)$ and $(1, m)$.

Properties

In $M = \mathbb{N}^2 \cup \{(0, 0)\}$, all the irreducibles are precisely elements of the form $(n, 1)$ and $(1, m)$.

If we have a non-unit of M , it is of the form (n, m) for $n, m \geq 2$, so it has a factorization into irreducibles as:

$(n, m) = (n - 1, 1)(1, m - 1)$. Therefore $\rho(M) = \infty$.

Properties

In $M = \mathbb{N}^2 \cup \{(0, 0)\}$, all the irreducibles are precisely elements of the form $(n, 1)$ and $(1, m)$.

If we have a non-unit of M , it is of the form (n, m) for $n, m \geq 2$, so it has a factorization into irreducibles as:

$(n, m) = (n - 1, 1)(1, m - 1)$. Therefore $\rho(M) = \infty$.

This also gives us that the catenary degree of M is $c(M) = 3$.

Properties

In $M = \mathbb{N}^2 \cup \{(0, 0)\}$, all the irreducibles are precisely elements of the form $(n, 1)$ and $(1, m)$.

If we have a non-unit of M , it is of the form (n, m) for $n, m \geq 2$, so it has a factorization into irreducibles as:

$$(n, m) = (n - 1, 1)(1, m - 1). \text{ Therefore } \rho(M) = \infty.$$

This also gives us that the catenary degree of M is $c(M) = 3$.

These properties transfer back to $\mathbb{Z}[\sqrt{-7}]$.