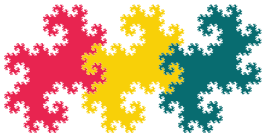
DOCTORAL PROGRAM
DISCRETE MATHEMATICS



TU & KFU GRAZ • MU LEOBEN
AUSTRIA

UNI GRAZ

Sets of Lengths in Krull monoids

Alfred Geroldinger

2015 International Meeting
AMS / EMS / SPM

Special Session on
Commutative Monoids
Porto, 2015

Outline

Sets of lengths in monoids

Let H be a multiplicatively written, commutative, cancellative semigroup, and let $a \in H$ be a non-unit.

- If $a = u_1 \cdot \ldots \cdot u_k$ where $u_1, \ldots, u_k$ are irreducibles (atoms), then k is called the length of the factorization.
- $\mathsf{L}(a) = \{k \mid a \text{ has a factorization of length } k\} \subset \mathbb{N}$ is the set of lengths of a.
- If $\mathsf{L}(a) = \{k_1, k_2, k_3, \ldots\}$ with $k_1 < k_2 < k_3 < \ldots$, then

$$\Delta\big(\mathsf{L}(a)\big) = \{k_2 - k_1, k_3 - k_2, \ldots\}$$

is the set of distances of $\mathsf{L}(a)$, and

$$\Delta(H) = \bigcup_{a \in H} \Delta\big(\mathsf{L}(a)\big) \subset \mathbb{N}$$

the set of distances of H.

The system of sets of lengths

MAIN TOPIC: Study the system of sets of lengths

$$\mathcal{L}(H) = \{\mathsf{L}(a) \mid a \in H\}$$

for Krull monoids H.

SIMPLE FACTS:

- H is half-factorial if $|L| = 1$ for all $a \in H$.
  By definition, H is half-factorial iff $\Delta(H) = \emptyset$.
- $\Delta(H) = \{d\}$ iff all sets of lengths are APs (arithmetical progressions) with difference d.
- If $|\mathsf{L}(a)| \geq 2$, then $|\mathsf{L}(a^m)| > m$ for each $m \in \mathbb{N}$.
- Let H be v-noetherian (ACC on divisorial ideals holds).
  - All sets of lengths are finite and nonempty.
  - EITHER H is half-factorial
    OR for every $m \in \mathbb{N}$ there is an $L \in \mathcal{L}(H)$ such that $|L| \geq m$.

Outline

Basics: Divisor homomorphisms and more

For any set P, $\mathcal{F}(P)$ is the free abelian monoid with basis P, and

$$a = \prod_{p \in P} p^{\mathsf{v}_p(a)} \in \mathcal{F}(P)\,.$$

A monoid homomorphism $\varphi\colon H \to D$ is said to be a

- divisor homomorphism if, for all $a, b \in H$,

$$a \,|\, b \text{ in } H \quad \text{if and only if} \quad \varphi(a) \,|\, \varphi(b) \text{ in } D\,.$$

- divisor theory if
  - φ is a divisor homomorphism,
  - $D = \mathcal{F}(P)$ is free abelian,
  - For every $p \in P$, there are $a_1, \ldots, a_m \in H$ such that $p = \gcd\big(\varphi(a_1), \ldots, \varphi(a_m)\big)$.

Characterization of Krull monoids

A monoid H is called a Krull monoid if it satisfies one of the following equivalent conditions:

(a) H is v-noetherian and completely integrally closed.

(b) H is v-noetherian and every non-empty v-ideal is v-invertible.

(c) The map $\partial\colon H \to \mathcal{I}_v^*(H)$ is a divisor theory.

(d) H has a divisor theory.

(e) There is a divisor homomorphism $\varphi\colon H \to \mathcal{F}(P)$.

- **Uniqueness:** If $\varphi_i\colon H \to D_i$ are divisor theories, then there is a unique isomorphism $\Phi\colon D_1 \to D_2$ such that $\Phi \circ \varphi_1 = \varphi_2$.
- A monoid H is Krull if and only if $H_{\mathrm{red}} = H/H^\times$ is Krull.

Class groups

If $H \hookrightarrow D = \mathcal{F}(P)$ is a divisor theory, then

$$G = \mathcal{C}(H) = \mathsf{q}(D)/\mathsf{q}(H)$$

is the (divisor) class group of H and

$$G_P = \{[p] = p\mathsf{q}(H) \mid p \in P\} \subset \mathcal{C}(H)$$

is the set of classes containing prime divisors.

FACTS:

- Since $\partial\colon H \to \mathcal{I}_v^*(H)$ is a divisor theory, we have

$$\mathcal{C}_v(H) = \mathsf{q}(\mathcal{I}_v^*(H))/\mathsf{q}(\{aH \mid a \in H\}) \cong \mathcal{C}(H)\,.$$

- A reduced Krull monoid is uniquely determined (up to isomorphism) by its class group and the number of prime divisors in the classes.

Examples: Ring theory

Domains: Let R be a domain. Then $(R^\bullet = R \setminus \{0\}, \cdot)$ is a monoid.

- R is a Krull domain if and only if $R^\bullet$ is a Krull monoid (Krause, Wauters, 1990s)
- The monoid algebra $R[H]$ is Krull if and only if R is Krull and H is Krull (for a reduced monoid H) (Chouinard: 1981)
- Integrally closed noetherian domains are Krull.
  - One-dimensional Krull: Dedekind domains
  - Higher dimensional Krull: affine K-algebras, rings of invariants

Submonoids of Domains: Regular congruence monoids in Krull domains are Krull.

Example: Let R be a non-principal order in a Dedekind domain $\overline{R}$ with conductor $\mathfrak{f} = (R : \overline{R})$. Then

$$H = \{a \in R^\bullet \mid aR + \mathfrak{f} = R\}$$

is a Krull monoid.

Examples: Module Theory

Let R be a commutative ring, $\mathcal{C}$ a class of R-modules closed under ismorphisms, finite direct sums and direct summands.
For a module M, let $[M]$ denote its ismorphism class.
Then

$$H = \{[M] \mid M \in \mathcal{C}\}$$

is an additive semigroup where addition is defined as

$$[M] + [N] = [M \oplus N]\,.$$

Theorem

- *(Krull-Schmidt 1930s) If $\mathrm{End}_R(M)$ is local for all $M \in \mathcal{C}$ (e.g., all M have finite length), then H is factorial.*
- *(Facchini, Herbera, Wiegand, 2000s) If $\mathrm{End}_R(M)$ is semilocal for all $M \in \mathcal{C}$, then H is a Krull monoid.*

More Examples

Rings with zero-divisors: Krull rings with zero divisors: Huckaba; Anderson, Chang, Kang, Kennedy, G., ...

Theorem

A v-Marot ring is a Krull ring if and only if the monoid of regular elements is a Krull monoid.

Finitely generated monoids:

- A finitely generated monoid is Krull iff it is root closed (normal).
- In particular, an affine monoid is Krull iff it is normal.

Monoids of Zero-Sum Sequences

Let G be an additively written abelian group.

- A sequence $S = (g_1, \ldots, g_\ell)$ over G: finite, unordered sequence of terms from G, repetition allowed.
- S has sum zero if $\sigma(S) = g_1 + \ldots + g_\ell = 0$.
- The set of (zero-sum) sequences is a monoid with concatenation of sequences as the operation. Indeed, consider sequences as elements of the free abelian monoid $\mathcal{F}(G)$. Then

$$\mathcal{B}(G) = \{S \in \mathcal{F}(G) \mid \sigma(S) = 0\} \hookrightarrow \mathcal{F}(G)$$

  is a Krull monoid (with class group isomorphic to G).
- The set $\mathcal{A}(G)$ of minimal zero-sum sequences is the set of irreducible elements of the monoid $\mathcal{B}(G)$.

The universal character of $\mathcal{B}(G)$

Proposition

1. *(Classic) If H is Krull with class group G such that each class contains a prime divisor, then $\mathcal{L}(H) = \mathcal{L}\big(\mathcal{B}(G)\big)$.*
2. *(Smertnig, J. Algebra 2013) Let $\mathcal{O}$ be a holomorphy ring in a global field K, A a central simple algebra over K, and H a classical maximal $\mathcal{O}$-order of A such that every stably free left R-ideal is free. Then $\mathcal{L}(H) = \mathcal{L}\big(\mathcal{B}(G)\big)$ for some finite abelian group G.*
3. *Let H be a seminormal order in a holomorphy ring of a global field with principal order $\widehat{H}$ such that the natural map $\mathfrak{X}(\widehat{H}) \to \mathfrak{X}(H)$ is bijective and there is an isomorphism $\overline{\vartheta}\colon \mathcal{C}_v(H) \to \mathcal{C}_v(\widehat{H})$ between the v-class groups. Then $\mathcal{L}(H) = \mathcal{L}\big(\mathcal{B}(G)\big)$ for some finite abelian group G.*

Outline

Arithmetical Characterization of Class Groups

Classical Philosophy in Algebraic Number Theory:

The class group determines the arithmetic.

If H is a ring of integers with class group G, then

- $\mathcal{L}(H) = \mathcal{L}(\mathcal{B}(G))$.
- H is factorial iff $|G| = 1$.
- (Carlitz 1960): H is half-factorial iff $|G| \leq 2$.

Narkiewicz 1970s:

Give arithmetical characterizations of class groups.

Do arithmetical phenomena characterize the class group ?

Kaczorowski, Halter-Koch, Rush, et al., 1980s: Yes, they do !!

The Characterization Problem

Abbreviation: $\mathcal{L}(G) := \mathcal{L}\big(\mathcal{B}(G)\big)$.

Characterization Problem:
Let G and G' be finite abelian groups such that $\mathcal{L}(G) = \mathcal{L}(G')$.

Does it follow that $G \cong G'$?

Observations:

- G and G' are isomorphic if and only if $\mathcal{B}(G)$ and $\mathcal{B}(G')$ are isomorphic.
- Chapman et al. 2007: There are non-isomorphic numerical monoids H and H' such that $\mathcal{L}(H) = \mathcal{L}(H')$.

Main Result

Theorem (G.+ Wolfgang A. Schmid, 2015)

Let G be an abelian group such that $\mathcal{L}(G) = \mathcal{L}(C_{n_1} \oplus C_{n_2})$ where $n_1, n_2 \in \mathbb{N}$ with $n_1 \mid n_2$ and $n_1 + n_2 > 4$. Then

$$G \cong C_{n_1} \oplus C_{n_2} .$$

SIMPLE FACTS:

- $\mathcal{L}(C_1) = \mathcal{L}(C_2) = \big\{\{m\} \mid m \in \mathbb{N}_0\big\}$.
- $\mathcal{L}(C_3) = \mathcal{L}(C_2 \oplus C_2) = \big\{y + 2k + [0, k] \;\big|\; y,\, k \in \mathbb{N}_0\big\}$.

Outline

Methods: Additive Combinatorics

Methods from Combinatorial and Additive Number Theory, as presented in

- M.B. Nathanson: Additive Number Theory I + II
- T. Tao and Van H. Vu: Additive Combinatorics
- A. G. and I. Ruzsa: Combinatorial Number Theory and Additive Group Theory
- D.J. Grynkiewicz: Structural Additive Theory

In particular,

- Addition Theorems: Kneser, Kemperman-Scherk, Grynkiewicz,...
- Polynomial Methods: group algebras,
- Inductive methods
- .....

The Davenport constant of a finite abelian group

The Davenport constant $\mathsf{D}(G)$ is the maximal length of a minimal zero-sum sequence over G, thus

$$\mathsf{D}(G) = \max\{|U| \mid U \in \mathcal{A}(G)\}\,.$$

Equivalently: $\mathsf{D}(G)$ is the smallest integer $\ell \in \mathbb{N}$ such that every sequence S of length $|S| \ge \ell$ has a nontrivial zero-sum subsequence.
Let

$$G = C_{n_1} \oplus \ldots \oplus C_{n_r} \quad \text{with} \quad 1 < n_1 \mid \ldots \mid n_r \qquad \text{and}$$

Some Facts:

1. $\mathsf{D}^*(G) := 1 + \sum_{i=1}^{r}(n_i - 1) \le \mathsf{D}(G)$.
2. 1960s: Equality holds for p-groups, for $r \le 2$ and others.
3. For every $r \ge 4$ there are infinitely many groups G of rank r for which inequality holds.
4. Limited progress for groups of small rank and groups close to p-groups: Bhowmik, Gao, Schlage-Puchta, Schmid, Liebmann-G.-Philipp, Savchev-Chen, ...

The arithmetical significance of the Davenport constant

Fix $k \in \mathbb{N}$ and consider equations of the form

$$U_1 \cdot \ldots \cdot U_k = W_1 \cdot \ldots \cdot W_\ell \, .$$

How large is $\rho_k(G) :=$ the maximal possible ℓ ?
For $k = 2$ we have

$$U_1 U_2 = W_1 \cdot \ldots \cdot W_\ell$$

$$(g_1, \ldots, g_s)(h_1, \ldots, h_t) = (g_1, g_5, h_3)(g_2, h_4, h_7, h_9) \ldots \ldots ,$$

where U_1, U_2, W_j are minimal zero-sum sequences.
A simple counting argument shows that

- $\rho_{2k}(G) = k\mathsf{D}(G)$
- $$1 + k\mathsf{D}(G) \le \rho_{2k+1}(G) \le k\mathsf{D}(G) + \lfloor \frac{\mathsf{D}(G)}{2} \rfloor \, .$$

Structure of minimal zero-sum sequences: Rank two groups

Let $G = C_m \oplus C_{mn}$ with $m, n \in \mathbb{N}$ and $m \geq 2$. A sequence S over G of length $\mathsf{D}(G) = m + mn - 1$ is a minimal zero-sum sequence if and only if it has one of the following two forms:

- $$S = e_1^{\mathsf{ord}(e_1)-1} \prod_{\nu=1}^{\mathsf{ord}(e_2)} (x_\nu e_1 + e_2), \qquad \text{where}$$

  $\{e_1, e_2\}$ is a basis of G, $x_1, \ldots, x_{\mathsf{ord}(e_2)} \in [0, \mathsf{ord}(e_1) - 1]$, and $x_1 + \ldots + x_{\mathsf{ord}(e_2)} \equiv 1 \mod \mathsf{ord}(e_1)$.

- $$S = g_1^{sm-1} g_2^{(n-s)m+1} \prod_{\nu=1}^{m-1} (-x_\nu g_1 + g_2), \qquad \text{where}$$

  $\{g_1, g_2\}$ is a generating set of G with $\mathsf{ord}(g_2) = mn$, $s \in [1, n]$, $x_1, \ldots, x_{m-1} \in [0, m-1]$, $x_1 + \ldots + x_{m-1} = m - 1$, and $\big(s = 1$ or $mg_1 = mg_2\big)$.

First observations

Let G be a finite abelian group.

- If G' is finite abelian with $\mathcal{L}(G) = \mathcal{L}(G')$, then

$$\mathsf{D}(G) = \rho_2(G) = \rho_2(G') = \mathsf{D}(G')\,.$$

- There are only finitely many G' with $\mathcal{L}(G) = \mathcal{L}(G')$.

HOWEVER

Theorem (G.+Halter-Koch 2006)

If $S = g_1 \cdot \ldots \cdot g_\ell$ is a zero-sum sequence and $\{g_1, \ldots, g_\ell\} \subset G$ is a subgroup, then $\mathsf{L}(A)$ is an arithmetical progression with difference 1.

COROLLARY: In every group G, "almost all" sets of lengths are are arithmetical progressions with difference 1!!

AAMPs: Almost Arithmetical Multiprogressions

Let $d \in \mathbb{N}$, $M \in \mathbb{N}_0$ and $\{0, d\} \subset \mathcal{D} \subset [0, d]$.
A subset $L \subset \mathbb{Z}$ is called an

AAMP with difference d, period $\mathcal{D}$, and bound M,

if

$$L = y + (L' \cup L^* \cup L'') \subset y + \mathcal{D} + d\mathbb{Z}$$

where

- $y \in \mathbb{Z}$ is a shift parameter,
- $L' \subset [-M, -1]$ and $L'' \subset \max L^* + [1, M]$, are the (short) beginning and end parts of L,
- L^* is (the) finite nonempty (important and long middle part) with $\min L^* = 0$ and

$$L^* = (\mathcal{D} + d\mathbb{Z}) \cap [0, \max L^*] .$$

Structure Theorem - Realization Theorem

Theorem (Freiman, G., Halter-Koch, Grynkiewicz, Kainrath)

Let G be a finite abelian group.
Then there is a constant $M = M(G) \in \mathbb{N}_0$ such that every set of lengths is an AAMP *with difference $d \in \Delta^*(G)$ and bound M.*

Theorem (Wolfgang A. Schmid, 2009)

Let $M \in \mathbb{N}_0$ and $\Delta \subset \mathbb{N}$ be a finite nonempty set. Then there exists a finite abelian group G such that:
For every AAMP *L with difference $d \in \Delta$ and bound M there is some $y_{H,L} \in \mathbb{N}$ such that*

$$y + L \in \mathcal{L}(G) \quad \text{for all} \quad y \geq y_{H,L}\,.$$