Notions of isoclinism for rings, with applications

3 July 2013

Steve Buckley
Dept of Maths and Stats, NUI Maynooth, Ireland

Noncommutative Rings and their Applications
Lens, 1–4 July 2013

What is isoclinism?

- P. Hall introduced **isoclinism** for groups (1940).
- He generalized it to **isologism** wrt a group variety (also 1940).

What is isoclinism?

- P. Hall introduced **isoclinism** for groups (1940).
- He generalized it to **isologism** wrt a group variety (also 1940).
- These are equivalence relations, coarser than isomorphism, and are important tools in modern group theory.

What is isoclinism?

- P. Hall introduced **isoclinism** for groups (1940).
- He generalized it to **isologism** wrt a group variety (also 1940).
- These are equivalence relations, coarser than isomorphism, and are important tools in modern group theory.
- Analogous isoclinism concepts for:
  - Rings (Kruse and Price, 1969);
  - Lie algebras (Moneyhun, 1994).

What is isoclinism?

- P. Hall introduced **isoclinism** for groups (1940).
- He generalized it to **isologism** wrt a group variety (also 1940).
- These are equivalence relations, coarser than isomorphism, and are important tools in modern group theory.
- Analogous isoclinism concepts for:
  - Rings (Kruse and Price, 1969);
  - Lie algebras (Moneyhun, 1994).
  - These do not appear to be as widely useful as the group concepts.

What is isoclinism?

- P. Hall introduced **isoclinism** for groups (1940).
- He generalized it to **isologism** wrt a group variety (also 1940).
- These are equivalence relations, coarser than isomorphism, and are important tools in modern group theory.
- Analogous isoclinism concepts for:
  - Rings (Kruse and Price, 1969);
  - Lie algebras (Moneyhun, 1994).
  - These do not appear to be as widely useful as the group concepts.
- Here we discuss a **different**, and flexible, concept of isoclinism/isologism.

What is isoclinism?

- P. Hall introduced **isoclinism** for groups (1940).
- He generalized it to **isologism** wrt a group variety (also 1940).
- These are equivalence relations, coarser than isomorphism, and are important tools in modern group theory.
- Analogous isoclinism concepts for:
  - Rings (Kruse and Price, 1969);
  - Lie algebras (Moneyhun, 1994).
  - These do not appear to be as widely useful as the group concepts.
- Here we discuss a **different**, and flexible, concept of isoclinism/isologism.
- Our concept is defined in a **universal algebra context** but has various applications in combinatorial ring theory.

Associativity and spectra

The formal "noncommutative polynomial" $f(X, Y) = aXY + bYX$, $a, b \in \mathbb{Z}$, is a symbol of

$$f^R : R \times R \to R, \qquad f^R(x, y) := axy + byx\,,$$

defined whenever R is a PN (= *possibly nonassociative*) ring. Now let

$$\mathrm{Pr}_f(R) := \frac{|\{(x, y) \in R \times R :\ f^R(x, y) = 0\}|}{|R|^2} \qquad (\text{if } |R| < \infty).$$

Associativity and spectra

The formal "noncommutative polynomial" $f(X,Y) = aXY + bYX$, $a, b \in \mathbb{Z}$, is a symbol of

$$f^R : R \times R \to R, \qquad f^R(x,y) := axy + byx\,,$$

defined whenever R is a PN (= *possibly nonassociative*) ring. Now let

$$\mathrm{Pr}_f(R) := \frac{|\{(x,y) \in R \times R :\ f^R(x,y) = 0\}|}{|R|^2} \qquad (\text{if } |R| < \infty).$$

The ***f*-spectrum** of a class $\mathcal{C}$ of finite PN rings is now

$$\mathfrak{S}_f(\mathcal{C}) := \{\mathrm{Pr}_f(R) \mid R \in \mathcal{C}\}\,.$$

Associativity and spectra

The formal "noncommutative polynomial" $f(X, Y) = aXY + bYX$, $a, b \in \mathbb{Z}$, is a symbol of

$$f^R : R \times R \to R, \qquad f^R(x, y) := axy + byx \,,$$

defined whenever R is a PN (= *possibly nonassociative*) ring. Now let

$$\mathrm{Pr}_f(R) := \frac{|\{(x, y) \in R \times R :\ f^R(x, y) = 0\}|}{|R|^2} \qquad (\text{if } |R| < \infty).$$

The ***f*-spectrum** of a class $\mathcal{C}$ of finite PN rings is now

$$\mathfrak{S}_f(\mathcal{C}) := \{\mathrm{Pr}_f(R) \mid R \in \mathcal{C}\} \,.$$

Associativity makes no difference for any of these spectra!

Theorem 1 (B.)
If $\mathcal{C}_1 := \{\textit{finite rings}\}$, $\mathcal{C}_2 := \{\textit{finite PN rings}\}$, *and* $f(X, Y) := aXY + bYX$, $a, b \in \mathbb{Z}$, *then*

$$\mathfrak{S}_f(\mathcal{C}_1) = \mathfrak{S}_f(\mathcal{C}_2) \,.$$

Spectral containments

We use special names and notation for $\mathrm{Pr}_f(R)$ and $\mathfrak{S}_f(\mathcal{C})$ in connection with two fundamental functions f of this type.

- $f(X, Y) = XY - YX$: **commuting probability $\mathbf{Pr_c}(R)$** and **commuting spectrum $\mathfrak{S}_\mathbf{c}(\mathcal{C})$**;
- $f(X, Y) = XY$: **annihilating probability $\mathbf{Pr_{ann}}(R)$** and **annihilating spectrum $\mathfrak{S}_\mathbf{ann}(\mathcal{C})$**.

Theorem 2 (B.)

If $\mathcal{C} := \{$*finite rings*$\}$, *and* $f(X, Y) := aXY + bYX$, $a, b \in \mathbb{Z}$, *then*

$$\mathfrak{S}_f(\mathcal{C}) \subseteq \mathfrak{S}_{\mathrm{ann}}(\mathcal{C})\,.$$

Definitions

The **commuting probability** of a finite ring R is

$$\mathrm{Pr_c}(R) := \frac{|\{(x,y) \in R \times R \;:\; xy = yx\}|}{|R|^2}$$

If G is a finite group, similarly define $\mathrm{Pr_c}(G)$.
The commuting spectrum $\mathfrak{S}_\mathrm{c}(\mathcal{C})$ is defined as before.

Definitions

The **commuting probability** of a finite ring R is

$$\mathrm{Pr_c}(R) := \frac{|\{(x,y) \in R \times R \ : \ xy = yx\}|}{|R|^2}$$

If G is a finite group, similarly define $\mathrm{Pr_c}(G)$.
The commuting spectrum $\mathfrak{S}_c(\mathcal{C})$ is defined as before.

- $\mathfrak{R} = \mathfrak{S}_c\{$finite (possibly non-unital) rings$\}$
  $\mathfrak{R}_p = \mathfrak{S}_c\{$finite (possibly non-unital) p-rings$\}$, p prime.
  $\mathfrak{G} = \mathfrak{S}_c\{$finite groups$\}$

Definitions

The **commuting probability** of a finite ring R is

$$\mathrm{Pr_c}(R) := \frac{|\{(x,y) \in R \times R \ : \ xy = yx\}|}{|R|^2}$$

If G is a finite group, similarly define $\mathrm{Pr_c}(G)$.
The commuting spectrum $\mathfrak{S}_c(\mathcal{C})$ is defined as before.

- $\mathfrak{R} = \mathfrak{S}_c\{\text{finite (possibly non-unital) rings}\}$
  $\mathfrak{R}_p = \mathfrak{S}_c\{\text{finite (possibly non-unital) } p\text{-rings}\}$, p prime.
  $\mathfrak{G} = \mathfrak{S}_c\{\text{finite groups}\}$

- Trivially, $\mathfrak{R} \subset (0,1] \cap \mathbb{Q}$.
- $\mathrm{Pr}(R_1 \oplus R_2) = \mathrm{Pr}(R_1)\,\mathrm{Pr}(R_2)$.

Definitions

The **commuting probability** of a finite ring R is

$$\mathrm{Pr_c}(R) := \frac{|\{(x,y) \in R \times R \;:\; xy = yx\}|}{|R|^2}$$

If G is a finite group, similarly define $\mathrm{Pr_c}(G)$.
The commuting spectrum $\mathfrak{S}_c(\mathcal{C})$ is defined as before.

- $\mathfrak{R} = \mathfrak{S}_c\{$finite (possibly non-unital) rings$\}$
  $\mathfrak{R}_p = \mathfrak{S}_c\{$finite (possibly non-unital) p-rings$\}$, p prime.
  $\mathfrak{G} = \mathfrak{S}_c\{$finite groups$\}$
- Trivially, $\mathfrak{R} \subset (0,1] \cap \mathbb{Q}$.
- $\mathrm{Pr}(R_1 \oplus R_2) = \mathrm{Pr}(R_1)\,\mathrm{Pr}(R_2)$.
- $\mathfrak{R}_p \cap (0,1) \subset (0, \alpha_p]$, where $\alpha_p = (p^2 + p - 1)/p^3$ (MacHale, 1976).

Definitions

The **commuting probability** of a finite ring R is

$$\mathrm{Pr_c}(R) := \frac{|\{(x,y) \in R \times R \;:\; xy = yx\}|}{|R|^2}$$

If G is a finite group, similarly define $\mathrm{Pr_c}(G)$.
The commuting spectrum $\mathfrak{S}_c(\mathcal{C})$ is defined as before.

- $\mathfrak{R} = \mathfrak{S}_c\{\text{finite (possibly non-unital) rings}\}$
  $\mathfrak{R}_p = \mathfrak{S}_c\{\text{finite (possibly non-unital) } p\text{-rings}\}$, p prime.
  $\mathfrak{G} = \mathfrak{S}_c\{\text{finite groups}\}$
- Trivially, $\mathfrak{R} \subset (0,1] \cap \mathbb{Q}$.
- $\mathrm{Pr}(R_1 \oplus R_2) = \mathrm{Pr}(R_1)\,\mathrm{Pr}(R_2)$.
- $\mathfrak{R}_p \cap (0,1) \subset (0, \alpha_p]$, where $\alpha_p = (p^2 + p - 1)/p^3$ (MacHale, 1976).
- Much more known about groups e.g.
  $\mathfrak{G} \cap (11/32, 1]$ completely understood (Rusin, 1979).

Definitions

The **commuting probability** of a finite ring R is

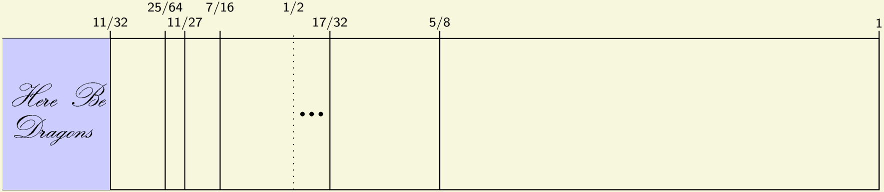
$$\mathrm{Pr_c}(R) := \frac{|\{(x,y) \in R \times R \ : \ xy = yx\}|}{|R|^2}$$

If G is a finite group, similarly define $\mathrm{Pr_c}(G)$.
The commuting spectrum $\mathfrak{S}_c(\mathcal{C})$ is defined as before.

- $\mathfrak{R} = \mathfrak{S}_c\{\text{finite (possibly non-unital) rings}\}$
  $\mathfrak{R}_p = \mathfrak{S}_c\{\text{finite (possibly non-unital) } p\text{-rings}\}$, p prime.
  $\mathfrak{G} = \mathfrak{S}_c\{\text{finite groups}\}$
- Trivially, $\mathfrak{R} \subset (0,1] \cap \mathbb{Q}$.
- $\mathrm{Pr}(R_1 \oplus R_2) = \mathrm{Pr}(R_1)\,\mathrm{Pr}(R_2)$.
- $\mathfrak{R}_p \cap (0,1) \subset (0, \alpha_p]$, where $\alpha_p = (p^2+p-1)/p^3$ (MacHale, 1976).
- Much more known about groups e.g.
  $\mathfrak{G} \cap (11/32, 1]$ completely understood (Rusin, 1979).
- Semigroups entirely different (MacHale, 1990; Ponomarenko and Selinski, 2012; B. 2013)

$\mathfrak{R}$ versus $\mathfrak{G}$

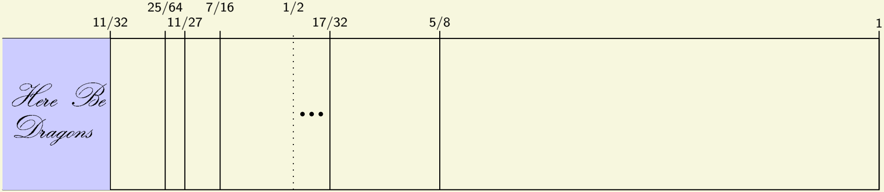
$\mathfrak{R}$ versus $\mathfrak{G}$



$$\left\{ \frac{2^{2k}+1}{2^{2k+1}} \;\middle|\; k \in \mathbb{N} \right\} \cup \left\{ 1, \frac{7}{16}, \frac{11}{27}, \frac{25}{64}, \frac{11}{32} \right\}$$

Values of $\Pr_c(R)$ in $[11/32, 1]$ *(B.-MacHale-Ní Shé)*

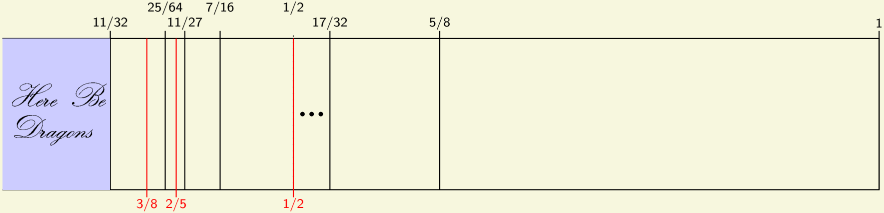
$\mathfrak{R}$ versus $\mathfrak{G}$



$$\left\{ \frac{2^{2k}+1}{2^{2k+1}} \;\middle|\; k \in \mathbb{N} \right\} \cup \left\{ 1, \frac{7}{16}, \frac{11}{27}, \frac{25}{64}, \frac{11}{32} \right\}$$

Values of $\mathrm{Pr_c}(R)$ in $[11/32, 1]$: R direct sum of $\mathbb{Z}_p$-algebras *(B.-MacHale-Ní Shé)*

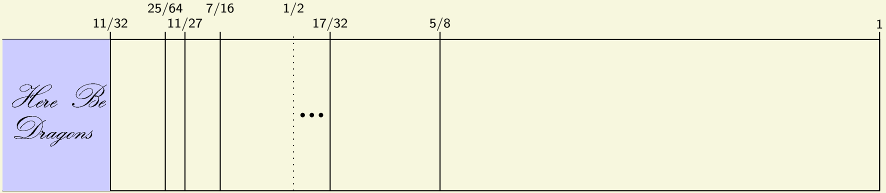
$\mathfrak{R}$ versus $\mathfrak{G}$



$$\left\{ \frac{2^{2k}+1}{2^{2k+1}} \;\middle|\; k \in \mathbb{N} \right\} \cup \left\{ 1, \frac{7}{16}, \frac{11}{27}, \frac{25}{64}, \frac{11}{32} \right\} \cup \left\{ \frac{1}{2}, \frac{2}{5}, \frac{3}{8} \right\}$$

Values of $\mathrm{Pr}_c(G)$ in $[11/32, 1]$

$\mathfrak{R}$ versus $\mathfrak{G}$



$$\left\{ \frac{2^{2k}+1}{2^{2k+1}} \;\middle|\; k \in \mathbb{N} \right\} \cup \left\{ 1, \frac{7}{16}, \frac{11}{27}, \frac{25}{64}, \frac{11}{32} \right\}$$

Values of $\mathrm{Pr_c}(G)$ in $[11/32, 1]$: G nilpotent (class 2)

Large values of the commuting probability

We define

$$\alpha_p = \frac{p^2+p-1}{p^3}, \quad \beta_p = \frac{2p^2-1}{p^4}, \quad \text{and } \gamma_p = \frac{p^3+p^2-1}{p^5}.$$

Note that

$$\gamma_p < \alpha_p^2 < \beta_p < \frac{1}{p} < \alpha_p, \qquad p \geq 2.$$

Large values of the commuting probability

We define

$$\alpha_p = \frac{p^2+p-1}{p^3}, \quad \beta_p = \frac{2p^2-1}{p^4}, \quad \text{and } \gamma_p = \frac{p^3+p^2-1}{p^5}.$$

Note that

$$\gamma_p < \alpha_p^2 < \beta_p < \frac{1}{p} < \alpha_p\,, \qquad p \geq 2\,.$$

Theorem 3 (B.-MacHale-Ní Shé)

$$\mathfrak{R}_p \cap [\gamma_p, 1] = \{1\} \cup \left\{ \frac{p^{2k}+p-1}{p^{2k+1}} \;\middle|\; k \in \mathbb{N} \right\} \cup \left\{\beta_p, \alpha_p^2, \gamma_p\right\}.$$

$$\begin{aligned}\mathfrak{R} \cap [\gamma_2, 1] &= (\mathfrak{R}_2 \cap [\gamma_2, 1]) \cup \{\alpha_3\} \\ &= \{1\} \cup \left\{ \frac{2^{2k}+1}{2^{2k+1}} \;\middle|\; k \in \mathbb{N} \right\} \cup \left\{ \frac{7}{16}, \frac{11}{27}, \frac{25}{64}, \frac{11}{32} \right\}.\end{aligned}$$

Commuting probability and Z-isoclinism

Theorem 4 (B.-MacHale-Ní Shé)

$\Pr(R) = t$ *uniquely determines Z-isoclinism type of* $R \in C$ *if:*

- $t \in \mathfrak{R}_p \cap (\gamma_p, 1]$, $C = \{p\text{-rings}\}$.
- $t \in \mathfrak{R} \cap (\gamma_2, 1]$, $C = \{\text{finite rings}\}$.

Commuting probability and Z-isoclinism

Theorem 4 (B.-MacHale-Ní Shé)
$\Pr(R) = t$ *uniquely determines Z-isoclinism type of* $R \in C$ *if:*

- $t \in \mathfrak{R}_p \cap (\gamma_p, 1]$, $C = \{p\text{-rings}\}$.
- $t \in \mathfrak{R} \cap (\gamma_2, 1]$, $C = \{\text{finite rings}\}$.

Theorem 5 (B.-MacHale-Ní Shé)
p-rings R *with* $\Pr(R) = \gamma_p$ *yield exactly:*

Commuting probability and Z-isoclinism

Theorem 4 (B.-MacHale-Ní Shé)
$\Pr(R) = t$ *uniquely determines Z-isoclinism type of* $R \in C$ *if:*

- $t \in \mathfrak{R}_p \cap (\gamma_p, 1]$, $C = \{p\text{-rings}\}$.
- $t \in \mathfrak{R} \cap (\gamma_2, 1]$, $C = \{\text{finite rings}\}$.

Theorem 5 (B.-MacHale-Ní Shé)
p-rings R *with* $\Pr(R) = \gamma_p$ *yield exactly:*

- *five Z-isoclinism types;*

Commuting probability and Z-isoclinism

Theorem 4 (B.-MacHale-Ní Shé)
$\mathrm{Pr}(R) = t$ *uniquely determines Z-isoclinism type of* $R \in C$ *if:*

- $t \in \mathfrak{R}_p \cap (\gamma_p, 1]$, $C = \{p\text{-rings}\}$.
- $t \in \mathfrak{R} \cap (\gamma_2, 1]$, $C = \{\text{finite rings}\}$.

Theorem 5 (B.-MacHale-Ní Shé)
p-rings R *with* $\mathrm{Pr}(R) = \gamma_p$ *yield exactly:*

- *five Z-isoclinism types;*
- *four* $R/Z(R)$ *group isomorphism types;*

Commuting probability and Z-isoclinism

Theorem 4 (B.-MacHale-Ní Shé)

$\Pr(R) = t$ *uniquely determines Z-isoclinism type of* $R \in C$ *if:*

- $t \in \mathfrak{R}_p \cap (\gamma_p, 1]$, $C = \{p\text{-rings}\}$.
- $t \in \mathfrak{R} \cap (\gamma_2, 1]$, $C = \{\text{finite rings}\}$.

Theorem 5 (B.-MacHale-Ní Shé)

p-rings R *with* $\Pr(R) = \gamma_p$ *yield exactly:*

- *five Z-isoclinism types;*
- *four* $R/Z(R)$ *group isomorphism types;*
- *three* $[R, R]$ *group isomorphism types.*

First steps

$$\Pr(R) = \frac{1}{|R|} \sum_{x \in R} \frac{1}{|R/C(x)|} = \frac{1}{|R|^2} \sum_{x \in R} |C(x)|$$

First steps

$$\Pr(R) = \frac{1}{|R|}\sum_{x\in R}\frac{1}{|R/C(x)|} = \frac{1}{|R|^2}\sum_{x\in R}|C(x)|$$
$$= \frac{1}{|R/Z(R)|}\sum_{x+Z(R)\in R/Z(R)}\frac{1}{|R/C(x)|},$$

(sum over one representative of each coset)

First steps

$$\Pr(R) = \frac{1}{|R|}\sum_{x\in R}\frac{1}{|R/C(x)|} = \frac{1}{|R|^2}\sum_{x\in R}|C(x)|$$
$$= \frac{1}{|R/Z(R)|}\sum_{x+Z(R)\in R/Z(R)}\frac{1}{|R/C(x)|},$$

(sum over one representative of each coset)

Observation

For $x \in R$, additive groups $R/C(x)$ and $[x,R]$ are isomorphic.
In particular, if R is a $\mathbb{Z}_p$-algebra, $\dim R/C(x) = \dim[x,R]$.

Z-Isoclinism

Definition

Rings R and S are *Z-isoclinic* if there are additive **group isomorphisms** $\phi : R/Z(R) \to S/Z(S)$ and $\psi : [R, R] \to [S, S]$ such that

$$\psi([u, v]) = [u', v']$$

whenever

$$\phi(u + Z(R)) = u' + Z(S) \qquad \text{and} \qquad \phi(v + Z(R)) = v' + Z(S).$$

Z-Isoclinism

Definition

Rings R and S are *Z-isoclinic* if there are additive **group isomorphisms** $\phi : R/Z(R) \to S/Z(S)$ and $\psi : [R, R] \to [S, S]$ such that

$$\psi([u, v]) = [u', v']$$

whenever

$$\phi(u + Z(R)) = u' + Z(S) \qquad \text{and} \qquad \phi(v + Z(R)) = v' + Z(S).$$

Kruse and Price's and Moneyhun's notions of isoclinism for rings and Lie algebras involve **ring isomorphisms**.

Isoclinism properties

- Z-isoclinism is an equivalence relation.
- Isomorphic $\Rightarrow$ Z-isoclinic; converse false.
- Z-isoclinism class determines gp isomorphism classes of $R/Z(R)$ and $[R, R]$.
- Z-isoclinism induces group isomorphisms of $[x, R]$ subgroups.
- **If R and S are Z-isoclinic, then $\mathrm{Pr}(R) = \mathrm{Pr}(S)$.**

Universal algebras: definition

If S is any set, $S^{\times 0} := \{\emptyset\}$, and $S^{\times m}$ is the cartesian product of m copies of S, $m \in \mathbb{N}$.

Universal algebras: definition

If S is any set, $S^{\times 0} := \{\emptyset\}$, and $S^{\times m}$ is the cartesian product of m copies of S, $m \in \mathbb{N}$.

An **algebra A** consists of an **underlying set**, also denoted A, with associated fundamental operations $g^A : A^{\times n} \to A$.
$n \geq 0$ is the **arity of g^A**.

Universal algebras: definition

If S is any set, $S^{\times 0} := \{\emptyset\}$, and $S^{\times m}$ is the cartesian product of m copies of S, $m \in \mathbb{N}$.

An **algebra A** consists of an **underlying set**, also denoted A, with associated fundamental operations $g^A : A^{\times n} \to A$.
$n \geq 0$ is the **arity of g^A**.

We speak of **nullary**, **unary**, or **binary** operations if $n = 0$, $n = 1$, or $n = 2$, respectively; a nullary operation is a significant constant e.g. 0 or 1 in a unital ring.

Universal algebras: definition

If S is any set, $S^{\times 0} := \{\emptyset\}$, and $S^{\times m}$ is the cartesian product of m copies of S, $m \in \mathbb{N}$.

An **algebra A** consists of an **underlying set**, also denoted A, with associated fundamental operations $g^A : A^{\times n} \to A$.
$n \geq 0$ is the **arity of g^A**.

We speak of **nullary**, **unary**, or **binary** operations if $n = 0$, $n = 1$, or $n = 2$, respectively; a nullary operation is a significant constant e.g. 0 or 1 in a unital ring.

If g^A is n-ary, write $g^A(\underline{x})$ to mean $g^A(x_1, \ldots, x_n)$.
Each x_i is a **coordinate** of $\underline{x}$.
The **coordinate set of $\underline{x}$** is $\mathrm{CS}(\underline{x}) = \{x_1, \ldots, x_n\}$.

Distributive algebras: definition

Suppose $(A, +)$ an abelian group, and g^A is n-ary, $n \in \mathbb{N}$.
g^A is **distributive over addition** if

$$g^A(\underline{z}) = g^A(\underline{x}) + g^A(\underline{y})$$

whenever $z_j = x_j + y_j$ for some j, and $z_k = x_k = y_k$ for $k \neq j$.

Distributive algebras: definition

Suppose $(A, +)$ an abelian group, and g^A is n-ary, $n \in \mathbb{N}$.
g^A is **distributive over addition** if

$$g^A(\underline{z}) = g^A(\underline{x}) + g^A(\underline{y})$$

whenever $z_j = x_j + y_j$ for some j, and $z_k = x_k = y_k$ for $k \neq j$.

Definition

Suppose I is an index set and $\rho : I \to \mathbb{N}$.
An **(I, ρ)-algebra** is an abelian group $(A, +)$ with $\rho(i)$-ary operations g_i^A on A, $i \in I$, that are distributive over $+$ whenever $\rho(i) > 0$; A has **type** (I, ρ).
A **distributive algebra** is an (I, ρ)-algebra for some type (I, ρ).

Distributive algebras: definition

Suppose $(A, +)$ an abelian group, and g^A is n-ary, $n \in \mathbb{N}$.
g^A is **distributive over addition** if

$$g^A(\underline{z}) = g^A(\underline{x}) + g^A(\underline{y})$$

whenever $z_j = x_j + y_j$ for some j, and $z_k = x_k = y_k$ for $k \neq j$.

Definition

Suppose I is an index set and $\rho : I \to \mathbb{N}$.
An **(I, ρ)-algebra** is an abelian group $(A, +)$ with $\rho(i)$-ary operations g_i^A on A, $i \in I$, that are distributive over $+$ whenever $\rho(i) > 0$; A has **type** (I, ρ).
A **distributive algebra** is an (I, ρ)-algebra for some type (I, ρ).

If $|I|$ is small, convenient to let $I = \{1, \ldots, k\}$ and write the type as $[\rho(1), \ldots, \rho(k)]$, so:

- PN rings and [2]-algebras coincide;
- a unital PN ring is a special kind of $[2, 0]$-algebra.

Distributive algebras: definition

Suppose $(A, +)$ an abelian group, and g^A is n-ary, $n \in \mathbb{N}$.
g^A is **distributive over addition** if

$$g^A(\underline{z}) = g^A(\underline{x}) + g^A(\underline{y})$$

whenever $z_j = x_j + y_j$ for some j, and $z_k = x_k = y_k$ for $k \neq j$.

Definition

Suppose I is an index set and $\rho : I \to \mathbb{N}$.
An **(I, ρ)-algebra** is an abelian group $(A, +)$ with $\rho(i)$-ary operations g_i^A on A, $i \in I$, that are distributive over $+$ whenever $\rho(i) > 0$; A has **type** (I, ρ).
A **distributive algebra** is an (I, ρ)-algebra for some type (I, ρ).

If $|I|$ is small, convenient to let $I = \{1, \ldots, k\}$ and write the type as $[\rho(1), \ldots, \rho(k)]$, so:

- PN rings and $[2]$-algebras coincide;
- a unital PN ring is a special kind of $[2, 0]$-algebra.

The **reduced index set I_0** consists of all $i \in I$ such that $\rho(i) > 0$, and $\boldsymbol{\rho_0 := \rho|_{I_0}}$.
(I_0, ρ_0) is the **reduced type corresponding to the type (I, ρ)**.

Ideals and quotients

Definition

An **ideal in an (I, ρ)-algebra A** is a subgp J of $(A, +)$ such that $g_i^A(\underline{x}) \in J$ whenever $i \in I_0$, $\underline{x} \in A^{\times \rho(i)}$, and $\mathrm{CS}(\underline{x}) \cap J$ is nonempty.
We write $J \trianglelefteq A$ or $A \trianglerighteq J$.

An ideal in an (I, ρ)-algebra is an (I_0, ρ_0)-algebra.

Lemma

If $J \trianglelefteq A$, then A/J naturally has same type as A, with natural maps $g_i^{A/J}$.

Annihilators and product ideals

Definition

The **annihilator of A** is $\mathrm{Ann}(A) = \bigcap_{i \in I_0} \mathrm{Ann}(A; i)$, where

$$\mathrm{Ann}(A; i) = \{a \in A \mid \forall\, \underline{x} \in A^{\times \rho(i)} : a \in \mathrm{CS}(\underline{x}) \Rightarrow g_i^A(\underline{x}) = 0\}, \quad i \in I_0 .$$

Annihilators and product ideals

Definition

The **annihilator of *A*** is $\mathrm{Ann}(A) = \bigcap_{i \in I_0} \mathrm{Ann}(A; i)$, where

$$\mathrm{Ann}(A; i) = \{a \in A \mid \forall\, \underline{x} \in A^{\times \rho(i)} : a \in \mathrm{CS}(\underline{x}) \Rightarrow g_i^A(\underline{x}) = 0\}, \quad i \in I_0 .$$

Definition

The **product ideal of *A***, $\pi(A)$, is the subgroup of $(A, +)$ generated by elements of $\pi(A; i)$, $i \in I_0$, where $\pi(A, i)$ is the subgroup of $(A, +)$ generated by $g_i^A(\underline{x})$, $\underline{x} \in A^{\times \rho(i)}$.

Annihilators and product ideals

Definition

The **annihilator of A** is $\operatorname{Ann}(A) = \bigcap_{i \in I_0} \operatorname{Ann}(A; i)$, where

$$\operatorname{Ann}(A; i) = \{a \in A \mid \forall\, \underline{x} \in A^{\times \rho(i)} : a \in \operatorname{CS}(\underline{x}) \Rightarrow g_i^A(\underline{x}) = 0\}, \quad i \in I_0 .$$

Definition

The **product ideal of A**, $\pi(A)$, is the subgroup of $(A, +)$ generated by elements of $\pi(A; i)$, $i \in I_0$, where $\pi(A, i)$ is the subgroup of $(A, +)$ generated by $g_i^A(\underline{x})$, $\underline{x} \in A^{\times \rho(i)}$.

Null algebra: $\operatorname{Ann}(A) = A$, or equivalently $\pi(A) = 0$.

Remark

$g_i^{A/\operatorname{Ann}(A)}$ factors through A to give natural map $\tilde{g}_i^A : (A/\operatorname{Ann}(A))^{\times n} \to A$.

Annihilator series

Definition

A finite sequence of ideals $(A_j)_{j=0}^{m}$, $m \geq 0$, in an (I, ρ)-algebra A is an **annihilator series (of length m)** if $A_0 = A$, $A_m = 0$,

$$A_0 \trianglerighteq A_1 \trianglerighteq \cdots A_m$$

and $A_{j-1}/A_j \leq \mathrm{Ann}(A/A_j)$ for $1 \leq i \leq m$.

A is **nilpotent** if it has an annihilator series.

Annihilator series

Definition

A finite sequence of ideals $(A_j)_{j=0}^m$, $m \geq 0$, in an (I,ρ)-algebra A is an **annihilator series (of length m)** if $A_0 = A$, $A_m = 0$,

$$A_0 \trianglerighteq A_1 \trianglerighteq \cdots A_m$$

and $A_{j-1}/A_j \leq \mathrm{Ann}(A/A_j)$ for $1 \leq i \leq m$.

A is **nilpotent** if it has an annihilator series.

The **exponent**, $\exp(A)$, is the minimal length of an annihilator series of A.

Annihilator series

Definition

A finite sequence of ideals $(A_j)_{j=0}^{m}$, $m \geq 0$, in an (I, ρ)-algebra A is an **annihilator series (of length *m*)** if $A_0 = A$, $A_m = 0$,

$$A_0 \trianglerighteq A_1 \trianglerighteq \cdots A_m$$

and $A_{j-1}/A_j \leq \mathrm{Ann}(A/A_j)$ for $1 \leq i \leq m$.

A is **nilpotent** if it has an annihilator series.
The **exponent**, $\exp(A)$, is the minimal length of an annihilator series of A.

We can define **upper** and **lower annihilator series**, as done by Kruse and Price for rings.

Isoclinism

Definition

An **isoclinism** from one (I, ρ)-algebra A to another one B consists of a pair of additive group isomorphisms

$$\phi : A/\operatorname{Ann}(A) \to B/\operatorname{Ann}(B) \text{ and } \psi : \pi(A) \to \pi(B)$$

such that if $i \in I_0$, $\phi(x_j + \operatorname{Ann}(A)) = y_j + \operatorname{Ann}(B)$, $j = 1, \ldots, \rho(i)$, then

$$\psi(g_i^A(\underline{x})) = g_i^B(\underline{y}).$$

(As usual, I_0 is the reduced index set.)

Isoclinism

Definition

An **isoclinism** from one (I, ρ)-algebra A to another one B consists of a pair of additive group isomorphisms

$$\phi : A/\operatorname{Ann}(A) \to B/\operatorname{Ann}(B) \text{ and } \psi : \pi(A) \to \pi(B)$$

such that if $i \in I_0$, $\phi(x_j + \operatorname{Ann}(A)) = y_j + \operatorname{Ann}(B)$, $j = 1, \ldots, \rho(i)$, then

$$\psi(g_i^A(\underline{x})) = g_i^B(\underline{y}).$$

(As usual, I_0 is the reduced index set.)

Alternative definition:

$$\begin{array}{ccc} (A/\operatorname{Ann}(A))^{\otimes n} & \xrightarrow[\cong]{\phi^{\otimes n}} & (B/\operatorname{Ann}(B))^{\otimes n} \\ {\scriptstyle g_i^{A;\otimes}} \big\downarrow & & \big\downarrow {\scriptstyle g_i^{B;\otimes}} \\ \pi(A;i) & \xrightarrow[\cong]{\psi|_{\pi(A,i)}} & \pi(B;i) \end{array}$$

A and B are isoclinic via (ϕ, ψ) if and only if the above diagram is commutative for each $i \in I_0$ and $n := \rho(i)$.

Isoclinism: basics

Theorem

- *Isoclinism is an equivalence relation on distributive algebras of any given type; equivalence classes are called* **isoclinism families***.*
- *All null algebras of a given type are isoclinic.*
- *If* (ϕ_j, ψ_j) *is an isoclinism from one* (I, ϕ)*-algebra* A_j *to another one* B_j*, for all* $j \in J \neq \emptyset$*, then* $\prod_{j \in J} A_j$ *is isoclinic to* $\prod_{j \in J} B_j$*, and* $\bigoplus_{j \in J} A_j$ *is isoclinic to* $\bigoplus_{j \in J} B_j$*.*
- *Isomorphic algebras are isoclinic.*

Canonical form

Definition

A distributive algebra A has **canonical form** if:

1. $(A, +)$ is the internal direct sum of subgroups A_1 and A_2.
2. $\pi(A) = \mathrm{Ann}(A) = A_2$.

A canonical form member of an isoclinism family is called a **canonical relative** of all algebras in that family.

Canonical form

Definition

A distributive algebra A has **canonical form** if:

1. $(A, +)$ is the internal direct sum of subgroups A_1 and A_2.
2. $\pi(A) = \mathrm{Ann}(A) = A_2$.

A canonical form member of an isoclinism family is called a **canonical relative** of all algebras in that family.

Theorem

- *Canonical relatives exist and are unique (up to isomorphism).*
- *Distributive algebras A and B are isoclinic if and only if their canonical relatives $\mathrm{Can}(A)$ and $\mathrm{Can}(B)$ are isomorphic.*
- *A canonical form distributive algebra is nilpotent of exponent ≤ 2.*
- *Nilpotency is not an isoclinism invariant.*

Invariant probability functions

Let

$$\Pr(A; g_i^A, n) := \frac{|\{\underline{a} \in A^{\times n} \ : \ g_i^A(\underline{a}) = 0\}|}{|A|^n} \, .$$

Invariant probability functions

Let

$$\Pr(A; g_i^A, n) := \frac{|\{\underline{a} \in A^{\times n} \ : \ g_i^A(\underline{a}) = 0\}|}{|A|^n} .$$

Lemma

Suppose (ϕ, ψ) is an isoclinism from one finite (I, ρ)-algebra A to another B. Then $\Pr(A; g_i^A, n) = \Pr(B; g_i^B, n)$ for all $i \in I$ and $n := \rho(i)$.

Invariant probability functions

Let

$$\Pr(A; g_i^A, n) := \frac{|\{\underline{a} \in A^{\times n} \ : \ g_i^A(\underline{a}) = 0\}|}{|A|^n}.$$

Lemma

Suppose (ϕ, ψ) is an isoclinism from one finite (I, ρ)-algebra A to another B. Then $\Pr(A; g_i^A, n) = \Pr(B; g_i^B, n)$ for all $i \in I$ and $n := \rho(i)$.

The argument in the above lemma can be generalized. In particular, we can replace g_i^A by $f^A : A^{\times m} \to A$, where

$$f^A(x_1, \ldots, x_m) := g_i^A(\sum_{j=1}^m a_{1j}x_j, \ldots, \sum_{j=1}^m a_{nj}x_j),$$

One simple example is $f^A(x) = g^A(x, x)$ in a PN ring A where $g^A(x, y) = xy$. So the proportion of **dinilpotents** (elements satisfying $x^2 = 0$) is an isoclinism invariant for PN rings.

Spectral identity

Theorem

Let C_0, $\mathcal{C}_1$, and $\mathcal{C}_2$ be the classes of all finite nilpotent rings of exponent at most 2, all finite rings, and all finite PN rings, respectively. Then for all $f(X,Y) := aXY + bYX$, $a, b \in \mathbb{Z}$, and all classes $\mathcal{C}$ such that $\mathcal{C}_0 \subseteq \mathcal{C} \subseteq \mathcal{C}_2$,

$$\mathfrak{S}_f(\mathcal{C}) = \mathfrak{S}_f(\mathcal{C}_1)\,.$$

Spectral identity

Theorem

Let C_0, $\mathcal{C}_1$, and $\mathcal{C}_2$ be the classes of all finite nilpotent rings of exponent at most 2, all finite rings, and all finite PN rings, respectively. Then for all $f(X,Y) := aXY + bYX$, $a, b \in \mathbb{Z}$, and all classes $\mathcal{C}$ such that $\mathcal{C}_0 \subseteq \mathcal{C} \subseteq \mathcal{C}_2$,

$$\mathfrak{S}_f(\mathcal{C}) = \mathfrak{S}_f(\mathcal{C}_1)\,.$$

Above theorem works for other function symbols f such as $f(X) = X^2$, so **the sets of possible dinilpotent proportions in finite rings and in finite PN rings coincide.**

Spectral identity

Theorem

Let $\mathcal{C}_0$, $\mathcal{C}_1$, and $\mathcal{C}_2$ be the classes of all finite nilpotent rings of exponent at most 2, all finite rings, and all finite PN rings, respectively. Then for all $f(X, Y) := aXY + bYX$, $a, b \in \mathbb{Z}$, and all classes $\mathcal{C}$ such that $\mathcal{C}_0 \subseteq \mathcal{C} \subseteq \mathcal{C}_2$,

$$\mathfrak{S}_f(\mathcal{C}) = \mathfrak{S}_f(\mathcal{C}_1)\,.$$

Above theorem works for other function symbols f such as $f(X) = X^2$, so **the sets of possible dinilpotent proportions in finite rings and in finite PN rings coincide.**

However idempotent proportion is not an isoclinism invariant and **the sets of possible idempotent proportions in finite rings and in finite PN rings do not coincide** (B.–Yu. Zelenyuk; work in progress)