SOLUTIONS OF THE YANG-BAXTER EQUATION: GROUPS, ALGEBRAS AND BRACES

Arne Van Antwerpen

VRIJE
UNIVERSITEIT
BRUSSEL

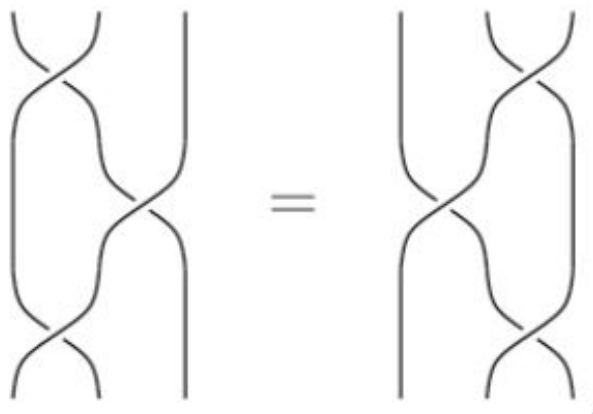
THE YANG-BAXTER EQUATION: A PICTURE

Definition

A set-theoretic solution to the Yang-Baxter equation is a tuple (X, r), where X is a set and $r : X \times X \longrightarrow X \times X$ a function such that (on X^3)

$$(r \times \mathrm{id}_X)\,(\mathrm{id}_X \times r)\,(r \times \mathrm{id}_X) = (\mathrm{id}_X \times r)\,(r \times \mathrm{id}_X)\,(\mathrm{id}_X \times r)\,.$$

For further reference, denote $r(x, y) = (\lambda_x(y), \rho_y(x))$.



APPLICATIONS OF YBE

Historical applications:

- Study of a system with delta function repulsive potential (Yang).
- Study of an 8-vertex model in statistical mechanics (Baxter)

Contemporary applications:

- Quasi-triangular Hopf algebras,
- Quantum computation,
- Differential geometry,
- Cryptography,
- Quadratic algebras.

DEFINITIONS AND EXAMPLES

Definition

A set-theoretic solution (X, r) is called

- left (resp. right) non-degenerate, if λ_x (resp. ρ_y) is bijective,
- non-degenerate, if it is both left and right non-degenerate,
- involutive, if $r^2 = \mathrm{id}_{X \times X}$,

Examples

- Twist solution: $r(x, y) = (y, x)$,
- Identity: $r(x, y) = (x, y)$.
- Let G be a group: $r(g, h) = (gh, 1_G)$.
- Lyubashenko, where $f, g : X \to X$ are maps with $fg = gf$: $r(x, y) = (f(y), g(x))$.

THE STRUCTURE MONOID AND GROUP

Definition

Let (X, r) be a set-theoretic solution of the Yang-Baxter equation. Then the monoid

$$M(X, r) = \left\langle x \in X \mid xy = \lambda_x(y)\rho_y(x) \right\rangle,$$

is called the structure monoid of (X, r).

THE STRUCTURE MONOID AND GROUP

Definition

Let (X, r) be a set-theoretic solution of the Yang-Baxter equation. Then the monoid

$$M(X, r) = \left\langle x \in X \mid xy = \lambda_x(y)\rho_y(x) \right\rangle,$$

is called the structure monoid of (X, r).
The group $G(X, r)$ generated by the same presentation is called the structure group of (X, r).

RECOVERING SOLUTIONS

Theorem (ESS, LYZ, S, GV, GM)

Let (X, r) be a non-degenerate solution to YBE, then there exists a unique solution r_G on the group $G(X, r)$ such that the associated solution r_G satisfies

$$r_G(i \times i) = (i \times i)r,$$

where $i : X \to G(X, r)$ is the canonical map.

RECOVERING SOLUTIONS

Theorem (ESS, LYZ, S, GV, GM)

Let (X, r) be a non-degenerate solution to YBE, then there exists a unique solution r_G on the group $G(X, r)$ such that the associated solution r_G satisfies

$$r_G(i \times i) = (i \times i)r,$$

where $i : X \to G(X, r)$ is the canonical map.

However, there exists a unique solution r_M on $M(X, r)$ such that $r_M|_{X \times X} = r$.

MONOIDS AND GROUPS FROM SOME SOLUTIONS

- If $r(x,y) = (y,x)$, then $M(X,r) \cong \mathbb{Z}_{\geq 0}^{|X|}$,
- if $r(x,y) = (x,y)$, then $M(X,r) \cong FM(X)$,
- if $r(g,h) = (gh, e_G)$, then $M(X,r) \hookrightarrow G \times \mathbb{Z}_{\geq 0}$.

MONOIDS AND GROUPS OF I-TYPE

Theorem (GIVdB, JO)

Let (X, r) be a finite, involutive non-degenerate set-theoretic solution. Then, $G(X, r)$ is a group of I-type.

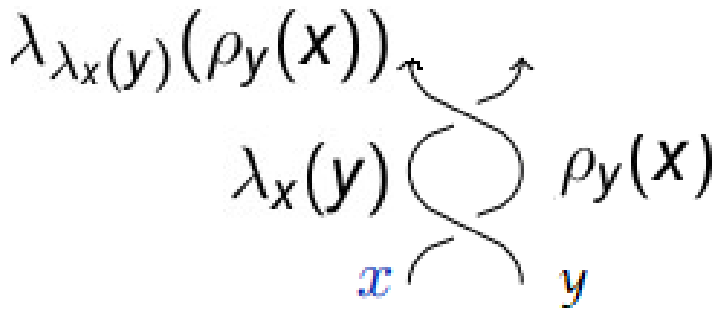
In particular, $G(X, r)$ is a regular subgroup of $\mathbb{Z}^{|X|} \rtimes \mathrm{Sym}(X)$ and $M(X, r)$ is a regular submonoid of $\mathbb{N}^{|X|} \rtimes \mathrm{Sym}(X)$.

DERIVED STRUCTURE MONOID

Definition

Let (X, r) be a set-theoretic solution. Denote the monoid

$$A(X,r) = \left\langle x \in X \mid x\lambda_x(y) = \lambda_x(y)\lambda_{\lambda_x(y)}(\rho_y(x)) \right\rangle .$$



DERIVED STRUCTURE MONOID

Definition

Let (X, r) be a set-theoretic solution. Denote the monoid

$$A(X, r) = \left\langle x \in X \mid x\lambda_x(y) = \lambda_x(y)\lambda_{\lambda_x(y)}(\rho_y(x)) \right\rangle .$$

If (X, r) is left non-degenerate, then for any $x \in X$ there exists a map $\sigma_x : X \longrightarrow X$ such that

$$A(X, r) = \left\langle x \in X \mid xy = y\sigma_y(x) \right\rangle .$$

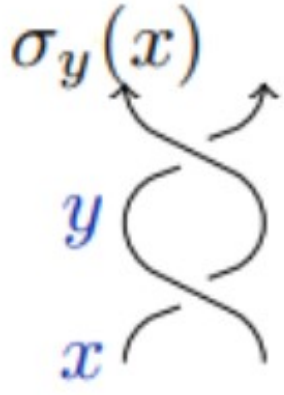
DERIVED STRUCTURE MONOID

Definition

Let (X, r) be a left non-degenerate set-theoretic solution. Then

$$A(X, r) = \langle x \in X \mid xy = y\sigma_y(x) \rangle .$$

Furthermore, $s(x, y) = (y, \sigma_y(x))$ defines a left non-degenerate set-theoretic solution.



RELATING BOTH MONOIDS

Theorem (LV, JKA)

Let (X, r) be a left non-degenerate set-theoretic solution. Then, $M(X, r)$ is a regular submonoid of

$$A(X, r) \rtimes \mathrm{Sym}(X),$$

where $x \in X$ is embedded as (x, λ_x).

WHAT IS THE MONOIDS STRUCTURE

For bijective left non-degenerate set-theoretic solutions, one extends $\sigma_\cdot : X \longrightarrow \mathrm{Sym}(X)$ to a map $\sigma_\cdot : A(X,r) \longrightarrow \mathrm{Aut}(A(X,r))$.

Theorem

Let (X,r) be a finite bijective left non-degenerate solution. Then, there exists a positive integer d such that a^d is central in $A(X,r)$ for every $a \in A(X,r)$.

WHAT IS THE MONOIDS STRUCTURE

For bijective left non-degenerate set-theoretic solutions, one extends $\sigma_\cdot : X \longrightarrow \mathrm{Sym}(X)$ to a map $\sigma_\cdot : A(X,r) \longrightarrow \mathrm{Aut}(A(X,r))$.

Theorem

Let (X,r) be a finite bijective left non-degenerate solution. Then, there exists a positive integer d such that a^d is central in $A(X,r)$ for every $a \in A(X,r)$.
Furthermore, $M(X,r)$ is an abelian-by-finite monoid

WHAT IS THE MONOIDS STRUCTURE

For bijective left non-degenerate set-theoretic solutions, one extends $\sigma_\cdot : X \longrightarrow \mathrm{Sym}(X)$ to a map $\sigma_\cdot : A(X,r) \longrightarrow \mathrm{Aut}(A(X,r))$.

Theorem

Let (X,r) be a finite bijective left non-degenerate solution. Then, there exists a positive integer d such that a^d is central in $A(X,r)$ for every $a \in A(X,r)$.
Furthermore, $M(X,r)$ is an abelian-by-finite monoid

If one drops the bijectivity, one can still extend to endomorphisms.

LND SOLUTIONS

General left non-degenerate solutions: HARD!

Sketch

- *For some positive d, σ_a^d is idempotent for all $a \in A(X, r)$.*
- *$A(X, r)$ is a finite LEFT $\left\langle x^d \mid x \in X \right\rangle$-module.*
- *Study divisibility in the latter to obtain a chain:*

$$B_n \subseteq \ldots \subseteq B_1 = \left\langle x^d \mid x \in X \right\rangle .$$

- *Somehow $\left\langle x^d \mid x \in X \right\rangle$ acts abelian on factors.*

LND SOLUTIONS

General left non-degenerate solutions: HARD!

Sketch

- *For some positive d, σ_a^d is idempotent for all $a \in A(X,r)$.*
- *$A(X,r)$ is a finite LEFT $\langle x^d \mid x \in X \rangle$-module.*
- *Study divisibility in the latter to obtain a chain:*

$$B_n \subseteq \ldots \subseteq B_1 = \left\langle x^d \mid x \in X \right\rangle .$$

- *Somehow $\langle x^d \mid x \in X \rangle$ acts abelian on factors.*

Hence, $A(X,r)$ and its algebra are Left Noetherian.

UNDERSTANDING THE ALGEBRAS

Theorem

Let (X, r) be a finite bijective left non-degenerate solution and K a field. Then, $KM = KM(X, r)$ is a Noetherian PI-algebra, with

$$\mathrm{ClKdim}(KM) = \mathrm{GKdim}(KM) = \mathrm{rk}(M) = \mathrm{rk}(A) \leq |X|.$$

ONE SHOULD WATCH OUT

Theorem (CCS,CJVAV)

Let (X, r) be a finite left non-degenerate set-theoretic solution. TFAE

- (X, r) *is bijective,*
- (X, r) *is right non-degenerate.*

ON A CONJECTURE OF GATEVA-IVANOVA

Conjecture

Let (X, r) *be a finite bijective left non-degenerate solution. Does the cancellativity of* $M(X, r)$ *imply that* (X, r) *is involutive?*

ON A CONJECTURE OF GATEVA-IVANOVA

Conjecture

Let (X, r) be a finite bijective left non-degenerate solution. Does the cancellativity of $M(X, r)$ imply that (X, r) is involutive?

Theorem

Let (X, r) be a finite bijective left non-degenerate solution. Then the following are equivalent:

- *(X, r) is an involutive solution,*
- *$M(X, r)$ is a cancellative monoid,*
- *KM is a prime algebra,*
- *KM is a domain,*
- *$GKdim(KM) = |X|$.*

PRIME IDEALS A AND M

Since every element in $A(X,r)$ is normal, it follows that every prime ideal is determined by invariant subsets of X under certain σ_x.

Theorem

Let (X,r) be a finite left non-degenerate solution. Then every prime ideal P of $M(X,r)$ of height k is determined by prime ideals $Q_1, ..., Q_n$ of $A(X,r)$ of height k, i.e.

$$P = (Q_1 \cap ... \cap Q_n)^e.$$

ONGOING RESEARCH

- Study $M(X, r)$ and $KM(X, r)$ for left non-degenerate idempotent solutions

ONGOING RESEARCH

- Study $M(X, r)$ and $KM(X, r)$ for left non-degenerate idempotent solutions
- Study $M(X, r)$ and $KM(X, r)$ for general left non-degenerate

OPEN PROBLEM

Can one prove that for (bijective) left non-degenerate solutions, the irreducible representations of the algebra $KM(X, r)$ are finite-dimensional?

SHIFT OF FOCUS

We used solutions to generate nice algebraic structures.
Can we do the reverse?

STRUCTURE GROUP AS MOTIVATING EXAMPLE

Recall following theorem.

Theorem

Let (X, r) be a bijective non-degenerate solution, then there exists a group morphism

$$G(X, r) \hookrightarrow A_{gr}(X, r) \rtimes \langle \lambda_x \mid x \in X \rangle ,$$

where $x \mapsto (x, \lambda_x)$ and the projection on $A(X, r)$ is bijective.

In fact, the resulting projection $G(X, r) \longrightarrow A_{gr}(X, r)$ is a bijective 1-cocycle.

CHARACTERIZATIONS

In fact, the results in the previous theorem are equivalent.

Theorem

Let $(G, \circ)$ and $(A, +)$ be groups. Then the following are equivalent:

- *There exists a bijective 1-cocycle $\pi : G \longrightarrow A$,*
- *there exists an embedding of groups $G \longrightarrow A \rtimes \mathrm{Aut}(A, +)$, where the projection on A is bijective,*
- *There exists a skew left brace $(G, \oplus, \circ)$, where $(G, \oplus)$ is isomorphic to $(A, +)$.*

WHAT ARE SKEW LEFT BRACES

Definition

Two groups $(A, +)$ and $(A, \circ)$ form a skew left brace $(A, +, \circ)$, if for any $a, b, c \in A$, it holds that

$$a \circ (b + c) = (a \circ b) - a + (a \circ c),$$

where $-a$ denotes the inverse of a in $(A, +)$.
Moreover, if $(A, +)$ is abelian, then $(A, +, \circ)$ is a left brace

EXAMPLES OF SKEW BRACES

Example

1. Every group $(G, +)$ has the skew left brace structure $(G, +, +)$, these are *trivial skew left braces*.
2. *Let (X, r) be a bijective non-degenerate solution, then $G(X, r)$ has a skew brace structure, which is a left brace if and only if (X, r) is involutive.*
3. *The dihedral group $D_{2n} = \langle a, b \mid a^n = b^2 = 1, bab = a^{-1} \rangle$ has a left brace structure, where $a^i b^j + a^k b^l = a^{i+k+jl} b^{j+l}$ with $j, l \in \{0, 1\}$.*

CREATING SOLUTIONS ON $G(X, R)$ (1)

Definition (Rump, CJO, GV)

Let $(B, +)$ and $(B, \circ)$ be groups on the same set B such that for any $a, b, c \in B$ it holds that

$$a \circ (b + c) = (a \circ b) - a + (a \circ c).$$

Then $(B, +, \circ)$ is called a skew left brace

If $(B, +)$ is abelian, one says that $(B, +, \circ)$ is a left brace.

CREATING SOLUTIONS ON $G(X, R)$ (1)

Definition (Rump, CJO, GV)

Let $(B, +)$ and $(B, \circ)$ be groups on the same set B such that for any $a, b, c \in B$ it holds that

$$a \circ (b + c) = (a \circ b) - a + (a \circ c).$$

Then $(B, +, \circ)$ is called a skew left brace

If $(B, +)$ is abelian, one says that $(B, +, \circ)$ is a left brace.
Denote for $a, b \in B$, the map $\lambda_a(b) = -a + a \circ b$. Then, $\lambda : (B, \circ) \longrightarrow \mathrm{Aut}(B, +) : a \mapsto \lambda_a$ is a well-defined group morphism.

CREATING SOLUTIONS ON $G(X, R)$ (2)

Theorem

Let $(B, +, \circ)$ be a skew left brace. Denote for any $a, b \in B$, the map $r_B(a, b) = (\lambda_a(b), \overline{(\overline{a} + b)} \circ b)$. Then (B, r_B) is a bijective non-degenerate solution. Moreover, if $(B, +)$ is abelian, then (B, r_B) is involutive.

Remark

Let (X, r) be a bijective non-degenerate set-theoretic solution. Then, $G(X, r)$ is a skew left brace.

THE *-OPERATION IN SKEW LEFT BRACES

Definition

Let $(A, +, \circ)$ be a skew left brace. For any $a, b \in A$, denote

$$a * b = -a + a \circ b - b = \lambda_a(b) - b.$$

Denote $X * Y$ for the additive subgroup generated by $x * y$, where $x \in X, y \in Y$ and $X, Y \subseteq A$.

Example

1. For $(G, +, +)$, one sees that $a * b = 0$. Actually a characterization.
2. For $(D_{2n}, +, \cdot)$ one can see that $(a^i b^j) * (a^k b^l) \in \langle a \rangle$.

WHERE DOES THE $*$-OPERATION ORIGINATE

Definition

Let $(A, +, \circ)$ be a skew left brace. We call A two-sided, if for any $a, b, c \in A$ it holds that

$$(b + c) \circ a = (b \circ a) - a + (c \circ a).$$

Theorem

Let $(A, +, \circ)$ be a left brace. Then, $(A, +, \circ)$ is two-sided if and only if $(A, +, *)$ is a Jacobson radical ring.

Proposition

Let $(A, +, \circ)$ be a left brace. Then A is two-sided if and only if the $*$-operation is associative.

Breaks down for skew left braces.

SOLUTIONS LIKE LYUBASHENKO'S

Definition (Retraction)

Let (X, r) be an involutive non-degenerate set-theoretic solution. Define the relation $x \sim y$ on X, when $\lambda_x = \lambda_y$. Then, there exists a natural set-theoretic solution on $X/\sim$ called the retraction $\mathrm{Ret}(X, r)$.

SOLUTIONS LIKE LYUBASHENKO'S

Definition (Retraction)

Let (X, r) be an involutive non-degenerate set-theoretic solution. Define the relation $x \sim y$ on X, when $\lambda_x = \lambda_y$. Then, there exists a natural set-theoretic solution on $X/\sim$ called the retraction $\mathrm{Ret}(X, r)$.

Denote for $n \geq 2$, $\mathrm{Ret}^n(X, r) = \mathrm{Ret}\left(\mathrm{Ret}^{n-1}(X, r)\right)$. If there exists a positive integer n such that $|\mathrm{Ret}^n(X, r)| = 1$, then (X, r) is called a multipermutation solution

WHY ARE MULTIPERMUTATION SOLUTIONS INTERESTING

Theorem (CJOBVAGI)

Let (X, r) be a finite involutive non-degenerate set-theoretic solution. The following statements are equivalent,

- *the solution (X, r) is a multipermutation solution,*
- *the group $G(X, r)$ is left orderable,*
- *the group $G(X, r)$ is diffuse,*
- *the group $G(X, r)$ is poly-$\mathbb{Z}$.*

STRUCTURE OF SKEW LEFT BRACES

Definition

Let $(B, +, \circ)$ be a skew left brace. Denote for any $a, b \in B$ the operation $a * b = \lambda_a(b) - b$ and denote for any positive integer $n > 1$, the set $B^{(n)} = B^{(n-1)} * B$. If there exists a positive integer n such that $B^{(n)} = 1$, we say that B is right nilpotent. If $B^{(2)} = 1$, we say that B is trivial.

Theorem (GIC)

Let (X, r) be an involutive non-degenerate set-theoretic solution. If the natural left brace $G(X, r)$ is right nilpotent, then the solutions $(G(X, r), r_G)$ and (X, r) are multipermutation solutions.

LEFT IDEALS AND IDEALS

Definition

Let $(B, +, \circ)$ be a skew left brace. Then, a (normal) subgroup I of $(B, +)$ such that $B * I \subseteq I$ is called a (strong) left ideal. Furthermore, if I is in addition a normal subgroup of $(B, \circ)$ then I is called an ideal of B.

Definition

Let $(B, +, \circ)$ be a skew left brace. If there exist left ideals I, J of B such that $I + J = B = J + I$, then B is called factorizable by I and J.

WHY INTERESTED IN STRONG LEFT IDEALS?

Definition

Let (X, r) be a bijective non-degenerate solution. Then, we call a split $X = Y \cup Z$ a decomposition if Y and Z are non-empty subsolutions and $r(X \times Y) = Y \times X$ and $r(Y \times X) = X \times Y$.

Proposition

A decomposition $X = Y \cup Z$ gives rise to a factorization $G(X, r) = \langle Y \rangle + \langle Z \rangle$. and both terms are strong left ideals in $G(X, r)$. Vice versa, every strong left ideal of a brace B gives rise to a decomposition of (B, r_B).

INTUITION: FACTORIZATIONS IN GROUPS

Theorem (Ito's Theorem)

Let $G = A + B$ be a factorized group. If A and B are both abelian, then G is metabelian (i.e. there exists an abelian normal subgroup N of G such that G/N is abelian).

Theorem

Let $G = A + B$ be a factorized group, where A and B are abelian. Then there exists a normal subgroup N of G contained in A or B.

Theorem (Kegel-Wielandt)

Let $G = A + B$ be a factorized group, where A and B are nilpotent. Then, G is solvable.

SURPRISING RESULTS

Theorem

Let $B = I + J$ be a factorized skew left brace. If I is a strong left ideal and both I and J are trivial skew left braces, then B is right nilpotent of class at most 4. If both are strong left ideals, then B is right nilpotent of class at most 3.

Theorem

Let $B = I + J$ be a factorized skew left brace. If I is a strong left ideal and both I and J are trivial skew left braces, then there exists an ideal N of B contained in I or J.

EXTENDING IS NOT POSSIBLE

Example (No Kegel-Wielandt)

There exists a simple (no non-trivial ideals) left brace of size 72, which is hence not solvable. By standard techniques one sees that this is factorizable by the additive Sylow subgroups.

Example (No relaxing conditions)

There exists a skew left brace of size 18 that is factorizable by 2 left ideals, both not strong left ideals. However, there is no ideal of the skew left brace contained in either of the left ideals.

WHERE DOES THE $*$-OPERATION ORIGINATE?

Theorem (Rump)

Let $(R, +, *)$ be a Jacobson radical ring. Then, the operation $a \circ b = a + ab + b$ defines a group operation on R. In particular, $(R, +, \circ)$ is a left brace satisfying

$$(b + c) \circ a = (b \circ a) - a + (c \circ a).$$

Vice versa, every such two-sided brace $(B, +, \circ)$ gives rise to a Jacobson radical ring $(B, +, *)$.

Theorem (Lau)

Let $(B, +, \circ)$ be a left brace. The operation $*$ is associative if and only if B is two-sided.

RING THEORETICAL INSPIRATION

- (Semi-)prime ideals (related to solvability),
- Radicals,
- Nil, nilpotent (what side?) (Köthe?),
- Modules? (widely open),
- Skew braces of size 64?

HOT FROM THE NEEDLE

Theorem (Smoktunowicz, Shalev)

Let $(B, +, \circ)$ *be a left brace of p-power order* (p^n). *If* $p > n + 1$, *then there exists a pre-Lie ring associated to* $B/ann(p^2)$ *and vice versa.*

Does this provide a framework to understand the counterexample of Bachiller?

Conjecture (false, Bachiller)

Let $(B, \circ)$ *be a finite solvable group. Then there exists an abelian group* $(B, +)$ *such that* $(B, +, \circ)$ *is a left brace.*

Conjecture (Byott)

Let $(B, +, \circ)$ *be a finite skew left brace with* $(B, +)$ *solvable. Is* $(B, \circ)$ *solvable?*

REFERENCES

1. T.Gateva-Ivanova and M.Van den Bergh, Semigroups of I-type, Journal of Algebra (1998).
2. E. Jespers, Ł. Kubat, A. Van Antwerpen and L. Vendramin, Factorizations of skew braces, Mathematische Annalen
3. E. Jespers, Ł. Kubat and A. Van Antwerpen, The structure monoid and algebra of a left non-degenerate set-theoretic solution of the Yang–Baxter equation, Trans. Amer. Math. Soc. (2019).
4. I. Colazzo, E. Jespers, A. Van Antwerpen and C. Verwimp, Left non-degenerate set-theoretic solutions of the Yang-Baxter equation and semitrusses, Journal of Algebra

PRIME IDEALS OF *KM*

Can we describe prime ideals of the algebra KM? Let us first consider prime ideals not intersecting the monoid.

PRIME IDEALS OF *KM*

Can we describe prime ideals of the algebra KM? Let us first consider prime ideals not intersecting the monoid.

Theorem

Let (X, r) be a finite left non-degenerate solution. Then there exists an inclusion preserving bijection between prime ideals of $KG(X, r)$ and prime ideals P of KM with $P \cap M = \emptyset$.

DIVISIBILITY IN M

Let $Y \subseteq X$. Denote $M_Y = \bigcap_{y \in Y} yM$ and $D_Y = M_Y \setminus \bigcup_{x \in X \setminus Y} M_{\{x\}}$.

DIVISIBILITY IN M

Let $Y \subseteq X$. Denote $M_Y = \bigcap_{y \in Y} yM$ and $D_Y = M_Y \setminus \bigcup_{x \in X \setminus Y} M_{\{x\}}$.

Theorem

Let (X, r) be a finite left non-degenerate solution. Let P be a prime ideal in KM with $P \cap M \neq \emptyset$. Then,

$$P \cap M = \bigcup_{Y \in \mathcal{F}} D_Y,$$

where $\mathcal{F} = \{Y \subseteq X \mid D_Y \cap P \neq \emptyset\}$.