Finite Coverings

A Journey through Groups, Loops, Rings, and Semigroups.

Luise-Charlotte Kappe
Binghamton University
menger@math.binghamton.edu

Definition

A group is said to have a finite covering by subgroups if it is the union of finitely many proper subgroups.

Definition

A group is said to have a finite covering by subgroups if it is the union of finitely many proper subgroups.

Claim

No group is the union of two proper subgroups.

Definition

A group is said to have a finite covering by subgroups if it is the union of finitely many proper subgroups.

Claim

No group is the union of two proper subgroups.

Proof.

Suppose A, B are proper subgroups of G with $G = A \cup B$. Then there exist $a \in A$ and $b \in B$ with $a \notin B$ and $b \notin A$.

Definition

A group is said to have a finite covering by subgroups if it is the union of finitely many proper subgroups.

Claim

No group is the union of two proper subgroups.

Proof.

Suppose A, B are proper subgroups of G with $G = A \cup B$. Then there exist $a \in A$ and $b \in B$ with $a \notin B$ and $b \notin A$.
We have $ab \in G$. So $ab \in A$ or $ab \in B$.

Definition

A group is said to have a finite covering by subgroups if it is the union of finitely many proper subgroups.

Claim

No group is the union of two proper subgroups.

Proof.

Suppose A, B are proper subgroups of G with $G = A \cup B$. Then there exist $a \in A$ and $b \in B$ with $a \notin B$ and $b \notin A$.
We have $ab \in G$. So $ab \in A$ or $ab \in B$.
If $ab \in A$, then $a^{-1}(ab) = b \in A$, a contradiction.

Definition

A group is said to have a finite covering by subgroups if it is the union of finitely many proper subgroups.

Claim

No group is the union of two proper subgroups.

Proof.

Suppose A, B are proper subgroups of G with $G = A \cup B$. Then there exist $a \in A$ and $b \in B$ with $a \notin B$ and $b \notin A$.
We have $ab \in G$. So $ab \in A$ or $ab \in B$.
If $ab \in A$, then $a^{-1}(ab) = b \in A$, a contradiction.
Similarly, if $ab \in B$.
Our claim follows. □

Theorem

A group is the union of finitely many proper subgroups if and only if it has a finite noncyclic homomorphic image.

Theorem

A group is the union of finitely many proper subgroups if and only if it has a finite noncyclic homomorphic image.

B.H. Neumann, Groups covered by finitely many cosets, Publ. Math. Debrecen 3 (1954) 227-242.

Definition

A group is a nonempty set with a binary operation $G \times G \to G$, satisfying the following conditions:

Definition

A group is a nonempty set with a binary operation $G \times G \to G$, satisfying the following conditions:

$$(G)\begin{cases} (1) & \textit{associative;} \\ (2) & \textit{identity } 1 \cdot a = a \cdot 1 = a; \\ (3) & \textit{for } a, b \in G \textit{ exist unique} \\ & x, y \in G \textit{ with } xa = b \textit{ and } ay = b. \end{cases}$$

Definition

A group is a nonempty set with a binary operation $G \times G \to G$, satisfying the following conditions:

$$(G)\begin{cases} (1) & \textit{associative;} \\ (2) & \textit{identity } 1 \cdot a = a \cdot 1 = a; \\ (3) & \textit{for } a, b \in G \textit{ exist unique} \\ & x, y \in G \textit{ with } xa = b \textit{ and } ay = b. \end{cases}$$

Loop $= (G) - (1)$; Quasigroup $= (G) - (1) - (2)$.

Definition

A group is a nonempty set with a binary operation $G \times G \to G$*, satisfying the following conditions:*

$$(G)\begin{cases} (1) & \textit{associative;} \\ (2) & \textit{identity } 1 \cdot a = a \cdot 1 = a; \\ (3) & \textit{for } a, b \in G \textit{ exist unique} \\ & x, y \in G \textit{ with } xa = b \textit{ and } ay = b. \end{cases}$$

Loop $= (G) - (1)$; Quasigroup $= (G) - (1) - (2)$.
Semigroup $= (G) - (2) - (3)$;
Monoid $= (G) - (3)$.

Exercise

No loop is the union of two proper subloops.

Exercise

No loop is the union of two proper subloops.

Example

Let $S = \mathbb{N}$*, the set of natural numbers under multiplication, and* $\mathbb{O}$ *and* $\mathbb{E}$ *the semigroups of odd and even integers. Then* $\mathbb{N} = \mathbb{O} \cup \mathbb{E}$*.*

Definition

Let R be a nonempty set with two binary operations, addition "$+$" and multiplication "$\cdot$". Then R is a ring if

Definition

Let R be a nonempty set with two binary operations, addition "$+$" and multiplication "$\cdot$". Then R is a ring if

(1) *R is a commutative (abelian) group with respect to addition;*

Definition

Let R be a nonempty set with two binary operations, addition "$+$" and multiplication "$\cdot$". Then R is a ring if

(1) *R is a commutative (abelian) group with respect to addition;*

(2) *the multiplication is associative;*

Definition

Let R be a nonempty set with two binary operations, addition "$+$" and multiplication "$\cdot$". Then R is a ring if

(1) *R is a commutative (abelian) group with respect to addition;*

(2) *the multiplication is associative;*

(3) *the two operations are distributive, i.e.*

$$a(b+c) = ab + ac \quad \text{and} \quad (a+b)c = ac + bc.$$

Definition

Let R be a nonempty set with two binary operations, addition "$+$" and multiplication "$\cdot$". Then R is a ring if

(1) *R is a commutative (abelian) group with respect to addition;*

(2) *the multiplication is associative;*

(3) *the two operations are distributive, i.e.*

$$a(b+c) = ab + ac \quad \text{and} \quad (a+b)c = ac + bc.$$

Theorem

No ring is the union of two proper subrings.

G. Scorza, *Gruppi che possone come somma di tre sotto gruppi*, Boll. Un. Mat. Ital. 5 (1926), 216-218.

G. Scorza, *Gruppi che possone come somma di tre sotto gruppi*, Boll. Un. Mat. Ital. 5 (1926), 216-218.

Theorem

For a group G we have $\sigma(G) = 3$ if and only if G has a homomorphic image isomorphic to the Klein 4-group.

J.E.H. Cohn, *On n-sum groups*, Math. Scand. 75 (1994), 44-58.

J.E.H. Cohn, *On n-sum groups*, Math. Scand. 75 (1994), 44-58.

Question

Given a group G with a finite covering, what is the minimum number $\sigma(G)$ of subgroups needed to cover G?

J.E.H. Cohn, *On n-sum groups*, Math. Scand. 75 (1994), 44-58.

Question

Given a group G with a finite covering, what is the minimum number $\sigma(G)$ of subgroups needed to cover G?

Conjecture

For a non-cyclic solvable group, the covering number has the form "prime power plus one".

J.E.H. Cohn, *On n-sum groups*, Math. Scand. 75 (1994), 44-58.

Question

Given a group G with a finite covering, what is the minimum number $\sigma(G)$ of subgroups needed to cover G?

Conjecture

For a non-cyclic solvable group, the covering number has the form "prime power plus one".

Gives examples of solvable groups with $\sigma(G) = p^\alpha + 1$ for all $p^\alpha + 1$ and shows $\sigma(A_5) = 10$, $\sigma(S_5) = 16$.

M.J. Tomkinson, *Groups as the union of proper subgroups*, Math. Scand. 81 (1997), 189-198.

M.J. Tomkinson, *Groups as the union of proper subgroups*, Math. Scand. 81 (1997), 189-198.

Theorem

Let G be a finite solvable group and let p^α be the order of the smallest chief factor having more than one complement. Then $\sigma(G) = p^\alpha + 1$.

M.J. Tomkinson, *Groups as the union of proper subgroups*, Math. Scand. 81 (1997), 189-198.

Theorem

Let G be a finite solvable group and let p^α be the order of the smallest chief factor having more than one complement. Then $\sigma(G) = p^\alpha + 1$.

Theorem

There exists no group G with $\sigma(G) = 7$.

M.J. Tomkinson, *Groups as the union of proper subgroups*, Math. Scand. 81 (1997), 189-198.

Theorem

Let G be a finite solvable group and let p^α be the order of the smallest chief factor having more than one complement. Then $\sigma(G) = p^\alpha + 1$.

Theorem

There exists no group G with $\sigma(G) = 7$.

Conjecture

There exist no groups with
$\sigma(G) = 11$, *13 or 15.*

R.A. Bryce, V. Fedri, and L. Serena, *Subgroup coverings of some linear groups*, Bull. Austral. Math. Soc. 60 (1999), 227-238.

R.A. Bryce, V. Fedri, and L. Serena, *Subgroup coverings of some linear groups*, Bull. Austral. Math. Soc. 60 (1999), 227-238.

Theorem

There exists a group G with $\sigma(G) = 15$, namely $G \cong \mathrm{PSL}(2,7)$.

A. Abdollahi, F. Ashraf and S.M. Shaker, *The symmetric group of degree six can be covered by* 13 *and no fewer subgroups*, Bull. Malays. Math. Sci. Soc. 30 (2007), 57-58.

A. Abdollahi, F. Ashraf and S.M. Shaker, *The symmetric group of degree six can be covered by* 13 *and no fewer subgroups*, Bull. Malays. Math. Sci. Soc. 30 (2007), 57-58.

E. Detomi and A. Lucchini, *On the structure of primitive n-sum groups*, CUBO, A Mathematical Journal, 10 (2008), 195-210.

A. Abdollahi, F. Ashraf and S.M. Shaker, *The symmetric group of degree six can be covered by* 13 *and no fewer subgroups*, Bull. Malays. Math. Sci. Soc. 30 (2007), 57-58.

E. Detomi and A. Lucchini, *On the structure of primitive n-sum groups*, CUBO, A Mathematical Journal, 10 (2008), 195-210.

Theorem

There exists no group with $\sigma(G) = 11$.

Methods used by Tomkinson, Detomi and Lucchini

"Assume to the contrary that there exists a group with covering number n ... and come up with a contradiction."

Methods used by Tomkinson, Detomi and Lucchini

"Assume to the contrary that there exists a group with covering number n … and come up with a contradiction."

New method

Find complement, i.e. all integers n which are covering numbers.

M. Garonzi, *Finite groups that are the union of at most* 25 *proper subgroups*, J. of Algebra and its Applications, 12 (2013), 1-10.

M. Garonzi, *Finite groups that are the union of at most* 25 *proper subgroups*, J. of Algebra and its Applications, 12 (2013), 1-10.

Theorem

There exists no group G with $\sigma(G) = 19$, 21, 22, or 25.

M. Garonzi, *Finite groups that are the union of at most 25 proper subgroups*, J. of Algebra and its Applications, 12 (2013), 1-10.

Theorem

There exists no group G with $\sigma(G) = 19, 21, 22,$ or 25.

$\sigma(G)$	2	7	11	13	15	16	19	21	22	23	25
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	S_6	PSL(2,7)	S_5, A_6	$\emptyset$	$\emptyset$	$\emptyset$	M_{11}	$\emptyset$

Observation

For $2 \leq n \leq 18$ there are only three integers which are not covering numbers, that is around 18%.

Observation

For $2 \leq n \leq 18$ there are only three integers which are not covering numbers, that is around 18%.

Question

Are there infintely many integers which are not covering numbers?

Observation

For $2 \leq n \leq 18$ there are only three integers which are not covering numbers, that is around 18%.

Question

Are there infintely many integers which are not covering numbers?

New results

For $2 \leq n \leq 129$ around 50% of the integers are not covering numbers.

Observation

For $2 \leq n \leq 18$ there are only three integers which are not covering numbers, that is around 18%.

Question

Are there infintely many integers which are not covering numbers?

New results

For $2 \leq n \leq 129$ around 50% of the integers are not covering numbers.

Conjecture

There are infinitely many integers which are not covering numbers.

Observation

For $2 \leq n \leq 18$ there are only three integers which are not covering numbers, that is around 18%.

Question

Are there infintely many integers which are not covering numbers?

New results

For $2 \leq n \leq 129$ around 50% of the integers are not covering numbers.

Conjecture

There are infinitely many integers which are not covering numbers.

M. Garonzi, L.-C. Kappe, E. Swartz, On integers that are covering numbers, submitted.

Some Definitions:

Some Definitions:

- A finite group is σ-elementary if $\sigma(G) < \sigma(G/N)$ for every nontrivial normal subgroup N of G with the convention that $\sigma(G) = \infty$ if G is cyclic.

Some Definitions:

- A finite group is σ-elementary if $\sigma(G) < \sigma(G/N)$ for every nontrivial normal subgroup N of G with the convention that $\sigma(G) = \infty$ if G is cyclic.
- A finite group is said to be monolithic if it admits a unique minimal normal subgroup.

Some Definitions:

- A finite group is σ-elementary if $\sigma(G) < \sigma(G/N)$ for every nontrivial normal subgroup N of G with the convention that $\sigma(G) = \infty$ if G is cyclic.
- A finite group is said to be monolithic if it admits a unique minimal normal subgroup.
- A finite group is said to be primitive if it admits a maximal subgroup M such that $M_G = \bigcap_{g \in G} g^{-1}Mg$, the normal core of M, is trivial. The index $[G : M]$ is called the primitivity degree of G with respect to M.

Theorem (GKS (2017+))

Let G be a nonabelian σ-elementary group with $\sigma(G) \leq 129$. Then G is primitive and monolithic with degree of primitivity at most 129, and the smallest degree of primitivity of G is at most $\sigma(G)$.

Theorem (GKS (2017+))

Let G be a nonabelian σ-elementary group with $\sigma(G) \leq 129$. Then G is primitive and monolithic with degree of primitivity at most 129, and the smallest degree of primitivity of G is at most $\sigma(G)$.

Remark

Reduction says we need "only" check primitive monolithic groups up to degree 129. (Counting repeats, over 700 nonsolvable groups.)

Theorem (GKS (2017+))

Let G be a nonabelian σ-elementary group with $\sigma(G) \leq 129$. Then G is primitive and monolithic with degree of primitivity at most 129, and the smallest degree of primitivity of G is at most $\sigma(G)$.

Remark

Reduction says we need "only" check primitive monolithic groups up to degree 129. (Counting repeats, over 700 nonsolvable groups.)

Conjecture

Every nonabelian σ-elementary group is a monolithic primitive group.

Theorem (GKS (2017+))

Let G be a nonabelian σ-elementary group with $\sigma(G) \leq 129$. Then G is primitive and monolithic with degree of primitivity at most 129, and the smallest degree of primitivity of G is at most $\sigma(G)$.

Remark

Reduction says we need "only" check primitive monolithic groups up to degree 129. (Counting repeats, over 700 nonsolvable groups.)

Conjecture

Every nonabelian σ-elementary group is a monolithic primitive group.

E. Detomi and A. Lucchini, On the structure of primitive *n*-sum groups, CUBO, 10 (2008), 195-210.

New results

New results

Theorem (Garonzi, Kappe, Swartz (2017+))

The integers between 26 *and* 129 *which are not covering numbers are* 27, 34, 35, 37, 39, 41, 43, 45, 47, 49, 51, 52, 53, 55, 56, 58, 59, 61, 66, 69, 70, 75, 76, 77, 78, 79, 81, 83, 87, 88, 89, 91, 93, 94, 95, 96, 97, 99, 100, 101, 103, 105, 106, 107, 109, 111, 112, 113, 115, 116, 117, 118, 119, 120, 123, 124, 125.

New results

Theorem (Garonzi, Kappe, Swartz (2017+))

The integers between 26 *and* 129 *which are not covering numbers are* 27, 34, 35, 37, 39, 41, 43, 45, 47, 49, 51, 52, 53, 55, 56, 58, 59, 61, 66, 69, 70, 75, 76, 77, 78, 79, 81, 83, 87, 88, 89, 91, 93, 94, 95, 96, 97, 99, 100, 101, 103, 105, 106, 107, 109, 111, 112, 113, 115, 116, 117, 118, 119, 120, 123, 124, 125.

Theorem (GKS (2017+))

Let $q = p^d$ *be a prime power and* $n \geq 2$, $n \neq 3$ *be a positive integer. Then* $(q^n - 1)/(q - 1)$ *is a covering number.*

- List of groups with primitivity degree n produced by GAP.

- List of groups with primitivity degree n produced by GAP.
- We need to study the covering numbers of primitive groups of "small" degree.

- List of groups with primitivity degree n produced by GAP.
- We need to study the covering numbers of primitive groups of "small" degree.
- Exact values are desirable; sometimes lower bounds suffice.

- List of groups with primitivity degree n produced by GAP.
- We need to study the covering numbers of primitive groups of "small" degree.
- Exact values are desirable; sometimes lower bounds suffice.

Main tools:

- List of groups with primitivity degree n produced by GAP.
- We need to study the covering numbers of primitive groups of "small" degree.
- Exact values are desirable; sometimes lower bounds suffice.

Main tools:

- known formulas/asymptotic results

- List of groups with primitivity degree n produced by GAP.
- We need to study the covering numbers of primitive groups of "small" degree.
- Exact values are desirable; sometimes lower bounds suffice.

Main tools:

- known formulas/asymptotic results
- linear programming (GAP, then Gurobi)

- List of groups with primitivity degree *n* produced by GAP.
- We need to study the covering numbers of primitive groups of "small" degree.
- Exact values are desirable; sometimes lower bounds suffice.

Main tools:

- known formulas/asymptotic results
- linear programming (GAP, then Gurobi)
- "greedy" search for "hardest to cover" conjugacy classes

Expansion beyond 129?

Expansion beyond 129?

- Prove conjecture about structure of σ-elementary groups or expand bound for which conjecture holds beyond 129.

Expansion beyond 129?

- Prove conjecture about structure of σ-elementary groups or expand bound for which conjecture holds beyond 129.
- Requires new methods for determining covering numbers of groups.

The covering number of rings

The covering number of rings

A. Lucchini and A. Maróti, *Rings as the union of proper subrings*, Algebras and Representation Theory, **15** (2012), 1035-1047.

The covering number of rings

A. Lucchini and A. Maróti, *Rings as the union of proper subrings*, Algebras and Representation Theory, **15** (2012), 1035-1047.

Theorem

A ring is the union of three proper subrings if and only if R has a factor ring (of order 4 or 8) isomorphic to five types of rings.

Nicholas J. Werner, *Covering Numbers of Finite Rings*, American Mathematical Monthly, **122** (2015), 552-556.

Nicholas J. Werner, *Covering Numbers of Finite Rings*, American Mathematical Monthly, **122** (2015), 552-556.

Notation

$\mathbb{F}_p$, $\mathbb{F}_q$ finite fields of order p and q, where $q = p^\alpha$, p a prime, $\alpha \in \mathbb{N}$.

Some Observations:

Some Observations:

$\mathbb{F}_p$, $\mathbb{F}_q$ have no finite covering.

Some Observations:

$\mathbb{F}_p$, $\mathbb{F}_q$ have no finite covering.

$\mathbb{F}_2 \times \mathbb{F}_2$ has a finite covering, in fact $\sigma(\mathbb{F}_2 \times \mathbb{F}_2) = 3$.

Some Observations:

$\mathbb{F}_p$, $\mathbb{F}_q$ have no finite covering.

$\mathbb{F}_2 \times \mathbb{F}_2$ has a finite covering, in fact $\sigma(\mathbb{F}_2 \times \mathbb{F}_2) = 3$.

Questions

Some Observations:
$\mathbb{F}_p$, $\mathbb{F}_q$ have no finite covering.
$\mathbb{F}_2 \times \mathbb{F}_2$ has a finite covering, in fact $\sigma(\mathbb{F}_2 \times \mathbb{F}_2) = 3$.
Questions

- What about $\mathbb{F}_p \times \mathbb{F}_p$, $p > 2$? $\mathbb{F}_p \times \mathbb{F}_p$ **has no finite covering for** $p > 2$**.**

Some Observations:
$\mathbb{F}_p$, $\mathbb{F}_q$ have no finite covering.
$\mathbb{F}_2 \times \mathbb{F}_2$ has a finite covering, in fact $\sigma(\mathbb{F}_2 \times \mathbb{F}_2) = 3$.
Questions

- What about $\mathbb{F}_p \times \mathbb{F}_p$, $p > 2$? $\mathbb{F}_p \times \mathbb{F}_p$ **has no finite covering for** $p > 2$**.**
- What about $\mathbb{F}_2 \times \mathbb{F}_4$? $\mathbb{F}_2 \times \mathbb{F}_4$ **has no finite covering.**

Some Observations:
$\mathbb{F}_p$, $\mathbb{F}_q$ have no finite covering.
$\mathbb{F}_2 \times \mathbb{F}_2$ has a finite covering, in fact $\sigma(\mathbb{F}_2 \times \mathbb{F}_2) = 3$.
Questions

- What about $\mathbb{F}_p \times \mathbb{F}_p$, $p > 2$? $\mathbb{F}_p \times \mathbb{F}_p$ **has no finite covering for** $p > 2$**.**
- What about $\mathbb{F}_2 \times \mathbb{F}_4$? $\mathbb{F}_2 \times \mathbb{F}_4$ **has no finite covering.**

Theorem

Let p be a prime and $R = \sum_{i=1}^{t} \mathbb{F}_p$, the direct sum of t copies of $\mathbb{F}_p$. Then R has a finite covering if and only if $t \geq p$ and $\sigma(R) = p + \binom{p}{2}$.

- There are rings R with $3 \leq \sigma(R) \leq 12$, in particular, there are rings R with $\sigma(R) = 7$ and $\sigma(R) = 11$.

- There are rings R with $3 \leq \sigma(R) \leq 12$, in particular, there are rings R with $\sigma(R) = 7$ and $\sigma(R) = 11$.
- Is there a ring with $\sigma(R) = 13$?

The covering number of semigroups

The covering number of semigroups

Theorem

Let S be a finite semigroup not generated by a single element. Then $\sigma(S) = 2$, if S is not a group.

The covering number of semigroups

Theorem

Let S be a finite semigroup not generated by a single element. Then $\sigma(S) = 2$, if S is not a group.

C. Donoven and L.-C. Kappe, *On the covering number of semigroups*, in preparation.

The covering number of loops

The covering number of loops

S.M. Gagola III and L.C. Kappe, *On the covering number of loops*, Expositiones Mathematica, 34, (2016) 436-447.

The covering number of loops

S.M. Gagola III and L.C. Kappe, *On the covering number of loops*, Expositiones Mathematica, 34, (2016) 436-447.

Theorem

For every integer $n > 2$ there exists a loop L with $\sigma(L) = n$.

The covering number of loops

S.M. Gagola III and L.C. Kappe, *On the covering number of loops*, Expositiones Mathematica, 34, (2016) 436-447.

Theorem

For every integer $n > 2$ there exists a loop L with $\sigma(L) = n$.

Proposition

For every integer $n > 2$, there exists an idempotent quasigroup $\mathcal{Q}_n$ of order n such that any two distinct elements generate $\mathcal{Q}_n$.

Definition of the loop $\mathcal{L}^{(n)}(\mathbb{F})$

Let $\mathbb{F}$ be a field with multiplicative group $\mathbb{F}^*$ and

$$\mathcal{L}^{(n)}(\mathbb{F}) = \{a_i(x) \mid x \in \mathbb{F}^*, i \in \mathcal{Q}_n\} \cup \{\mathbf{1}\}.$$

Definition of the loop $\mathcal{L}^{(n)}(\mathbb{F})$

Let $\mathbb{F}$ be a field with multiplicative group $\mathbb{F}^*$ and

$$\mathcal{L}^{(n)}(\mathbb{F}) = \{a_i(x) \mid x \in \mathbb{F}^*, i \in \mathcal{Q}_n\} \cup \{\mathbf{1}\}.$$

A binary operation on $\mathcal{L}^{(n)}(\mathbb{F})$ is defined as follows:

(i) For any $l \in \mathcal{L}^{(n)}(\mathbb{F})$, $\mathbf{1}l = l \cdot \mathbf{1} = l$;

Definition of the loop $\mathcal{L}^{(n)}(\mathbb{F})$

Let $\mathbb{F}$ be a field with multiplicative group $\mathbb{F}^*$ and

$$\mathcal{L}^{(n)}(\mathbb{F}) = \{a_i(x) \mid x \in \mathbb{F}^*, i \in \mathcal{Q}_n\} \cup \{\mathbf{1}\}.$$

A binary operation on $\mathcal{L}^{(n)}(\mathbb{F})$ is defined as follows:

(i) For any $l \in \mathcal{L}^{(n)}(\mathbb{F})$, $\mathbf{1}l = l \cdot \mathbf{1} = l$;

(ii) For $x, y \in \mathbb{F}^*$ and $i \in \mathcal{Q}_n$,

$$a_i(x)a_i(y) = \begin{cases} a_i(x+y) & \text{if } x+y \neq 0, \\ \mathbf{1} & \text{otherwise;} \end{cases}$$

Definition of the loop $\mathcal{L}^{(n)}(\mathbb{F})$

Let $\mathbb{F}$ be a field with multiplicative group $\mathbb{F}^*$ and

$$\mathcal{L}^{(n)}(\mathbb{F}) = \{a_i(x) \mid x \in \mathbb{F}^*, i \in \mathcal{Q}_n\} \cup \{\mathbf{1}\}.$$

A binary operation on $\mathcal{L}^{(n)}(\mathbb{F})$ is defined as follows:

(i) For any $l \in \mathcal{L}^{(n)}(\mathbb{F})$, $\mathbf{1}l = l \cdot \mathbf{1} = l$;

(ii) For $x, y \in \mathbb{F}^*$ and $i \in \mathcal{Q}_n$,

$$a_i(x)a_i(y) = \begin{cases} a_i(x+y) & \text{if } x+y \neq 0, \\ \mathbf{1} & \text{otherwise;} \end{cases}$$

(iii) For $x, y \in \mathbb{F}^*$ and $i, j \in \mathcal{Q}_n$ with $i \neq j$,

$$a_i(x)a_j(y) = a_{i*j}(xy).$$