Dedekind Skew Braces

Massimiliano Di Matteo

Università degli Studi della Campania "Luigi Vanvitelli"
Dipartimento di Matematica e Fisica

Advances in Group Theory and Applications 2025
Napoli, June 23–28, 2025

Dedekind Groups

Massimiliano Di Matteo

Definition

A group is called **Dedekind** *if all its subgroups are normal.*

Dedekind Groups

Definition

A group is called **Dedekind** *if all its subgroups are normal.*

For example, all abelian groups are Dedekind.

Dedekind Groups

Definition

A group is called **Dedekind** *if all its subgroups are normal.*

For example, all abelian groups are Dedekind.

The smallest non-abelian Dedekind group is Q_8, the quaternion group.

Characterization of Dedekind Groups

Richard Dedekind
Ueber Gruppen, deren sämmtliche Theiler Normaltheiler sind
Mathematische Annalen 48 (1897), 548–561.

Characterization of Dedekind Groups

Richard Dedekind
Ueber Gruppen, deren sämmtliche Theiler Normaltheiler sind
Mathematische Annalen 48 (1897), 548–561.

Reinhold Baer
Situation der Untergruppen und Struktur der Gruppe
Sitz.-Ber. Heidelberg. Akad. Wiss. 2, pp. 12–17, 1933.

Characterization of Dedekind Groups

Richard Dedekind
Ueber Gruppen, deren sämmtliche Theiler Normaltheiler sind
Mathematische Annalen 48 (1897), 548–561.

Reinhold Baer
Situation der Untergruppen und Struktur der Gruppe
Sitz.-Ber. Heidelberg. Akad. Wiss. 2, pp. 12–17, 1933.

Theorem (Dedekind, Baer)

A group G is Dedekind if and only if G is abelian or $G = Q_8 \times A \times E$, where

- *Q_8 is the quaternion group of order 8;*
- *A is an abelian group in which all elements have odd order;*
- *E is an elementary abelian 2-group.*

Nilpotency of Dedekind Groups

This theorem also tells us that Dedekind groups are always *nil-potent*, which means there is a finite chain of normal subgroups

$$\{1\} = H_0 \lhd H_1 \lhd \cdots \lhd H_{n-1} \lhd H_n = G$$

such that for all $i = 0, \ldots, n-1$,

$$\frac{H_{i+1}}{H_i} \leq Z\left(\frac{G}{H_i}\right).$$

Nilpotency of Dedekind Groups

This theorem also tells us that Dedekind groups are always *nilpotent*, which means there is a finite chain of normal subgroups

$$\{1\} = H_0 \lhd H_1 \lhd \cdots \lhd H_{n-1} \lhd H_n = G$$

such that for all $i = 0, \ldots, n-1$,

$$\frac{H_{i+1}}{H_i} \leq Z\left(\frac{G}{H_i}\right).$$

The smallest length of a chain of this type is called the *nilpotency class*.

Nilpotency of Dedekind Groups

This theorem also tells us that Dedekind groups are always *nilpotent*, which means there is a finite chain of normal subgroups

$$\{1\} = H_0 \lhd H_1 \lhd \cdots \lhd H_{n-1} \lhd H_n = G$$

such that for all $i = 0, \ldots, n-1$,

$$\frac{H_{i+1}}{H_i} \leq Z\left(\frac{G}{H_i}\right).$$

The smallest length of a chain of this type is called the *nilpotency class*.

Corollary

The nilpotency class of a Dedekind group is at most 2.

Skew Braces

Definition

A **(left) skew brace** *is a triple* $(B, +, \circ)$*, where* $(B, +)$ *and* $(B, \circ)$ *are groups such that*

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

for all $a, b, c \in B$.

Skew Braces

Definition

A **(left) skew brace** *is a triple* $(B, +, \circ)$*, where* $(B, +)$ *and* $(B, \circ)$ *are groups such that*

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

for all $a, b, c \in B$.

The following function plays an important role in the study of skew braces:

$$\lambda : a \in (B, \circ) \mapsto \lambda_a \in Aut(B, +)$$

where $\lambda_a(b) = -a + a \circ b$, for all $b \in B$.

Skew Braces

Definition

A **(left) skew brace** *is a triple* $(B, +, \circ)$*, where* $(B, +)$ *and* $(B, \circ)$ *are groups such that*

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

for all $a, b, c \in B$*.*

The following function plays an important role in the study of skew braces:

$$\lambda : a \in (B, \circ) \mapsto \lambda_a \in Aut(B, +)$$

where $\lambda_a(b) = -a + a \circ b$, for all $b \in B$.

If $(G, \cdot)$ is a group, then $(G, \cdot, \cdot)$ is a skew brace, called *trivial*.

Substructures in Skew Braces

Let $(B, +, \circ)$ be a skew brace. A subset X of B is said to be:

1. a *sub-skew brace* if it is a subgroup of both $(B, +)$ and $(B, \circ)$;
2. a *left-ideal* if it is a subgroup of $(B, +)$ and $\lambda_a(X) = X$, for all $a \in B$;
3. an *ideal* if it is a left-ideal that is normal in both $(B, +)$ and $(B, \circ)$;

Substructures in Skew Braces

Let $(B, +, \circ)$ be a skew brace. A subset X of B is said to be:

1. a *sub-skew brace* if it is a subgroup of both $(B, +)$ and $(B, \circ)$;
2. a *left-ideal* if it is a subgroup of $(B, +)$ and $\lambda_a(X) = X$, for all $a \in B$;
3. an *ideal* if it is a left-ideal that is normal in both $(B, +)$ and $(B, \circ)$; in this case B/I is a skew brace with induced operations.

Substructures in Skew Braces

Massimiliano Di Matteo

Let $(B, +, \circ)$ be a skew brace. A subset X of B is said to be:

1. a *sub-skew brace* if it is a subgroup of both $(B, +)$ and $(B, \circ)$;
2. a *left-ideal* if it is a subgroup of $(B, +)$ and $\lambda_a(X) = X$, for all $a \in B$;
3. an *ideal* if it is a left-ideal that is normal in both $(B, +)$ and $(B, \circ)$; in this case B/I is a skew brace with induced operations.

$\zeta(B) = Z(B, +) \cap \ker(\lambda) \cap Z(B, \circ)$, which is called the *center* of the skew brace, is always an ideal.

Andrea Caranti, Ilaria Del Corso, M.D.M.,
Maria Ferrara, Marco Trombetti
Dedekind Skew Braces
to appear

Dedekind Skew Braces

Andrea Caranti, Ilaria Del Corso, M.D.M., Maria Ferrara, Marco Trombetti
Dedekind Skew Braces
to appear

Definition

A skew brace is called **Dedekind** *if all its sub-skew braces are ideals.*

Andrea Caranti, Ilaria Del Corso, M.D.M., Maria Ferrara, Marco Trombetti
Dedekind Skew Braces
to appear

Definition

A skew brace is called **Dedekind** *if all its sub-skew braces are ideals.*

If $(G, \cdot)$ is a Dedekind group, $(G, \cdot, \cdot)$ and $(G, \cdot, \cdot^{op})$ are Dedekind skew braces, where $a \cdot^{op} b = b \cdot a$.

Example

A non trivial example of a Dedekind skew brace is

$$B = \texttt{SmallSkewbrace(8,39)},$$

in which $(B,+) \simeq (Q_8,+)$ and $(B,\circ) \simeq (C_8,\cdot)$.
In this case $\ker(\lambda) = \langle -1 \rangle$ and

$$\lambda_i : \begin{aligned} i &\mapsto j \\ j &\mapsto -i \\ k &\mapsto k \end{aligned} \qquad \lambda_j : \begin{aligned} i &\mapsto -j \\ j &\mapsto i \\ k &\mapsto k \end{aligned} \qquad \lambda_k : \begin{aligned} i &\mapsto -i \\ j &\mapsto -j \\ k &\mapsto k \end{aligned}$$

Dedekind Braces

A.Ballester-Bolinches, R.Esteban-Romero, L.A.Kurdachenko, V.Pérez-Calabuig

On left braces in which every subbrace is an ideal

Results in Mathematics, 2024

Dedekind Braces

A.Ballester-Bolinches, R.Esteban-Romero, L.A.Kurdachenko, V.Pérez-Calabuig
On left braces in which every subbrace is an ideal
Results in Mathematics, 2024

Theorem

If B is a finite Dedekind skew brace in which $(B, +)$ is abelian, then B is centrally nilpotent.

Central nilpotency in Skew Braces

Massimiliano Di Matteo

What does central nilpotency mean?

Central nilpotency in Skew Braces

What does central nilpotency mean? There is a finite chain of ideals

$$\{0\} = I_0 \lhd I_1 \lhd \cdots \lhd I_{n-1} \lhd I_n = B$$

such that for all $i = 0, \ldots, n-1$,

$$\frac{I_{j+1}}{I_j} \leq \zeta\left(\frac{B}{I_j}\right).$$

Central nilpotency in Skew Braces

What does central nilpotency mean? There is a finite chain of ideals

$$\{0\} = I_0 \lhd I_1 \lhd \cdots \lhd I_{n-1} \lhd I_n = B$$

such that for all $i = 0, \dots, n-1$,

$$\frac{I_{j+1}}{I_j} \leq \zeta\left(\frac{B}{I_j}\right).$$

The smallest length of a chain of this type is called the *central nilpotency class*.

Hypercentrality in Groups

If $(G, \cdot)$ is a group, we can define $Z_0(G) = \{1\}$ and known $Z_n(G)$ for an ordinal n, $Z_{n+1}(G)$ is the normal subgroup such that

$$\frac{Z_{n+1}(G)}{Z_n(G)} = Z\left(\frac{G}{Z_n(G)}\right);$$

instead, if α is a limit ordinal

$$Z_\alpha(G) = \bigcup_{\beta<\alpha} Z_\beta(G).$$

Hypercentrality in Groups

If $(G, \cdot)$ is a group, we can define $Z_0(G) = \{1\}$ and known $Z_n(G)$ for an ordinal n, $Z_{n+1}(G)$ is the normal subgroup such that

$$\frac{Z_{n+1}(G)}{Z_n(G)} = Z\left(\frac{G}{Z_n(G)}\right);$$

instead, if α is a limit ordinal

$$Z_\alpha(G) = \bigcup_{\beta<\alpha} Z_\beta(G).$$

Definition

A group G is called **hypercentral** *if and only if there exists an ordinal α such that $Z_\alpha(G) = G$.*

Hypercentrality in Skew Braces

Massimiliano Di Matteo

Replacing the group G with a skew brace B and using the center of the skew brace, we can define similarly $\zeta_\alpha(B)$ for every ordinal α.

Hypercentrality in Skew Braces

Replacing the group G with a skew brace B and using the center of the skew brace, we can define similarly $\zeta_\alpha(B)$ for every ordinal α.

Definition

A skew brace B is called **hypercentral** *if and only if there exists an ordinal α such that $\zeta_\alpha(B) = B$.*

Hypercentrality in Dedekind Skew Braces

With this definition, we can generalize the theorem.

Hypercentrality in Dedekind Skew Braces

Massimiliano Di Matteo

With this definition, we can generalize the theorem.

Theorem

Every locally finite Dedekind skew brace is hypercentral.

Hypercentrality in Dedekind Skew Braces

With this definition, we can generalize the theorem.

Theorem

Every locally finite Dedekind skew brace is hypercentral.

Corollary

Every finite Dedekind skew brace is centrally nilpotent.

Central nilpotency class

Unfortunately, we cannot define a bound for the central nilpotency class.

Central nilpotency class

Unfortunately, we cannot define a bound for the central nilpotency class.

Let $(B, +) = (\mathbb{Z}_{2^n}, +)$ and define

$$a \circ b = a + (-1)^a b,$$

for all $a, b \in B$.

Central nilpotency class

Unfortunately, we cannot define a bound for the central nilpotency class.

Let $(B,+) = (\mathbb{Z}_{2^n},+)$ and define

$$a \circ b = a + (-1)^a b,$$

for all $a, b \in B$.

$(B,+,\circ)$ is a skew brace such that $(B,\circ)$ is isomorphic to the dihedral group of order 2^n and the central nilpotency class of this brace is always $n-1$.

Skew Braces of Cyclic Type

To identify Dedekind skew braces, one needs to consider hypercentral groups.

Theorem

Let $(B, +, \circ)$ be a finite skew brace such that either $(B, +)$ or $(B, \circ)$ is cyclic and the other nilpotent. Then B is Dedekind.

Skew Braces of Cyclic Type

To identify Dedekind skew braces, one needs to consider hypercentral groups.

Theorem

Let $(B, +, \circ)$ be a finite skew brace such that either $(B, +)$ or $(B, \circ)$ is cyclic and the other nilpotent. Then B is Dedekind.

Theorem

Let $(B, +, \circ)$ be a skew brace such that either $(B, +)$ or $(B, \circ)$ is infinite cyclic. Then following conditions are equivalent:

(1) *B is trivial.*

(2) *B is Dedekind.*

(3) *$(B, +)$ and $(B, \circ)$ are nilpotent.*

Braces of locally cyclic type and $\ker(\lambda) \neq 0$

Theorem

Let $(B, +, \circ)$ be a non-trivial skew brace in which $(B, +)$ is locally cyclic and torsion-free and $K = \mathrm{Ker}(\lambda) \neq 0$. Then $|B/K| = 2$ and

$$a \circ b = a + (-1)^{\varphi(a+K)} b$$

for all $a, b \in B$, where $\varphi : (B/K, +) \to \mathbb{Z}_2$ is an isomorphism. Thus, $(B, \circ)$ is isomorphic to the dihedral group $\mathbb{Z}_2 \ltimes (B, +)$ and B is not Dedekind.

Converse of the theorem

Theorem

Let $(X, +)$ *be any subgroup of* $(\mathbb{Q}, +)$ *containing the rational number* 1*. If* $2X < X$*, then we can define a group* $(X, \circ)$ *by putting*

$$x \circ y = x + (-1)^{\varphi(x+2X)} y$$

for every $x, y \in X$*, where* $\varphi : X/2X \to \mathbb{Z}_2$ *is an isomorphism. Then* $(X, +, \circ)$ *defines a skew brace such that* $\mathrm{Ker}(\lambda) = 2X \neq \{0\}$*.*

V: Braces of locally cyclic type and $\ker(\lambda) = 0$

Massimiliano Di Matteo

Theorem

Let $(B, +, \circ)$ be a non-trivial skew brace in which $(B, +)$ is locally cyclic and torsion-free and $\mathrm{Ker}(\lambda) = 0$. Then $(B, \circ)$ is abelian and there is a rational number $0 \neq \frac{m_1}{m_2} \in B$ such that for all $a, b \in B$

$$a \circ b = a + b - ab + \frac{m_1}{m_2} ab.$$

In this case, $(B, +)$ is actually isomorphic to a sub-ring of $(\mathbb{Q}, +)$. Moreover, B is not Dedekind.

Converse of the second theorem

Theorem

Let $(X,+)$ be any subgroup of $(\mathbb{Q},+)$ containing the rational number 1. If X is a sub-ring of $\mathbb{Q}$ for which there exists a non-zero rational number $\frac{m_1}{m_2}$ for which the operation

$$x \circ y = x + y - xy + \frac{m_1}{m_2}xy \qquad (x, y \in X)$$

defines an abelian group $(X,\circ)$, then $(X,+,\circ)$ is a skew brace with $\mathrm{Ker}(\lambda) = \{0\}$.

Skew Braces in $\mathbb{Q}$ e $\mathbb{Z}$

Skew braces in which $(B, +)$ is isomorphic to $(\mathbb{Z}, +)$ have already been characterized.

Wolfgang Rump
Classification of Cyclic Braces
J. Pure Appl. Algebra, 209(3):671–685, 2007

Skew Braces in $\mathbb{Q}$ e $\mathbb{Z}$

Skew braces in which $(B, +)$ is isomorphic to $(\mathbb{Z}, +)$ have already been characterized.

Wolfgang Rump
Classification of Cyclic Braces
J. Pure Appl. Algebra, 209(3):671–685, 2007

Corollary

If $(B, +, \circ)$ is a skew brace such that $(B, +) \simeq (\mathbb{Q}, +)$, then B is trivial.

THANK YOU FOR YOUR ATTENTION