MODULE BRACES: THEORY AND APPLICATIONS

Ilaria Del Corso

Omaha, May 30, 2023

Dipartimento di Matematica
Università di Pisa

Generalities on skew braces

A *skew brace* is a group $(N, +)$ together with one of the following

- an additional group operation "$\circ$" on N such that the following brace axiom holds for $x, y, z \in N$

$$x \circ (y + z) = (x \circ y) - x + (x \circ z).$$

- a Gamma Function, namely a function $\gamma \colon N \to \mathrm{Aut}(N, +)$ such that, for $x, y \in N$,

$$\gamma(\mathbf{x} + \gamma_{\mathbf{x}}(\mathbf{y})) = \gamma_{\mathbf{x}}\gamma_{\mathbf{y}}$$

- an additional binary operation $\star$ such that, for all $x, y, z \in N$,

$$\mathbf{x} \star (\mathbf{y} + \mathbf{z}) = \mathbf{x} \star \mathbf{y} + \mathbf{y} + \mathbf{x} \star \mathbf{z} - \mathbf{y}$$

  with the additional condition that the operation $\circ$ defined by

$$\mathbf{x} \circ \mathbf{y} = \mathbf{x} + \mathbf{x} \star \mathbf{y} + \mathbf{y}$$

  defines on N a group structure.

Relations between $(N, +, \circ)$, $(N, +, \gamma)$ and $(N, +, \star)$

The relations between the $\circ$ operation and the GF γ and the $\star$ operation defining the same skew brace, are given by

$$\gamma_x(y) = -x + x \circ y \qquad \gamma_x(y) = x \star y + y \qquad \forall x, y \in N$$

and the properties of $\circ$, $\star$ and the function γ correspond to each other.

Let I be subset of a skew brace $(N, +, \circ) = (N, +, \gamma)$.

- I is a subskew brace if it is a subgroup both of $(N, +)$ and $(N, \circ)$; In terms of the GF: I is a subgroup of $(N, +)$ and it is $\gamma(I)$ invariant, $(\gamma_x(I) \subseteq I$ for each $x \in I)$. This means that $\gamma_{|I}$ is a GF for $(I, +)$).
- I is a left ideal if it is a subgroup of $(N, +)$ and is $\gamma(N)$ invariant.
- I is an ideal if it is $\gamma(N)$ invariant and it is a normal subgroup of both $(N, +)$ and $(N, \circ)$.

$$\{\text{ideals of } N\} \subseteq \{\text{left ideals of } N\} \subseteq \{\text{subskew braces of } N\}$$

Let $(M, +, \gamma)$ and $(N, +', \gamma')$ be skew braces, and let $f\colon M \to N$ be an isomorphism of the additive groups.
f **is skew brace isomorphism** $\iff$ f is also a morphism of the multiplicative groups $\iff$ $f\gamma_x = \gamma'_{f(x)} f$, for each $x \in M$.

Braces and radical rings

A *brace* is a skew brace with abelian additive group.

Example. Let $(N, +, \cdot)$ be a *radical ring*.

$(N, +, \cdot)$ is a brace when we take $\star = \cdot$.

The operation $\circ$ of this brace is $x \circ y = x + x \cdot y + y$ and it is called the adjoint operation.

Any radical ring is a two-sided brace, namely a brace for which both the left-brace-axiom and the right-brace-axiom hold.

Conversely, if $(N, +, \circ)$ is a two-sided brace, then defining

$$x \cdot y = -x + x \circ y - y$$

we have that $(N, +, \cdot)$ is a radical ring.

The gamma function associated to the brace $(N, +, \circ)$ arising from a radical ring, is given by

$$\gamma_x(y) = -x + x \circ y = (x + 1)y.$$

Module braces

Module braces

Let $(N, +, \circ) = (N, +, \gamma) = (N, +, \star)$ be a brace and assume that $(N, +)$ is a R-module over some ring R.

We say that N is an R-(module) brace if

$$\gamma \colon N \to \mathrm{Aut}_R(N)$$

namely, for all $x, y \in N$ and $r \in R$,

$$r\gamma_x(y) = \gamma_x(ry).$$

Equivalently, in terms of the $\star$ operation,

$$r(x \star y) = x \star ry.$$

With this language, a brace is called $\mathbb{Z}$-brace.

The case when R is a field has been already considered by F. Catino, I. Colazzo, and P. Stefanelli (2015, 2019) and by A. Smoktunowicz (2022)

Examples

1) An R-module N with the trivial brace structure is always an R-brace, since the corresponding gamma function is the trivial map $x \mapsto \gamma_x = \mathrm{id}$.

2) Let $N = (N, +, \cdot)$ be a radical ring.
The associated gamma function is $\gamma_x(y) = (1 + x)y$.
If $(N, +)$ has a right R-module structure, then $(N, +, \circ)$ is an R-module brace since $\gamma_x \in \mathrm{Aut}_R(N)$ for all x.

3) Let $R = \mathbb{Z}[i]$, let $(N, +)$ be the additive group $\mathbb{Z}[i] \times \mathbb{Z}[i]$, and define

$$(\alpha_1, \beta_1) \circ (\alpha_2, \beta_2) = (\alpha_1 + (-1)^{\Re(\alpha_1)}\alpha_2, \beta_1 + (-1)^{\Re(\alpha_1)}\beta_2)$$

Then $(N, +, \circ)$ is an R-brace.

4) Let $N = \mathbb{Z}[i]$ considered as a $\mathbb{Z}[i]$-module, and let $\gamma\colon \mathbb{Z}[i] \to Aut(\mathbb{Z}[i])$ be the map defined by

$$\gamma_{(a+ib)}(x + iy) = ((-1)^a x + iy).$$

It is easy to verify that γ is a gamma function, so $(N, +, \circ)$ is a brace.
However, N is not a $\mathbb{Z}[i]$-brace, since $\gamma_{(a+ib)} \notin \mathrm{Aut}_{\mathbb{Z}[i]}(\mathbb{Z}[i])$ for a odd.

Substructures

Def. Let $(N, +, \circ)$ be a R-brace and let $I \subseteq N$. We call I an

R-subbrace / left R-ideal / R-ideal

if it is a

subbrace / left ideal / ideal + R-submodule

The substructures of an R-braces have a good behaviour

- If I is an R-ideal of N, then the quotient brace N/I is an R-brace
- The elements of the right series of an R-brace are R-ideals
- The elements of the left series of an R-brace are left R-ideals

A splitting theorem

Let R be a commutative ring with 1, and let

$$R = \bigoplus_{i=1}^{t} R_i$$

be a direct sum decomposition of R into ideals. Let $e_1, \dots, e_t$ be the *orthogonal idempotents* associated to the decomposition ($1 = \sum_{i=1}^{t} e_i$).

Proposition. *Let $(N, +)$ be an R-module. Then,*

$$N = \bigoplus_{i=1}^{t} e_i N, \tag{1}$$

where $e_i N$ is an R-module, which is annihilated by R_j for all $j \neq i$.
If $(N, +, \circ)$ is an R-brace, then, each $e_i N$ is a left R-ideal of the brace N.
Moreover,

(1) *is an R-braces decomposition* $\iff$ *all the $e_i N$ are (R-)ideals of N.*

Finite braces

Let $R = \mathbb{Z}$ and let $(N, +, \circ)$ be a finite brace.

The action of $\mathbb{Z}$ on N can not be faithful, so N is a $\mathbb{Z}/d\mathbb{Z}$-module for some $d \neq 0$.

Let $d = p_1^{a_1} \dots p_t^{a_t}$, where the p_i's are pairwise distinct primes, then

$$\mathbb{Z}/d\mathbb{Z} \cong \bigoplus_{i=1}^{t} \mathbb{Z}/p_i^{a_i}\mathbb{Z}$$

$$N = \bigoplus_{i=1}^{t} N_i,$$

where N_i is the Sylow p_i-subgroup of $(N, +)$ and they are also Sylow p_i-subgroup of $(N, \circ)$.

If $(N, \circ)$ is nilpotent we recover the core of [Theorem 1, Byott JA 2013] for braces.

Finite $\mathcal{O}_K$-braces

Let K be a number field and let $\mathcal{O}_K$ be its ring of integers.

Let $(N, +, \circ)$ be a finite $\mathcal{O}_K$-brace.

The action of $\mathcal{O}_K$ on N can not be faithful, so N is a $\mathcal{O}_K/I$-module for some *non-zero* ideal I.

Let $I = P_1^{a_1} \dots P_t^{a_t}$, where the P_i's are pairwise distinct prime ideals of $\mathcal{O}_K$, then

$$\mathcal{O}_K/I \cong \bigoplus_{i=1}^{t} \mathcal{O}_K/P_i^{a_i}.$$

We get

$$N = \bigoplus_{i=1}^{t} N_i,$$

where N_i is the P_i-component of $(N, +)$ and is a left $\mathcal{O}_K$-ideal of the brace N.

The previous proposition says that the decomposition of N is an $\mathcal{O}_K$-brace decomposition if and only if all the N_i are ideals of N.

Corollary. *Let* $R = \bigoplus_{i=1}^{t} R_i$ *be a commutative ring with identity, with associated orthogonal idempotents* $\{e_1, \dots, e_t\}$*.*

Let $(N, +, \cdot)$ *be a radical ring. If* N *is an* R*-algebra, then,*

$$N = \bigoplus_{i=1}^{t} e_i N \tag{2}$$

as R*-braces, namely*

$$1 + N = \bigoplus_{i=1}^{t} (1 + e_i N).$$

Relation between the additive and the multiplicative group of a module brace

Module braces of small rank

Let D be a PID, and let M be a f.g. torsion D-module. We define

$\mathrm{rank}_D M = \#$*indecomp.* cyclic factors of the D-mod decomposition of M

Theorem 1. *Let p be a prime number, and let D be a PID such that p is a prime in D. Let $(N, +, \circ)$ be a D-brace of order a power of p.*

Assume that $r = \mathrm{rank_D N < p - 1}$.

Then $(N, +)$ and $(N, \circ)$ have the same number of elements of each order. In particular, if $(N, \circ)$ is abelian, then $(N, +) \cong (N, \circ)$.

- [FCC12, Bac16] give the same result for $D = \mathbb{Z}$.
- For a D-braces, the condition of having few ciclic factors in the D-module decomposition can be much weaker than the condition of having few ciclic factors in the $\mathbb{Z}$-module decomposition. In fact, if $D/pD = \mathbb{F}_{p^\lambda}$, then

$$\mathrm{rank_{\mathbb{Z}} N = \lambda \cdot rank_D N.}$$

Module braces over $\mathbb{Z}_p(\lambda)$

Let $\mathbb{Q}_p(\lambda)$ be the unramified extensions of degree λ of the field of the p-adic numbers $\mathbb{Q}_p$. Its ring of integers $\mathbb{Z}_p(\lambda)$ is an examples of ring D fulfilling the request of the theorem.

Corollary. *Let $(N, +, \circ)$ be a $\mathbb{Z}_p(\lambda)$-brace of order a power of p. If*

$$\mathrm{rank}_{\mathbb{Z}_p(\lambda)} N < (p-1),$$

$$\mathrm{rank}_{\mathbb{Z}} N < \lambda(p-1),$$

then $(N, +)$ and $(N, \circ)$ have the same number of elements of each order. In particular, if $(N, \circ)$ is abelian, then $(N, +) \cong (N, \circ)$.

Module braces over local rings

Lemma. Let $(S, \mathfrak{m}, \mathbb{F}_{p^\lambda})$ be a finite local ring. Then every S-brace is also a $\mathbb{Z}_p(\lambda)$-brace, by restriction of scalars.

Proof. Use an Hensel's type argument.

Corollary. Let $(S, \mathfrak{m}, \mathbb{F}_{p^\lambda})$ be a local ring, and let $(N, +, \circ)$ be an S-brace of order a power of p, such that $\mathrm{rank}_{\mathbb{Z}} \mathrm{N} < \lambda(\mathrm{p} - 1)$.

Then $(N, +)$ and $(N, \circ)$ have the same number of elements of each order.

In particular, if $(N, \circ)$ is abelian, then $(N, +) \cong (N, \circ)$.

Finite module brace over a general ring

Let R be any commutative ring, and let N be a finite R-brace.

Then $A = R/\mathrm{Ann}_R(N)$ is finite, and therefore artinian. So,

$$A = \bigoplus_{i=1}^{t} A_i$$

where each $(A_i, \mathfrak{m}_i, \mathbb{F}_{p_i^{\lambda_i}})$ is a local finite ring.

Let $e_1, \ldots, e_t$ be the orthogonal idempotents of the decomposition of A.

Letting $N_i = Ne_i$, we have

$$N = \bigoplus_{i=1}^{t} N_i, \tag{3}$$

where this equality holds for N as a module, and for N as a module brace in the case when $N_1, \ldots, N_t$ are ideals of N.

Since N_i is a A_i-brace, we can study each of them by our method, if they are small.

In particular

Proposition. Let N be a finite A-brace and assume that $N_1, \ldots, N_t$ are ideals of the brace N. If, $\forall i \in \{1, \ldots, t\}$,

$$\mathrm{rank}_{\mathbb{Z}}(N_i) < \lambda_i(p_i - 1)$$

then $(N, +)$ and $(N, \circ)$ have the same number of elements of each order, and if $(N, \circ)$ is abelian, then $(N, +) \cong (N, \circ)$.

An application to Fuchs' problem

In Fuchs' book "Abelian Groups" (1960) the following question is posed (Problem 72)

> *Characterize the groups which are the groups of all units in a commutative and associative ring with identity.*

The problem had already been considered in some particular cases

- The Dirichlet's Unit Thm (1846): K number field $[K:\mathbb{Q}] = r + 2s$, $\mathcal{O}_K$ ring of integers

$$\mathcal{O}_K^* \cong \mathbb{Z}/2n\mathbb{Z} \times \mathbb{Z}^{r+s-1}$$

- G. Higman (1940) discovered a perfect analogue of Dirichlet's Unit Theorem for a group ring $\mathbb{Z}[T]$ where T is a finite abelian group:

$$(\mathbb{Z}[T])^* \cong \mathbb{Z}/2\mathbb{Z} \times T \times \mathbb{Z}^n$$

for a suitable explicit constant $n = n(T)$.

Finitely generated abelian groups

Fuchs' question for finitely generated abelian groups

(idc+ R.Dvornicich AMPA18 and BLMS18; idc JLMS 2020)

A ring with 1, A^* group of units of A. Assume that A^* is finitely generated and abelian

$$A^* \cong (A^*)_{tors} \times \mathbb{Z}^{r_A}$$

Problem: what groups arise?

- T finite abelian group: $\exists\ A \in \mathcal{C}$ such that $(A^*)_{tors} \cong T$?
- if $(A^*)_{tors} \cong T$ what can we say on r_A?

We are interested in the minimum value that the rank can assume for a fixed torsion part T, since increase the rank is easy.

Reduction step 1

Let $A_0(=\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z})$ be the fundamental subring of A and consider the ring $R = A_0[(A^*)_{tors}]$, which is a subring of A. Then $R^* \leq A^*$, so

$$(A^*)_{tors} = (R^*)_{tors}$$

and

$$r_A \geq r_R.$$

So, up to changing $A \longleftrightarrow R = A_0[(A^*)_{tors}]$, we can restrict ourself to consider:

commutative rings which are finitely gen. and integral over A_0.
This class of rings is much simpler to study, but allow us to obtain ALL the realisable groups of units.

Reduction step 2: splitting of the ring

Proposition (Pearson & Schneider 1970)

Let A be a commutative ring which is finitely generated and integral over its fundamental subring. Then $A = A_1 \oplus A_2$, where A_1 is a finite ring and the torsion ideal of A_2 is contained in its nilradical.

We will say that A is a TN ring if its torsion ideal is contained in the nilradical.

We are left to study finite rings and TN rings.

How do module braces come out?

Let A be a commutative ring with nilradical $\mathfrak{N}$. For any ideal $\mathfrak{I} \subseteq \mathfrak{N}$ we have the following exact sequence

$$1 \to 1 + \mathfrak{I} \to A^* \to (A/\mathfrak{I})^* \to 1$$

- the ring $A/\mathfrak{I}$ is simpler to study, for example for $\mathfrak{I} = \mathfrak{N}$ is reduced;
- $\mathfrak{I}$ is a radical (nilpotent) ring and also a A-algebra, so we can study the A-brace $(\mathfrak{I}, +, \circ)$ via our previous result that, for radical rings, holds in the following stronger form.

Theorem 2. Let N be a commutative radical ring of order a power of an odd prime p. Suppose that $(N, +, \circ)$ is a A-brace. If $(N, +)$ or $(N, \circ)$ is *"small with respect to A"*, then $(N, +) \cong (N, \circ)$.

Proof (sketch). If $(N, +)$ is "A-small" we can apply Theorem 1, and get $(N, +) \cong (N, \circ)$.

If $(N, \circ)$ is "A-small" we have an argument, specific for nilpotent rings, which guarantees that also $(N, +)$ is small, so Theorem 1 gives $(N, +) \cong (N, \circ)$.

Finite rings

- We can reduce to consider the case $(A, \mathfrak{m}, \mathbb{F}_{p^\lambda})$ finite local ring.
- The exact sequence for $\mathfrak{I} = \mathfrak{m}$ becomes

$$1 \to 1 + \mathfrak{m} \to A^* \to \mathbb{F}_{p^\lambda}^* \to 1.$$

and splits, so

$$A^* = \mathbb{F}_{p^\lambda}^* \times 1 + \mathfrak{m}$$

Theorem 3. The *small* finite abelian groups occurring as group of units of finite local rings $(A, \mathfrak{m}, \mathbb{F}_{p^\lambda})$ of characteristic a power of an odd prime p are **exactly** those of the form

$$\mathbb{F}_{p^\lambda}^* \times H^\lambda,$$

where λ is a positive integer, and H varies in the class of finite abelian p-groups with $rank_{\mathbb{Z}}(H) < p - 1$.

Here small means λ-small, i.e., $rank_{\mathbb{Z}}(A^*)_p < \lambda(p-1)$

TN rings

If A is TN, by choosing $\mathfrak{I} = \mathfrak{N}_{tors}$, we get the following exact sequence

$$1 \to 1 + \mathfrak{N}_{tors} \hookrightarrow A^* \xrightarrow{\phi} (A/\mathfrak{N}_{tors})^* \to 1.$$

where $A/\mathfrak{N}_{tors}$ is a torsion free ring.

The possibility for $(A/\mathfrak{N}_{tors})^*$ are known, by the following

Theorem (idc JLMS20). Let T be a finite abelian group of even order. Then there exists an explicit constant $g(T)$ such that the following holds:

$$T \times \mathbb{Z}^r$$

is the group of units of a torsion-free ring if and only if $r \geq g(T)$.

- We are left to study $1 + \mathfrak{N}_{tors}$.

The radical ring $\mathfrak{N}_{tors}$

$1 + \mathfrak{N}_{tors}$ is the adjoint group of $\mathfrak{N}_{tors}$ and

$$(\mathfrak{N}_{tors}, +, \circ) \text{ is a module brace over the ring } A$$

We appeal again to our Thm 2 applied to the p-Sylow of $\mathfrak{N}_{tors}$ ($p \neq 2$).

Theorem 2. Let N be a commutative radical ring of order a power of an odd prime p. Suppose that $(N, +, \circ)$ is a A-brace. If $(N, +)$ or $(N, \circ)$ is *"small with respect to A"*, then $(N, +) \cong (N, \circ)$.

A-small means $rank_{\mathbb{Z}} N < \lambda(p-1)$ where λ can be described case by case...

Remark. Very few is known in case $p = 2$.

Cyclic groups

Theorem (Pearson and Schneider (1970))

A *finite cyclic group* is the group of units of a ring if and only if its order is the product of a set of pairwise coprime integers of the following list:

a) $p^\lambda - 1$ where p is a prime and $\lambda \geq 1$;
b) $(p-1)p^k$ where $p > 2$ is a prime and $k \geq 1$;
c) $2d$ where $d > 0$ is odd;
d) $4d$ where d is an odd integer and $\forall p|d,\ p \equiv 1 \pmod 4$.

Remark. $\mathbb{Z}/44\mathbb{Z}$ and $\mathbb{Z}/328\mathbb{Z}$ are not realisable ($44 = 4 \times 11$, and $328 = 8 \times 41$ are not in the list). On the other hand $\mathbb{Z}[\zeta_{44}]^* \cong \mathbb{Z}/44\mathbb{Z} \times \mathbb{Z}^9$ and $\mathbb{Z}[\zeta_{328}]^* \cong \mathbb{Z}/328\mathbb{Z} \times \mathbb{Z}^{79}$ (these are the minimum values for the rank also in the class of torsion free rings).

Theorem

$\mathbb{Z}/44\mathbb{Z} \times \mathbb{Z}^r$ is realisable $\iff r \geq 9$

$\mathbb{Z}/328\mathbb{Z} \times \mathbb{Z}^r$ is realisable $\iff r \geq 1$

DEL CORSO I., Module braces: relations between the additive and the multiplicative group *arXiv:2208.01592*

DEL CORSO I., STEFANELLO L., Fuchs'problem via module braces, *work in progress.*

Thank you!