Hopf Algebras and Galois Module Theory
May 28 - 31, 2024

Left braces of size $p^2(2p+1)^2$, for p an odd Germain prime

Teresa Crespo

Wednesday May 29th

Braces

A *(left) brace* is a triple $(B, +, \cdot)$, where B is a set and $+$ and $\cdot$ are operations on B such that

- $(B, +)$ is an abelian group,
- $(B, \cdot)$ is a group,
- for all $a, b, c \in B$,

$$a(b + c) = ab - a + ac, \quad \text{(brace relation)}.$$

We call $(B, +)$ the *additive group* and $(B, \cdot)$ the *multiplicative group* of the brace. The cardinal of B is called the *size* of the brace.

For any abelian group $(A, +)$, $(A, +, +)$ is a brace, called *trivial brace*.

For B_1 and B_2 braces, a map $f : B_1 \to B_2$ is a *brace morphism* if $f(b + b') = f(b) + f(b')$ and $f(bb') = f(b)f(b')$ for all $b, b' \in B_1$. If f is bijective, we say that f is an *isomorphism*. In that case we say that the braces B_1 and B_2 are *isomorphic*.

Braces vs. holomorph

If $(B, +)$ is an abelian group and G a regular subgroup of $\mathrm{Hol}(B) \simeq B \rtimes \mathrm{Aut}\, B$, then $\pi_{1|G} : G \to B, \quad (a, f) \mapsto a$ is bijective.

For a left brace $(B, +, \cdot)$ and each $a \in B$, we have a bijective map

$$\lambda_a : B \to B, \quad b \mapsto -a + a \cdot b.$$

We have $\lambda_a(b + c) = \lambda_a(b) + \lambda_a(c),\ a \cdot b = a + \lambda_a(b),\ \lambda_{a \cdot b} = \lambda_a \circ \lambda_b$.

Proposition. (Bachiller) *Let $(B, +, \cdot)$ be a left brace. Then*

$$\{(a, \lambda_a) \,:\, a \in B\}$$

is a regular subgroup of $\mathrm{Hol}(B, +)$*, isomorphic to* $(B, \cdot)$*.*
Conversely, if $(B, +)$ is an abelian group and G is a regular subgroup of $\mathrm{Hol}(B, +)$*, then B is a left brace with $(B, \cdot) \simeq G$, where*

$$a \cdot b = a + f(b), \quad (\pi_{1|G})^{-1}(a) = (a, f) \in G.$$

These assignments give a bijective correspondence between isomorphism classes of left braces $(B, +, \cdot)$ and conjugacy classes of regular subgroups of $\mathrm{Hol}(B, +)$*.*

Semidirect product of braces

Let $(B_1, +, \cdot)$ and $(B_2, +, \cdot)$ be braces and $\tau : (B_2, \cdot) \to \mathrm{Aut}(B_1, +, \cdot)$ be a group morphism. Define in $B_1 \times B_2$

$$(a, b) + (a', b') = (a + a', b + b'), \quad (a, b) \cdot (a', b') = (a \cdot \tau(b)(a'), b \cdot b')$$

Then $(B_1 \times B_2, +, \cdot)$ is a brace which is called the *semidirect product* of the braces B_1 and B_2 via τ.

If τ is the trivial morphism, then $(B_1 \times B_2, +, \cdot)$ is the *direct product* of B_1 and B_2.

Hypothesis. m and n are relatively prime integer numbers such that each group of order mn has a normal subgroup of order m.

By the Schur-Zassenhaus theorem, the hypothesis on m and n implies that any group G of order mn is $G = G_1 \rtimes G_2$, with $|G_1| = m, |G_2| = n$ and any subgroup of G of order n is conjugate to G_2.

Proposition. *Each brace of size mn is a semidirect product of a brace of size m and a brace of size n.*

Proof.
Let B be a brace of size mn with additive group N and multiplicative group G.

$N = N_1 \times N_2$, with N_1 abelian group of order m, N_2 abelian group of order n.

$G = G_1 \rtimes G_2$, with G_1 group of order m, G_2 group of order n.

$\mathrm{Aut}(N) \simeq \mathrm{Aut}(N_1) \times \mathrm{Aut}(N_2) \Rightarrow \mathrm{Hol}(N) \simeq \mathrm{Hol}(N_1) \times \mathrm{Hol}(N_2)$.

$$\mathrm{Hol}(N) \ni (a, f, b, g),\ \ a \in N_1, f \in \mathrm{Aut}(N_1), b \in N_2, g \in \mathrm{Aut}(N_2)$$

$$(a_1, f_1, b_1, g_1)(a_2, f_2, b_2, g_2) = (a_1 + f_1(a_2), f_1 f_2, b_1 + g_1(b_2), g_1 g_2) \tag{1}$$

$$(a_1, f_1, b_1, g_1)^{-1} = (-f^{-1}(a_1), f_1^{-1}, -g_1^{-1}(b_1), g_1^{-1}). \tag{2}$$

The regular subgroup of $\mathrm{Hol}(N)$ corresponding to B is $\widetilde{G} = \{(x, \lambda_x) : x \in N\}$.

For $x = (0, b) \in N$, $(x, \lambda_x) = (0, f_b, b, g_b)$ for some $f_b \in \mathrm{Aut}(N_1), g_b \in \mathrm{Aut}(N_2)$.

$\widetilde{G}_2 := \{(0, f_b, b, g_b) : b \in N_2\}$ is a subgroup of $\widetilde{G}$ of order n, conjugate to G_2.

For $x = (a, 0) \in N$, $(x, \lambda_x) = (a, f_a, 0, g_a)$, for some $f_a \in \mathrm{Aut}(N_1), g_a \in \mathrm{Aut}(N_2)$.

$\widetilde{G}_1 := \{(a, f_a, 0, g_a) \,:\, a \in N_2\}$ is a subgroup of $\widetilde{G}$ of order m, equal to G_1.

We have then $\widetilde{G} = \widetilde{G}_1 \rtimes \widetilde{G}_2$. Moreover

$$\widetilde{G}_1 \lhd \widetilde{G} \implies g_a = \mathrm{Id}, \forall a \in N_1.$$

Now consider

$$\overline{G}_1 := \{(a, f_a) \,:\, a \in N_1\} \subset \mathrm{Hol}(N_1), \quad \overline{G}_2 := \{(b, g_b) \,:\, b \in N_2\} \subset \mathrm{Hol}(N_2).$$

$\overline{G}_1$ is a regular subgroup of $\mathrm{Hol}(N_1)$, isomorphic to G_1 and $\overline{G}_2$ is a regular subgroup of $\mathrm{Hol}(N_2)$, isomorphic to G_2, corresponding to two braces B_1, B_2 of sizes m and n, respectively. We define

$$\tau : \overline{G}_2 \to \mathrm{Aut}(N_1),\ \tau(b, g_b) = f_b.$$

We check that f_b is also a morphism with respect to the product $\cdot$ in $\overline{G}_1$ and that B is the semidirect product of B_1 and B_2 via τ.

Corollary. *Let* B_1, B_2 *be braces of sizes* m, n*, respectively. Let* $G_1 := \{(a, \lambda_a) : a \in (B_1, +)\} \subset \mathrm{Hol}(B_1, +), G_2 := \{(b, \lambda_b) : b \in (B_1, +)\} \subset \mathrm{Hol}(B_2, +)$ *be the regular subgroups corresponding to* B_1, B_2*, respectively. Let* τ *be a group morphism from* $(B_2, \cdot)$ *to* $\mathrm{Aut}(B_1, +, \cdot)$*. Then*

$$G := \{(a, \lambda_a \tau(b, \lambda_b), b, \lambda_b) : (a, b) \in (B_1 \times B_2, +)\} \subset \mathrm{Hol}(B_1 \times B_2, +)$$

is a regular subgroup of $\mathrm{Hol}(B_1 \times B_2, +)$ *corresponding to the semidirect product of* B_1 *and* B_2 *via* τ*.*

Proposition. *Isomorphism classes of braces of size* mn *correspond to triples* (G_1, G_2, τ)*, where* G_1 *and* G_2 *ranges over conjugation classes of regular subgroups of* $\mathrm{Hol}(N_1)$ *and* $\mathrm{Hol}(N_2)$*, respectively, and* τ *ranges over equivalence classes of morphisms from* G_2 *to* $\mathrm{Aut}\, B_1$*, where* B_1 *denotes the brace corresponding to* G_1*, under the relation*

$$\tau \sim \tau' \Leftrightarrow \tau' \circ conj_{h_2}|G_2 = conj_{h_1} \circ \tau$$

for $(h_1, h_2) \in \mathrm{Aut}\, N$ *such that* $conj_{h_1}(G_1) = G_1$ *and* $conj_{h_2}(G_2) = G_2$*.*

We shall apply the preceding results to determine all left braces of size p^2q^2, for p an odd Germain prime, $q = 2p + 1$.

Using the Sylow theorems, we obtain that $m = q^2, n = p^2$ satisfy the assumed hypothesis, i.e. each group of order p^2q^2 has a normal subgroup of order q^2.

Braces of size p^2, for p an odd prime number (Bachiller)

In all cases, $(B,\cdot) \simeq (B,+)$.

I) **Cyclic additive group.**

1) **Trivial brace**:

$\operatorname{Aut} B = \operatorname{Aut}(\mathbb{Z}/(p^2)) \simeq (\mathbb{Z}/(p^2))^*$,

$G := \{(x, \mathrm{Id}) \,:\, x \in B\} \subset \operatorname{Hol}(\mathbb{Z}/(p^2))$.

2) **Brace with $\cdot$ defined by** $x_1 \cdot x_2 = x_1 + x_2 + p x_1 x_2$:

$\operatorname{Aut} B = \{k \in (\mathbb{Z}/(p^2))^* \,:\, k \equiv 1 \pmod{p}\}$,

$G = \{(x, 1 + px) \,:\, x \in B\} \subset \operatorname{Hol}(\mathbb{Z}/(p^2))$.

II) **Noncyclic additive group.**

1) **Trivial brace:**

$\operatorname{Aut} B = \operatorname{Aut}(\mathbb{Z}/(p) \times \mathbb{Z}/(p)) \simeq \mathrm{GL}(2,p)$,

$G = \{(\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right), \mathrm{Id}) \,:\, \left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) \in B\} \subset \operatorname{Hol}(\mathbb{Z}/(p) \times \mathbb{Z}/(p))$.

2) **Brace with $\cdot$ defined by** $\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \cdot \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 + y_1 y_2 \\ y_1 + y_2 \end{pmatrix}$:

$$\operatorname{Aut} B = \left\{ \begin{pmatrix} d^2 & b \\ 0 & d \end{pmatrix} \,:\, b \in \mathbb{Z}/(p), d \in (\mathbb{Z}/(p))^* \right\}$$

$$G = \left\{ \left(\begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \right) \,:\, \begin{pmatrix} x \\ y \end{pmatrix} \in B \right\} \subset \operatorname{Hol}(\mathbb{Z}/(p) \times \mathbb{Z}/(p)).$$

Groups of order p^2q^2, p, q primes, $q = 2p+1$

$G = G_1 \rtimes_\tau G_2$, $|G_1| = q^2$, $|G_2| = p^2$, $\tau : G_2 \to \mathrm{Aut}(G_1)$.
$G_1 \rtimes_\tau G_2 \simeq G_1 \rtimes_{\tau'} G_2 \Leftrightarrow$ there exist automorphisms f of G_1, g of G_2 such that $conj_f \circ \tau = \tau' \circ g$.

1) $\boxed{G_1 = \mathbb{Z}/(q^2)}$
Let $\langle \alpha \rangle$ be the subgroup of order p of $\mathrm{Aut}(\mathbb{Z}/(q^2)) = (\mathbb{Z}/(q^2))^*$.

1.1) $\underline{G_2 = \mathbb{Z}/(p^2)}$

$G = \mathbb{Z}/(p^2q^2)$

$\mathbb{Z}/(q^2) \rtimes \mathbb{Z}/(p^2)$, $(x_1, y_1) \cdot (x_2, y_2) = (x_1 + \alpha^{y_1} x_2, y_1 + y_2)$,

1.2) $\underline{G_2 = \mathbb{Z}/(p) \times \mathbb{Z}/(p)}$

$G = \mathbb{Z}/(pq^2) \times \mathbb{Z}/(p)$

$G = \mathbb{Z}/(q^2) \rtimes (\mathbb{Z}/(p) \times \mathbb{Z}(p))$, $(x_1, \left(\begin{smallmatrix} y_1 \\ z_1 \end{smallmatrix}\right)) \cdot (x_2, \left(\begin{smallmatrix} y_2 \\ z_2 \end{smallmatrix}\right)) = \Big(x_1 + \alpha^{y_1} x_2, \left(\begin{smallmatrix} y_1+y_2 \\ z_1+z_2 \end{smallmatrix}\right)\Big)$.

2) $\boxed{G_1 = \mathbb{Z}/(q) \times \mathbb{Z}/(q)}$

$\mathrm{Aut}(\mathbb{Z}/(q) \times \mathbb{Z}/(q)) = \mathrm{GL}(2,q)$ has $(p+3)/2$ subgroups of order p, up to conjugacy,

$$\left\langle \begin{pmatrix} 1 & 0 \\ 0 & \beta \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} \beta & 0 \\ 0 & \beta \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} \beta & 0 \\ 0 & \beta^{k} \end{pmatrix} \right\rangle, \tag{3}$$

where $\langle \beta \rangle$ is the unique subgroup of order p of $(\mathbb{Z}/(q))^*$, $k \in (\mathbb{Z}/(p))^*$, $k \neq -1, 1$, $k \sim l \Leftrightarrow kl \equiv 1 \pmod p$.

2.1) $\underline{G_2 = \mathbb{Z}/(p^2)}$

$G = \mathbb{Z}/(p^2 q) \times \mathbb{Z}/(q)$

$G = (\mathbb{Z}/(q) \times \mathbb{Z}/(q)) \rtimes_M \mathbb{Z}/(p^2)$

$$\left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, z_1 \right) \cdot \left(\begin{pmatrix} x_2 \\ y_2 \end{pmatrix}, z_2 \right) = \left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + M^{z_1} \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}, z_1 + z_2 \right),$$

for M one of the matrices in (3). This gives $(p+3)/2$ groups.

2.2) $\underline{G_2 = \mathbb{Z}/(p) \times \mathbb{Z}/(p)}$

$G = \mathbb{Z}/(pq) \times \mathbb{Z}/(pq)$

$G = (\mathbb{Z}/(q) \times \mathbb{Z}/(q)) \rtimes_M (\mathbb{Z}/(p) \times \mathbb{Z}/(p)),$

$$\left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \begin{pmatrix} z_1 \\ t_1 \end{pmatrix}\right) \cdot \left(\begin{pmatrix} x_2 \\ y_2 \end{pmatrix}, \begin{pmatrix} z_2 \\ t_2 \end{pmatrix}\right) = \left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + M^{z_1} \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}, \begin{pmatrix} z_1 + z_2 \\ t_1 + t_2 \end{pmatrix}\right),$$

for M one of the matrices in (3). This gives $(p+3)/2$ groups.

$G = (\mathbb{Z}/(q) \times \mathbb{Z}/(q)) \rtimes_\beta (\mathbb{Z}/(p) \times \mathbb{Z}/(p)),$

$$\left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \begin{pmatrix} z_1 \\ t_1 \end{pmatrix}\right) \cdot \left(\begin{pmatrix} x_2 \\ y_2 \end{pmatrix}, \begin{pmatrix} z_2 \\ t_2 \end{pmatrix}\right) = \left(\begin{pmatrix} x_1 + \beta^{t_1} x_2 \\ y_1 + \beta^{z_1 + t_1} y_2 \end{pmatrix}, \begin{pmatrix} z_1 + z_2 \\ t_1 + t_2 \end{pmatrix}\right).$$

Given an abelian group N of order p^2q^2 (p, q primes, $q = 2p + 1$), $N = N_1 \times N_2$, $|N_1| = q^2, |N_2| = p^2$, we want to determine all braces with additive group N.

We consider the pairs of braces B_1, B_2 of sizes q^2, p^2, with additive groups N_1, N_2. Let G_1, G_2 denote their multiplicative groups.

For each of the group morphisms $\tau : G_2 \to \mathrm{Aut}(G_1)$, we need to perform the following steps.

1) Check if the image of τ is contained in $\mathrm{Aut}(B_1)$.

2) Split the equivalence class of τ under the relation

$$\tau \sim \tau' \Leftrightarrow \tau' \circ g = conj_f \circ \tau, f \in \mathrm{Aut}\, G_1, g \in \mathrm{Aut}\, G_2$$

into equivalence classes under the relation

$$\tau \sim \tau' \Leftrightarrow \tau' \circ conj_{h_2}|G_2 = conj_{h_1} \circ \tau,$$

$$(h_1, h_2) \in \mathrm{Aut}\, N \text{ such that } conj_{h_1}(G_1) = G_1 \text{ and } conj_{h_2}(G_2) = G_2.$$

The braces $(B,+,\cdot)$ of size p^2q^2, with p odd Germain prime, $q=2p+1$ are

I) $p+4$ braces with $(B,+)\simeq \mathbb{Z}/(p^2q^2)$. From these

- ▶ 4 braces with $(B,\cdot)\simeq \mathbb{Z}/(p^2q^2)$,
- ▶ p braces with $(B,\cdot)\simeq \mathbb{Z}/(q^2)\rtimes \mathbb{Z}/(p^2)$.

II) 8 braces with $(B,+)\simeq \mathbb{Z}/(pq^2)\times \mathbb{Z}/(p)$. From these

- ▶ 4 braces with $(B,\cdot)\simeq \mathbb{Z}/(pq^2)\times \mathbb{Z}/(p)$,
- ▶ 4 braces with $(B,\cdot)\simeq \mathbb{Z}/(q^2)\rtimes (\mathbb{Z}/(p)\times \mathbb{Z}(p))$.

III) $(p^2+4p+9)/2$ braces with $(B,+)\simeq \mathbb{Z}/(p^2q)\times \mathbb{Z}/(q)$. From these

- ▶ 4 braces with $(B,\cdot)\simeq \mathbb{Z}/(p^2q)\times \mathbb{Z}/(q)$,
- ▶ p braces with $(B,\cdot)\simeq (\mathbb{Z}/(q)\times \mathbb{Z}/(q))\rtimes_M \mathbb{Z}/(p^2)$, for each $M\neq \left(\begin{smallmatrix}\beta & 0\\ 0 & \beta^{-1}\end{smallmatrix}\right)$ and $M\neq \left(\begin{smallmatrix}\beta & 0\\ 0 & \beta^{(p+1)/2}\end{smallmatrix}\right)$,
- ▶ $(p+1)/2$ braces with $(B,\cdot)\simeq (\mathbb{Z}/(q)\times\mathbb{Z}/(q))\rtimes_M\mathbb{Z}/(p^2)$, for $M=\left(\begin{smallmatrix}\beta & 0\\ 0 & \beta^{-1}\end{smallmatrix}\right)$,
- ▶ $2p$ braces with $(B,\cdot)\simeq (\mathbb{Z}/(q)\times \mathbb{Z}/(q))\rtimes_M \mathbb{Z}/(p^2)$, for $M=\left(\begin{smallmatrix}\beta & 0\\ 0 & \beta^{(p+1)/2}\end{smallmatrix}\right)$.

IV) $\dfrac{p^2+5p}{2}+14$ (resp. $\dfrac{p^2+5p}{2}+13$) braces with $(B,+)\simeq \mathbb{Z}/(pq)\times\mathbb{Z}/(pq)$ if $p\equiv 1 \pmod 4$ (resp. if $p\equiv 3 \pmod 4$). From these

- ▶ 4 braces with $(B,\cdot)\simeq \mathbb{Z}/(pq)\times\mathbb{Z}/(pq)$,
- ▶ 4 braces with $(B,\cdot)\simeq (\mathbb{Z}/(q)\times\mathbb{Z}/(q))\rtimes_M(\mathbb{Z}/(p)\times\mathbb{Z}/(p))$, for each $M\neq \left(\begin{smallmatrix}\beta & 0\\ 0 & \beta^{-1}\end{smallmatrix}\right)$ and $M\neq \left(\begin{smallmatrix}\beta & 0\\ 0 & \beta^{(p+1)/2}\end{smallmatrix}\right)$,
- ▶ 4 (resp. 3) braces with $(B,\cdot)\simeq (\mathbb{Z}/(q)\times\mathbb{Z}/(q))\rtimes_M(\mathbb{Z}/(p)\times\mathbb{Z}/(p))$, for $M=\left(\begin{smallmatrix}\beta & 0\\ 0 & \beta^{-1}\end{smallmatrix}\right)$, if $p\equiv 1 \pmod 4$ (resp. if $p\equiv 3 \pmod 4$),
- ▶ 8 braces with $(B,\cdot)\simeq (\mathbb{Z}/(q)\times\mathbb{Z}/(q))\rtimes_M(\mathbb{Z}/(p)\times\mathbb{Z}/(p))$, for $M=\left(\begin{smallmatrix}\beta & 0\\ 0 & \beta^{(p+1)/2}\end{smallmatrix}\right)$,
- ▶ $(p^2+p)/2$ braces with $(B,\cdot)\simeq (\mathbb{Z}/(q)\times\mathbb{Z}/(q))\rtimes_\beta(\mathbb{Z}/(p)\times\mathbb{Z}/(p))$.