A First Sylow Theorem for skew braces?

Andrea Caranti (Trento)
Ilaria Del Corso (Pisa)
Massimiliano Di Matteo (Napoli)
Maria Ferrara (Pegaso)
Marco Trombetti (Napoli)

Storrs, 5 June 2025

The First Sylow Theorem for groups

Theorem

Let G be a finite group.

Let r be a prime dividing the order of G.

Let r^n be the largest power of r dividing the order of G.

Then G contains a subgroup of order r^n.

A First Sylow Theorem for skew braces?

Theorem? (Unlikely)

Let B be a finite skew brace.

Let r be a prime dividing the order of B.

Let r^n be the largest power of r dividing the order of B.

Then B contains a sub-skew brace of order r^n.

Here a sub-skew brace of $B = (B, \cdot, \circ)$ is a subset $A \subseteq B$ which satisfies any two (and then all three) of

1. $A \leq (B, \cdot)$,
2. $A \leq (B, \circ)$,
3. A is invariant under $\gamma(A)$.

Thus, a Sylow r-sub-skew brace of B is a subset that is simultaneously a Sylow r-subgroup of the additive group and a Sylow r-subgroup of the multiplicative group.

Of gammas and lambdas, and right and left

To a (right) skew brace $(B, \cdot, \circ)$ one attaches a group morphism

$$\gamma : (B, \circ) \to \mathrm{Aut}(B, \cdot)$$

(more commonly called λ in the literature) such that

$$x \circ y = x^{\gamma(y)} \cdot y.$$

Where we stand

We have a proof for finite, supersolvable skew braces.

We are tackling the finite, solvable case.

The proof actually shows that in a finite supersolvable skew brace there are Hall π-sub-skew braces for every set π of primes.

Here a sub-skew brace A of the finite skew brace B is said to be a Hall π-sub-skew brace if

$$|A| \text{ is a } \pi\text{-number}$$

and

$$\gcd(|A|, |B|/|A|) = 1.$$

Supersolvable groups and skew braces

A finite group is said to be supersolvable if all of its non-trivial quotient groups have a normal subgroup of some prime order.

So for instance S_3 is supersolvable, while S_4 is only ~~super~~solvable.

A finite skew brace is said to be supersolvable if all of its non-trivial quotient skew braces have an ideal of some prime order.

A. Ballester-Bolinches, R. Esteban-Romero, M. Ferrara, V. Pérez-Calabuig, M. Trombetti
Finite skew braces of square-free order and supersolubility
Forum Math. Sigma **12** (2024), Paper No. e39, 33 pp.

Ideals in skew braces correspond to normal subgroups in groups — they are the objects with respect to which one can take quotients.

Statement and beginning of proof

Theorem

Let B be a finite skew brace.

If B is supersolvable, then B satisfies Sylow's First Theorem.

Let B be a counterexample of minimum order.

Let M be an ideal of B of order a prime p, and consider the quotient skew brace B/M.

In B/M there is a Sylow p-sub-skew brace P/M. Then P will be a Sylow p-sub-skew brace of B.

Let $q \neq p$ be a prime dividing the order of B.

In B/M there is a Sylow q-sub-skew brace A/M.

If A a proper sub-skew brace of B, then A has a Sylow q-sub-skew brace, which is also a Sylow q-sub-skew brace of B. Thus $A = B$.

Reduction

Thus $A = B$, and we have reduced to the case when

1. B has order $p \cdot q^n$, for $p \neq q$ primes, and
2. B has an ideal M of order p.

Let Q be a Sylow p-subgroup of $(B, \cdot)$, so that

$$(B, \cdot) = Q \ltimes M.$$

Trivial case: if $(B, \cdot) = Q \times M$, then Q is characteristic in $(B, \cdot)$, hence invariant under the whole of $\gamma(B)$, and thus Q is the Sylow q-sub-skew brace we are looking for. So from now on assume

$$[Q, M] \neq 1.$$

Since the values of γ are automorphisms of $(B, \cdot)$, we are interested in the automorphism group of $(B, \cdot)$.

Automorphisms

M. J. Curran
Automorphisms of semidirect products
Math. Proc. R. Ir. Acad. **108**, n. 2 (2008), 205–210

Let $G = Q \ltimes M$ be a semidirect product, with M abelian and characteristic in G.

An automorphism ϑ of G can be described as

$$(xy)^{\vartheta} = x^{\delta} x^{\beta} y^{\alpha}, \qquad \text{for } x \in Q \text{ and } y \in M$$

where

1. $\delta \in \mathrm{Aut}(Q)$, $\alpha \in \mathrm{Aut}(M)$,
2. $(y^{x})^{\alpha} = (y^{\alpha})^{x^{\delta}}$, for $x \in Q$ and $y \in M$,
3. $\beta : Q \to M$ is a 1-cocycle, that is

$$(x_1 \cdot x_2)^{\beta} = (x_1^{\beta})^{x_2^{\delta}} \cdot x_2^{\beta}, \quad \text{for } x_1, x_2 \in Q.$$

The values of γ on M

For $m \in M$, the automorphism $\gamma(m)$ of $(B, \cdot) = Q \ltimes M$ can be described as

$$(xy)^{\gamma(m)} = x^{\delta} x^{\beta} y^{\alpha}, \qquad \text{for } x \in Q \text{ and } y \in M,$$

where $\delta \in \operatorname{Aut}(Q)$, $\alpha \in \operatorname{Aut}(M)$, $\beta : Q \to M$ a 1-cocycle.

Since M is an ideal of B, we have $[\gamma(M), B] \subseteq M$, that is, $\delta = 1$.

Notation: for $m \in M$ and $b \in B$ we write $m^{\circ b} = b^{\ominus 1} \circ m \circ b$.

Indeed for $m \in M$ and $b \in B$ we have

$$\begin{aligned} M \ni b^{\ominus 1} \circ m \circ b &= b^{-\gamma(b)^{-1}\gamma(m)\gamma(b)} \cdot m^{\gamma(b)} \cdot b \\ &= b^{-\gamma(m^{\circ(b)})} \cdot b \cdot b^{-1} \cdot m^{\gamma(b)} \cdot b \\ &= [\gamma(m^{\circ b}), b] \cdot b^{-1} \cdot m^{\gamma(b)} \cdot b, \end{aligned}$$

where $b^{-1} \cdot m^{\gamma(b)} \cdot b \in M$, as M is an ideal, hence M is $\gamma(B)$-invariant, and normal in both groups.

The values of γ on M

The automorphism $\gamma(m)$ of $(B, \cdot) = Q \ltimes M$, for $m \in M$ can be described as

$$(xy)^{\gamma(m)} = x^{\delta} x^{\beta} y^{\alpha}, \qquad \text{for } x \in Q \text{ and } y \in M,$$

where $\delta \in \operatorname{Aut}(Q)$, $\alpha \in \operatorname{Aut}(M)$, $\beta : Q \to M$ a 1-cocycle.

We have just seen that $\delta = 1$.

But we also have $\alpha = 1$, as $\langle \gamma(M) \rangle$ is a finite p-group acting on the group $(M, \cdot)$ of order p.

What about $\beta : Q \to M$, a 1-cocycle $(x_1 x_2)^{\beta} = (x_1^{\beta})^{x_2} x_2^{\beta}$?

Since $\gcd(|Q|, |M|) = 1$, we have $H^1(Q, M) = \{ 0 \}$, that is, all 1-cocycles b are inner, of the form

$$x \mapsto [x, m_0] = m_0^{-x} \cdot m_0,$$

for a suitable $m_0 \in M$.

Elementary

We have seen that all 1-cocycles $\beta : Q \to M$ are inner as $H^1(Q, M) = 0$. In this particular case, there is an elementary proof.

For $c_1, c_2 \in C_Q(M)$, the centraliser of M in Q within $(B, \cdot)$, we have

$$(c_1 c_2)^\beta = (c_1^\beta)^{c_2} \cdot c_2^\beta = c_1^\beta \cdot c_2^\beta,$$

so $\beta_{\restriction C_Q(M)} : C_Q(M) \to M$ is a group morphism, and thus it is trivial, as $\gcd(|Q|, |M|) = 1$.

The group $Q / C_Q(M)$ is isomorphic to a subgroup of $\mathrm{Aut}(M, \cdot)$. As M has prime order, this group is cyclic, say $Q = \langle\, t \,\rangle C_Q(M)$.

Thus β is determined by its value on t. Now there are only $|M|$ such possible values, which are already covered by the (distinct!) inner 1-cocycles

$$x \mapsto [x, m_0] = m_0^{-x} \cdot m_0, \quad \text{for } m_0 \in M.$$

Summing it up

We have found that there is a function τ on M such that for $x \in Q$ and $y, m \in M$ we have

$$(x \cdot y)^{\gamma(m)} = x \cdot [x, m^{\tau}] \cdot y = (x \cdot y)^{m^{\tau}},$$

that is, $\gamma(m) = \iota(m^{\tau})$, where

$$\begin{aligned} \iota : (B, \cdot) &\to \mathrm{Aut}(B, \cdot) \\ b &\mapsto (z \mapsto b^{-1} \cdot z \cdot b). \end{aligned}$$

It is immediate to see that $\tau \in \mathrm{End}(M)$, as

$$\begin{aligned} \iota((m_1 \cdot m_2)^{\tau}) &= \gamma(m_1 \cdot m_2) = \gamma(m_1^{\gamma(m_2)^{-1}})\gamma(m_2) \\ &= \gamma(m_1)\gamma(m_2) = \iota(m_1^{\tau})\iota(m_2^{\tau}) = \iota(m_1^{\tau} \cdot m_2^{\tau}), \end{aligned}$$

and $[Q, M] \neq 1$, so that $\iota_{\restriction M} : M \to \mathrm{Aut}(B, \cdot)$ is injective.

Note that in our case $\mathrm{End}(M) \cong \mathbf{Z}/p\mathbf{Z}$, but in the following we are keeping things slightly more general for a while.

A computation

It is convenient to write $\tau = -\sigma$, that is,

$$\gamma(m) = \iota(m^{-\sigma}).$$

We reprise a calculation from

Elena Campedel, A.C. and Ilaria Del Corso, I.
Hopf-Galois structures on extensions of degree p^2q and skew braces of order p^2q: the cyclic Sylow p-subgroup case
J. Algebra **556**, (2020), 1165–1210

Since $\gamma : (B, \circ) \to \operatorname{Aut}(B, \cdot)$ is a morphism, and $\gamma(m) = \iota(m^{-\sigma})$, we have first of all

$$\gamma(m^{\circ t}) = \gamma(m)^{\gamma(t)} = \iota(m^{-\sigma})^{\gamma(t)} = \iota(m^{-\sigma\gamma(t)}).$$

A computation II

Recall

$$t^{\ominus 1} = t^{-\gamma(t)^{-1}} \quad \text{and} \quad \gamma(m) = \iota(m^{-\sigma}).$$

Let us compute then:

$$\begin{aligned} m^{\circ t} &= t^{\ominus 1} \circ m \circ t \\ &= t^{-\gamma(t)^{-1}\gamma(m)\gamma(t)} \cdot m^{\gamma(t)} \cdot t \\ &= t^{-\gamma(t)^{-1}\iota(m^{-\sigma})\gamma(t)} \cdot t \cdot t^{-1} \cdot m^{\gamma(t)} \cdot t \\ &= t^{-m^{-\sigma\gamma(t)}} \cdot t \cdot m^{\gamma(t)\iota(t)} \\ &= m^{\sigma\gamma(t)} \cdot t^{-1} m^{-\sigma\gamma(t)} \cdot t \cdot m^{\gamma(t)\iota(t)} \\ &= m^{\sigma\gamma(t)} \cdot m^{-\sigma\gamma(t)\iota(t)} \cdot m^{\gamma(t)\iota(t)} \\ &= m^{\sigma\gamma(t)-\sigma\gamma(t)\iota(t)+\gamma(t)\iota(t)}. \end{aligned}$$

A computation III

Putting the two calculations together, we obtain:

$$\iota(m^{-\sigma\gamma(t)}) = \gamma(m^{\circ t}) = \gamma(m^{\sigma\gamma(t)-\sigma\gamma(t)\iota(t)+\gamma(t)\iota(t)})$$
$$= \iota(m^{(\sigma\gamma(t)-\sigma\gamma(t)\iota(t)+\gamma(t)\iota(t))(-\sigma)}),$$

so that, writing $\overline{\gamma(t)} = \gamma(t)_{\restriction M}$ and $\overline{\iota(t)} = \iota(t)_{\restriction M}$,

$$\sigma\overline{\gamma(t)} = \sigma\overline{\gamma(t)}\sigma - \sigma\overline{\gamma(t)}\,\overline{\iota(t)}\sigma + \overline{\gamma(t)}\,\overline{\iota(t)}\sigma,$$

or

$$\sigma\overline{\gamma(t)}(\sigma - 1) = (\sigma - 1)\overline{\gamma(t)}\,\overline{\iota(t)}\sigma$$

When M is cyclic of order p, so that $\sigma, \overline{\gamma(t)}, \overline{\iota(t)}$ are all in $\mathrm{End}(M) \cong \mathbf{Z}/p\mathbf{Z}$, we get

$$\sigma(\sigma - 1)\overline{\gamma(t)}(\overline{\iota(t)} - 1) = 0.$$

Now $\gamma(t) \in \mathrm{Aut}(B, \cdot)$. Also $[Q, M] \neq 1$ and $Q = \langle\, t \,\rangle C_Q(M)$, so that t does not act trivially on M, i.e $\overline{\iota(t)} \neq 1$.

Thus either $\sigma = 0$ or $\sigma = 1$.

Duality

The cases $\sigma = 0$ and $\sigma = 1$ are dual to each other.

If $\sigma = 0$, this means $M \leq \ker(\gamma)$, as $\gamma(m) = \iota(m^{-\sigma})$.

Alan Koch and Paul Truman
Opposite skew left braces and applications
J. Algebra **546**, (2020), 218–235

If $\sigma = 1$, courtesy of Alan Koch and Paul Truman we have for the gamma function $\tilde{\gamma}$ of the opposite skew brace of B

$$\tilde{\gamma}(m) = \gamma(m^{-1})\iota(m^{-1}) = \iota(m^{-(-\sigma)})\iota(m^{-1}) = \iota(m)\iota(m^{-1}) = 1,$$

so that $M \leq \ker(\tilde{\gamma})$.

Since the sub-skew braces of a skew brace and of its opposite are the same, it is enough to consider the case $\sigma = 0$.

Conclusion

So we have

$$(B, \cdot) = Q \ltimes M,$$

with M of order p, and Q a q-group, for $q \neq p$.

Since $\gamma : (B, \circ) \to \mathrm{Aut}(B, \cdot)$ is a group morphism, and $M \leq \ker(\gamma)$, we have that $\gamma(B)$ is a q-group.

$\gamma(B)$ acts by automorphisms on the set of Sylow q-subgroups of $(B, \cdot)$, which has size $\equiv 1 \pmod q$, by Sylow's Third Theorem.

Hence there is a Sylow q-subgroup R of $(B, \cdot)$ which is invariant under $\gamma(B)$, and thus under $\gamma(R) \subseteq \gamma(B)$.

Therefore R is the Sylow q-sub-skew brace we were looking for.

That's All, Thanks!