An approach to a conjecture of Rump on quasi-linear cycle sets of prime cardinality

Nigel Byott

University of Exeter

Keele, 4 August 2023

§1 Quasi-linear Cycle Sets

Cycle sets were introduced by Rump (2016). There is a bijection between finite cycle sets and nondegenerate set-theoretic solutions of the Yang-Baxter Equation.

§1 Quasi-linear Cycle Sets

Cycle sets were introduced by Rump (2016). There is a bijection between finite cycle sets and nondegenerate set-theoretic solutions of the Yang-Baxter Equation.

Definition: A **cycle set** $(X, \cdot)$ is a set with a binary operation such that

$$(x \cdot y) \cdot (x \cdot z) = (y \cdot x) \cdot (y \cdot z) \qquad \forall x, y, z \in X$$

and, for each x, the function

$$\pi_x : X \to X, \qquad y \mapsto x \cdot y$$

is bijective.

§1 Quasi-linear Cycle Sets

Cycle sets were introduced by Rump (2016). There is a bijection between finite cycle sets and nondegenerate set-theoretic solutions of the Yang-Baxter Equation.

Definition: A **cycle set** $(X, \cdot)$ is a set with a binary operation such that

$$(x \cdot y) \cdot (x \cdot z) = (y \cdot x) \cdot (y \cdot z) \qquad \forall x, y, z \in X$$

and, for each x, the function

$$\pi_x : X \to X, \qquad y \mapsto x \cdot y$$

is bijective.

Defining $x \star y = z$ if $x \cdot z = y$, the corresponding solution is

$$r(x, y) = (x \star y, (x \star y) \cdot x).$$

One way to obtain a cycle set is from an abelian group with a suitable permutation:

One way to obtain a cycle set is from an abelian group with a suitable permutation:

Definition: Let $(A, +)$ be an abelian group. Let $\tau \in \mathrm{Sym}(A)$ and suppose that

- $\tau(0) = 0$,
- the operation $\cdot = \cdot_\tau$ given by

$$a \cdot b = \tau(b - a) - \tau(-a)$$

  makes A into a cycle set.

Then we say that (A, τ) is a **quasi-linear cycle set** (QLCS).

This happens if and only if

$$\tau(\tau(b-a) - \tau(-a)) = \tau(\tau(b) - \tau(a)) - \tau(-\tau(a)) \text{ for all } a, b \in A.$$

This identity does hold if τ is a group automorphism, $\tau \in \mathrm{Aut}_{\mathrm{gp}}(A)$.

Rump conjectured that if (A, τ) is a finite QLCS then the corresponding solution is retractible. In particular, this means that if $|A| > 1$ then the subgroup

$$\mathrm{Soc}(A) = \{b \in A : a \cdot b = 0 \cdot b \quad \forall\, a \in A\}$$

cannot be trivial.

When $\tau \in \mathrm{Aut}_{\mathrm{gp}}(A)$,

$$a \cdot_\tau b = \tau(b - a) - \tau(-a) = \tau(b) \quad \forall a, b \in A,$$

so $\mathrm{Soc}(A) = A$.

In the special case that $|A|$ is a prime number, Rump's conjecture amounts to the converse:

Rump conjectured that if (A, τ) is a finite QLCS then the corresponding solution is retractible. In particular, this means that if $|A| > 1$ then the subgroup

$$\mathrm{Soc}(A) = \{b \in A : a \cdot b = 0 \cdot b \quad \forall\, a \in A\}$$

cannot be trivial.

When $\tau \in \mathrm{Aut}_{\mathrm{gp}}(A)$,

$$a \cdot_\tau b = \tau(b - a) - \tau(-a) = \tau(b) \quad \forall a, b \in A,$$

so $\mathrm{Soc}(A) = A$.

In the special case that $|A|$ is a prime number, Rump's conjecture amounts to the converse:

Conjecture 1 (Rump)

If (A, τ) is a QLCS of prime order p, then τ is a group automorphism of A.

Rump checked this for $p \leq 13$ and Colazzo & Vendramin did so up to $p \leq 23$.

An alternative viewpoint

Given an abelian group $(A,+)$ and any permutation

$$\tau \in \mathrm{Sym}_0(A) := \{\pi \in \mathrm{Sym}(A) : \tau(0) = 0\},$$

define $\cdot_\tau$ as before:

$$a \cdot_\tau b = \tau(b-a) - \tau(-a).$$

Then $(A, \cdot_\tau)$ is a set with a binary operation and a distinguished element 0, i.e. $(A, \cdot_\tau)$ is a **pointed magma**.

An alternative viewpoint

Given an abelian group $(A, +)$ and any permutation

$$\tau \in \mathrm{Sym}_0(A) := \{\pi \in \mathrm{Sym}(A) : \tau(0) = 0\},$$

define $\cdot_\tau$ as before:

$$a \cdot_\tau b = \tau(b - a) - \tau(-a).$$

Then $(A, \cdot_\tau)$ is a set with a binary operation and a distinguished element 0, i.e. $(A, \cdot_\tau)$ is a **pointed magma**.

Some obvious properties:

- $a \cdot_\tau 0 = 0$;
- $0 \cdot_\tau b = \tau(b)$;
- $a \cdot a = -\tau(-a) =: \widetilde{\tau}(a)$;
- for each a, the map $\pi_a : b \mapsto a \cdot_\tau b$ is a permutation;
- τ is a group automorphism of $A \Leftrightarrow a \cdot_\tau b = \tau(b)$ for all a, b.

Let's consider the automorphisms of the pointed magma $(A, \cdot_\tau)$:

$$\mathrm{Aut}_{\mathrm{pm}}(A, \tau) := \{\sigma \in \mathrm{Sym}_0(A) : \sigma(a \cdot_\tau b) = \sigma(a) \cdot_\tau \sigma(b)\ \forall a, b \in A\}.$$

This is obviously a group (under composition of permutations).

For "most" permutations τ, we expect the operation $\cdot_\tau$ to be badly behaved and have few symmetries, so $\mathrm{Aut}_{\mathrm{pm}}(A, \tau)$ should be "small".

Examples

Let $A = \mathbb{Z}/7\mathbb{Z}$.
(i) $\tau = (134)(26)$.

	0	1	2	3	4	5	6	
0	0	3	6	4	1	5	2	$\pi_0 = \tau$
1	0	5	1	4	2	6	3	$\pi_1 = (156342)$
2	0	4	2	5	1	6	3	$\pi_2 = (14)(2)(356)$
3	0	4	1	6	2	5	3	$\pi_3 = (142)(36)(5)$
4	0	4	1	5	3	6	2	$\pi_4 = (143562)$
5	0	5	2	6	3	1	4	$\pi_5 = (15)(2)(364)$
6	0	3	1	5	2	6	4	$\pi_6 = (135642)$

Let $\sigma \in \mathrm{Aut}_{\mathrm{pm}}(A, \tau)$. From π_2, π_3, π_5 we see $\sigma(2) = 2$, $\sigma(5) = 5$, etc.

$$\mathrm{Aut}_{\mathrm{pm}}(A, \tau) = \{\mathrm{id}\}.$$

(ii) $\tau = (356)$.

	0	1	2	3	4	5	6	
0	0	1	2	5	4	6	3	$\pi_0 = \tau$
1	0	4	5	6	2	1	3	$\pi_1 = (1425)(36)$
2	0	4	1	2	3	6	5	$\pi_2 = (1432)(56)$
3	0	2	6	3	4	5	1	$\pi_3 = (126)(3)(4)(5)$
4	0	6	1	5	2	3	4	$\pi_4 = (1642)(35)$
5	0	3	2	4	1	5	6	$\pi_5 = (134)(2)(5)(6)$
6	0	1	4	3	5	2	6	$\pi_6 = (1)(245)(3)(6)$

We find

$$\mathrm{Aut}_{\mathrm{pm}}(A, \tau) = \{\mathrm{id}, (124)(365), (142)(356)\}.$$

In this case, $\mathrm{Aut}_{\mathrm{pm}}(A, \tau)$ consists of group automorphisms of A which commute with τ.

Why should we care about $\mathrm{Aut}_{\mathrm{pm}}(A, \tau)$?

The condition for (A, τ) to be a QLCS

$$\tau(\tau(b-a) - \tau(-a)) = \tau(\tau(b) - \tau(a)) - \tau(-\tau(a)) \text{ for all } a, b \in A$$

says precisely that

$$\tau(a \cdot_\tau b) = \tau(a) \cdot_\tau \tau(b),$$

that is,

$$\tau \in \mathrm{Aut}_{\mathrm{pm}}(A, \tau).$$

Why should we care about $\mathrm{Aut}_{\mathrm{pm}}(A, \tau)$?

The condition for (A, τ) to be a QLCS

$$\tau(\tau(b-a)-\tau(-a)) = \tau(\tau(b)-\tau(a)) - \tau(-\tau(a)) \text{ for all } a, b \in A$$

says precisely that

$$\tau(a \cdot_\tau b) = \tau(a) \cdot_\tau \tau(b),$$

that is,

$$\tau \in \mathrm{Aut}_{\mathrm{pm}}(A, \tau).$$

According to Conjecture 1, if $|A| = p$ then this should only happen if $\tau \in \mathrm{Aut}_{\mathrm{gp}}(A)$.

Some easy results

Let $(A, +)$ be an arbitrary abelian group, and let $\tau \in \mathrm{Sym}_0(A)$.
Define $\widetilde{\tau}(a) = -\tau(-a)$.

Proposition 1

If $\sigma \in \mathrm{Aut}_{\mathrm{pm}}(A, \tau)$ *then* $\sigma\tau = \tau\sigma$ *and* $\sigma\widetilde{\tau} = \widetilde{\tau}\sigma$*.*

Hence $\mathrm{Aut}_{\mathrm{pm}}(A, \tau)$ *is contained in the centraliser of* $\langle \tau, \widetilde{\tau} \rangle$ *in* $\mathrm{Sym}_0(A)$*.*

Some easy results

Let $(A, +)$ be an arbitrary abelian group, and let $\tau \in \mathrm{Sym}_0(A)$.
Define $\widetilde{\tau}(a) = -\tau(-a)$.

Proposition 1

If $\sigma \in \mathrm{Aut}_{\mathrm{pm}}(A, \tau)$ then $\sigma\tau = \tau\sigma$ and $\sigma\widetilde{\tau} = \widetilde{\tau}\sigma$.

Hence $\mathrm{Aut}_{\mathrm{pm}}(A, \tau)$ is contained in the centraliser of $\langle \tau, \widetilde{\tau} \rangle$ in $\mathrm{Sym}_0(A)$.

Proof.

For all a, $b \in A$, we have $\sigma(a \cdot_\tau b) = \sigma(a) \cdot_\tau \sigma(b)$, so

$$\sigma(\tau(b - a) - \tau(-a)) = \tau(\sigma(b) - \sigma(a)) - \tau(-\sigma(a)).$$

Putting $a = 0$ and recalling $\sigma(0) = \tau(0) = 0$, we have $\sigma(\tau(b)) = \tau(\sigma(b))$.
Putting $b = a$, we have $\sigma(-\tau(-a)) = -\tau(-\sigma(a))$, so
$\sigma(\widetilde{\tau}(a)) = \widetilde{\tau}(\sigma(a))$. □

Proposition 2

$$\sigma \in \mathrm{Aut}_{\mathrm{pm}}(A, \tau) \Leftrightarrow \tau \in \mathrm{Aut}_{\mathrm{pm}}(A, \sigma).$$

Proposition 2

$$\sigma \in \mathrm{Aut}_{\mathrm{pm}}(A, \tau) \Leftrightarrow \tau \in \mathrm{Aut}_{\mathrm{pm}}(A, \sigma).$$

Proof.

Suppose $\sigma \in \mathrm{Aut}_{\mathrm{pm}}(A, \tau)$, so $\sigma(a \cdot_\tau b) = \sigma(a) \cdot_\tau \sigma(b) \; \forall a, b \in A$. Then

$$\sigma(\tau(b-a) - \tau(-a)) = \tau(\sigma(b) - \sigma(a)) - \tau(-\sigma(a)).$$

Put $c = b - a$, $d = -a$. For all c, $d \in A$, we have

$$\sigma(\tau(c) - \tau(d)) = \tau(\sigma(c-d) - \sigma(-d)) - \tau(-\sigma(-d)).$$

But $-\tau(-\sigma(-d)) = \widetilde{\tau}(\sigma(-d)) = \sigma(\widetilde{\tau}(-d)) = \sigma(-\tau(d))$. So

$$\sigma(\tau(c) - \tau(d)) - \sigma(-\tau(d)) = \tau(\sigma(c-d) - \sigma(-d)),$$

i.e. $\tau(d) \cdot_\sigma \tau(c) = \tau(d \cdot_\sigma c)$. $\square$

Proposition 3

If $\sigma\tau = \tau\sigma$ *and either* $\sigma \in \mathrm{Aut}_{\mathrm{gp}}(A)$ *or* $\tau \in \mathrm{Aut}_{\mathrm{gp}}(A)$, *then* $\sigma \in \mathrm{Aut}_{\mathrm{pm}}(A, \tau)$.

So if $\tau \in \mathrm{Aut}_{\mathrm{gp}}(A)$ *then*

$$\mathrm{Aut}_{\mathrm{pm}}(A, \tau) = \{\sigma \in \mathrm{Sym}_0(A) : \sigma\tau = \tau\sigma\}.$$

Proposition 3

If $\sigma\tau = \tau\sigma$ and either $\sigma \in \mathrm{Aut}_{\mathrm{gp}}(A)$ or $\tau \in \mathrm{Aut}_{\mathrm{gp}}(A)$, then $\sigma \in \mathrm{Aut}_{\mathrm{pm}}(A, \tau)$.

So if $\tau \in \mathrm{Aut}_{\mathrm{gp}}(A)$ then

$$\mathrm{Aut}_{\mathrm{pm}}(A, \tau) = \{\sigma \in \mathrm{Sym}_0(A) : \sigma\tau = \tau\sigma\}.$$

Proof.

e.g. if $\sigma \in \mathrm{Aut}_{\mathrm{gp}}(A)$ then

$$\begin{aligned}
\sigma(a \cdot_\tau b) &= \sigma(\tau(b-a) - \tau(-a)) \\
&= \sigma(\tau(b-a)) - \sigma(\tau(-a)) \\
&= \tau(\sigma(b-a)) - \tau(\sigma(-a)) \\
&= \tau(\sigma(b) - \sigma(a)) - \tau(-\sigma(a)) \\
&= \sigma(a) \cdot_\tau \sigma(b).
\end{aligned}$$

$\square$

A new conjecture

Conjecture 2

Let $(A,+)$ be a finite group of prime order p, and let $\tau \in \mathrm{Sym}_0(A)$. If $\tau \notin \mathrm{Aut}_{\mathrm{gp}}(A)$ then

$$\mathrm{Aut}_{\mathrm{pm}}(A,\tau) = \{\sigma \in \mathrm{Aut}_{\mathrm{gp}}(A) : \sigma\tau = \tau\sigma\}.$$

Remarks

(i) *We have just proved the inclusion "$\supseteq$".*

(ii) *Conjecture 2 implies Conjecture 1: if $\tau \notin \mathrm{Aut}_{\mathrm{gp}}(A)$ then $\tau \notin \mathrm{Aut}_{\mathrm{pm}}(A,\tau)$.*

(iii) *Conjecture 2 implies that if $\tau \notin \mathrm{Aut}_{\mathrm{gp}}(A)$ then $\mathrm{Aut}_{\mathrm{pm}}(A,\tau)$ is cyclic of order dividing $p-1$, and each element acts on $A\backslash\{0\}$ as a product of cycles of the same length.*

I will give two pieces of evidence for Conjecture 2.

Submagmas

Definition

A (pointed) **submagma** *of* $(A, \cdot_T)$ *is a subset* $S \subseteq A$ *such that* $0 \in S$ *and* $a \cdot_T b \in S$ *for all* $a, b \in S$.

Submagmas

Definition

A (pointed) **submagma** *of* $(A, \cdot_\tau)$ *is a subset* $S \subseteq A$ *such that* $0 \in S$ *and* $a \cdot_\tau b \in S$ *for all* $a, b \in S$*.*

Since $0 \cdot_\tau b = \tau(b)$ and $a \cdot_\tau a = \widetilde{\tau}(a)$, any submagma is a union of orbits of the group $\langle \tau, \widetilde{\tau} \rangle \leq \mathrm{Sym}_0(A)$.

Submagmas

Definition

A (pointed) **submagma** *of* $(A, \cdot_\tau)$ *is a subset* $S \subseteq A$ *such that* $0 \in S$ *and* $a \cdot_\tau b \in S$ *for all* $a, b \in S$.

Since $0 \cdot_\tau b = \tau(b)$ and $a \cdot_\tau a = \widetilde{\tau}(a)$, any submagma is a union of orbits of the group $\langle \tau, \widetilde{\tau} \rangle \leq \mathrm{Sym}_0(A)$.

Example: If $a \neq 0$ and $\tau(a) = a$, $\tau(-a) = -a$ then $a \cdot_\tau a = a$ and $(-a) \cdot_\tau (-a) = -a$. Hence $\{0, a\}$ is a submagma. Similarly for $\{0, -a\}$.

Submagmas

Definition

A (pointed) **submagma** *of $(A, \cdot_\tau)$ is a subset $S \subseteq A$ such that $0 \in S$ and $a \cdot_\tau b \in S$ for all a, $b \in S$.*

Since $0 \cdot_\tau b = \tau(b)$ and $a \cdot_\tau a = \widetilde{\tau}(a)$, any submagma is a union of orbits of the group $\langle \tau, \widetilde{\tau} \rangle \leq \mathrm{Sym}_0(A)$.

Example: If $a \neq 0$ and $\tau(a) = a$, $\tau(-a) = -a$ then $a \cdot_\tau a = a$ and $(-a) \cdot_\tau (-a) = -a$. Hence $\{0, a\}$ is a submagma. Similarly for $\{0, -a\}$.

Example: If $\tau \in \mathrm{Aut}_{\mathrm{gp}}(A)$ then $\widetilde{\tau} = \tau$ and $a \cdot_\tau b = \tau(b)$, so any union S of τ-orbits which includes 0 is a submagma. In fact, S is a (pointed left) ideal: $a \cdot_\tau b \in S$ for all $a \in A$, $b \in S$.

Submagmas

Definition

A (pointed) **submagma** *of $(A, \cdot_\tau)$ is a subset $S \subseteq A$ such that $0 \in S$ and $a \cdot_\tau b \in S$ for all a, $b \in S$.*

Since $0 \cdot_\tau b = \tau(b)$ and $a \cdot_\tau a = \widetilde{\tau}(a)$, any submagma is a union of orbits of the group $\langle \tau, \widetilde{\tau} \rangle \leq \mathrm{Sym}_0(A)$.

Example: If $a \neq 0$ and $\tau(a) = a$, $\tau(-a) = -a$ then $a \cdot_\tau a = a$ and $(-a) \cdot_\tau (-a) = -a$. Hence $\{0, a\}$ is a submagma. Similarly for $\{0, -a\}$.

Example: If $\tau \in \mathrm{Aut}_{\mathrm{gp}}(A)$ then $\widetilde{\tau} = \tau$ and $a \cdot_\tau b = \tau(b)$, so any union S of τ-orbits which includes 0 is a submagma. In fact, S is a (pointed left) ideal: $a \cdot_\tau b \in S$ for all $a \in A$, $b \in S$.

Apart from these two special cases, proper non-trivial submagmas seem to be fairly rare.

However, we have the following (easy) observation:
If $\sigma \in \mathrm{Aut}_{\mathrm{pm}}(A, \tau)$ then

$$\mathrm{Fix}(\sigma) := \{a \in A : \sigma(a) = a\}$$

is a submagma of $(A, \cdot_\tau)$.

However, we have the following (easy) observation:
If $\sigma \in \mathrm{Aut}_{\mathrm{pm}}(A, \tau)$ then

$$\mathrm{Fix}(\sigma) := \{a \in A : \sigma(a) = a\}$$

is a submagma of $(A, \cdot_\tau)$.

Hence we have:

Theorem 1

If $(A, \cdot_\tau)$ has no nontrivial proper submagmas, then the stabiliser in $\mathrm{Aut}_{\mathrm{pm}}(A, \tau)$ of any $a \in A\backslash\{0\}$ is $\{id\}$.

In particular, every element of $\mathrm{Aut}_{\mathrm{pm}}(A, \tau)$ acts on $A\backslash\{0\}$ as a product of cycles of the same length, and $|\mathrm{Aut}_{\mathrm{pm}}(A, \tau)|$ divides $|A| - 1$.

However, we have the following (easy) observation:
If $\sigma \in \mathrm{Aut}_{\mathrm{pm}}(A, \tau)$ then

$$\mathrm{Fix}(\sigma) := \{a \in A : \sigma(a) = a\}$$

is a submagma of $(A, \cdot_\tau)$.

Hence we have:

Theorem 1

If $(A, \cdot_\tau)$ has no nontrivial proper submagmas, then the stabiliser in $\mathrm{Aut}_{\mathrm{pm}}(A, \tau)$ of any $a \in A \backslash \{0\}$ is $\{id\}$.

In particular, every element of $\mathrm{Aut}_{\mathrm{pm}}(A, \tau)$ acts on $A \backslash \{0\}$ as a product of cycles of the same length, and $|\mathrm{Aut}_{\mathrm{pm}}(A, \tau)|$ divides $|A| - 1$.

If $|A| = p$ is prime and $(A, \cdot_\tau)$ has no nontrivial proper submagmas, then $\mathrm{Aut}_{\mathrm{pm}}(A, \tau)$ at least "looks like" a subgroup of $\mathrm{Aut}_{\mathrm{gp}}(A)$.

However, we have the following (easy) observation:
If $\sigma \in \mathrm{Aut}_{\mathrm{pm}}(A, \tau)$ then

$$\mathrm{Fix}(\sigma) := \{a \in A : \sigma(a) = a\}$$

is a submagma of $(A, \cdot_\tau)$.

Hence we have:

Theorem 1

If $(A, \cdot_\tau)$ has no nontrivial proper submagmas, then the stabiliser in $\mathrm{Aut}_{\mathrm{pm}}(A, \tau)$ of any $a \in A \backslash \{0\}$ is $\{id\}$.

In particular, every element of $\mathrm{Aut}_{\mathrm{pm}}(A, \tau)$ acts on $A \backslash \{0\}$ as a product of cycles of the same length, and $|\mathrm{Aut}_{\mathrm{pm}}(A, \tau)|$ divides $|A| - 1$.

If $|A| = p$ is prime and $(A, \cdot_\tau)$ has no nontrivial proper submagmas, then $\mathrm{Aut}_{\mathrm{pm}}(A, \tau)$ at least "looks like" a subgroup of $\mathrm{Aut}_{\mathrm{gp}}(A)$.

If $(A, \cdot_\tau)$ does contain submagmas then any $\sigma \in \mathrm{Aut}_{\mathrm{pm}}(A, \tau)$ must preserve the lattice of submagmas, and this again severely restricts the possibilities for σ.

When τ moves few elements

Fix $\tau \in \mathrm{Sym}_0(A)$, and let S be the support of $\widetilde{\tau}$:

$$S = \{a \in A : -\tau(-a) \neq a\}.$$

Suppose $\sigma \in \mathrm{Aut}_{\mathrm{pm}}(A, \tau)$. If S is not too big, we can get some information about σ with no information about τ other than S.
First observe that, since $\sigma\widetilde{\tau} = \widetilde{\tau}\sigma$, we have $\sigma(S) = S$.

Lemma

For each $b \in A$,

$$\sigma\big((b + S)\backslash S\big) = (\sigma(b) + S)\backslash S.$$

Proof.

Suppose $a \notin S$, so $\tau(-a) = -a$ and $\tau(-\sigma(a)) = -\sigma(a)$. For $b \in A$,

$$\begin{aligned} a \cdot_\tau b = b \quad &\Leftrightarrow \quad \tau(b-a) - \tau(-a) = b \\ &\Leftrightarrow \quad \tau(b-a) = b - a \\ &\Leftrightarrow \quad a - b \in S \\ &\Leftrightarrow \quad a \in b + S. \end{aligned}$$

But also

$$\begin{aligned} a \cdot_\tau b = b \quad &\Leftrightarrow \quad \sigma(a) \cdot_\tau \sigma(b) = \sigma(b) \\ &\Leftrightarrow \quad \sigma(a) \in \sigma(b) + S. \end{aligned}$$

So, for $a \notin S$,

$$a \in b + S \Leftrightarrow \sigma(a) \in \sigma(b) + S.$$

$$\text{Thus } \sigma\big((b+S)\backslash S\big) = (\sigma(b) + S)\backslash \sigma(S) = (\sigma(b)+S)\backslash S.$$

$\square$

Theorem 2

Suppose $|A| = p$, and let $\tau = (a, b)$ be a transposition. Then

$$\mathrm{Aut}_{\mathrm{pm}}(A, \tau) = \begin{cases} \{\mathrm{id}\} & \text{if } b \neq -a, \\ \{\mathrm{id}, \mathrm{inv}\} & \text{if } b = -a, \end{cases}$$

where $\mathrm{inv}(a) = -a$. Thus Conjecture 2 holds for transpositions.

Proof.

We have $S = \{-a, -b\}$.
Write out the sets $c + S$ in the order

$$a + S, a + (a - b) + S, a + 2(a - b) + S, \ldots, b + S,$$

and remove the intersections with S:

□

$$
\begin{aligned}
a + S &= \{0, a-b\}, \\
a + (a-b) + S &= \{a-b, 2(a-b)\}, \\
&\vdots \\
&\vdots \\
a + (p-2)(a-b) + S &= \{(p-2)(a-b), (p-1)(a-b)\}, \\
b + S &= \{(p-1)(a-b), 0\}.
\end{aligned}
$$

$$
\begin{aligned}
a+S &= \{0, a-b\}, \\
a+(a-b)+S &= \{a-b, 2(a-b)\}, \\
&\vdots \\
a+(j-1)(a-b)+S &= \{b-2a, -a\}, \\
a+j(a-b)+S &= \{-a, -b\} = S, \\
a+(j+1)(a-b)+S &= \{-b, a-2b\}, \\
&\vdots \\
a+(p-2)(a-b)+S &= \{(p-2)(a-b), (p-1)(a-b)\}, \\
b+S &= \{(p-1)(a-b), 0\}.
\end{aligned}
$$

$$
\begin{aligned}
(a+S)\backslash S &= \{0, a-b\}, \\
(a+(a-b)+S)\backslash S &= \{a-b, 2(a-b)\}, \\
&\vdots \qquad\qquad \vdots \\
(a+(j-1)(a-b)+S)\backslash S &= \{b-2a, \qquad \}, \\
(a+j(a-b)+S)\backslash S &= \{ \qquad\qquad \} = S, \\
(a+(j+1)(a-b)+S)\backslash S &= \{ \qquad , a-2b\}, \\
&\vdots \qquad\qquad \vdots \\
(a+(p-2)(a-b)+S)\backslash S &= \{(p-2)(a-b), (p-1)(a-b)\}, \\
(b+S)\backslash S &= \{(p-1)(a-b), 0\}.
\end{aligned}
$$

$$
\begin{array}{rcl}
(a+S)\backslash S &=& \{0, a-b\},\\
(a+(a-b)+S)\backslash S &=& \{a-b, 2(a-b)\},\\
\vdots && \vdots\\
(a+(j-1)(a-b)+S)\backslash S &=& \{b-2a, \quad\quad \},\\
(a+j(a-b)+S)\backslash S &=& \{ \quad\quad\quad\quad \} = S,\\
(a+(j+1)(a-b)+S)\backslash S &=& \{ \quad\quad , a-2b\},\\
\vdots && \vdots\\
(a+(p-2)(a-b)+S)\backslash S &=& \{(p-2)(a-b), (p-1)(a-b)\},\\
(b+S)\backslash S &=& \{(p-1)(a-b), 0\}.
\end{array}
$$

These sets are permuted by σ, so the two sets containing 0 are either fixed or swapped.

If they are fixed, $\sigma(a) = a$, $\sigma(a-b) = a-b$,
$\sigma(a+(a-b)) = a+(a-b)$, etc, so $\sigma = \mathrm{id}$.

If they are swapped, $\sigma(a-b) = (p-1)(a-b)$, etc, and the empty set must occur exactly in the middle, so $b = -a$ and $\sigma = \mathrm{inv}$. QED