A "power" conjugate equation in the symmetric group

Szilvia Homolya and Jenő Szigeti

ABSTRACT. First we consider the solutions of the general "cubic" equation

$$\alpha_1 \circ x^{r_1} \circ \alpha_2 \circ x^{r_2} \circ \alpha_3 \circ x^{r_3} = 1$$

(with $r_1, r_2, r_3 \in \{1, -1\}$) in the symmetric group S_n. In certain cases this equation can be rewritten as $\alpha \circ y \circ \alpha^{-1} = y^2$ or as $\alpha \circ y \circ \alpha^{-1} = y^{-2}$, where $\alpha \in \mathrm{S}_n$ depends on the α_i's and the new unknown permutation $y \in \mathrm{S}_n$ is a product of x (or x^{-1}) and one of the permutations $\alpha_i^{\pm 1}$. Using combinatorial arguments and some basic number theoretical facts, we obtain results about the solutions of the so-called power conjugate equation $\alpha \circ y \circ \alpha^{-1} = y^e$ in S_n, where $e \in \mathbb{Z}$ is an integer exponent. Under certain conditions, the solutions are exactly the solutions of $y^{e-1} = 1$ in the centralizer of α.

1. INTRODUCTION

One of the starting points of classical algebra is the solution of polynomial equations in fields. Thus, the investigation of equations in groups is a natural idea. Recently a good number of publications appeared that are related to complexity, taking an algorithmic approach to solving such equations. In the present paper we are interested only in the explicit solutions, so we restrict our consideration to the non-algorithmic aspects. It is a surprising fact that the authors found only a limited number of results about the explicit solutions of equations in groups. One of the earliest results (due to Frobenius) is about the number of solutions of $x^m = 1$ in a finite group (see [IR]). Further results concerning the equation $x^m = 1$ in the symmetric group S_n consisting of all bijective $\{1, 2, \ldots, n\} \longrightarrow \{1, 2, \ldots, n\}$ functions can be found in [CHS], [MW] and [FM]. A general equation (containing constants and group operations) for a single unknown permutation $x \in \mathrm{S}_n$ is of the form:

$$\alpha_1 \circ x^{r_1} \circ \alpha_2 \circ \cdots \circ \alpha_k \circ x^{r_k} = 1,$$

where $k \geq 1$, $\alpha_i \in \mathrm{S}_n$ and $r_i \in \{1, -1\}$ for each $1 \leq i \leq k$. Our first impression is that the complete solution of the above equation is hopeless, on the other hand to deal with some special cases seems to be a challenging problem. We note that in the above equation $r_1 = 1$ can be assumed, otherwise $\alpha_1 \circ x^{-r_1} \circ \alpha_2 \circ \cdots \circ \alpha_k \circ x^{-r_k} = 1$ is the same equation for the inverse x^{-1} and $-r_1 = 1$.

The solutions in the "quadratic" case $k = 2$ can easily be obtained by a simple procedure. If $1 = r_1 = r_2$, then $\alpha_1 \circ x \circ \alpha_2 \circ x = 1$ is equivalent to

$$(x \circ \alpha_2)^2 = \alpha_1^{-1} \circ \alpha_2.$$

The above square root equation has a solution if and only if the number of the $2i$-element cycles in $\alpha_1^{-1} \circ \alpha_2$ is even for all integers $i \geq 1$. If $1 = r_1 = -r_2$, then $\alpha_1 \circ x \circ \alpha_2 \circ x^{-1} = 1$ is equivalent to

$$x \circ \alpha_2 \circ x^{-1} = \alpha_1^{-1}.$$

The above equation has a solution if and only if the permutations α_2 and α_1^{-1} are of the same type. The type of a permutation $\pi \in \mathrm{S}_n$ is a sequence $\mathrm{type}(\pi) = \langle t_1, t_2, \ldots, t_n \rangle$ of integers, where $t_i \geq 0$ denotes the number of cycles in π of length $i \geq 1$. A well-known fact is that for $\pi_1, \pi_2 \in \mathrm{S}_n$ the equality $\mathrm{type}(\pi_1) = \mathrm{type}(\pi_2)$ is equivalent to the conjugate relation between π_1 and π_2 (there exists a permutation $\tau \in \mathrm{S}_n$ such that $\tau \circ \pi_1 \circ \tau^{-1} = \pi_2$). Further details (about the complete solutions in the case $k = 2$) are left to the readers.

The situation in the case $k \geq 3$ is far more complicated. A nice summary about the general situation can be found in [L]. An important direction of research is to find solutions of a given group-equation in an appropriate extension of the base group. The Kervaire–Laudenbach (KL) conjecture asserts that if the length $r_1 + r_2 + \cdots + r_k$ of the equation $\alpha_1 \circ x^{r_1} \circ \alpha_2 \circ \cdots \circ \alpha_k \circ x^{r_k} = 1$ over an arbitrary group G is nonzero, then this equation has a solution in a group H containing G (here we assume that $r_{i-1} + r_i \neq 0$ if $\alpha_i = 1$, $2 \leq i \leq k$). A consequence of a general extension theorem of Gerstenhaber and Rothaus (see [GR]) is that (KL) holds for finite groups. For $k = 5$ the conjecture (KL) is proved in [E].

Now consider the "general cubic" equation

$$(*) \qquad \alpha_1 \circ x^{r_1} \circ \alpha_2 \circ x^{r_2} \circ \alpha_3 \circ x^{r_3} = 1$$

in S_n, where $r_1 = 1$. According to the choice of the exponents we have the following four possibilities

$$(*1) \ \alpha_1 \circ x \circ \alpha_2 \circ x \circ \alpha_3 \circ x^{-1} = 1, \quad (*2) \ \alpha_1 \circ x \circ \alpha_2 \circ x^{-1} \circ \alpha_3 \circ x = 1,$$

$$(*3) \ \alpha_1 \circ x \circ \alpha_2 \circ x^{-1} \circ \alpha_3 \circ x^{-1} = 1, \quad (*4) \ \alpha_1 \circ x \circ \alpha_2 \circ x \circ \alpha_3 \circ x = 1.$$

Clearly, the above equations can be rewritten as follows

$$(*1) \ \alpha \circ y \circ \beta = y^2, \text{ where } y = x \circ \alpha_2 \text{ and } \alpha = \alpha_1^{-1}, \beta = \alpha_2 \circ \alpha_3^{-1} \circ \alpha_2^{-1},$$

$$(*2) \ \alpha \circ y \circ \beta = y^2, \text{ where } y = x^{-1} \circ \alpha_1^{-1} \text{ and } \alpha = \alpha_2, \beta = \alpha_1 \circ \alpha_3 \circ \alpha_1^{-1},$$

$$(*3) \ \alpha \circ y \circ \beta = y^2, \text{ where } y = x \circ \alpha_3^{-1} \text{ and } \alpha = \alpha_1, \beta = \alpha_3 \circ \alpha_2 \circ \alpha_3^{-1},$$

$$(*4) \ \alpha \circ y \circ \beta = y^{-2}, \text{ where } y = \alpha_3 \circ x \text{ and } \alpha = \alpha_1 \circ \alpha_3^{-1}, \beta = \alpha_2 \circ \alpha_3^{-1}.$$

Thus, the solution of the "cubic" equation can be reduced to the solution of the equations

$$\alpha \circ y \circ \beta = y^2 \text{ and } \alpha \circ y \circ \beta = y^{-2},$$

where $\alpha, \beta \in \mathrm{S}_n$ are constants and the new unknown permutation is $y \in \mathrm{S}_n$. In both cases we assume that $y = 1$ is a solution of the given equation. Our requirement is quite natural, however the weaker assumption, that we have at least one solution in S_n is even more natural. The condition that $y = 1$ is a solution is equivalent

to the fact that $\beta = \alpha^{-1}$ is the inverse of α (in both cases). In view of the above observations, we consider the "power conjugate" equation

$$(e * \alpha) \quad \alpha \circ y \circ \alpha^{-1} = y^e,$$

where $e \in \mathbb{Z}$ is an integer exponent. If $e \in \{-1, 1\}$, then $(e * \alpha)$ is quadratic and the case $e = 0$ is trivial. Therefore in the rest of the paper we assume that $e \notin \{-1, 0, 1\}$. Using combinatorial arguments and some basic number theoretical facts, in certain cases (depending on the type of α) we are able to obtain essential information about the solutions of $(e * \alpha)$ in S_n (see Theorems 2.8, 2.11, 2.12 and 2.14). One of our main results reveals that under certain conditions, the solutions of $(e * \alpha)$ are exactly the solutions of $y^{e-1} = 1$ in the centralizer of α.

2. THE SOLUTIONS OF THE POWER CONJUGATE EQUATION $\alpha \circ y \circ \alpha^{-1} = y^e$

Let $\delta = \tau \circ \alpha \circ \tau^{-1}$ be a conjugate of α (here $\tau \in \mathrm{S}_n$ is fixed). Since the conjugation is an automorphism of S_n, the solutions of $(e * \delta)$: $\delta \circ z \circ \delta^{-1} = z^e$ can be obtained as the conjugates $z = \tau \circ y \circ \tau^{-1}$ of the solutions of $(e * \alpha)$. Thus, the number of solutions of $(e * \alpha)$ depends only on the conjugacy class (or the type) of α.

For a given permutation $\alpha \in \mathrm{S}_n$ with $\mathrm{type}(\alpha) = \langle g_1, g_2, \ldots, g_n \rangle$ and for an integer $1 \leq d \leq n$ we define a set of integers (the d-range of α) as

$$F_d(\alpha) = \left\{ \sum_{1 \leq j \leq n,\ d|j} q_j \cdot j \,\middle|\, 0 \leq q_j \leq g_j \text{ for all } 1 \leq j \leq n \right\} =$$

$$\{ q_d \cdot d + q_{2d} \cdot 2d + \cdots + q_{\lfloor n/d \rfloor d} \cdot \lfloor n/d \rfloor d \mid 0 \leq q_{id} \leq g_{id} \text{ for all } 1 \leq i \leq \lfloor n/d \rfloor \}.$$

Now $g_1 \cdot 1 + g_2 \cdot 2 + \cdots + g_n \cdot n = n$ gives that $F_d(\alpha) \subseteq \{d, 2d, \ldots, \lfloor n/d \rfloor d\}$ and $g_n = 1$ implies that $g_1 = g_2 = \cdots = g_{n-1} = 0$, whence $F_1(\alpha) = \{0, n\}$ follows. Clearly, the divisibility $d_1 \mid d_2$ implies that $F_{d_2}(\alpha) \subseteq F_{d_1}(\alpha)$.

2.1. Lemma. *If the containment $\alpha(H) \subseteq H$ holds for some subset $H \subseteq \{1, 2, \ldots, n\}$, then $\alpha(H) = H$ and $H = D_1 \cup D_2 \cup \cdots \cup D_m$ is a union of certain pairwise disjoint cycles of α. If $1 \leq d \leq n$ and $d \mid |D_j|$ holds for all $1 \leq j \leq m$, then for the number of elements we have*

$$|H| = |D_1| + |D_2| + \cdots + |D_m| \in F_d(\alpha).$$

Proof. Obvious. $\square$

2.2. Lemma. *If $\alpha \circ y \circ \alpha^{-1} = z$ holds for $\alpha, y, z \in \mathrm{S}_n$ and $(c_1, c_2, \ldots, c_r)$ is a cycle of y, then $(\alpha(c_1), \alpha(c_2), \ldots, \alpha(c_r))$ is a cycle of z.*

Proof. Clearly, $z(\alpha(c_i)) = (z \circ \alpha)(c_i) = (\alpha \circ y)(c_i) = \alpha(y(c_i)) = \alpha(c_{i+1})$ (indices $1 \leq i \leq r$ are considered modulo r). $\square$

2.3. Lemma. *Consider the union $\{1, 2, \ldots, n\} = H_1 \cup H_2 \cup \cdots \cup H_s$ of the pairwise disjoint fixed subsets $H_k \subseteq \{1, 2, \ldots, n\}$, $1 \leq k \leq s$ of $\alpha \in \mathrm{S}_n$ (now $\alpha(H_k) = H_k$ for each $1 \leq k \leq s$) and let $y_k \in \mathrm{S}_{H_k}$ (here $y_k : H_k \longrightarrow H_k$ is a permutation) be a solution of $(e * (\alpha \upharpoonright H_k))$, where $(\alpha \upharpoonright H_k) : H_k \longrightarrow H_k$ is the restriction of α to H_k. Now the disjoint union $y_1 \sqcup y_2 \sqcup \cdots \sqcup y_s$ of the permutations y_k $(1 \leq k \leq s)$ is a solution of $(e * \alpha)$ in S_n. Notice that for $i \in \{1, 2, \ldots, n\}$*

$$(y_1 \sqcup y_2 \sqcup \cdots \sqcup y_s)(i) = y_k(i), \text{ where } 1 \leq k \leq s \text{ is the unique index with } i \in H_k.$$

Proof. Obvious. $\square$

2.4. Lemma. *If $y_1, y_2 \in S_n$ are solutions of $(e * \alpha)$ such that $y_1 \circ y_2 = y_2 \circ y_1$, then the product $y_1 \circ y_2$ is also a solution of $(e * \alpha)$. If $y \in S_n$ is a solution of $(e * \alpha)$, then $y^{-1} \in S_n$ is also a solution of $(e * \alpha)$ and for all $i \in \mathbb{Z}$ and $k \geq 0$ we have*

$$\alpha^k \circ y^i = y^{e^k i} \circ \alpha^k.$$

Proof. Since $\alpha \circ y_1 \circ \alpha^{-1} = y_1^e$ and $\alpha \circ y_2 \circ \alpha^{-1} = y_2^e$ hold, the multiplicative property of the conjugation gives that

$$\alpha \circ y_1 \circ y_2 \circ \alpha^{-1} = (\alpha \circ y_1 \circ \alpha^{-1}) \circ (\alpha \circ y_2 \circ \alpha^{-1}) = y_1^e \circ y_2^e = (y_1 \circ y_2)^e.$$

If $y \in S_n$ is a solution of $(e * \alpha)$, then

$$\alpha \circ y^{-1} \circ \alpha^{-1} = (\alpha \circ y \circ \alpha^{-1})^{-1} = (y^e)^{-1} = (y^{-1})^e.$$

Since y^i is also a solution of $(e*\alpha)$, we have $\alpha \circ y^i \circ \alpha^{-1} = (y^i)^e$, whence $\alpha \circ y^i = y^{ei} \circ \alpha$ follows for all $i \geq 0$. For $k \geq 0$ we use an induction:

$$\alpha^{k+1} \circ y^i = \alpha \circ (\alpha^k \circ y^i) = \alpha \circ (y^{e^k i} \circ \alpha^k) = (\alpha \circ y^{e^k i}) \circ \alpha^k = (y^{e(e^k i)} \circ \alpha) \circ \alpha^k = y^{e^{k+1} i} \circ \alpha^{k+1} \square$$

2.5. Lemma. *If $y \in S_n$ is a solution of $(e * \alpha)$, then y and y^e are of the same type $\langle t_1, t_2, \ldots, t_n \rangle$, $y^{e^w - 1} = 1$ and for any cycle $(c_1, c_2, \ldots, c_r)$ of y the cycle length $r \geq 1$ is a divisor of $e^w - 1$ (i.e. $r \mid e^w - 1$), where $\mathrm{type}(\alpha) = \langle g_1, g_2, \ldots, g_n \rangle$ and*

$$w = \mathrm{ord}(\alpha) = \mathrm{lcm}\{a \mid 1 \leq a \leq n, g_a \neq 0\}$$

is the order of α. We also have $\gcd(r, e) = 1$ and $(c_1, c_{e+1}, c_{2e+1}, \ldots, c_{(r-1)e+1})$ is a cycle of y^e, where the indices $ie + 1$, $0 \leq i \leq r - 1$ are taken in $\{1, 2, \ldots, r\}$ modulo r. This cycle of y^e has the same elements as the original cycle and each cycle of y^e can be obtained by the above construction, starting from a uniquely determined cycle of y.

Proof. According to $(e*\alpha)$, the permutation y^e is the conjugate of y (by α), whence $\mathrm{type}(y) = \mathrm{type}(y^e)$ follows. The application of Lemma 2.4 gives that $\alpha^w \circ y = y^{e^w} \circ \alpha^w$. Now $\alpha^w = 1$ implies that $y^{e^w - 1} = 1$, whence we obtain that any cycle length $r \geq 1$ of y is a divisor of $e^w - 1$. Clearly, $\gcd(r, e) = 1$ is a consequence of $r \mid e^w - 1$. If $(c_1, c_2, \ldots, c_r)$ is a cycle of y, then $(c_1, c_{e+1}, c_{2e+1}, \ldots, c_{(r-1)e+1})$ is obviously a cycle of y^e of the same length r (notice that $c_{ie+1} \neq c_{je+1}$ follows from $r \nmid (j - i)e$ for all $1 \leq i < j \leq r - 1$). If $(c_1, y^e(c_1), \ldots, y^{(r-1)e}(c_1))$ is a cycle of y^e of length $r \geq 1$, then $y^{re}(c_1) = c_1$ and $s \mid re$, where $y^s(c_1) = c_1$ and $1 \leq s \leq n$ is the length of the y-cycle strating with c_1. Since $\gcd(s, e) = 1$, we obtain that $s \mid r$. The containment $\{c_1, y^e(c_1), \ldots, y^{(r-1)e}(c_1)\} \subseteq \{c_1, y(c_1), \ldots, y^{s-1}(c_1)\}$ implies that $r \leq s$, whence $r = s$ follows. Thus, the above cycle of y^e can be constructed by the given process starting from the cycle $(c_1, y(c_1), \ldots, y^{r-1}(c_1))$ of y. $\square$

2.6. Lemma. *Let $y \in S_n$ be a solution of $(e * \alpha)$ with $\mathrm{type}(y) = \langle t_1, t_2, \ldots, t_n \rangle$ and for a given $1 \leq r \leq n$ with $t_r \geq 1$ consider the base sets*

$$C_i^{(r)} \subseteq \{1, 2, \ldots, n\}, 1 \leq i \leq t_r$$

of all r-element cycles of y $\left(\left|C_i^{(r)}\right| = r \text{ for all } 1 \leq i \leq t_r\right)$. Then there exists a permutation γ of the index set $\{1, 2, \ldots, t_r\}$ such that

$$\alpha(C_i^{(r)}) = C_{\gamma(i)}^{(r)}.$$

Since γ is uniquely determined by α, it is natural to use the notation $\gamma = \alpha^{(r)}$. Now $t_r r \in F_1(\alpha)$ and if $\alpha^{(r)}$ has a cycle $(i_1, i_2, \ldots, i_d)$ of length $1 \leq d \leq t_r$, then $d \mid w = \text{ord}(\alpha)$ and $dr \in F_d(\alpha)$.

Proof. In view of Lemmas 2.2 and 2.5, any r-element cycle of y^e can be obtained as the α image of a unique r-element cycle of y. Since the base sets of the r-element cycles in y and in y^e coincide, we obtain that $\alpha(C_i^{(r)}) = C_{\gamma(i)}^{(r)}$ for some permutation γ of the indices. Now $H = C_1^{(r)} \cup C_2^{(r)} \cup \cdots \cup C_{t_r}^{(r)}$ is a fixed set of α, whence $t_r r = |H| \in F_1(\alpha)$ follows by Lemma 2.1. If $(i_1, i_2, \ldots, i_d)$ is a cycle of $\alpha^{(r)}$, then

$$\alpha(C_{i_1}^{(r)}) = C_{i_2}^{(r)}, \alpha(C_{i_2}^{(r)}) = C_{i_3}^{(r)}, \ldots, \alpha(C_{i_{d-1}}^{(r)}) = C_{i_d}^{(r)}, \alpha(C_{i_d}^{(r)}) = C_{i_1}^{(r)}.$$

Now $H(d) = C_{i_1}^{(r)} \cup C_{i_2}^{(r)} \cup \cdots \cup C_{i_d}^{(r)}$ is a fixed set of α and the above property of α (or $\alpha^{(r)}$) gives that

$$H(d) = D_1 \cup D_2 \cup \cdots \cup D_m,$$

where $D_1, D_2, \ldots, D_m$ are certain pairwise disjoint cycles of α such that $d \mid |D_j|$ and $|D_j| \mid w$ hold for all $1 \leq j \leq m$. Thus, $d \mid w$ and

$$dr = |H(d)| = |D_1| + |D_2| + \cdots + |D_m| \in F_d(\alpha)$$

follows by the repeated application of Lemma 2.1. $\square$

2.7. Lemma. Let $y \in S_n$ be a solution of $(e * \alpha)$ with $\text{type}(y) = \langle t_1, t_2, \ldots, t_n \rangle$. If $t_r \neq 0$ and the induced permutation $\alpha^{(r)}$ of the indices $\{1, 2, \ldots, t_r\}$ (see Lemma 2.6) has a cycle $(i_1, i_2, \ldots, i_d)$ of length $1 \leq d \leq t_r$ and $\gcd(e^d - 1, r) = 1$, then α also has a cycle of length d in $C_{i_1}^{(r)} \cup C_{i_2}^{(r)} \cup \cdots \cup C_{i_d}^{(r)}$.

Proof. Let $C_{i_1}^{(r)} = \{c_1, c_2, \ldots, c_r\}$ be the set of all elements in a cycle $(c_1, c_2, \ldots, c_r)$ of y (notice that $r \mid e^w - 1$ by Lemma 2.5). Since $c_1 \in C_{i_1}^{(r)}$ and

$$\alpha(C_{i_1}^{(r)}) = C_{i_2}^{(r)}, \alpha(C_{i_2}^{(r)}) = C_{i_3}^{(r)}, \ldots, \alpha(C_{i_{d-1}}^{(r)}) = C_{i_d}^{(r)}, \alpha(C_{i_d}^{(r)}) = C_{i_1}^{(r)},$$

the containment $\alpha^d(c_1) \in C_{i_1}^{(r)}$ holds, whence $\alpha^d(c_1) = y^s(c_1)$ follows for some $1 \leq s \leq r$. Now $\gcd(e^d - 1, r) = 1$ implies that $(e^d - 1)u + s = rv$ for some $u, v \in \mathbb{Z}$ and $y^u(c_1)$ is a fixed point of α^d. Indeed, the application of Lemma 2.4 gives that

$$\alpha^d(y^u(c_1)) = (\alpha^d \circ y^u)(c_1) = (y^{e^d u} \circ \alpha^d)(c_1) = y^{e^d u}(\alpha^d(c_1)) = y^{e^d u}(y^s(c_1)) =$$

$$y^{e^d u + s}(c_1) = y^{u + rv}(c_1) = y^u(c_1).$$

Thus, $(y^u(c_1), \alpha(y^u(c_1)), \ldots, \alpha^{d-1}(y^u(c_1)))$ is a d-element cycle of α. $\square$

2.8. Theorem. Let $r \geq 2$ be a divisor of the integer $n \geq 3$ such that $e^{\frac{n}{r}} - 1$ is divisible by r (i.e. $r \mid e^{\frac{n}{r}} - 1$). Then for any cyclic permutation $\alpha \in S_n$ of length n (say $\alpha = (1, 2, \ldots, n)$) equation $(e * \alpha)$ has a non-trivial solution $y \neq 1$ such that each cycle of y is of length r and $y^r = 1$. If $e = 2$, then $n = 6, 20, 21, 60$ are examples of such integers with $3 \mid 2^{\frac{6}{3}} - 1$, $5 \mid 2^{\frac{20}{5}} - 1$, $7 \mid 2^{\frac{21}{7}} - 1$ and $15 \mid 2^{\frac{60}{15}} - 1$. If $e = -2$, then $n = 55$ is an example of such integer with $11 \mid (-2)^{\frac{55}{11}} - 1$.

Proof. Take $q = n/r$ and define an n-element set P_n of ordered pairs and a function $\varepsilon : P_n \longrightarrow P_n$ as follows:

$$P_n = \{(i,j) \mid 1 \le i \le q \text{ and } 1 \le j \le r\},$$

$$\varepsilon(i,j) = \begin{cases} (i+1, ej) \text{ if } 1 \le i \le q-1 \text{ and } 1 \le j \le r \\ (1, ej+1) \text{ if } i = q \text{ and } 1 \le j \le r \end{cases},$$

where ej and $ej+1$ are taken in $\{1, 2, \ldots, r\}$ modulo r. It is straightforward to check that ε is injective (hence a permutation of P_n). Clearly, the definition of ε immediately gives that the length of a cycle in ε is a multiple of q. If $1 \le k \le q-1$ and $1 \le j \le r$, then $\varepsilon^k(1,j) = (1+k, e^k j)$ and $r \mid e^q - 1$ ensures that $\varepsilon^q(1,j) = (1, e^q j + 1) = (1, j+1)$. Thus,

$$\varepsilon^q(1,j) = (1, j+1), \varepsilon^{2q}(1,j) = (1, j+2), \ldots, \varepsilon^{(r-1)q}(1,j) = (1, j+r-1)$$

are distinct elements and $\varepsilon^{rq}(1,j) = (1, j+r) = (1,j)$ (in P_n). It follows that ε has exactly one cycle of length $n = rq$. Now define a permutation $y : P_n \longrightarrow P_n$ as follows:

$$y(i,j) = (i, j+1),$$

where $1 \le i \le q$, $1 \le j \le r$ and $j+1$ is taken in $\{1, 2, \ldots, r\}$ modulo r. The number of cycles in y is exactly q and each cycle of y is of the form

$$((i,1), (i,2), \ldots, (i,r)).$$

An easy calculation shows that $\varepsilon \circ y = y^e \circ \varepsilon$. If $1 \le i \le q-1$ and $1 \le j \le r$, then

$$\varepsilon(y(i,j)) = \varepsilon((i, j+1)) = (i+1, ej+e)$$

and

$$y^e(\varepsilon(i,j)) = y^e((i+1, ej)) = (i+1, ej+e).$$

If $i = q$ and $1 \le j \le r$, then

$$\varepsilon(y(q,j)) = \varepsilon((q, j+1)) = (1, ej+e+1)$$

and

$$y^e(\varepsilon(q,j)) = y^e((1, ej+1)) = (1, ej+1+e).$$

Thus, y is a required solution of $(e * \varepsilon)$. Finally, we deduce, that $(e * \alpha)$ has a similar solution for any permutation $\alpha \in S_n$ with $\text{type}(\alpha) = \text{type}(\varepsilon)$. $\square$

2.9. Corollary. *Let $\alpha \in S_n$ be a cyclic permutation of length n (say $\alpha = (1, 2, \ldots, n)$). If $\gcd(n, e^n - 1) = d \ne 1$, then $(e * \alpha)$ has a non-trivial solution $y \ne 1$ such that $y^d = 1$.*

Proof. If $\gcd(n, e^n - 1) = d$, then there is a common prime divisor $p \ge 2$ of n and $e^n - 1$. Now $n = n_1 p$ and

$$e^{\frac{n}{p}} - 1 = e^{n_1} - 1 = (e^{n_1 p} - 1) - e^{n_1}(e^{n_1(p-1)} - 1) = (e^n - 1) - e^{n_1}(e^{n_1(p-1)} - 1)$$

is divisible by p (i.e. $p \mid e^{\frac{n}{p}} - 1$) by Fermat's divisibility $p \mid e^{p-1} - 1$. The application of Theorem 2.8 gives the existence of a solution $y \ne 1$ of $(e * \alpha)$ such that $y^p = 1$. Clearly, $p \mid d$ implies that $y^d = 1$. $\square$

2.10. Corollary. *If $\alpha \in S_n$ is a permutation of type $\text{type}(\alpha) = \langle g_1, g_2, \ldots, g_n \rangle$ such that $g_a \ne 0$ and $\gcd(a, e^a - 1) = d \ne 1$ for some $2 \le a \le n$, then $(e * \alpha)$ has a non-trivial solution $y \ne 1$ such that $y^d = 1$.*

Proof. If $(i, \alpha(i), \ldots, \alpha^{a-1}(i))$ is an a-element cycle of α, then $\{1, 2, \ldots, n\} = H_1 \cup H_2$, where $H_1 = \{i, \alpha(i), \ldots, \alpha^{a-1}(i)\}$ and $H_2 = \{1, 2, \ldots, n\} \smallsetminus H_1$ are disjoint fixed sets of α. Now Corollary 2.9 ensures the existence of a solution $1_{H_1} \neq y_1 \in S_{H_1}$ (here $y_1 : H_1 \longrightarrow H_1$ is a permutation) of $(e * (\alpha \restriction H_1))$ such that $y_1^d = 1$, where $(\alpha \restriction H_1) : H_1 \longrightarrow H_1$ is the restriction of α to H_1. The application of Lemma 2.3 gives that $y_1 \sqcup y_2 \neq 1$ is a solution of $(e * \alpha)$ in S_n such that $(y_1 \sqcup y_2)^d = 1$, where $y_2 = 1$ is the identity permutation on H_2. $\square$

2.11. Theorem. *Let $p \geq 2$ be a prime divisor of n such that $p \mid e^{\frac{n}{p}} - 1$ and $\gcd(\frac{n}{p}, e^n - 1) = 1$. If $\alpha = (1, 2, \ldots, n) \in S_n$ is a cyclic permutation, then the only solutions of $(e * \alpha)$ are the powers $y, y^2, \ldots, y^{p-1}, y^p = 1$ of an arbitrary solution $1 \neq y \in S_n$. If $e = 2$, then $n = 20, 21$ are examples of such integers with $5 \mid 2^{\frac{20}{5}} - 1$, $\gcd(\frac{20}{5}, 2^{20} - 1) = 1$ and $7 \mid 2^{\frac{21}{7}} - 1$, $\gcd(\frac{21}{7}, 2^{21} - 1) = 1$. If $e = -2$, then $n = 55$ is an example with $11 \mid (-2)^{\frac{55}{11}} - 1$, $\gcd(\frac{55}{11}, 2^{55} - 1) = 1$.*

Proof. The application of Theorem 2.8 gives the existence of a non-trivial solution of $(e * \alpha)$. Fix an element $a \in \{1, 2, \ldots, n\}$ and let $1 \neq y \in S_n$ be an arbitrary solution of $(e * \alpha)$ with $\text{type}(y) = \langle t_1, t_2, \ldots, t_n \rangle$. Now y has at least one cycle of length $r \geq 2$ and Lemma 2.5 ensures that $r \mid e^n - 1$, where $n = \text{ord}(\alpha)$. Let $C_i^{(r)} \subseteq \{1, 2, \ldots, n\}$, $1 \leq i \leq t_r$ be the pairwise disjoint base sets of the r-element cycles of y. The type of α and Lemma 2.6 ensure that $t_r r \in F_1(\alpha) = \{0, n\} = \{0, p \cdot \frac{n}{p}\}$. Since $t_r r = p \cdot \frac{n}{p}$, $r \mid e^n - 1$ and $\gcd(\frac{n}{p}, e^n - 1) = 1$, we obtain that $r = p$ and $t_p = \frac{n}{p} = q$. Thus, $t_k = 0$ for each $1 \leq k \leq n$, $k \neq p$ and the powers $y, y^2, \ldots, y^{p-1}, y^p = 1$ are distinct solutions of $(e * \alpha)$.

If $1 \leq d \leq t_p = q$ is the length of a cycle $(i_1, i_2, \ldots, i_d)$ of the induced permutation $\alpha^{(p)}$, then Lemma 2.6 gives $dp \in F_d(\alpha) \subseteq F_1(\alpha) = \{0, p \cdot q\}$ and $d = q$. It follows that $\alpha^{(p)}$ has only one cycle of length $d = q$ and we can assume that $\alpha^{(p)} = (1, 2, \ldots, q)$ and $a \in C_1^{(p)}$ (hence $\alpha(C_j^{(p)}) = C_{j+1}^{(p)}$ for $1 \leq j \leq q - 1$ and $\alpha(C_q^{(p)}) = C_1^{(p)}$). The above cyclic property of $\alpha^{(p)}$ and $1 \leq q = n/p \leq n-1$ ensure that $a \neq \alpha^q(a) \in C_1^{(p)}$, whence $\alpha^q(a) = y^s(a)$ follows for some $1 \leq s \leq p-1$ (s depends on the choice of a). We claim that $y(\alpha^i(a)) = \alpha^{\overline{s}(i)q+i}(a)$ holds for all integers $0 \leq i \leq pq = n$, where $1 \leq \overline{s}(i) \leq p - 1$ denotes the multiplicative inverse (reciprocal) of $e^i s$ in the prime field $\mathbb{Z}_p$ (notice that $p \mid e^i s$ would contradict to $1 \leq s \leq p-1$ and $p \mid e^{\frac{n}{p}} - 1$).

First we use $\alpha^i \circ y^s = y^{e^i s} \circ \alpha^i$ (in Lemma 2.4) to get

$$\alpha^q(\alpha^i(a)) = \alpha^i(\alpha^q(a)) = \alpha^i(y^s(a)) = y^{e^i s}(\alpha^i(a))$$

and then we prove by induction, that $\alpha^{kq}(\alpha^i(a)) = y^{ke^i s}(\alpha^i(a))$ holds for all integers $k \geq 0$. Lemma 2.4 gives $\alpha^{kq} \circ y^{e^i s} = y^{e^{kq} e^i s} \circ \alpha^{kq}$ and $e^{kq} e^i s - e^i s = (e^{kq} - 1)e^i s$ is divisible by $e^q - 1$ and hence by p. Now $e^{kq} e^i s - e^i s = pv$ and the validity of the above equality for $k + 1$ can be derived as

$$\alpha^{(k+1)q}(\alpha^i(a)) = \alpha^{kq}(\alpha^q(\alpha^i(a))) = \alpha^{kq}(y^{e^i s}(\alpha^i(a))) =$$

$$y^{e^{kq} e^i s}(\alpha^{kq}(\alpha^i(a))) = y^{e^{kq} e^i s}(y^{ke^i s}(\alpha^i(a))) = y^{e^{kq} e^i s - e^i s}(y^{(k+1)e^i s}(\alpha^i(a))) =$$

$$y^{pv}(y^{(k+1)e^i s}(\alpha^i(a))) = y^{(k+1)e^i s}(\alpha^i(a)).$$

In view of $\overline{s}(i)e^i s = 1 + pu$, the substitution $k = \overline{s}(i)$ into $\alpha^{kq}(\alpha^i(a)) = y^{ke^i s}(\alpha^i(a))$ gives our claim

$$y(\alpha^i(a)) = y^{\overline{s}(i)e^i s}(\alpha^i(a)) = \alpha^{\overline{s}(i)q}(\alpha^i(a)) = \alpha^{\overline{s}(i)q+i}(a).$$

Since $\{\alpha^i(a) \mid 0 \leq i \leq n - 1\} = \{1, 2, \ldots, n\}$, the permutation y is completely determined by s. The fact that $1 \leq s \leq p - 1$ can be chosen in $p - 1$ different ways implies that the number of non-trivial solutions of $(e * \alpha)$ is at most $p - 1$. It follows that $y, y^2, \ldots, y^{p-1}, y^p = 1$ is the complete list of solutions. $\square$

2.12. Theorem. *Let $w = \mathrm{ord}(\alpha) = \mathrm{lcm}\{a \mid 1 \leq a \leq n, g_a \neq 0\}$ be the order of the permutation $\alpha \in S_n$ of $\mathrm{type}(\alpha) = \langle g_1, g_2, \ldots, g_n \rangle$ with $g_1 = 0$. Assume that for any choice of the integers $r \geq 2$ and $d \geq 2$ with $\gcd(e - 1, r) = 1$, $r \mid e^w - 1$, $d \mid w$ and $dr \in F_d(\alpha)$ we have $g_d = 0$ and $\gcd(e^d - 1, r) = 1$. If y is a solution of $(e * \alpha)$ such that $\gcd(e - 1, s) = 1$ for any cycle length $s \geq 2$ of y, then $y = 1$.*

Proof. Let $y \in S_n$ be a solution of $(e * \alpha)$ with $\mathrm{type}(y) = \langle t_1, t_2, \ldots, t_n \rangle$. Assume that $y \neq 1$, then y has at least one cycle of length $r \geq 2$. Now we have $\gcd(e-1, r) = 1$ and Lemma 2.5 ensures that $r \mid e^w - 1$. Let $C_i^{(r)} \subseteq \{1, 2, \ldots, n\}$, $1 \leq i \leq t_r$ be the pairwise disjoint base sets of the r-element cycles of y. In view of Lemma 2.6 we have $\alpha(C_i^{(r)}) = C_{\gamma(i)}^{(r)}$, $1 \leq i \leq t_r$, where $\gamma = \alpha^{(r)}$ is the induced permutation of the indices $\{1, 2, \ldots, t_r\}$. Consider an arbitrary cycle $(i_1, i_2, \ldots, i_d)$ of $\alpha^{(r)}$, then $1 \leq d \leq t_r$ and Lemma 2.6 gives $d \mid w$ and $dr \in F_d(\alpha)$. If $d \geq 2$, then we have $g_d = 0$ and $\gcd(e^d - 1, r) = 1$. If $d = 1$, then we also have $\gcd(e^d - 1, r) = 1$. Thus, the application of Lemma 2.7 gives that α also has a cycle of length d, in contradiction with $g_d = 0$. $\square$

2.13. Corollary. *Let $\alpha = (1, 2, \ldots, a) \circ (a + 1, a + 2, \ldots, a + b) \in S_n$ be a product of two cyclic permutations, where $2 \leq a < b \leq n = a + b$ are integers such that a is not a divisor of b. If $\gcd(u, e^u - 1) = 1$ for any choice of $u \in \{a, b, a + b\}$, then $(e * \alpha)$ has only the trivial solution $y = 1$. If $e = 2$, then $a = 10$ and $b = 15$ provide an example. If $e = -2$, then $a = 35$ and $b = 77$ provide an example.*

Proof. We use Theorem 2.12. Let $r \geq 2$ and $d \geq 2$ be integers such that $\gcd(e - 1, r) = 1$, $r \mid e^{\mathrm{lcm}(a,b)} - 1$, $d \mid \mathrm{lcm}(a, b)$ and

$$u = dr \in F_d(\alpha) \subseteq F_1(\alpha) = \{0, a, b, a + b\}.$$

Since $a < b$ and a is not a divisor of b, we obtain that $d \notin \{a, b\}$. It follows that $g_1 = g_d = 0$ in $\mathrm{type}(\alpha)$. Now $\gcd(e^d - 1, r) = 1$ is a consequence of $\gcd(e^{dr} - 1, dr) = \gcd(e^u - 1, u) = 1$. If y is a solution of $(e * \alpha)$ with $\mathrm{type}(y) = \langle t_1, t_2, \ldots, t_n \rangle$ and $s \geq 2$ is a cycle length of y, then $t_s s \in F_1(\alpha) = \{0, a, b, a + b\}$ by Lemma 2.6. In view of $\gcd(e - 1, a) = \gcd(e - 1, b) = \gcd(e - 1, a + b) = 1$, we obtain that $\gcd(e - 1, s) = 1$. Thus Theorem 2.12 ensures that $y = 1$. $\square$

For an integer $2 \leq v$ with $\gcd(v, e - 1) = 1$ let $q(e, v)$ denote the smallest prime divisor of $e^v - 1$ not dividing $e - 1$ (if there is no such prime, then take $q(e, v) = +\infty$). If v is odd, then $7 \leq q(2, v)$. Similarly, if v is not divisible by 2 and 3, then $23 \leq q(2, v)$. Indeed, $2 \nmid v$ and $3 \nmid v$ imply that $2, 3, 5, 7, 11, 13, 17, 19 \nmid 2^v - 1$. Notice that $q(2, 2) = 2^2 - 1$, $q(2, 3) = 2^3 - 1$, $q(2, 4) = 3$, $q(2, 5) = 2^5 - 1$, $q(2, 6) = 3$, $q(2, 7) = 2^7 - 1$, $q(2, 8) = 3$, $q(2, 9) = 7$, $q(2, 10) = 3$ and $q(2, 11) = 23 \neq 2^{11} - 1$ (clearly, $2^{11} - 1$ is not a Mersenne prime). We also note that $q(-2, 2) = +\infty$,

$q(-2,4) = 5$, $q(-2,5) = 11$, $q(-2,7) = 43$, $q(-2,8) = 5$, $q(-2,10) = 11$ and $q(-2,11) = 683$.

2.14. Theorem. *Let $w = \mathrm{ord}(\alpha) = \mathrm{lcm}\{a \mid 1 \leq a \leq n, g_a \neq 0\}$ be the order of the permutation $\alpha \in \mathrm{S}_n$ of type $\mathrm{type}(\alpha) = \langle g_1, g_2, \ldots, g_n \rangle$ such that $g_1 = 0$ and $\gcd(a, b) = 1$ for all $1 \leq a < b \leq n$ with $g_a \neq 0 \neq g_b$ (two different cycle lengths are relative primes). Assume that $1 \leq g_a \leq q(e, w) - 1$ and $\gcd(a, e^a - 1) = 1$ hold for all $1 \leq a \leq n$ with $g_a \neq 0$ (i.e. for all cycle lengths of α). If $y \in \mathrm{S}_n$ is a solution of $(e * \alpha)$, then $y^{e-1} = 1$ and $\alpha \circ y = y \circ \alpha$. On the other hand, if $y \in \mathrm{S}_n$ is a permutation with $y^{e-1} = 1$ and $\alpha \circ y = y \circ \alpha$, then y is a solution of $(e * \alpha)$.*

Proof. Let $y \in S_n$ be a solution of $(e * \alpha)$. Any cycle C of $y^{(e-1)^n}$ can be obtained from a uniquely determined cycle D of y (notice that $C \subseteq D$). If $s = |D|$ is the length of D, then $|C| = \frac{s}{d}$ with $d = \gcd((e-1)^n, s)$. Since $\gcd(e-1, \frac{s}{d}) = 1$, we can apply Theorem 2.12 on $y^{(e-1)^n}$. Let $r \geq 2$ and $d \geq 2$ be integers such that $\gcd(e-1, r) = 1$, $r \mid e^w - 1$, $d \mid w$ and $dr \in F_d(\alpha)$. Our conditions on the type of α ensure the existence of a unique integer $k \geq 1$ such that $1 \leq dk \leq n$ and $g_{dk} \neq 0$, whence $F_d(\alpha) = F_{dk}(\alpha) = \{0, dk, 2dk, \ldots, g_{dk}dk\}$ follows. Now we have $dr = jdk$ as well as $r = jk$ for some $1 \leq j \leq g_{dk}$. Since $r \mid e^w - 1$, we obtain that $j \mid e^w - 1$. Clearly, $\gcd(e-1, j) = 1$ and $2 \leq j \leq g_{dk} \leq q(e, w) - 1$ would contradict to the definition of $q(e, w)$. It follows that $j = 1$ and $g_{dr} = g_{dk} \neq 0$. Thus, $g_d = 0$ and $\gcd(e^{dr} - 1, dr) = 1$ are also consequences of our conditions on the type of α, whence $\gcd(e^d - 1, r) = 1$ follows. The application of Theorem 2.12 gives that $y^{(e-1)^n} = 1$. We also have $y^{e^w - 1} = 1$ by Lemma 2.5. Since $\gcd(a, e-1) = 1$ holds for all $1 \leq a \leq n$ with $g_a \neq 0$ (our assumption that $\gcd(a, e^a - 1) = 1$ is stronger) and $w = \mathrm{lcm}\{a \mid 1 \leq a \leq n, g_a \neq 0\}$, we obtain that $\gcd(w, e-1) = 1$. In view of

$$e^w - 1 = (e-1)(w + (e-1) + (e^2 - 1) + \cdots + (e^{w-1} - 1)),$$

$\gcd(e^w - 1, (e-1)^n) = e - 1$ can be derived, whence $(e^w - 1)u + (e-1)^n v = e - 1$ follows for some $u, v \in \mathbb{Z}$. As a consequence we have

$$y^{e-1} = y^{(e^w - 1)u + (e-1)^n v} = (y^{e^w - 1})^u \circ (y^{(e-1)^n})^v = 1.$$

Since $y^{e-1} = 1$ implies that $y^e = y$, equation $(e * \alpha)$ can be rewritten as $\alpha \circ y \circ \alpha^{-1} = y$. It follows that $\alpha \circ y = y \circ \alpha$. On the other hand, if $y \in S_n$ is a permutation with $y^{e-1} = 1$ and $\alpha \circ y = y \circ \alpha$, then we have $y^e = y$ and $\alpha \circ y \circ \alpha^{-1} = y = y^e$. Thus, y is a solution of $(e * \alpha)$. $\square$

2.15. Remarks. Theorem 2.14 reveals that under certain conditions, the solutions of $(e * \alpha)$ are exactly the solutions of $y^{e-1} = 1$ in the centralizer of α. If $a = p^t$ is a prime power and $p \nmid e - 1$, then it is straightforward to check that

$$e = e^{p^0} \equiv e^{p^1} \equiv \cdots \equiv e^{p^{t-1}} \equiv e^{p^t} \bmod(p),$$

whence $\gcd(a, e^a - 1) = 1$ follows. As $\gcd(w, e-1)$ appears in the above proof of 2.14, we add the following simple observation. If $\alpha \in \mathrm{S}_n$ is arbitrary and $\gcd(w, e-1) = d \neq 1$, then $y = \alpha^{\frac{w}{d}} \neq 1$ is a non-trivial solution of $(e * \alpha)$ such that $y^d = 1$ and $\alpha \circ y = y \circ \alpha$.

REFERENCES

[CHS] S. Chowla, I.N. Herstein, W.R. Scott: *The solutions of $x^d = 1$ in symmetric groups,*
Norske Vid. Selsk. (Trindheim) 25, 29-31 (1952)
[E] A. Evangelidou: *The Solution of Length Five Equations Over Groups,*
Communications in Algebra, 35:6, 1914-1948 (2007)
[FM] H.Finkelstein, K.I. Mandelberg: *On Solutions of "Equations in Symmetric Groups",*
Journal of Combinatorial Theory, Series A, 25, 142-152 (1978)
[GR] M. Gerstenhaber, O. S. Rothaus: *The solution of sets of equations in groups,*
Proc. Nat. Acad. Sci. U.S.A. 48, 1531-1533 (1962)
[IR] I. M. Isaacs, G. R. Robinson: *On a Theorem of Frobenius: Solutions of $x^n = 1$ in Finite Groups,*
American Mathematical Monthly, Vol. 99, No. 4, pp. 352-354 (Apr., 1992)
[I] I. Martin Isaacs: *Finite Group Theory,*
American Mathematical Society, 2008
[L] R. C. Lyndon: *Equations in groups,*
Boletim Da Sociedade Brasileira de Matemática, 11(1), 79–102 (1980)
[MW] L. Moser, M. Wyman: *On solutions of $x^d = 1$ in symmetric groups,*
Canad. J. Math. 7, 159-168 (1955)

INSTITUTE OF MATHEMATICS, UNIVERSITY OF MISKOLC,, 3515 MISKOLC-EGYETEMVÁROS, HUNGARY
Email address: szilvia.homolya@uni-miskolc.hu

INSTITUTE OF MATHEMATICS, UNIVERSITY OF MISKOLC,, 3515 MISKOLC-EGYETEMVÁROS, HUNGARY
Email address: matjeno@uni-miskolc.hu