On the enumeration of skew-morphisms of cyclic groups

István Kovács

University of Primorska, Koper, Slovenia

Roman Nedela

Matej Bel University, Banská Bystrica, Slovakia

GEMS'09, Tále, Slovakia

Definition and examples

After Jajcay and Širáň, we say that a permutation $\sigma : G \to G$ is a **skew-morphism** of a group G with a **power function** $\pi\colon G \to \{0, 1, \ldots, \text{ord}(\sigma) - 1\}$ if

- $\sigma(1_G) = 1_G$,
- $\sigma(xy) = \sigma(x)\sigma^{\pi(x)}(y)$ for all $x, y \in G$.

EXM: every automorphism of G is a SM of G with $\pi(x) = 1$ for all $x \in \mathbb{Z}_n$.

EXM: $G = \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$.

The permutation

$$\sigma(x) = \begin{cases} x & \text{if } x \text{ is even} \\ x \oplus 2 & \text{if } x \text{ is odd} \end{cases}$$

is a SM of $\mathbb{Z}_6$ with power function

$$\pi(x) = \begin{cases} 1 & \text{if } x \text{ is even} \\ 2 & \text{if } x \text{ is odd} \end{cases}$$

$$\sigma(x \oplus y) = \sigma(x) \oplus \sigma^{\pm}(y).$$

Motivation

• A group G admits a regular Cayley map iff G has a skew-morphism σ with an orbit T such that $\langle T\rangle = G$, and $T = T^{-1}$ (Jajcay and Širáň, 2002)

• A classification of regular embeddings of $K_{n,n}$ is equivalent to find the set of SM's σ of $\mathbb{Z}_n$ s. t. ord(σ) $\mid n$, and $\pi(x) = -\sigma^{-x}(-1)$ for all $x \in \mathbb{Z}_n$ (Feng, Kwak, Nedela).

(Du, Jones, Kwak, Kwon, Nedela, Škoviera, Zlatoš 2002-2007)

Skew product group

Prop. (i) Let σ be a SM of G, G_L is the left regular repr. of G. Then $P = \langle G_L, \sigma \rangle$ is a permutation group in Sym(G) such that $P_{1_G} = \langle \sigma \rangle$.

(ii) Let $P \leq$ Sym(G) such that $G_L \leq P$, and P_{1_G} is a cyclic group. Then any generator of P_{1_G} is a SM of G.

After Conder, Jajcay and Tucker, we call $\langle G_L, \sigma \rangle$ the **skew product group** over G induced by σ.

Action on a generating orbit

Prop. If σ is a SM of G, and T is an orbit of σ, $\langle T \rangle = G$, then σ acts regularly on T.

In particular, for the orbit T in the above proposition, $\mathrm{ord}(T) = |T|$.

S-rings induced by SM's

S-rings over G are certain subalgebras of the group algebra $\mathbb{Q}G$.

Some notations: for $S \subset G$, denote $\underline{S} = \sum_{x \in G} a_x x \in \mathbb{Q}G$ such that $a_x = 1$ if $x \in S$ and $x = 0$ if $x \notin S$ (such elements are called simple quantities). The transpose of an element $\eta = \sum_{x \in G} a_x x$ in $\mathbb{Q}G$ is the element $\eta^t = \sum_{x \in G} a_x x^{-1}$.

An **S-ring** over G is a subalgebra $\mathcal{A}$ of $\mathbb{Q}G$ which satisfies:

- $\mathcal{A}$ has a basis of elements $\underline{T}_1, \ldots, \underline{T}_r$ for subsets T_i of G,
- $T_1 = \{1_G\}$, $T_i \cap T_j = \emptyset$ for all i, j, and $T_1 \cup \cdots \cup T_r = G$,
- for every $i \in \{1, \ldots, r\}$ there exists $j \in \{1, \ldots, r\}$ such that $\underline{T}_i^t = \underline{T}_j$.

T_i: basic sets, r: the rank.

S-rings arise from permutation groups as follows: Let P be of a rank r permutation group in Sym(G). Suppose $G_L \leq P$, and let P_{1_G} be the stabilizer of 1_G in P. Denote by $T_{1_G} = \{1_G\}, T_2 \ldots, T_r$ the the orbits of P_{1_G}.

Then $T_1, \ldots, T_r$ are the basic sets of a rank r S-ring over G (Schur, 1933) – also called the transitivity module of G induced by P_{1_G}.

Every SM σ of G induces an S-ring over G, we denote this by $\mathcal{A}_\sigma$.

S-rings over cyclic groups have been developed much (Klin, Pöschel, Muzychuk, Leung, Ma, Man, Evdokimov and Ponomarenko).

The following related question seems to be natural.

Question. What are the S-rings over cyclic groups which are induced by skew-morphisms?

Theorem. Let $n = p_1^{e_1} \cdots p_r^{e_r}$, n is odd, $(p_i, p_j - 1) = 1$ for all i, j. Then for every SM σ of $\mathbb{Z}_n$ there exists an automorphism α of $\mathbb{Z}_n$ s. t. $\mathcal{A}_\sigma = \mathcal{A}_\alpha, \alpha \in \mathrm{Aut}(\mathbb{Z}_n)$.

SM's with trivial radicals

Motivated by Evdokimov and Ponomarenko, we define the **radical** of a SM σ of $\mathbb{Z}_n$ as

$$\mathrm{rad}(\sigma) = \{x \in \mathbb{Z}_n \mid T + x = T\},$$

where T is an orbit of $\sigma, \langle T \rangle = \mathbb{Z}_n$.

$\mathrm{rad}(\sigma) \leq \mathbb{Z}_n$ (does not depend on the orbit T).

In fact, $\mathrm{rad}(\sigma)$ is the same as $\mathrm{rad}(\mathcal{A}_\sigma)$.

Prop. If σ is a SM of $\mathbb{Z}_n$. If $\mathrm{rad}(\sigma) = 1$, then σ is in $\mathrm{Aut}(\mathbb{Z}_n)$.

This follows directly from a structure theorem of S-rings over cyclic groups with trivial radical (Evdokimov and Ponomarenko, 2002).

As corollaries, we obtain that

- $(\mathrm{ord}(\sigma), n) = 1 \Rightarrow \sigma \in \mathrm{Aut}(\mathbb{Z}_n)$,
- $\mathrm{ord}(\sigma) \mid n\varphi(n)$.

SM's of prime order

Prop. Let σ be a SM of $\mathbb{Z}_n$, ord$(\sigma) = p$, p is a prime, σ is not in Aut$(\mathbb{Z}_n)$, and let π be the power function of σ. Then

- $n = pm$, $d = (m, p-1) > 1$, and
- there are $a, b \in \mathbb{Z}_p$, $a \neq 0$, $b \neq 1$, $b^d = 1$, such that

$$\sigma(xm + y) = \Big(x + a(1 + b + \cdots + b^{y-1})\Big)m + y,\ x \in \mathbb{Z}_p,\ y \in \mathbb{Z}_m.$$

and $\pi(z) = b^z$, $z \in \mathbb{Z}_n$.

EXM: Let $n = pq$, $(n, \varphi(n)) = 1$, σ be a SM of $\mathbb{Z}_{pq}$.

Suppose that rad$(\sigma) = \langle q \rangle$. Then ord$(\sigma) = pl$, and the $\langle q \rangle$-cosets form a block system of $G = \langle 1_L, \sigma \rangle$. The kernel of G permuting the blocks is the group $K = \langle q_L, \sigma^l \rangle$. Thus the stabilizer of 0 in $K\mathbb{Z}_L$ is $\langle \sigma^l \rangle$, so σ^l is a SM of order p, σ^l is not in Aut$(\mathbb{Z}_n)$, a contradiction to the previous Prop.

Therefore rad$(\sigma) = 1$, σ is in Aut$(\mathbb{Z}_{pq})$.

Letting $\mathbb{Z}_{pq} = \mathbb{Z}_p \times \mathbb{Z}_q$, Aut$(\mathbb{Z}_{pq})$ = Aut$(\mathbb{Z}_p) \times$ Aut$(\mathbb{Z}_q)$, we have $\sigma = \sigma_1\sigma_2$, $\sigma_1 \in$ Aut$(\mathbb{Z}_p)$ and $\sigma_2 \in$ Aut$(\mathbb{Z}_q)$.

Decomposition Theorem

Let $n = n_1 n_2$, $(n_1, n_2) = 1$, $\mathbb{Z}_n = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$. Let σ_1 be a SM of $\mathbb{Z}_{n_1}$. The the mapping

$$\widehat{\sigma}_1 \colon (x_1, x_2) \mapsto (\sigma_1(x_1), x_2)$$

is a SM of $\mathbb{Z}_n$, this we call the **extension** of σ_1 to $\mathbb{Z}_n$.

Extension $\widehat{\sigma}_2$ is defined analogously.

We say that two natural numbers n_1 and n_2 are **disjoint** if

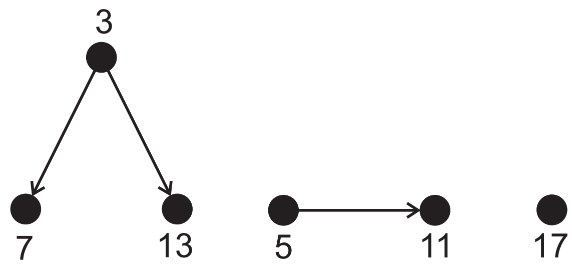
$$(n_1 \varphi(n_1), n_2 \varphi(n_2)) = 1.$$

Note that, if n_1 and n_2 are disjoint, then $\widehat{\sigma}_1 \widehat{\sigma}_2$ is a SM of $\mathbb{Z}_n$.

Theorem. Let $n = n_1 n_2$, n_1 and n_2 are disjoint. Then every SM of $\mathbb{Z}_n$ is of the form $\widehat{\sigma}_1\,\widehat{\sigma}_2$, where σ_i is a SM of $\mathbb{Z}_{n_i}$.

We can interpret the theorem in terms of a digraph (which also occurs in the formula of Jones, 2007, enumerating regular embeddings of $K_{n,n}$.)

EXM: $n = 3 \times 5 \times 7 \times 11 \times 13 \times 17$.



.

$\varphi_s(n) = \varphi_s(3 \times 7 \times 13) \times \varphi_s(5 \times 11) \times \varphi_s(17)$

$n = p^m$, p is a prime

Lem. Let σ be a SM of $\mathbb{Z}_{p^n}$, p is a prime. If $\mathrm{ord}(\sigma) = p^v$, then σ^p is also a SM of $\mathbb{Z}_{p^n}$.

Therefore, if G is a skew product p-group, then every element in G_0 is a SM. Enumeration in this case is reduced to finding the poset of skew product p-groups.

Note that, if $p = 2$, then all SM's are found this way.

Lem. Let σ be a SM of $\mathbb{Z}_{p^n}$ of order $p^v d$, $d > 1$, $d \mid (p-1)$ $(p > 2)$. Then
(1) the Sylow-p-subgroup P of $\langle \tau, \sigma \rangle$ is a skew product p-group.
(2) $P \triangleleft \langle \tau, \sigma \rangle$, hence σ^{p^v} acts by conjugation on P as an automorphism of order d.

Note that,

- Skew product p-groups are metacyclic if $p > 2$ (Huppert, 1953).

- A nonsplit metacyclic p-group is also a p-group (Menegazzo, 1993), hence the group P in the above lemma must be a split metacyclic p-group.

- The automorphism groups of split metacyclic p-groups are explicitely described by Bidwell and Curran, 2006.

We have the following strategy of enumerating SM's of $\mathbb{Z}_{p^n}$:

- Determine the poset of skew product p-groups.

- If $p > 2$, then determine those groups which are split meta-cyclic p-groups.

- If $p > 2$ and P is a split metacyclic skew product p-group, then describe a correspondence between skew product groups G with $P = \mathrm{Syl}_p(G)$ and $\mathrm{Aut}(P)$.

- Derive formula for $\varphi_s(p^n)$.

Skew product p-groups, $p > 2$

Let α be the automorphism of $\mathbb{Z}_{p^n}$ defined by $\alpha(x) = (p+1) \odot x$.

For $i, j \in \{0, 1, \ldots, p^{n-1}-1\}$, define the permutations $\beta_j, \sigma_{i,j}$ in Sym($\mathbb{Z}_{p^n}$) as $\beta_j(0) = 0$, and if $x \neq 0$,

$\beta_j(x) = 1 \oplus (p+1)^j \oplus (p+1)^{2j} \oplus \cdots \oplus (p+1)^{(x-1)j}$, and

$\sigma_{i,j} = \beta_j{}^{-1} \alpha^i \beta_j,\ i \in \{0, 1, \ldots, p^{n-1} - 1\}$.

Lem. Every permutation $\sigma_{i,j}$ is a SM of $\mathbb{Z}_{p^n}$.

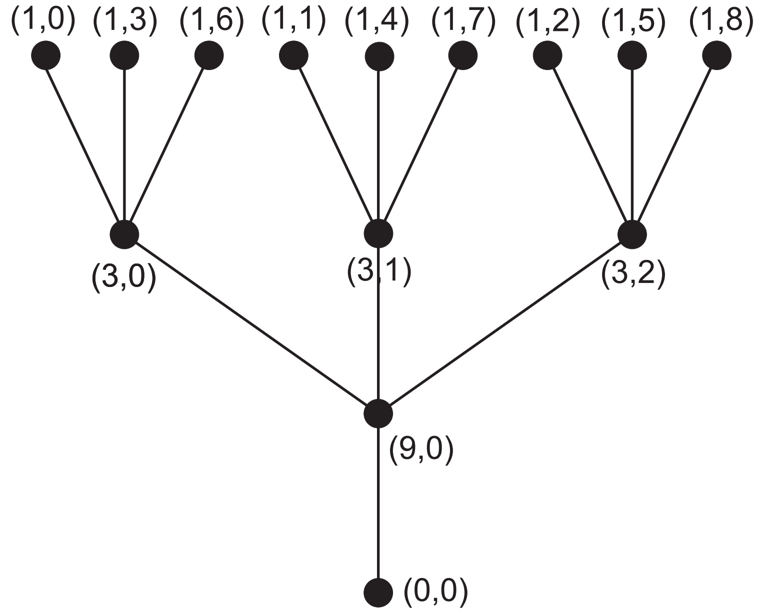
Prop. If σ is a SM of $\mathbb{Z}_n$ of p-power order and $p > 2$, then $\sigma = \sigma_{i,j}$ for some $i, j \in \mathbb{Z}_{p^n}$.

Proof First, let $\mathrm{ord}(\sigma) = p^{n-1}$. Let $G = \langle 1_L, \sigma \rangle$. There exists a cyclic subgroup $N \triangleleft G$, G/N is cyclic. Thus $|G/N| = \max\{\mathrm{ord}(N1_L), \mathrm{ord}(N\sigma)\} = \max\{\mathrm{ord}(N1_L), p^{n-1}\} = p^{n-1}$, as $\langle p^{n-1} \rangle \leq \mathbf{Z}(G) \cap N$. Also, $|N| = p^n$, hence N is a regular normal subgroup. Then $N^\beta = \mathbb{Z}_L$, $\sigma^\beta = \alpha^i$. From these $\beta = \beta_j$, $\sigma = \sigma_{i,j}$.

The proof is completed by showing that every skew product p-group of order less then p^{2n-1} is properly contained in a skew product p-group.

Prop. $\sigma_{i,j} = \sigma_{i',j'}$ iff $i = i'$ and $j \equiv j' \pmod{p^{n-2}/(p^{n-i}, i)}$.

EXM: The poset of Skew product 3-groups over $\mathbb{Z}_{81}$, label (i, j) identifies group $\langle 1_L, \sigma_{i,j} \rangle$:



.

The number of SM's of $\mathbb{Z}_{p^n}$ of p-power order is $\frac{p^{2n-2}+p}{p+1}$.

Thank you!