Skew-morphisms of cyclic p-groups

István Kovács

University of Primorska, Slovenia

istvan.kovacs@upr.si

Joint work with Roman Nedela

UNIVERSITÀ DEL LITORALE
UNIVERZA NA PRIMORSKEM

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA IZOBRAŽEVANJE, ZNANOST IN ŠPORT

Naložba v vašo prihodnost
OPERACIJO DELNO FINANCIRA EVROPSKA UNIJA
Evropski socialni sklad

SCDO, Queenstown
February 14-19 , 2016

Skew-morphism

Definition (Jajcay–Širáň)

A permutation φ of a finite group G is a **skew-morphism** if

1. $\varphi(1_G) = 1_G$;
2. $\forall x, y \in G : \varphi(xy) = \varphi(x)\varphi^{\pi(x)}(y)$ for a function $\pi : G \to \{1, \ldots, k\}$, where k is the order of φ.

The above function π is called the **power function** of φ.

We denote by $\mathrm{Skew}(G)$ the set of all skew-morphisms of G.

Regular Cayley maps

- Let $X \subset G$ with $1_G \notin X$, $X = X^{-1}$ and $\langle X \rangle = G$. The **Cayley graph** $\mathrm{Cay}(G, X)$ has vertex set G, and edges $\{y, yx\}$, $y \in G$ and $x \in X$.
- Let $X = \{x_1, \ldots, x_k\}$ and $p = (x_1, \ldots, x_k)$. The **Cayley map** $\mathrm{CM}(G, X, p)$ is the embedding of $\mathrm{Cay}(G, X)$ in an oriantable surface with local orientation around the vertex y is given as

$$(yx_1, \ldots, yx_k).$$

- A permutation γ of $V(\mathrm{Cay}(G, X))$ is an **automorphism** of $\mathrm{CM}(G, X, p)$ if

$$\forall x, y \in G : x \sim y \iff \gamma(x) \sim \gamma(y);$$

$$\forall y \in G \forall x \in X : \gamma(yp(x)) = \gamma(y)p(\gamma(x)).$$

- $\mathrm{CM}(G, X, p)$ is **regular** if its automorphism group acts regularly on the darts.

Regular Cayley maps

Theorem (Jajcay–Širáň)

The Cayley map $CM(G, X, p)$ is regular if and only if there exsits a skew-morphism $\varphi \in \mathrm{Skew}(G)$ such that $\varphi(x) = p(x)$ for all $x \in X$.

Note that not every skew-morphism is related with a Cayley map.

The skew-product group

- For $g \in G$, the **left translation** L_g is the permutation of G acting as $L_g(x) = gx, x \in G$.
- Left translations form a regular group isomorphic to G, notation: $L(G)$.
- The **skew-product group** of $\varphi \in \mathrm{Skew}(G)$ is the group $\langle L(G), \varphi \rangle$.
- $\langle L(G), \varphi \rangle = L(G) \langle \varphi \rangle$.
- If ψ is any permutation of G with $\psi(1_G) = 1_G$, then

$$\psi \in \mathrm{Skew}(G) \iff |\langle L(G), \psi \rangle| = |G| \cdot |\psi|.$$

Skew-morphisms and factorizations of groups

- A group G has a **complementary factorization** if $G = AB$ where A and B are subgroups and $A \cap B = 1$.
- If the above subgroup B is cyclic and b is a generator, then there is a unique permutation f of A defined by

$$\forall a \in A : baB = f(a)B.$$

- The above permutation $f \in \mathrm{Skew}(A)$.
- Every skew-morphism arises in this way through the natural factoriaztion of the skew-product group.

More on this relation can be found in:

M. Conder, R. Jajcay, T. Tucker. Cyclic complements and skew-morphisms of groups, to apper in J. Algebra.

Skew-morphisms of cyclic groups

In this rest of the talk we turn to skew-morphisms of cyclic groups.

The skew-morphisms are known in special cases:

- Skew-morphisms arising from Cayley maps (Conder–Tucker).
- Skew-morphisms arising from complementary factorizations $G = AB$, where A and B are cyclic groups of the same order switched by an involution in $\mathrm{Aut}(G)$ (Du, Feng, Jones, Kwak, Nedela, Škoviera).
- Computational results (Yuan–Wang–Kwak, Conder).
- Special orders: p, p^2 and pq for primes $p \neq q$. (K–Nedela, Conder–Jajcay–Tucker).
- Coset-preserving skew-morphisms (Bachratý–Jajcay).

Skew-morphism of cyclic p-groups, p is an odd prime

From now on p is an odd prime and e is a positive integer.

Some more notation:

- $\mathbb{Z}_n = \{0, \ldots, n-1\}$ is the additivie group modulo n;
- $t : x \mapsto x + 1$;
- a : the automorphims of $\mathbb{Z}_{p^e}$ acting as $x \mapsto (p+1)x$;
- b : any automorphism of $\mathbb{Z}_{p^e}$ of order $p - 1$;
- s : any skew-morphism of $\mathbb{Z}_{p^e}$.

On the order of a skew-morphism

Theorem (Conder–Jajcay–Tucker)

If $\varphi \in \mathrm{Skew}(G)$ *then its order* $|\varphi| \leq |G| - 1$.

Proposition (K–Nedela; Conder–Jajcay–Tucker)

If $\varphi \in \mathrm{Skew}(\mathbb{Z}_n)$ *then its order* $|\varphi|$ *divides* $n\phi(n)$, *where* ϕ *is the Euler function.*

Corollary

If $\varphi \in \mathrm{Skew}(\mathbb{Z}_{p^e})$ *then its order* $|\varphi|$ *divides* $\phi(p^e) = p^{e-1}(p-1)$.

Reduction to skew product p-groups

- Let $s \in \mathrm{Skew}(\mathbb{Z}_{p^e})$ of order $p^c d$, $c \in \{0, 1, \ldots, e-1\}$ and $d \mid (p-1)$.
- Let P be the Sylow p-subgroup of $\langle t, s \rangle$ with $t \in P$.
- Then $P = \langle t, s^d \rangle$, $s^d \in \mathrm{Skew}(\mathbb{Z}_{p^e})$, and by Sylow Theorems,

$$\langle t, s \rangle = P \rtimes \langle s^{p^c} \rangle.$$

- By Huppert Theorem, P is metacyclic.
- s^{p^c} acts on P as an automorphism of order d.

  If $d > 1$, then P is a split metacyclic group, and we find s^{p^c} using the description of $\mathrm{Aut}(P)$ due to Bidwell and Curran.

The skew-morpshisms $s_{i,j}$

Definition

For $i, j \in \{0, \dots, p^{e-1} - 1\}$, let

$$s_{i,j} = b_j^{-1} a^i b_j,$$

where b_j is the permutation of $\mathbb{Z}_{p^e}$ such that $b_j(0) = 0$ and

$$b_j(x) = 1 + (p+1)^j + \cdots + (p+1)^{j(x-1)} \text{ if } x > 0.$$

Proposition

Every $s_{i,j}$ is a skew-morphism of $\mathbb{Z}_{p^e}$. Furthermore, if $e \geq 2$ then

$$s_{i,j} = s_{i',j'} \iff i = i' \text{ and } j \equiv j' \pmod{p^{e-2}/\gcd(i, p^{e-2})}.$$

.

The skew-morpshisms $s_{i,j}$

The proof of the first part of the proposition explains the choice of b_j:

Proposition

Every $s_{i,j}$ is a skew-morphism of $\mathbb{Z}_{p^e}$.

Proof.

We use the following property: if s is a skew-morphism of $\mathbb{Z}_{p^e}$ of p-power order, then s^p is a skew-morphism too.

Let $i = p^c i'$ with $\gcd(i', p) = 1$. Then $s_{i,j} = s_{i',j}^{p^c}$, and

$$|\langle t, s_{i',j} \rangle| = |\langle t^{b_j}, s_{i',j}^{b_j} \rangle| = |\langle ta^j, a^{i'} \rangle| = p^e \cdot |s_{i',j}|,$$

hence $s_{i',j}$ is a skew-morphism. □

The skew-morphisms of $\mathbb{Z}_{p^e}$ of p-power order

Theorem

The skew-morphisms of $\mathbb{Z}_{p^e}$ of p-power order are exactly the skew-morphisms $s_{i,j}$.

The key step in the proof was the following lemma.

Lemma

If s is any skew-morphism of $\mathbb{Z}_{p^e}$ of p-power order, then $\langle t, s\rangle$ is isomorphic to some $\langle t, s_{i,j}\rangle$.

In the proof of the lemma we used a result of King about unique presentations of split metacyclic groups.

The skew-morpshisms $s_{i,j,k,l}$

Definition

Let
$$s_{i,j,k,l} = b_j^{-1} a^i b^k b_l b_j$$
where the integers i, j, k, l satisfy the following conditions

(C0) $i, l \in \{0, \ldots, p^{e-1} - 1\}$, $k \in \{0, \ldots, p - 2\}$, $j \in \{0, \ldots, p^{e-2-c} - 1\}$, where $p^c = \gcd(i, p^{e-2})$;

(C1) if $i = 0$ or $k = 0$, then $l = 0$;

(C2) if $i \neq 0$ and $k \neq 0$, then $p^c \mid j$ and $p^{\max\{c,e-2-c\}} \mid l$.

A 4-tuple (i, j, k, l) of integers satisfying (C0)–(C2) is called **admissible**.

The skew-morpshisms of $\mathbb{Z}_{p^e}$ whose order is not a p-power

Theorem

The skew-morphisms of $\mathbb{Z}_{p^e}$ whose order is not a p-power are exactly the skew-morphisms $s_{i,j,k,l}$ with $k \neq 0$.

Enumeration

Proposition

Every skew-morphism $s_{i,j,k,l}$ is uniquelly determined by the admissible 4-tuple (i,j,k,l).

Theorem

The number of skew-morphisms of $\mathbb{Z}_{p^e}$ is eqal to

$$\frac{(p-1)(p^{2e-1}-p^{2e-2}+2)}{p+1}.$$

$$|\operatorname{Aut}(\mathbb{Z}_{p^e})| = (p-1)p^{e-1}.$$

$$|\operatorname{Skew}(\mathbb{Z}_{p^2})| = (p-1)(p^2-2p+2).$$