Cayley maps and skew morphisms

5th Theme Area
Symmetries of Surfaces, Maps and Dessins
BIRS 2017

September 25, 2017

Skew-Morphisms

Definition

A *skew-morphism* of a group G is a permutation φ of G preserving the identity and satisfying the property

$$\varphi(gh) = \varphi(g)\varphi^{\pi(g)}(h)$$

for all $g, h \in G$ and a function $\pi : G \to \mathbb{Z}_{|\varphi|}$, called the *power function* of G.

Skew-Morphisms

Definition

A *skew-morphism* of a group G is a permutation φ of G preserving the identity and satisfying the property

$$\varphi(gh) = \varphi(g)\varphi^{\pi(g)}(h)$$

for all $g, h \in G$ and a function $\pi : G \to \mathbb{Z}_{|\varphi|}$, called the *power function* of G.

- skew-morphisms were originally introduced for the study of regular Cayley maps

Skew-Morphisms

Definition

A *skew-morphism* of a group G is a permutation φ of G preserving the identity and satisfying the property

$$\varphi(gh) = \varphi(g)\varphi^{\pi(g)}(h)$$

for all $g, h \in G$ and a function $\pi : G \to \mathbb{Z}_{|\varphi|}$, called the *power function* of G.

- skew-morphisms were originally introduced for the study of regular Cayley maps
- they have since proved central in the theory of cyclic group extensions

Orientable Maps

- an **orientable map** $\mathcal{M}$ is a 2-cell embedding of a graph in an orientable surface

Orientable Maps

- an **orientable map** $\mathcal{M}$ is a 2-cell embedding of a graph in an orientable surface
- an **orientation-preserving map automorphism** of a map $\mathcal{M}$ is a permutation of its darts that preserves the orientation, adjacency, and faces

(Orientably) Regular Maps

Definition

An orientable map $\mathcal{M}$ is called **(orientably) regular** if any pair of arcs admits the existence of an orientation preserving automorphism of $\mathcal{M}$ that maps the first arc to the second.

(Orientably) Regular Maps

Definition

An orientable map $\mathcal{M}$ is called **(orientably) regular** if any pair of arcs admits the existence of an orientation preserving automorphism of $\mathcal{M}$ that maps the first arc to the second.

An orientable map $\mathcal{M}$ is regular if and only if

$$|Aut\mathcal{M}| = |D(\mathcal{M})|$$

Cayley Maps

Definition

A **Cayley map** $CM(G, X, p)$ is an embedding of a connected Cayley graph, $C(G, X)$, that has the same local orientation p at each vertex.

Cayley Maps

Definition

A **Cayley map** $CM(G, X, p)$ is an embedding of a connected Cayley graph, $C(G, X)$, that has the same local orientation p at each vertex.

Equivalently, a Cayley map is a drawing of a Cayley graph on a surface such that the outgoing darts are ordered the same way around each vertex; the local successor of the dart (g, x) is the dart $(g, p(x))$.

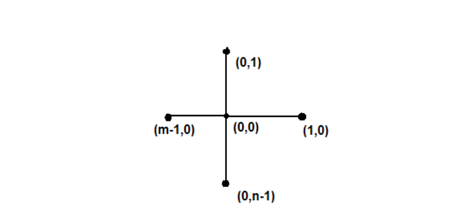


Figure : $CM(\mathbb{Z}_m \times \mathbb{Z}_n, ((0,1),(1,0),(0,n-1),(m-1,0)))$

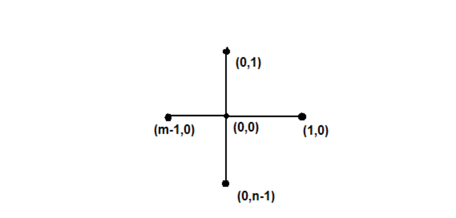
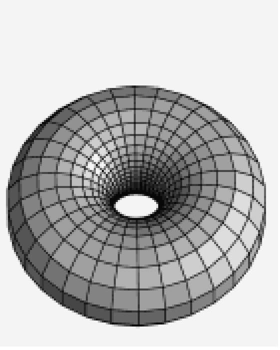


Figure : $CM(\mathbb{Z}_m \times \mathbb{Z}_n, ((0,1),(1,0),(0,n-1),(m-1,0)))$



Why are Cayley maps interesting?

- all the left multiplications of the underlying group G induce map automorphisms of the Cayley map
$\Longrightarrow |Aut(CM(G,X,p))| \geq |G|$

Why are Cayley maps interesting?

- all the left multiplications of the underlying group G induce map automorphisms of the Cayley map $\Longrightarrow |Aut(CM(G,X,p))| \geq |G|$
- $\Longrightarrow$ Cayley maps are *'almost'* regular from the beginning

Why are Cayley maps interesting?

- all the left multiplications of the underlying group G induce map automorphisms of the Cayley map
$\Longrightarrow |Aut(CM(G,X,p))| \geq |G|$
- $\Longrightarrow$ Cayley maps are *'almost'* regular from the beginning
- many of the well-known families of orientably regular maps turn out to be Cayley maps
(e.g., orientably regular emebddings of K_n, orientably regular embeddings of graphs of prime order)

Why are Cayley maps interesting?

- all the left multiplications of the underlying group G induce map automorphisms of the Cayley map
  $\Longrightarrow |Aut(CM(G, X, p))| \geq |G|$
- $\Longrightarrow$ Cayley maps are *'almost'* regular from the beginning
- many of the well-known families of orientably regular maps turn out to be Cayley maps
  (e.g., orientably regular emebddings of K_n, orientably regular embeddings of graphs of prime order)
- four of the five Platonic solids are Cayley maps

Why are Cayley maps interesting?

- all the left multiplications of the underlying group G induce map automorphisms of the Cayley map
$\Longrightarrow |Aut(CM(G,X,p))| \geq |G|$
- $\Longrightarrow$ Cayley maps are *'almost'* regular from the beginning
- many of the well-known families of orientably regular maps turn out to be Cayley maps
(e.g., orientably regular emebddings of K_n, orientably regular embeddings of graphs of prime order)
- four of the five Platonic solids are Cayley maps
- all orientably regular maps are factors of regular Cayley maps

How important are Cayley maps?

- we do not know what is the proportion of Cayley maps among orientably regular maps

How important are Cayley maps?

- we do not know what is the proportion of Cayley maps among orientably regular maps
- we do not know what is the proportion of Cayley graphs among the vertex-transitive graphs

Orientably Regular Cayley Maps

- $|Aut(CM(G, X, p))| \geq |G|$

Orientably Regular Cayley Maps

- $|Aut(CM(G, X, p))| \geq |G|$
- $|\mathcal{D}(CM(G, X, p))| = |G| \cdot |X|$

Orientably Regular Cayley Maps

- $|Aut(CM(G, X, p))| \geq |G|$
- $|\mathcal{D}(CM(G, X, p))| = |G| \cdot |X|$
- $\implies$ in order for a Cayley map to be regular, the stabilizer of any vertex in $Aut(CM(G, X, p))$ must be of size $|X|$

Orientably Regular Cayley Maps

- $|Aut(CM(G, X, p))| \geq |G|$
- $|\mathcal{D}(CM(G, X, p))| = |G| \cdot |X|$
- $\implies$ in order for a Cayley map to be regular, the stabilizer of any vertex in $Aut(CM(G, X, p))$ must be of size $|X|$
- $\implies$ since the stabilizers of orientable maps are cyclic, in order for a Cayley map to be regular, there must exist an automorphism that maps $(1, x)$ to $(1, p(x))$

Skew-Morphisms

Definition

A **skew-morphism** of a group G is a permutation φ of G preserving the identity and satisfying the property

$$\varphi(gh) = \varphi(g)\varphi^{\pi(g)}(h)$$

for all $g, h \in G$ and a function $\pi : G \to \mathbb{Z}_{|\varphi|}$, called the *power function* of G.

Theorem

Let $\mathcal{M} = CM(G, X, p)$ be any Cayley map. Then $\mathcal{M}$ is regular iff there exists a skew-morphism φ of G satisfying the property $\varphi(x) = p(x)$ for all $x \in X$.

In order to construct **all** regular Cayley maps for a given group G:

In order to construct **all** regular Cayley maps for a given group G:

- **construct all skew-morphisms of** G

In order to construct **all** regular Cayley maps for a given group G:

- **construct all skew-morphisms of G**
- every regular Cayley map on G is of the form

$$CM(G, \{x, \varphi(x), \ldots, \varphi^{n-1}(x)\}, (x, \varphi(x), \ldots, \varphi^{n-1}(x))),$$

where φ is a skew-morphisms with a **generating orbit** $\{x, \varphi(x), \ldots, \varphi^{n-1}(x)\}$ that is **closed under inverses**

In order to construct **all** regular Cayley maps for a given group G:

- **construct all skew-morphisms of G**
- every regular Cayley map on G is of the form

$$CM(G, \{x, \varphi(x), \ldots, \varphi^{n-1}(x)\}, (x, \varphi(x), \ldots, \varphi^{n-1}(x))),$$

  where φ is a skew-morphisms with a **generating orbit** $\{x, \varphi(x), \ldots, \varphi^{n-1}(x)\}$ that is **closed under inverses**
- $\Longrightarrow$ regular Cayley maps on G correspond to orbits of skew-morphisms of G that generate G and are closed under inverses

In order to construct **all** regular Cayley maps for a given group G:

- **construct all skew-morphisms of G**
- every regular Cayley map on G is of the form

$$CM(G, \{x, \varphi(x), \ldots, \varphi^{n-1}(x)\}, (x, \varphi(x), \ldots, \varphi^{n-1}(x))),$$

  where φ is a skew-morphisms with a **generating orbit** $\{x, \varphi(x), \ldots, \varphi^{n-1}(x)\}$ that is **closed under inverses**
- $\Longrightarrow$ regular Cayley maps on G correspond to orbits of skew-morphisms of G that generate G and are closed under inverses
- each skew-morphism of G gives rise to a regular or a half-regular Cayley map on a non-trivial subgroup of G

Algebraic Properties of Skew-Morphisms

Lemma

Let φ be a skew-morphism of a group G and let π be the power function of φ. Then the following holds :

1. *the set* $Ker\varphi = \{g \in G \mid \pi(g) = 1\}$ *is a subgroup of* G*;*
2. $\pi(g) = \pi(h)$ *if and only if* g *and* h *belong to the same right coset of the subgroup* $Ker\varphi$ *in* G*.*

Algebraic Properties of Skew-Morphisms

Lemma

Let φ be a skew-morphism of a group G and let π be the power function of φ. Then the following holds :

1. *the set* $Ker\varphi = \{g \in G \mid \pi(g) = 1\}$ *is a subgroup of* G*;*
2. $\pi(g) = \pi(h)$ *if and only if* g *and* h *belong to the same right coset of the subgroup* $Ker\varphi$ *in* G*.*

Lemma

If A is a finite abelian group and φ is a skew-morphism of A, then

1. φ *preserves* $Ker\,\pi$ *setwise;*
2. *the restriction of* φ *to* $Ker\,\pi$ *is a group automorphism.*

The Structure of the Auto Group of a Cayley Map

The automorphism group of a(ny) Cayley map $CM(G, X, p)$ is a complementary product of the subgroup of automorphisms induced by G_L and the cyclic group generated by the automorphism induced by the skew-morphism of $CM(G, X, p)$:

$$Aut(CM(G, X, p)) \cong G_L \cdot \langle \varphi \rangle, \qquad G_L \cap \langle \varphi \rangle = \langle 1_G \rangle$$

Cyclic Extensions from Skew-Morphisms

Let G be a group, and φ be a(ny) skew-morphism of G with power function π, and let

$$s(i,b) = \sum_{j=0}^{i-1} \pi(\varphi^j(b)).$$

Cyclic Extensions from Skew-Morphisms

Let G be a group, and φ be a(ny) skew-morphism of G with power function π, and let

$$s(i, b) = \sum_{j=0}^{i-1} \pi(\varphi^j(b)).$$

Define a multiplication $*$ on $G \times \langle \varphi \rangle$ as follows:

$$(a, \varphi^i) * (b, \varphi^j) = (a\varphi^i(b), \varphi^{s(i,b)+j}),$$

for all $a, b \in G$ and all $i, j \in \mathbb{Z}_{|\varphi|}$.

Cyclic Extensions from Skew-Morphisms

Let G be a group, and φ be a(ny) skew-morphism of G with power function π, and let

$$s(i,b)=\sum_{j=0}^{i-1}\pi(\varphi^j(b)).$$

Define a multiplication $*$ on $G\times\langle\varphi\rangle$ as follows:

$$(a,\varphi^i)*(b,\varphi^j)=(a\varphi^i(b),\varphi^{s(i,b)+j}),$$

for all $a,b\in G$ and all $i,j\in\mathbb{Z}_{|\varphi|}$.

Theorem

Let G be a group and φ be a skew-morphism of G of finite order m and power function π. Then $A=(G\times\langle\varphi\rangle,*)$ is a group and $G\times\langle\varphi\rangle$ is a complementary factorization of A.

Skew-Morphisms from Cyclic Extensions

Let $G = A\langle\rho\rangle$, $A \cap \langle\rho\rangle = \langle 1_G \rangle$ (a complementary factorization).

Skew-Morphisms from Cyclic Extensions

Let $G = A \langle \rho \rangle$, $A \cap \langle \rho \rangle = \langle 1_G \rangle$ (a complementary factorization).

For every $a \in G$,

$$\rho a = a' \rho^i,$$

for some unique $a' \in A$ and some unique nonnegative integer i less than the order of ρ.

Skew-Morphisms from Cyclic Extensions

Let $G = A\langle\rho\rangle$, $A \cap \langle\rho\rangle = \langle 1_G \rangle$ (a complementary factorization).

For every $a \in G$,

$$\rho a = a' \rho^i,$$

for some unique $a' \in A$ and some unique nonnegative integer i less than the order of ρ.

Define $\varphi(a) = a'$ and $\pi(a) = i$. Then for any a, b in A,

$$\varphi(ab) = \varphi(a)\varphi^{\pi(a)}(b).$$

Skew-Morphisms from Cyclic Extensions

Let $G = A\langle\rho\rangle$, $A \cap \langle\rho\rangle = \langle 1_G \rangle$ (a complementary factorization).

For every $a \in G$,

$$\rho a = a' \rho^i,$$

for some unique $a' \in A$ and some unique nonnegative integer i less than the order of ρ.

Define $\varphi(a) = a'$ and $\pi(a) = i$. Then for any a, b in A,

$$\varphi(ab) = \varphi(a)\varphi^{\pi(a)}(b).$$

Already observed in the 1930's (e.g., Oystein Ore, 1938).

Complementary Cyclic Extensions

Theorem

If G is any finite group with a complementary subgroup factorisation $G = AY$ with Y cyclic, then for any generator y of Y, the order of the skew morphism φ of A is the index in Y of its core in G, or equivalently, the smallest index in Y of a normal subgroup of G.

Complementary Cyclic Extensions

Theorem

If G is any finite group with a complementary subgroup factorisation $G = AY$ with Y cyclic, then for any generator y of Y, the order of the skew morphism φ of A is the index in Y of its core in G, or equivalently, the smallest index in Y of a normal subgroup of G.

Moreover, in this case the quotient $\overline{G} = G/\mathrm{Core}_G(Y)$ is the skew product group associated with the skew morphism φ, with complementary subgroup factorisation $\overline{G} = \overline{A}\,\overline{Y}$ where $\overline{A} = AY/Y \cong A/(A \cap Y) \cong A$ and $\overline{Y} = Y/\mathrm{Core}_G(Y)$.

Some Group Theory

Theorem (Lucchini)

If P is a transitive permutation group of degree $n > 1$ with cyclic point-stabilizers, then $|P| \leq n(n-1)$.

Theorem (Herzog and Kaplan)

Let A be a non-trivial finite group of order n with a cyclic subgroup $\langle x \rangle$ satisfying the property $|x| \geq \sqrt{n}$. Then $\langle x \rangle$ contains a non-trivial normal subgroup of A.

Precise Orbits of Group Automorphisms

An orbit of a group-automorphism φ of G whose length is equal to the order of φ (as a permutation of the set of elements of G) is called a **precise orbit**.

Precise Orbits of Group Automorphisms

An orbit of a group-automorphism φ of G whose length is equal to the order of φ (as a permutation of the set of elements of G) is called a **precise orbit**.

Theorem (Khoroshevskij)

1. *The order of every automorphism of a finite group H is less than $|H|$.*

Precise Orbits of Group Automorphisms

An orbit of a group-automorphism φ of G whose length is equal to the order of φ (as a permutation of the set of elements of G) is called a **precise orbit**.

Theorem (Khoroshevskij)

1. *The order of every automorphism of a finite group H is less than $|H|$.*
2. *All group automorphisms of finite nilpotent groups and of finite groups that do not contain a non-trivial normal solvable subgroup possess a precise orbit.*

Precise Orbits of Group Automorphisms

An orbit of a group-automorphism φ of G whose length is equal to the order of φ (as a permutation of the set of elements of G) is called a **precise orbit**.

Theorem (Khoroshevskij)

1. *The order of every automorphism of a finite group H is less than $|H|$.*
2. *All group automorphisms of finite nilpotent groups and of finite groups that do not contain a non-trivial normal solvable subgroup possess a precise orbit.*
3. *If the order of a group automorphism φ of a finite group is relatively prime to the order of the group, then φ possesses a precise orbit.*

Orders of Skew-Morphisms

Every skew-morphism that gives rise to a regular Cayley map possesses a precise orbit.

Orders of Skew-Morphisms

Every skew-morphism that gives rise to a regular Cayley map possesses a precise orbit.

Theorem

If φ is a skew morphism of a finite group H, then the order of φ is less than $|H|$.

Orders of Skew-Morphisms

Every skew-morphism that gives rise to a regular Cayley map possesses a precise orbit.

Theorem

If φ is a skew morphism of a finite group H, then the order of φ is less than $|H|$.

Corollary

Every skew morphism of a non-trivial finite group has non-trivial kernel.

Orders of Skew-Morphisms

Every skew-morphism that gives rise to a regular Cayley map possesses a precise orbit.

Theorem

If φ is a skew morphism of a finite group H, then the order of φ is less than $|H|$.

Corollary

Every skew morphism of a non-trivial finite group has non-trivial kernel.

Corollary

Every skew morphism of a cyclic group of prime order is an automorphism.

Kernels of Skew-Morphisms

Theorem

If A is a finite abelian group of order greater than 2, then the kernel of every skew morphism of A has order greater than 2.

Kernels of Skew-Morphisms

Theorem

If A is a finite abelian group of order greater than 2, then the kernel of every skew morphism of A has order greater than 2.

Theorem

Let A be a finite abelian group of order greater than 2. If K is the kernel of any skew morphism of A, then every prime divisor of $|K|$ is larger than every prime that divides $|A|$ but not $|K|$.
In particular if q is the largest prime divisor of $|A|$, then the order of the kernel of every skew morphism of A is divisible by q when q is odd, or by 4 when $q = 2$.

Kernels of Skew-Morphisms

Theorem

If A is a finite abelian group of order greater than 2, then the kernel of every skew morphism of A has order greater than 2.

Theorem

Let A be a finite abelian group of order greater than 2. If K is the kernel of any skew morphism of A, then every prime divisor of $|K|$ is larger than every prime that divides $|A|$ but not $|K|$.
In particular if q is the largest prime divisor of $|A|$, then the order of the kernel of every skew morphism of A is divisible by q when q is odd, or by 4 when $q = 2$.

Corollary

Every skew morphism of an elementary abelian 2-group is an automorphism.

Further Results

Theorem

Let φ be a skew morphism of C_n. Then the order m of φ divides $n\phi(n)$. Moreover, if $gcd(m, n) = 1$ or $gcd(\phi(n), n) = 1$, then φ is an automorphism of C_n.

Further Results

Theorem

Let φ be a skew morphism of C_n. Then the order m of φ divides $n\phi(n)$. Moreover, if $gcd(m, n) = 1$ or $gcd(\phi(n), n) = 1$, then φ is an automorphism of C_n.

Theorem

Let A be any finite abelian group. Then every skew morphism of A is an automorphism of A if and only if A is is cyclic of order n where $n = 4$ or $\gcd(n, \phi(n)) = 1$, or A is an elementary abelian 2-group.

Further Results

Theorem

Let φ be a skew morphism of C_n. Then the order m of φ divides $n\phi(n)$. Moreover, if $gcd(m,n) = 1$ or $gcd(\phi(n), n) = 1$, then φ is an automorphism of C_n.

Theorem

Let A be any finite abelian group. Then every skew morphism of A is an automorphism of A if and only if A is is cyclic of order n where $n = 4$ or $\gcd(n, \phi(n)) = 1$, or A is an elementary abelian 2-group.

Classification and enumeration of the skew-morphisms of the cyclic groups C_{p^2} and C_{pq}, $C_p \times C_p$ and finite simple groups.

A Generalization and An Open Problem:

Definition

Let $G = A \cdot K$ be a complementary factorization. Then G is a **skew-product** of A and K if for each pair $a \in A$ and $h \in K$ there exists an $a' \in A$ and i such that

$$ah = h^i a'.$$

A Generalization and An Open Problem:

Definition

Let $G = A \cdot K$ be a complementary factorization. Then G is a **skew-product** of A and K if for each pair $a \in A$ and $h \in K$ there exists an $a' \in A$ and i such that

$$ah = h^i a'.$$

Conjecture: The set of all skew-morphisms of a finite group A is a subgroup of $\mathbb{S}_A$ if and only if all the skew-morphisms of A are group automorphisms of A.