Skew morphisms of groups

SYGN IV, Rogla, June 2014

Marston Conder
University of Auckland

m.conder@auckland.ac.nz

Maps

A map is an embedding of a connected graph or multigraph into a surface, breaking it into simply connected faces.

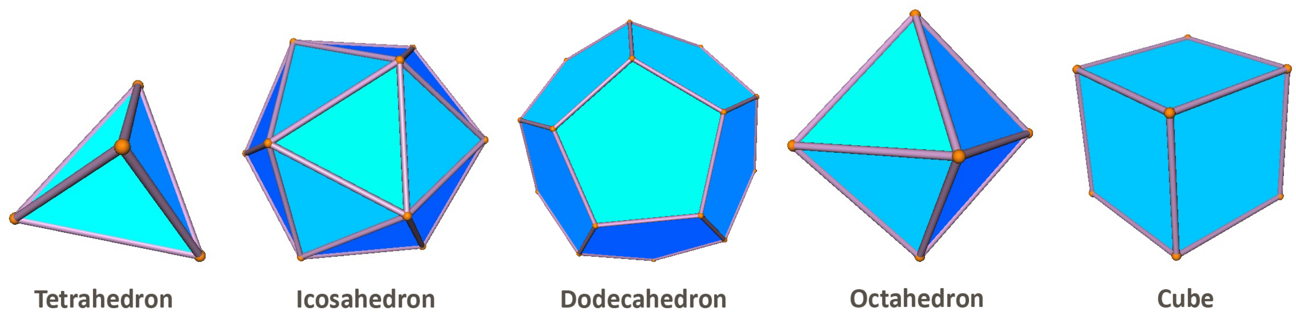
Except in weird cases, an automorphism of a map is a bijection (on vertices, on edges and on faces) preserving incidence, and connectedness implies that every automorphism is uniquely determined by its effect on any incident vertex-edge-face triple (v, e, f) ... called a flag.

Orientably-regular maps

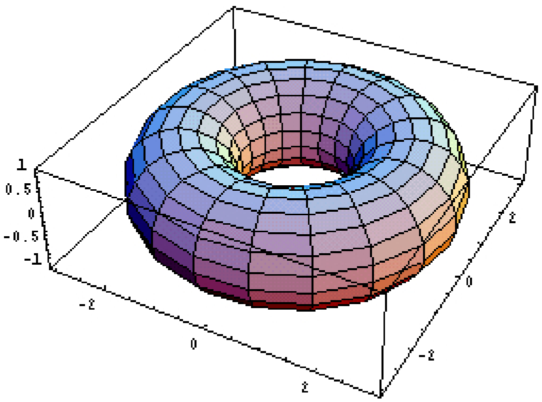
A map M is regular if its automorphism group is transitive (and hence regular) on the flags of M.

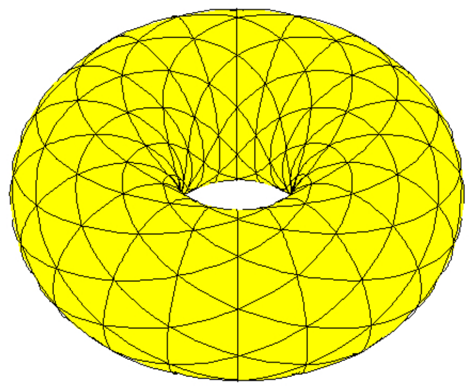
A little more loosely, a map M on an orientable surface is orientably-regular if the group of its orientation-preserving automorphisms is transitive (and hence regular) on the arcs (incident vertex-edge pairs) of M.

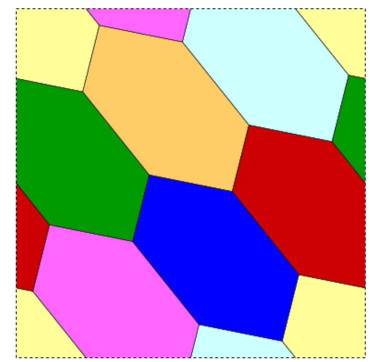
The Platonic solids give rise to regular maps on the sphere:



There are infinitely many orientably-regular maps on the torus. Some are fully regular, while others are chiral:







There are also (finitely many) examples on every orientable surface of genus $g > 1$, and on non-orientable surfaces of genus p for infinitely many $p > 2$.

Regular Cayley maps

Suppose M is an orientably-regular map, and the group G of orientation-preserving automorphisms of M has a subgroup A that acts regularly (i.e. sharply transitively) on vertices.

Then the underlying graph of M a Cayley graph for A, and M is called a regular Cayley map for A.

In this case, G has a complementary factorisation $G = AY$, where Y is the stabiliser of any vertex v, and $A \cap Y = 1$.

Moreover, the map M can be defined by taking a Cayley graph Cay(A, X) for A and prescribing the rotation of edges at the vertex v by assigning an order on the generating set X consistent with the effect of a generator y of Y.

Regular Cayley maps (cont.)

Indeed, let y be a generator of the stabiliser Y of the vertex v.

Then since $G = AY$ with $A \cap Y = 1$, we know that for any $a \in A$, there exist a unique element $a' \in A$ and a unique power y^j of y such that $ya = a'y^j$.

Defining $\varphi(a) = a'$ and $\pi(a) = j$, we have

$$yab = a'y^j b = \varphi(a)y^{\pi(a)}b = \varphi(a)\varphi^{\pi(a)}(b)y^k \quad \text{for some } k$$

and therefore $\varphi(ab) = \varphi(a)\varphi^{\pi(a)}(b)$ for all $a, b \in A$.

This makes φ look like an isomorphism, but 'with a twist'. It's called a skew morphism [Jajcay & Širáň (Bled, 1999)].

Definition of skew morphism

A skew morphism of a group A is a bijection $\varphi\colon A \to A$ with the property that φ fixes the identity element of A and

$$\varphi(ab) = \varphi(a)\varphi^{\pi(a)}(b) \quad \text{for all } a, b \in A$$

where the integer $\pi(a)$ depends only on a. The associated function $\pi\colon A \to \mathbb{Z}$ is called the power function of φ.

Note that if $\pi(a) = 1$ for all a, then φ is an automorphism. More generally, the set $\{a \in A \mid \pi(a) = 1\}$ is the kernel of φ.

Also note that if φ has finite order m, then π may be viewed as a function from A to $\mathbb{Z}_m$.

Examples

- C_6, cyclic group of order 6, generated by x

The permutation $\varphi = (x, x^3, x^5)$ fixing all other elements is a skew morphism with kernel $K = \langle x^2 \rangle$ of index 2 in C_6, and power function π taking value 1 on K and value 2 on Kx

- $D_3 = \langle\, u, v \mid u^2 = v^3 = (uv)^2 = 1 \,\rangle$, dihedral of order 6

The permutation $\varphi = (u, v, v^{-1}, uv)$ fixing 1 and uv^{-1} is a skew morphism with kernel $K = \langle uv \rangle$ of index 3 in D_3, and power function π taking values 1, 2 and 3 on K, Ku and Kv.

Note: The second of these two examples shows that the kernel is not always normal in the group!

Elementary properties of skew morphisms

Let φ be a skew morphism of A, with power function π. Then

(a) $\varphi^j(ab) = \varphi^j(a)\varphi^{\sigma(j,a)}(b)$ where $\sigma(j,a) = \sum_{0 \le i < j} \pi(\varphi^i(a))$

(b) the kernel $K = \ker\varphi$ is a subgroup of A

(c) $\pi(a) = \pi(b)$ if and only if $Ka = Kb$

(d) the set $\text{Fix}(\varphi) = \{a \in A \mid \varphi(a) = a\}$ is a subgroup of A

(e) the intersection $\ker\varphi \cap \text{Fix}(\varphi)$ is a normal subgroup of A

(f) if A is finite, and φ has order m, then

$$\pi(ab) \equiv \sum_{0 \le i < \pi(a)} \pi(\varphi^i(b)) \equiv \sigma(\pi(a), b) \mod m \quad \forall a, b \in A.$$

Computations

Computations using MAGMA show that

- C_2 has just one skew morphism (the identity autom)
- C_3 has two skew morphisms (the two automorphisms)
- C_4 has two skew morphisms (the two automorphisms)
- V_4 has six skew morphisms – all automorphisms
- C_5 has four skew morphisms – all automorphisms
- C_6 has four skew morphisms – two of which are automs
- D_3 has 12 skew morphisms – six of which are automs

Up to group order 12, all non-identity skew morphisms have non-trivial kernel.

Generalisation of Horosevskii's theorem

Until recently, attempts to prove the kernel of every non-trivial skew morphism is non-trivial foundered on a lack of theory about the orders of skew morphisms.

Theorem [MC]: The order of every skew morphism of a finite group A is at most $|A|$.

This generalises a 1974 theorem of Horosevskii, which says the same thing for automorphisms. It is easy to prove when the skew morphism comes from a regular Cayley map, since in that case the skew morphism has a cycle/orbit X which generates A, and hence its order is $|X| < |A|$. For arbitrary skew morphisms, however, something else was needed.

The skew product

Let $\varphi\colon A \to A$ be a skew morphism of a finite group A.

Consider A as a subgroup of Sym(A), in its action on A by left multiplication, and let Y be the cyclic group of Sym(A) generated by the permutation y induced on A by φ. Then

$$(ya)b = y(ab) = \varphi(ab) = \varphi(a)\varphi^{\pi(a)}(b) = \varphi(a)y^{\pi(a)}(b) \ \forall b \in A$$

so $ya = \varphi(a)y^{\pi(a)}$ $\forall a \in A$, and so $YA \subseteq AY$. Then finiteness gives $AY = YA$, so $G = AY$ is a subgroup of Sym(A), which we call a skew product (of A by Y, or of A by φ).

Conversely, if G is any group with a complementary factorisation $G = AY$ with Y cyclic, then the rule $ya = \varphi(a)y^{\pi(a)}$ gives a skew morphism φ of A, of order $|Y : \mathrm{Core}_G(Y)|$.

Digression

Consider the group PSL(2, 11). This has a subgroup of index 11 isomorphic to A_5. In fact PSL(2, 11) has a complementary factorisation as AY where $A \cong A_5$ and $Y \cong C_{11}$.

This gives to a skew morphism φ of A_5, of order 11, with kernel K of index 10 in A_5.

In particular, the associated power function takes all possible values in $\{1, 2, \ldots, 10\} = \mathbb{Z}_{11}^*$.

Proof of theorem (generalising Horosevskii)

Let $\varphi: A \to A$ be any skew morphism of the finite group A, and let $G = AY$ be the skew product associated with φ. Note that the core of Y in G is trivial.

Now let P be the transitive permutation group induced by G on right cosets of Y, by right multiplication. The degree of P is $|G\!:\!Y| = |A|$, and since $\mathrm{Core}_G(Y)|$ is trivial, $P \cong G$.

By a theorem of Lucchini (1998) on transitive permutation groups with cyclic point-stabilisers, $|P| \leq |A|(|A|-1)$. Hence we have $|A||Y| = |AY| = |G| = |P| \leq |A|(|A|-1)$, and this gives $|Y| \leq |A|-1 < |A|$, so the order of φ is at most $|A|$. $\square$

And as a consequence, we have ...

Theorem [MC]: Every skew morphism of a non-trivial finite group has non-trivial kernel.

Proof. Let φ be a skew morphism of the finite group A, with kernel K and power function $\pi : A \to \mathbb{Z}_m$, where m is the order of φ. By earlier theory, the number of distinct values taken by π is equal to the index $|A:K|$, so $|A:K| \leq m$. But also we now know that $m < |A|$, and so $|A:K| \leq m < |A|$, which implies $|K| > 1$.

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

Improved computations

- The 'non-trivial kernel' theorem gives an inductive method for computing skew morphisms of groups of larger order
- This can be further improved, by using the fact that every skew morphism of a finite abelian group preserves its kernel
  [Easy theorem, using lengths of orbits]
- We now know all skew morphisms of
  - all cyclic groups of order < 60
  - all abelian groups of order ≤ 32
  - all finite groups of order < 24.

Note: All 'map' skew morphisms of cyclic groups have been completely determined [MC & Tom Tucker]

Skew morphisms of abelian groups

[Joint work with Robert Jajcay and Tom Tucker]

The ‘non-trivial kernel’ theorem is helpful, but also can be extended even further for abelian groups:

Lemma: Let φ be a skew morphism of the finite abelian group A, with power function π, and let N be any non-trivial subgroup of $K = \ker \varphi$ preserved by φ. Also let m be the order of φ, let e be the exponent of N.

If b is any element of A for which $\bar{b} = Nb$ lies in the kernel of the skew morphism φ^* of the quotient group $\overline{A} = A/N$ induced by φ, then $e\pi(b) - e$ is divisible by m. In particular, if $\gcd(e, m) = 1$ then $\pi(b) \equiv 1 \bmod m$, so $b \in K$.

Equivalently, if $K \neq A$ then $\gcd(e, m) \neq 1$.

Additional theorems for abelian groups

[extending & refining theorems of Kovacs & Nedela (2011)]

- If φ is a skew morphism of the finite abelian group A, then $|\ker\varphi|$ is divisible by the largest prime divisor of $|A|$

- If φ is a skew morphism of a finite abelian p-group, then φ is an automorphism, or the order of φ is divisible by p

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

- If φ is a skew morphism of the cyclic group C_n, then its order m divides $n\phi(n)$; moreover, if $\gcd(m,n) = 1$ or $\gcd(\phi(n),n) = 1$ then φ is an automorphism.

More examples (abelian groups)

- Cyclic groups: If $n = 2m$ with $m > 2$, or $n = p^e$ where p is an odd prime and $e > 1$, then C_n has skew morphisms that are not automorphisms

- If p and q are primes with $p < q$, and φ is a skew morphism of $A = C_{pq}$ with kernel K, then either φ is an automorphism, or $p \mid (q-1)$ and $K \cong C_q$ and φ acts trivially on K and A/K

- All skew morphisms of C_{pq} and C_{p^2} are known [IK & RN]

- All skew morphisms of $C_p \times C_p$ are known [IK & RN]

Also (for later):

- $C_2 \times C_4$ and $C_4 \times C_4$ have skew morphisms that are not automorphisms.

General question: **When does a group have skew morphisms that are not automorphisms?**

Some groups do: e.g. C_6 and D_3 and A_5, but some don't, e.g. C_4 and $(C_2)^n$.

Kovács and Nedela (2011) used Schur rings to determine exactly which cyclic groups C_n have this property.

Lemma [Tom Tucker]: If the group A has a 'non-auto' skew morphism, then so does $A \times B$ for every group B

Proof. Given a skew morphism φ of A with kernel K, define $\theta\colon A \times B \to A \times B$ by setting $\theta(a, b) = (\varphi(a), b)$ for all (a, b). Then θ is a skew morphism of $A \times B$ with kernel $K \times B$. □

So now let A be any finite abelian group, written as a direct product $C_{q_1} \times \cdots \times C_{q_s}$ of cyclic groups of prime-power order, and suppose every skew morphism of A is an automorphism.

Then:

a) each q_i is 2, 4 or an odd prime (by theorems for C_n)

b) if some q_i is odd, then $\gcd(q_i, \phi(q_j)) = 1$ whenever $i \neq j$ by what we know about skew morphisms for $Cp \times C_q \cong C_{pq}$

c) if some q_i is even, then A is a 2-group (by (b)), and $(q_1, \ldots, q_s) = (4)$ or $(2, \ldots, 2)$, by what we know about skew morphisms for $C_2 \times C_4$ and $C_4 \times C_4$.

Thus we have the following ...

Theorem [MC & TT (2013)]: A finite abelian group has non-auto skew morphisms if and only if it is not isomorphic to C_4, or C_n with $\gcd(n, \phi(n)) = 1$, or $(C_2)^s$ for any s.

Corollary: Let A be any finite abelian group, and let $\mathcal{C}$ be the class of all finite groups G that have a complementary factorisation $G = AY$ with Y cyclic. Then:

- if A is cyclic of order n where $n = 4$ or $\gcd(n, \phi(n)) = 1$, or A is an elementary abelian 2-group, then every group in $\mathcal{C}$ is a semi-direct product $A \rtimes Y$, while
- if A is not one of those groups, then there exists at least one G in $\mathcal{C}$ such that A is not normal in G.

Skew morphisms of dihedral groups

[Joint work with Robert Jajcay and Tom Tucker]

It's easy to prove the following:

Theorem: If p is a prime with $p > 3$, then every skew morphism of the dihedral group D_p is an automorphism, and gives rise to a 'balanced' regular Cayley map for D_p.

Theorem [proved earlier by MC & Young Soo Kwon (2009)]: If φ is any skew morphism of the dihedral group D_n, where $n \geq 3$, then the kernel of φ cannot be C_n.

Conjecture [MC]: If φ is any skew morphism of the dihedral group D_n, then the kernel of φ cannot be a subgroup of C_n.

Finally, some shameless advertising ...

Australasian Conference on
Combinatorial Mathematics & Computing
Wellington, New Zealand, 1–5 December 2014

Summer School on

Algebra, Discrete Maths & Number Theory

Nelson, New Zealand, 11–16 January 2015

Second Conference on
Symmetries of Discrete Objects (& ATCAGC?)
Queenstown, New Zealand, February 2016

Thank You

Abstract

A skew morphism of a group is a variant of an automorphism, which arises in the study of regular Cayley maps (regular embeddings of Cayley graphs on surfaces, with the property that the ambient group induces a vertex-regular group of automorphisms of the embedding). More generally, skew morphisms arise in the context of any group expressible as a product AB of subgroups A and B with B cyclic and $A \cap B = \{1\}$. Specifically, a skew morphism of a group A is a bijection $\varphi \colon A \to A$ fixing the identity element of A and having the property that $\varphi(xy) = \varphi(x)\varphi^{\pi(x)}(y)$ for all $x, y \in A$, where $\pi(x)$ depends only on x. The kernel of φ is the subgroup of all $x \in A$ for which $\pi(x) = 1$. In this

talk I will present some of the theory of skew morphisms, including some very new theorems: two about the order and kernel of a skew morphism of a finite group, and a complete determination of the finite abelian groups for which every skew morphism is an automorphism.

Much of this is joint work with Robert Jajcay and Tom Tucker.