Origamis and permutation groups

David Zmiaikou

UNIVERSITÉ PARIS-SUD 11

École Doctorale de Mathématiques de la région Paris-Sud (ED 142)

Laboratoire de Mathématiques d'Orsay

THÈSE DE DOCTORAT

présentée par : **David ZMIAIKOU**

soutenue le : **8 septembre 2011**

pour obtenir le grade de : **Docteur de l'Université Paris-Sud 11**

Spécialité : **Mathématiques**

Origamis et groupes de permutation

THÈSE dirigée par

M. Jean-Christophe YOCCOZ — *Professeur, Collège de France*

RAPPORTEURS

M. Frank HERRLICH — *Professeur, Karlsruhe Institute of Technology*
M. Pascal HUBERT — *Professeur, Université Paul Cézanne*

EXAMINATEURS

M. Frédéric PAULIN — *Professeur, Université Paris-Sud 11*
M. Anton ZORICH — *Professeur, Université de Rennes 1*

"The symbols only dreamt about by most human beings are expressed in graphic form by the artists... We participate in the myth of creation. Order comes out of disorder, form out of chaos, as it did in the creation of the universe."
"But what the artist or creative scientist feels is not anxiety or fear; it is joy."
"The harmony of an internal form, the inner consistency of a theory, the character of beauty that touches your sensibilities – these are significant factors that determine why one given insight comes into consciousness rather than another."

Rollo May – The courage to create.

Acknowledgements

I would like to thank my Ph.D. advisor, *Jean-Christophe Yoccoz*, for his personal support, guidance at all stages, his encouragement and help. He gave me many amazing examples of what a professional researcher does to solve problems.

I am grateful to Frank Herrlich and Pascal Hubert for accepting to be the reviewers of my Ph.D. thesis. Their works in the domain of translations surfaces have a remarkable impact on the present research.

I am grateful to *Samuel Lelièvre* for introducing me to the fascinating world of square-tiled surfaces during my internship at the University of Warwick, and for helping me ever since.

I am grateful to *Emmanuel Lecouturier* with whom I wrote a joint paper [57] for his constant support during my thesis.

I would like to thank *Gabriela Schmithüsen* for her Ph.D. thesis [84] that served as an inspiration source to mine (especially to the chapters 4 and 6), and for her brilliant insights.

I am grateful to *Carlos Matheus* for many useful discussions and advice.

I am thankful to *Vincent Delecroix* for writing the Sage programs involved in the chapter 3.

I would like to thank the following mathematicians for interesting and helpful discussions: *Pierre Arnoux*, *Xavier Bressaud*, *Moon Duchin*, *Giovanni Forni*, *Rostislav Grigorchuk*, *Erwan Lanneau*, *Yves Laszlo*, *Curtis T. McMullen*, *Thierry Monteil*, *Barak Weiss*, *Anton Zorich*.

I am grateful to *Hakan Eliasson* and *Pascal Hubert* for giving me the opportunity to talk at the Université Pierre et Marie Curie and the Université de Provence.

During my studies, I was surrounded by my many friends and colleagues – they played an important role in my life. With some of them I organised numerous mathematical activities for high school students such as clubs, seminars, national and international tournaments and olympiads. I am especially grateful to *Martin Andler*, *Albin Andrieux*, *Julyan Arbel*, *Evgenij Barabanov*, *Dmitry Bodiagin*, *Claire Chavaudret*, *Julien Cojan*, *Bernardo da Costa*, *Dzmitry Doryn*, *Gabriel Dospinescu*, *David Harari*, *Viktor Kaskevich*, *Igor Kortchemski*, *Artem Kozhevnikov*, *Trafim Lasy*, *Victoria Lebed'*, *François Lo Jacomo*, *Ivan Loseu*, *Ruslan Maksimov*, *Pavel Mandrik*, *Roger Mansuy*, *Luca Marchese*, *Sergei Markouski*, *Sergei Mazanik*, *Pierre Pansu*, *Elena Pirutka*, *Louis Santharoubane*, *Vladimir Shchur*, *Valentin Telyak*, *Alexandr Usnich*, *Igor Voronovich*, *Thomas Zamojski*, *Maksim Zhykhovich*, *Evgenij Zorin*.

I would like to thank *Vasiliy Bernik* for his very positive influence on the developement of mathematics in Belarus.

I am grateful to my former university professors *Youri Syroid* and *Barys Zadvorny* with whom we are now good friends. Due to *Barys Zadvorny*, I have learned how important it is to help high school students discover their talents.

Contents

List of Figures

List of Tables

Notation

$\mathbb{N} = \{1, 2, 3, \ldots\}$	set of natural numbers (positive integers)
$\mathbb{Z}, \mathbb{Q}, \mathbb{C}$	sets of integer, rational and complex numbers
$\mathbb{R}, \mathbb{R}^2$	real line and real plane
$\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}_n$	ring of residue classes modulo n
$\mathbb{F}_p = \{0, 1, \ldots, p-1\}$	field of residue classes modulo the prime p
$\mathbb{F}_q$	finite field with q elements
$\mathbb{F}_q^\times$	multiplicative group of the field $\mathbb{F}_q$
$\mathbb{P}^1(\mathbb{F}_q)$	projective line over $\mathbb{F}_q$
$K[x], K(x)$	ring of polynomials and field of rational fractions over K
$\mathbb{T}^2$	torus of dimension 2
$\mathrm{Diff}^+(M)$	group of orientation-preserving homeomorphisms of M
$\Omega(M)$	vector space of holomorphic 1-forms on M
$\chi(M)$	Euler characteristic of M
$\mathcal{M}_g$	moduli space of compact connected Riemann surfaces of genus g
$\Omega\mathcal{M}_g$	moduli space of Abelian differentials
$\mathcal{H}(d_1, \ldots, d_s)$	stratum of connected translation surfaces (M, ω) such that ω has zeros of orders $d_1, \ldots, d_s$
$H^1(M, \Sigma; \mathbb{C})$	first relative cohomology group of M over $\mathbb{C}$
$\dim_{\mathbb{C}} V$	complex dimension of V
$T(m, n)$	trivial origami with mn squares
$L(m, n)$	corner origami with $m+n-1$ squares
$X(n)$, $E(n)$	tress and stair origamis with n squares
$\mathrm{Sq}(O)$	set of squares of the origami O
$\mathcal{M}on(O)$	monodromy group of O
$\mathrm{Aff}^+(M, \omega)$	affine group of the translation surface (M, ω)
$\mathrm{Aut}(M, \omega)$	automorphism group of (M, ω)
$\Gamma(M, \omega)$	real Veech group of (M, ω)
$\mathrm{SL}(M, \omega)$, $\mathrm{GL}(M, \omega)$	integer Veech groups of (M, ω)
$\mathrm{GL}(O)$	direct integer Veech group of O
$\mathrm{GL}^\times(O)$	dual integer Veech group of O
$\mathscr{N}_n^{\mathrm{pr}}(d_1, \ldots, d_s)$	number of primitive n-square origamis in $\mathcal{H}(d_1, \ldots, d_s)$
$\mathscr{A}_n(d_1, \ldots, d_s)$	number of n-square origamis in $\mathcal{H}(d_1, \ldots, d_s)$ with monodromy A_n
$\mathscr{S}_n(d_1, \ldots, d_s)$	number of n-square origamis in $\mathcal{H}(d_1, \ldots, d_s)$ with monodromy S_n
O_{G, g_1, g_2}	regular origami with monodromy group G generated by g_1, g_2
$O_{G/H, g_1, g_2}$	coset origami defined by the group G, the subgroup H and the pair of generators (g_1, g_2) of G

$\mathcal{R}(\Upsilon)$	realizer of the origamal digraph Υ
$G = \langle X \mid R \rangle$	presentation of G in terms of generators X and relators R
$C(X;\, R)$	Cayley diagram of the group $G = \langle X \mid R \rangle$
$\mathtt{gp}\,\{g_1, \ldots, g_k\}$	subgroup generated by $g_1, \ldots, g_k$
F_k	free group of rank k
C_n or $\mathbb{Z}_n$	cyclic group of order n
D_n	dihedral group of order $2n$
H_p	Heisenberg group of order p^3
Q_8	quaternion group of order 8
Q_{4n}	generalized quaternion group of order $4n$
Tet, Oct, Ico	tetrahedral, octahedral and icosahedral groups
$B(m, k)$	Burnside m-generator groups
$G_n(p)$	polynomial group $\left\{x + a_2x^2 + \cdots + a_nx^n \mid a_i \in \mathbb{F}_p\right\}$
$\mathrm{GL}(m, K)$, $\mathrm{GL}(m, q)$	general linear groups of degree m over K and $\mathbb{F}_q$
$\mathrm{GL}(m, \mathbb{Z})$ or $\mathrm{GL}_m(\mathbb{Z})$	integer general linear group of degree m
$\mathrm{GL}^+(m, K)$, $\mathrm{GL}^+(m, \mathbb{Q})$	groups of $m \times m$ matrices over K and $\mathbb{Q}$ with positive determinant
$\mathrm{SL}(m, K)$, $\mathrm{SL}(m, q)$	special linear groups of degree m over K and $\mathbb{F}_q$
$\mathrm{SL}(m, \mathbb{Z})$ or $\mathrm{SL}_m(\mathbb{Z})$	integer special linear group of degree m
$\mathrm{SO}(m, K)$	special orthogonal group of degree m over K
$Tr(m, q)$	group of m-dimensional translations over $\mathbb{F}_q$
$\mathrm{AGL}(m, q)$, $\mathrm{ASL}(m, q)$	general and special affine groups of degree m over $\mathbb{F}_q$
$\mathrm{PGL}(m, q)$, $\mathrm{PSL}(m, q)$	projective general and special linear groups of degree m over $\mathbb{F}_q$
$\Gamma\mathrm{L}(m, q)$	general semilinear group of degree m over $\mathbb{F}_q$
$\mathrm{A}\Gamma\mathrm{L}(m, q)$	affine semilinear group of degree m over $\mathbb{F}_q$
$\mathrm{P}\Gamma\mathrm{L}(m, q)$	projective semilinear group of degree m over $\mathbb{F}_q$
$\mathrm{tr}(A)$	trace of the matrix A
$\det(A)$	determinant of A
$\Gamma(n)$, $\Gamma^0(n)$, $\Gamma_0(n)$, ...	congruence subgroups of level n
$M_{11}, \ldots, M_{24}$	Mathieu groups of degree $11, \ldots, 24$
$Alt(\Omega)$, $Sym(\Omega)$	alternating and symmetric groups on Ω
$\Omega^{(k)}$	set of k-tuples with distinct entries from Ω
A_n, S_n	alternating and symmetric groups of degree n
G_x	stabilizer of x for the action of G
G_Δ	subgroup of G stabilizing all elements $x \in \Delta$
$\mathrm{fix}(\sigma)$, $\mathrm{supp}(\sigma)$	set of fixed points and support of σ
$m(G)$	minimal degree of G, *i.e.* $\min\{\lvert\mathrm{supp}(\sigma)\rvert \mid \sigma \in G\}$
$\mathrm{Graph}(\Theta)$	orbital graph of Θ
$r(G)$	rank of G
$\rho_{\mathrm{reg}} : G \hookrightarrow Sym(G)$	left regular permutation representation of G
$\rho_H : G \to Sym(G/H)$	representation defined by the action of G on the left cosets of H
$H \subseteq G$, $H \trianglelefteq G$	subgroup, normal sungroup
G/H	left cosets of H in G
$[g_1, g_2]$	commutator of g_1 and g_2, *i.e.* $g_1g_2g_1^{-1}g_2^{-1}$
$[G : H]$ or $\lvert G/H\rvert$	index of the subgroup H in G
$N_G(H)$, $C_G(H)$	normalizer and centralizer of H in G
$Z(G)$	center of G
$[G, G]$	commutator subgroup of G

$M(G)$	Schur multiplier of G
$G \times H$, G^m	direct product, direct power
$G \rtimes H$	semidirect product
$H_1 \cdot H_2$	set of products $h_1 \cdot h_2$ with $h_1 \in H_1$ and $h_2 \in H_2$
$(G \times G)^*$	conjugacy classes of pairs, *i.e.* $(G \times G)/\mathrm{Inn}(G)$
$(g_1, g_2)^*$	conjugacy class of the pair (g_1, g_2)
$A \hookrightarrow B$	mapping from A into B
$A \twoheadrightarrow B$	mapping from A onto B
$\ker(f)$, $\mathrm{Im}(f)$	kernel and image of f
$\mathrm{Aut}(G)$	automorphism group of G
$\mathrm{Inn}(G)$, $\mathrm{Out}(G)$	inner and outer automorphisms of G
$\mathrm{Hom}(G, H)$	set of homomorphisms from G to H
$\mathrm{Epi}(G, H)$	set of epimorphisms from G onto H
$d(G)$ or $\mathrm{rg}(G)$	minimal number of generators of G
$\mathcal{G}_k(G)$	set of k-tuples generating G
$\widehat{\mathcal{G}}_k(G)$	set of $\mathrm{Aut}(G)$-orbits on $\mathcal{G}_k(G)$
$\mathrm{NT}(G^k)$	set of Nielsen transformations of G^k
$\mathfrak{g} \overset{\mathrm{N}}{\sim} \mathfrak{g}'$	Nielsen equivalence of tuples
$e_x(w)$	sum of the exponents of x in the word w
$[r]$	largest integer not greater than r
φ	Euler's totient function
$\gcd(x_1, \ldots, x_n)$	greatest common divisor of $x_1, \ldots, x_n$

Chapter 1
Introduction

1.1 English version

An **origami** is a covering of the torus $\mathbb{T}^2$, possibly ramified above the origin. It is endowed with a flat metric coming from that on the torus and having conical singularities at the ramification points. If the covering is connected then the origami is also called **connected**.

Notice that the torus is obtained from a unit square by identifying the opposite sides, and the preimages of that square under a covering $f : O \to \mathbb{T}^2$ provide a tiling of O. Therefore, an origami can be viewed as a finite collection of copies of the unitary Euclidian square together with a gluing of the edges:

- the right edge of each square is identified to the left edge of some square,

- the top edge of each square is identified to the bottom edge of some square.

That is why origamis are widely called **square-tiled surfaces** – the term was first suggested to Anton Zorich by Alex Eskin. It seems that the connected square-tiled surfaces came into sight in 1970s through the works of William P. Thurston [92] and William A. Veech [95] on the moduli spaces of curves. Their growing popularity is due to research papers by Alex Eskin, Giovanni Forni, Eugene Gutkin, Frank Herrlich, Pascal Hubert, Chris Judge, Maksim Kontsevich, Samuel Lelièvre, Howard Masur, Carlos Matheus, Curtis T. McMullen, Martin Möller, Andrei Okounkov, Thomas A. Schmidt, Gabriela Schmithüsen, John Smillie, Barak Weiss, Jean-Christophe Yoccoz, Anton Zorich and others. The name 'origami' appeared around 2000 and is attributed to Pierre Lochak [60].

An n-square origami can be encoded by a pair of permutations $(\sigma, \tau) \in S_n \times S_n$, where S_n is the symmetric group on the set $\{1, 2, \ldots, n\}$. Indeed, number the squares by the integers from 1 to n and define the permutations as follows:

$$\sigma(i) = j, \quad \text{if the right edge of the } i^{\text{th}} \text{ square is glued to the left edge of the } j^{\text{th}} \text{ one,}$$
$$\tau(i) = k, \quad \text{if the top edge of the } i^{\text{th}} \text{ square is glued to the bottom edge of the } k^{\text{th}} \text{ one.}$$

Since an origami is defined regardless of numbering of the squares, it corresponds to the conjugacy class of (σ, τ) which we denote by $(\sigma, \tau)^* = \big\{(\mu^{-1}\sigma\mu,\, \mu^{-1}\tau\mu) \mid \mu \in S_n\big\}$.

Let O be a connected square-tiled surface with s ramification points over the origin of $\mathbb{T}^2$. A small circle of length $2\pi \cdot \varepsilon$ around the origin of the torus $\mathbb{T}^2$ lifts to a closed curve of length $2\pi(d_i + 1) \cdot \varepsilon$ around the i^{th} ramification point of O with $d_i \in \mathbb{N}$. By the Gauss-Bonnet formula we have

$$d_1 + d_2 + \ldots + d_s = 2g - 2,$$

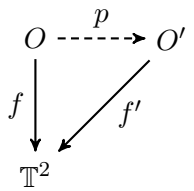
where g is the genus of the surface O. The set of connected origamis with the same parameters $\{d_1, d_2, \ldots, d_s\}$ forms a 'discrete' subset of a complex-analytic orbifold $\mathcal{H}(d_1, d_2, \ldots, d_s)$ which is called a **stratum** (see the chapter 2).

It is easy to check that the origami O encoded by a pair (σ, τ) is connected if and only if the subgroup $\mathtt{gp}\{\sigma, \tau\} \subseteq S_n$ is transitive, and O belongs to $\mathcal{H}(d_1, d_2, \ldots, d_s)$ if and only if the commutator $[\sigma, \tau]$ is a product of s nontrivial disjoint cycles of lengths $(d_1 + 1)$, $(d_2 + 1)$, ..., $(d_s + 1)$. The group $\mathtt{gp}\{\sigma, \tau\}$ will be called the **monodromy group** of the origami O and denoted by $\mathcal{M}on(O)$. This group is defined up to isomorphism. Conversely, if we have

- a finite two-generator group G,
- a pair of generators (g, h) of G,
- a faithful representation $\rho : G \hookrightarrow S_n$,

then the pair of permutations $(\rho(g), \rho(h))$ gives an n-square origami O with $\mathcal{M}on(O) \simeq G$. By the way, any finite non-abelian simple group is generated by two elements. There are two types of faithful permutation representations: the first is induced by the action of G on its elements and the second by the action of G on the cosets $\{g_1 H, \ldots, g_n H\}$ for some proper subgroup $1 \subset H \subset G$ such that $\bigcap_{g \in G} gHg^{-1} = 1$. An origami O obtained in the first case will be called **regular** and in the second case – **coset**. Due to the classification of transitive representations (Proposition 2.10), any connected origami is either regular or coset.

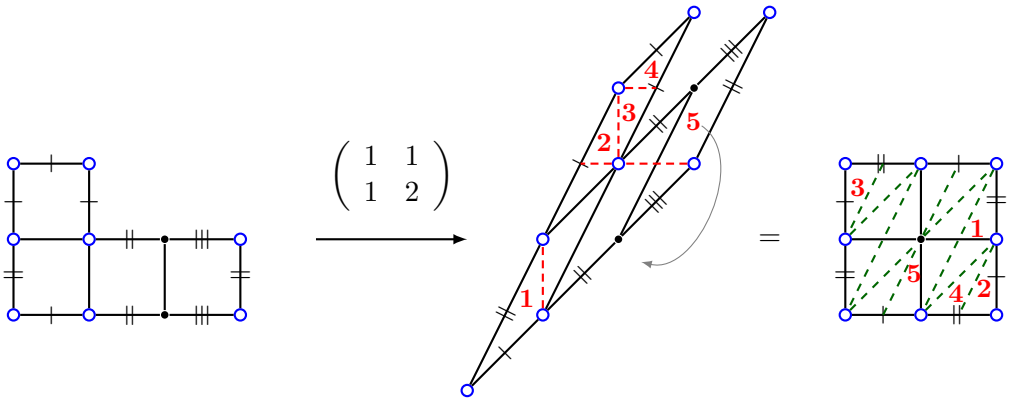
We say that O **covers** an origami O' if the following diagram



commutes for a (possibly ramified) covering p. A square-tiled surface is called **primitive** if the only square-tiled surfaces it covers are the torus $\mathbb{T}^2$ and itself.

A nonempty subset Δ of $\Lambda_n = \{1, 2, \ldots, n\}$ is called a **block** for a permutation group $G \subseteq S_n$ if, for each $g \in G$, either $g(\Delta) = \Delta$ or $g(\Delta) \cap \Delta = \emptyset$. A permutation group G is said to be **primitive** if it has no blocks except the singletons and the entire set Λ_n. It is straightforward that a connected n-square-tiled surface O is primitive if and only if its monodromy group $\mathcal{M}on(O) \subseteq S_n$ is primitive (see Proposition 2.4). We can thus apply results from the theory of permutation groups, *e.g.* Theorems 2.5 and 2.6, to conclude that in a given stratum for large enough n the monodromy group of any primitive n-square origami is either A_n or S_n.

There is a natural action of the general linear group $\mathrm{GL}_2(\mathbb{Z})$ on the square-tiled surfaces. It is seen geometrically in the plane: a matrix transforms the squares that can be cut and re-glued in order to get new squares, as shown in the figure below (parallel edges with the same marking are identified).



In terms of permutations, we will have

$$\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\cdot(\sigma,\,\tau)^* = (\sigma,\tau^{-1})^*,\quad \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\cdot(\sigma,\,\tau)^* = (\sigma,\tau\sigma^{-1})^*,$$

$$\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\cdot(\sigma,\,\tau)^* = (\tau^{-1},\sigma)^*,\quad \begin{pmatrix}1 & 0\\ -1 & 1\end{pmatrix}\cdot(\sigma,\,\tau)^* = (\sigma\tau,\tau)^*.$$

The stabilizer of an origami O for this action is called the **integer Veech group** of O and is denoted by $\mathrm{GL}(O)$. An immediate and important remark is that the monodromy group is an **invariant** of the $\mathrm{GL}_2(\mathbb{Z})$-orbits.

For any group G, the automorphism group $\mathrm{Aut}(F_2)$ acts on the set $G\times G$ by Nielsen transformations. Recall the exact sequence (see the section 2.4):

$$0\to \mathrm{Inn}(F_2)\to \mathrm{Aut}(F_2)\xrightarrow{\Phi}\mathrm{GL}(2,\,\mathbb{Z})\to 0,\quad \Phi:\gamma\longmapsto\begin{pmatrix}e_x(\gamma(x)) & e_x(\gamma(y))\\ e_y(\gamma(x)) & e_y(\gamma(y))\end{pmatrix},$$

where $e_x(w)$ and $e_y(w)$ denote the sums of the exponents of x and y, respectively, in the word $w\in F_2$. This induces a $\mathrm{GL}_2(\mathbb{Z})$-action on the set $(G\times G)^* = (G\times G)/\mathrm{Inn}(G)$ of conjugacy classes of pairs such that the following diagram commutes

$$\begin{array}{ccc}\mathrm{Aut}(F_2)\times(G\times G) & \longrightarrow & G\times G\\ \downarrow & & \downarrow\\ \mathrm{GL}_2(\mathbb{Z})\times(G\times G)^* & \longrightarrow & (G\times G)^*\end{array}$$

which is given explicitly in section 2.6. It turns out that the case of $G=S_n$ corresponds to the action of $\mathrm{GL}_2(\mathbb{Z})$ on the n-square origamis.

Structure of the thesis

Chapter 2

We recall and discuss some known notions and facts on translation surfaces, permutation groups, Nielsen equivalence classes. An interpretation of those notions in the language of square-tiled surfaces leads to the definition of primitivity, monodromy groups, direct and dual $\mathrm{GL}_2(\mathbb{Z})$-actions on origamis.

Chapter 3

We start by noticing that in the stratum $\mathcal{H}(2)$, due to the works [45] and [67], the monodromy group is a **complete invariant** of the $\mathrm{GL}_2(\mathbb{Z})$-orbits of primitive square-tiles surfaces: for any $n \geq 4$ there is exactly one orbit corresponding to S_n and at most one orbit corresponding to A_n. A natural question arises what monodromy group can a primitive origami from a given stratum have. Using results from the 19th, 20th and 21st centuries we obtain the following theorem:

Theorem (3.12)**.** *If $p \geq 5$ is a prime but not Mersenne, then in the stratum $\mathcal{H}(p-1)$ the monodromy group of any primitive n-square-tiled surface with $n \geq p+2$ is either A_n or S_n. If $p \geq 7$ is a Mersenne prime, then the same is true for $n \geq p+3$.*

In the stratum $\mathcal{H}(m)$, where m is an even positive integer, the monodromy group of any primitive n-square-tiled surface with $n \geq \frac{3}{2}m + 2$ (the bound is not exact) is either A_n or S_n.

Due to a work of Camille Jordan [53] going back to 1875, we also get:

Theorem (3.21)**.** *For each integer $n \neq 6$, the monodromy group of any primitive n-square-tiled surface from $\mathcal{H}(1,1)$ is either A_n or S_n.*

Afterwards, we construct and study two families of n-square-tiled surfaces in $\mathcal{H}(1,1)$ for which the alternating and symmetric groups are realized.

Chapter 4

We investigate the regular square-tiled surfaces corresponding to Cayley diagrams of finite two-generator groups. We develop a method of determining the Veech group of such an origami through a presentation of its monodromy group in terms of generators and relations. It turns out that the $\mathrm{GL}_2(\mathbb{Z})$-orbits of regular origamis such that $\mathcal{M}on(O) = G$ are in bijection with the T_2-systems of G (see Theorem 4.4). Among all square-tiled surfaces with a given monodromy group, the regular ones possess the largest Veech groups:

Theorem (4.7)**.** *Consider a finite group G generated by two elements g and h. Let $\rho_{\mathrm{reg}} : G \hookrightarrow Sym(G)$ be its regular representation, and $\rho : G \hookrightarrow S_m$ another faithful permutation representation. Denote by O_{reg} and O_ρ the origamis defined by the pairs $(\rho_{\mathrm{reg}}(g), \rho_{\mathrm{reg}}(h))$ and $(\rho(g), \rho(h))$ respectively. Then*

$$\mathrm{GL}(O_\rho) \subseteq \mathrm{GL}(O_{\mathrm{reg}}).$$

Moreover, if the representation ρ is structural[1]*, then one has the equality* $\mathrm{GL}(O_\rho) = \mathrm{GL}(O_{\mathrm{reg}})$.

In this chapter, several old families of regular square-tiled surfaces are revisited and new interesting families are constructed. The idea is to take a finite two-generator group (for instance, a simple one), to fix a pair of generators and to consider a presentation with (if possible) few relations. In some cases we succeed to find the strata and the Veech groups for a family of origamis, in the others we explain the degree of difficulty and connect the questions with well-known conjectures.

We also estimate the number of distinct $\mathrm{GL}(2, \mathbb{Z})$-orbits and strata of regular square-tiled surfaces with a given monodromy group. In order to find a lower bound for alternating origamis, we prove the following theorem:

Theorem (4.26)**.** *Let d be a positive integer, and let p be the least prime number such that $\left[\frac{3d}{4}\right] \leq p \leq d-3$. Every permutation $\mu \in A_d$ moving at least $p+2$ points can be presented as the commutator of a generating pair of A_d, one of the elements being a p-cycle.*

Remark that when $d \geq 14$ and $d \neq 19$, there exists a prime p such that $\left[\frac{3d}{4}\right] \leq p \leq d-3$.

[1] that is, for each automorphism $\phi \in \mathrm{Aut}(\rho(G))$ there exists $\sigma \in S_m$ such that $\phi(\tau) = \sigma\tau\sigma^{-1}$ for all $\tau \in \rho(G)$.

Corollary (4.31)**.** *For some real $C > 0$ and any positive integer d, the number of different strata containing a regular origami O such that $\mathcal{M}on(O) = A_d$ is greater than $\frac{C}{d}e^{\pi\sqrt{\frac{2d}{3}}}$.*

Chapter 5

We partially generalize the theory of the chapter 4, and consider the square-tiled surfaces corresponding to coset digraphs of groups. Projective and alternating coset origamis are studied. In particular, since the permutation representations $\mathrm{PSL}(2,p) \hookrightarrow S_{p+1}$ and $A_n \hookrightarrow S_n$ in question are structural, we apply Theorem 4.7 to show that the Veech groups coincide with those of the regular origamis.

Chapter 6

We consider the orbits of the Veech group $\mathrm{SL}(O)$ of an origami on the projective line $\mathbb{P}^1(\mathbb{Q})$. It turns out that in particular cases, the set of elements $\bar{A} \in \mathrm{PSL}_2(\mathbb{Z})$ such that $\frac{p}{q}$ and $\bar{A} \cdot \frac{p}{q}$ lie in the same $\mathrm{SL}(O)$-orbit for all $\frac{p}{q} \in \mathbb{P}^1(\mathbb{Q})$ coincides with $\mathrm{SL}(O)/\{\pm I\}$. This inspires us to introduce the following notion. Let G be a group acting transitively on a set M, A subgroup $\Gamma \subseteq G$ is called **M-straining** if the stabilizer of the Γ-orbits on M is exactly Γ. When $G = \mathrm{PSL}_2(\mathbb{Z})$ we have:

Theorem (6.3)**.** *There exist infinitely many subgroups $\Gamma \subseteq \mathrm{PSL}_2(\mathbb{Z})$ of finite index which are not $\mathbb{P}^1(\mathbb{Q})$-straining.*

1.2 Version française

Un **origami** est un revêtement du tore $\mathbb{T}^2$, éventuellement ramifié au-dessus de l'origine. Il est muni d'au moins une métrique plate provenant de celle standard sur le tore et ayant des singularités coniques en les points de ramification. Si le revêtement est connexe, alors on dit que l'origami est **connexe**.

Remarquons que le tore est obtenu du carreau unitaire en collant ses côté opposés, et les images réciproques de ce carreau pour un revêtement $f : O \to \mathbb{T}^2$ fournissent un pavage de O. Donc, un origami peut être vu comme un ensemble fini de copies du carreau unitaire euclidien qui sont collées en respectant les règles suivantes :

- chaque côté droit est identifié par translation avec un et un seul côté gauche,

- chaque côté haut est identifié par translation avec un et un seul côté bas.

Voilà pourquoi les origamis sont aussi appelés **surfaces à petits carreaux**, le terme ayant été proposé à Anton Zorich par Alex Eskin. Les surfaces à petits carreaux ont été découvertes dans les années 1970 à travers des travaux de William P. Thurston [92] et William A. Veech [95] sur les espaces des modules de courbes. Leur popularité croissante est due à des articles de Alex Eskin, Giovanni Forni, Eugene Gutkin, Frank Herrlich, Pascal Hubert, Chris Judge, Maksim Kontsevich, Samuel Lelièvre, Howard Masur, Carlos Matheus, Curtis T. McMullen, Martin Möller, Andrei Okounkov, Thomas A. Schmidt, Gabriela Schmithüsen, John Smillie, Barak Weiss, Jean-Christophe Yoccoz, Anton Zorich et d'autres. Le nom "origami" est apparu autour de 2000, il est attribué à Pierre Lochak [60].

Un origami à n carreaux peut être encodé par une paire de permutations $(\sigma, \tau) \in S_n \times S_n$, où S_n est le groupe symétrique sur l'ensemble $\{1, 2, \ldots, n\}$. En effet, on numérote les carreaux de l'origami par les entiers de 1 à n et on lui associe deux permutations σ and τ telles que :

$$\begin{aligned} \sigma(i) &= j, \quad \text{si le côté droit du carreau } i \text{ est collé au côté gauche du carreau } j, \\ \tau(i) &= k, \quad \text{si le côté haut du carreau } i \text{ est collé au côté bas du carreau } k. \end{aligned}$$

Puisqu'un origami ne dépend pas de la numérotation de ses carreaux, il correspond à la classe de conjugaison diagonale de (σ, τ) que nous allons désigner par $(\sigma, \tau)^* = \big\{(\mu^{-1}\sigma\mu,\, \mu^{-1}\tau\mu) \mid \mu \in S_n\big\}$.

Soit O une surface à petits carreaux connexe avec s points de ramification au-dessus de l'origine de $\mathbb{T}^2$. Un petit cercle de longueur $2\pi \cdot \varepsilon$ autour de l'origine du tore $\mathbb{T}^2$ se relève en une courbe fermée de longueur $2\pi(d_i + 1) \cdot \varepsilon$ autour du $i^{\text{ième}}$ point de ramification de O avec $d_i \in \mathbb{N}$. D'après la formule de Gauss-Bonnet on a

$$d_1 + d_2 + \ldots + d_s = 2g - 2,$$

où g est le genre de la surface O. L'ensemble des origamis connexes avec les mêmes paramètres $\{d_1, d_2, \ldots, d_s\}$ forme un sous-ensemble "discret" d'une orbifolde complexe analytique $\mathcal{H}(d_1, d_2, \ldots, d_s)$ que l'on appellera une **strate**.

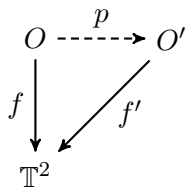
Il est facile de vérifier que l'origami O encodé par une paire (σ, τ) est connexe si et seulement si le sous-groupe $\mathtt{gp}\{\sigma, \tau\} \subseteq S_n$ est transitif, et que O appartient à la strate $\mathcal{H}(d_1, d_2, \ldots, d_s)$ si

et seulement si le commutateur $[\sigma, \tau]$ est un produit de s cycles non-triviaux disjoints de longueurs (d_1+1), (d_2+1), ..., (d_s+1). Le groupe $\mathtt{gp}\{\sigma, \tau\}$ sera appelé le **groupe de monodromie** de O, on le désignera par $\mathcal{M}on(O)$. Ce groupe est défini à isomorphisme près. Inversement, si l'on a

- un groupe fini G,
- un couple générateur (g, h) de G,
- une représentation fidèle $\rho : G \hookrightarrow S_n$,

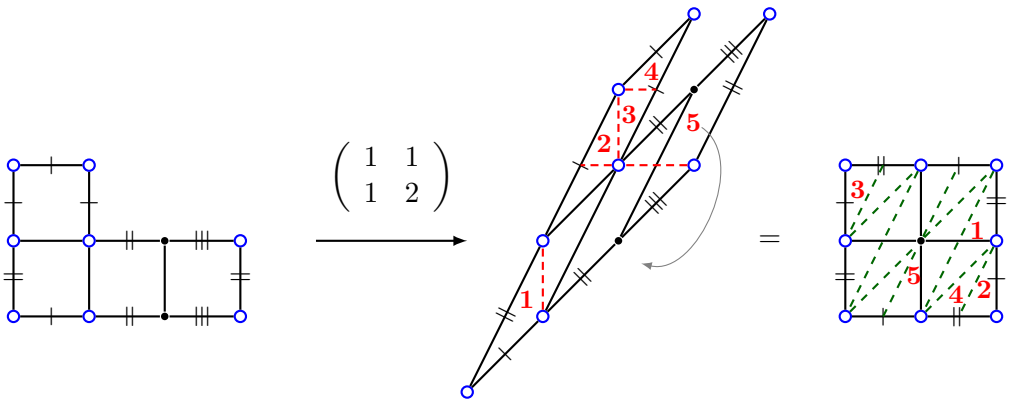
alors la paire de permutations $(\rho(g), \rho(h))$ détermine un origami O à n carreaux avec $\mathcal{M}on(O) \simeq G$. (Par ailleurs, tout groupe fini non-abélien simple est engendré par deux éléments.) Il y a deux types de représentations fidèles : la première est induite par l'action de G sur ses éléments et la deuxième par l'action de G sur les classes $\{g_1H, \ldots, g_nH\}$ suivant un sous-groupe propre $1 \subset H \subset G$ tel que $\bigcap_{g\in G} gHg^{-1} = 1$. Un origami O obtenu dans le premier cas sera appelé **régulier** et celui obtenu dans le deuxième cas **quotient**. Selon la classification des représentations transitives (le théoréme 2.10), tout origami connexe est soit régulier soit quotient.

On dit que O est un **revêtement** d'un origami O' si le diagramme suivant



commute pour un revêtement p (éventuellement ramifié). Une surface à petits carreaux O est dite **primitive** si le tore $\mathbb{T}^2$ et O sont les seules surfaces à petits carreaux dont elle est un revêtement.

Un sous-ensemble non vide Δ de $\Lambda_n = \{1, 2, \ldots, n\}$ est appelé un **bloc** pour le groupe de permutation $G \subseteq S_n$ si pour tout $g \in G$ on a $g(\Delta) = \Delta$ ou $g(\Delta) \cap \Delta = \emptyset$. Un groupe G est dit **primitif** s'il n'a pas de blocs excepté les singletons et l'ensemble Λ_n. Il est immédiat qu'une surface à n carreaux O est primitive si et seulement si son groupe de monodromie $\mathcal{M}on(O) \subseteq S_n$ est primitif (voir la proposition 2.4). Ainsi, nous pouvons appliquer des résultats de la théorie des groupes de permutation, par exemple les théorèmes 2.5 et 2.6, afin de conclure que dans une strate donnée pour n suffisamment grand le groupe de monodromie d'un origami primitif à n carreaux est soit A_n soit S_n.



Il y a une action naturelle du groupe général linéaire $\mathrm{GL}_2(\mathbb{Z})$ sur les surfaces à petits carreaux. On la décrit géométriquement dans le plan : une matrice transforme les carreaux en parallélogrammes que l'on peut découper en morceaux, que l'on recolle en respectant les identifcations de telle façon que

l'ensemble obtenu soit encore un origami (*cf.* un exemple sur la figure ci-dessus, où les côtés parallèles avec le même nombre de traits sont identifiés). En termes de permutations, on aura

$$\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\cdot(\sigma,\,\tau)^* = (\sigma,\tau^{-1})^*,\quad \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\cdot(\sigma,\,\tau)^* = (\sigma,\tau\sigma^{-1})^*,$$

$$\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\cdot(\sigma,\,\tau)^* = (\tau^{-1},\sigma)^*,\quad \begin{pmatrix}1 & 0\\ -1 & 1\end{pmatrix}\cdot(\sigma,\,\tau)^* = (\sigma\tau,\tau)^*.$$

Le stabilisateur d'un origami O pour cette action s'appelle le **groupe de Veech entier** de O et est désigné par $\mathrm{GL}(O)$. Une remarque immédiate et importante est que le groupe de monodromie est un **invariant** des $\mathrm{GL}_2(\mathbb{Z})$-orbites.

Pour tout groupe G, en notant F_2 le groupe libre sur $\{x, y\}$, le groupe des automorphismes $\mathrm{Aut}(F_2)$ agit sur l'ensemble $G\times G$ par les transformations de Nielsen. Rappellons la suite exacte (voir la partie 2.4) :

$$0\to \mathrm{Inn}(F_2)\to \mathrm{Aut}(F_2)\xrightarrow{\Phi}\mathrm{GL}(2,\,\mathbb{Z})\to 0,\quad \Phi:\gamma\longmapsto\begin{pmatrix}e_x(\gamma(x)) & e_x(\gamma(y))\\ e_y(\gamma(x)) & e_y(\gamma(y))\end{pmatrix},$$

où $e_x(w)$ et $e_y(w)$ désignent les sommes des exposants de x et y respectivement dans le mot $w\in F_2$. Cela induit une $\mathrm{GL}_2(\mathbb{Z})$-action sur l'ensemble $(G\times G)^* = (G\times G)/\mathrm{Inn}(G)$ des classes de conjugaison diagonale des paires telle que le diagramme suivant commute

$$\begin{array}{ccc}\mathrm{Aut}(F_2)\times(G\times G) & \longrightarrow & G\times G\\ \downarrow & & \downarrow\\ \mathrm{GL}_2(\mathbb{Z})\times(G\times G)^* & \longrightarrow & (G\times G)^*\end{array}$$

ce qui est explicitement donné dans la section 2.6. Il se trouve que le cas $G = S_n$ correspond à l'action de $\mathrm{GL}_2(\mathbb{Z})$ sur les origamis à n carreaux.

La structure de la thèse

Chapitre 2

Nous rappelons et discutons plusieurs notions et faits connus concernant les surfaces de translation, les groupes de permutation, les classes d'équivalence de Nielsen. Une interprétation de ces notions en langage des surfaces à petits carreaux nous conduit à la définition de la primitivité, d'un groupe de monodromie, des $\mathrm{GL}_2(\mathbb{Z})$-actions directe et duale sur les origamis.

Chapitre 3

On commence par remarquer que dans la strate $\mathcal{H}(2)$, grâce aux travaux [45] et [67], le groupe de monodromie est un **invariant complet** des $\mathrm{GL}_2(\mathbb{Z})$-orbites de surfaces à petits carreaux primitives : pour tout $n\geq 4$, il y a exactement une orbite correspondant au groupe S_n et au plus une orbite correspondant à A_n. Une question naturelle se pose : dans une strate donnée, quels groupes apparaissent comme groupe de monodromie d'un origami primitif ? En utilisant des résultats des 19$^{\text{ième}}$, 20$^{\text{ième}}$ et 21$^{\text{ième}}$ siècles, nous obtenons le théorème suivant :

Théorème (3.12). *Si $p \geq 5$ est un nombre premier qui n'est pas de Mersenne, alors dans la strate $\mathcal{H}(p-1)$ le groupe de monodromie de toute surface à n petits carreaux primitive avec $n \geq p+2$ est A_n ou S_n. Si $p \geq 7$ est un nombre premier de Mersenne, alors le même résultat est vrai pour $n \geq p+3$.*

Dans la strate $\mathcal{H}(m)$, où m est un entier positif pair, le groupe de monodromie de toute surface à n petits carreaux primitive avec $n \geq \frac{3}{2}m+2$ (la borne n'est pas exacte) est A_n ou S_n.

Grâce à un travail de Camille Jordan [53] publié en 1875, on obtient aussi :

Théorème (3.21). *Pour tout entier $n \neq 6$, le groupe de monodromie de toute surface à n petits carreaux primitive dans $\mathcal{H}(1,1)$ est A_n ou S_n.*

Ensuite, nous construisons et étudions deux familles de surfaces à n petits carreaux dans $\mathcal{H}(1,1)$ pour lesquelles les groupes alterné et symétrique sont réalisés.

Chapitre 4

Nous examinons les surfaces à petits carreaux régulières correspondant aux diagrammes de Cayley de groupes finis à deux générateurs. Nous développons une méthode pour déterminer le groupe de Veech d'un tel origami en utilisant une présentation de son groupe de monodromie en termes de générateurs et relations. Il se trouve que les $\mathrm{GL}_2(\mathbb{Z})$-orbites des origamis réguliers O tels que $\mathcal{M}on(O) = G$ sont en bijection avec les T_2-systèmes de G (voir le théorème 4.4). Parmi les surfaces à petits carreau avec un groupe de monodromie donnée, les origamis réguliers possèdent le plus grand groupe de Veech :

Théorème (4.7). *On considère un groupe fini G engendré par deux éléments g et h. Soit $\rho_{\mathrm{reg}} : G \hookrightarrow Sym(G)$ une représentation régulière, et soit $\rho : G \hookrightarrow S_m$ une autre représentation fidèle. On désigne par O_{reg} et O_ρ les origamis définis par les paires $(\rho_{\mathrm{reg}}(g), \rho_{\mathrm{reg}}(h))$ et $(\rho(g), \rho(h))$ respectivement. Alors*

$$\mathrm{GL}(O_\rho) \subseteq \mathrm{GL}(O_{\mathrm{reg}}).$$

De plus, si la représentation ρ est structurelle[2] *alors on a l'égalité* $\mathrm{GL}(O_\rho) = \mathrm{GL}(O_{\mathrm{reg}})$.

Dans ce chapitre, plusieurs familles connues de surfaces à petits carreaux régulières sont revisitées, et de nouvelles familles intéressantes sont construites. L'idée est de prendre un groupe fini à deux générateurs (par exemple, un groupe simple), de fixer une paire de génératrice et de considérer une présentation avec (si possible) peu de relations. Dans certains cas, nous réussissons à trouver les strates et les groupes de Veech pour des familles d'origamis, dans d'autres cas, on explique le degré de difficulté et on lie les questions avec des problèmes ouverts.

Nous estimons également le nombre de $\mathrm{GL}(2,\mathbb{Z})$-orbites et strates distinctes des surfaces à petits carreaux régulières avec un groupe de monodromie donné. Afin de trouver une borne inférieure pour les origamis alternés, nous montrons le théorème suivant :

Théorème (4.26). *Soit d un entier positif, et soit p le plus petit nombre premier tel qu'on ait les inégalités $\left[\frac{3d}{4}\right] \leq p \leq d-3$. Alors chaque permutation $\mu \in A_d$ qui bouge au moins $p+2$ points peut être présentée comme le commutateur d'une paire engendrant A_d, dont l'un des éléments est un p-cycle.*

Remarquons que quand $d \geq 14$ et $d \neq 19$, il existe un nombre premier p tel que $\left[\frac{3d}{4}\right] \leq p \leq d-3$.

Corollaire (4.31). *Il existe un réel $C > 0$ tel que, pour tout entier positif d, le nombre de strates différentes qui contiennent un origami régulier O tel que $\mathcal{M}on(O) = A_d$ est au moins $\frac{C}{d}e^{\pi\sqrt{\frac{2d}{3}}}$.*

[2] c'est-à-dire pour tout automorphisme $\phi \in \mathrm{Aut}(\rho(G))$ il existe $\sigma \in S_m$ telle que $\phi(\tau) = \sigma\tau\sigma^{-1}$ pour tout $\tau \in \rho(G)$.

Chapitre 5

Nous généralisons partiellement la théorie du chapitre 4 et considérons les surfaces à petits carreaux correspondant aux graphes quotients de groupes. Les origamis réguliers projectifs et alternés sont étudiés. En particulier, puisque les représentations $\mathrm{PSL}(2,p) \hookrightarrow S_{p+1}$ et $A_n \hookrightarrow S_n$ en question sont structurelles, nous appliquons le théorème 4.7 pour montrer que les groupes de Veech coïncident avec ceux des origamis réguliers.

Chapitre 6

Nous considérons les orbites du groupe de Veech $\mathrm{SL}(O)$ d'un origami sur la ligne projective $\mathbb{P}^1(\mathbb{Q})$. Il se trouve que dans des cas particuliers, l'ensemble des éléments $\bar{A} \in \mathrm{PSL}_2(\mathbb{Z})$ tels que $\frac{p}{q}$ et $\bar{A} \cdot \frac{p}{q}$ sont dans la même $\mathrm{SL}(O)$-orbite pour tout $\frac{p}{q} \in \mathbb{P}^1(\mathbb{Q})$ coïncide avec $\mathrm{SL}(O)/\{\pm I\}$. Cela nous invite à introduire la notion suivante. Soit G un groupe agissant transitivement sur un ensemble M, un sous-groupe $\Gamma \subseteq G$ est dit **M-contraint** si le stabilisateur de toutes les Γ-orbites sur M est exactement Γ. Pour $G = \mathrm{PSL}_2(\mathbb{Z})$, nous montrons :

Théorème (6.3)**.** *Il existe une infinité de sous-groupes $\Gamma \subseteq \mathrm{PSL}_2(\mathbb{Z})$ d'indice fini qui ne sont pas $\mathbb{P}^1(\mathbb{Q})$-contraints.*

Chapter 2
Conception

2.1 Translation surfaces

In this work, a surface is a two-dimensional topological manifold that is not necessarily connected. Let $\mathcal{M}_g$ denote the *moduli space* of compact connected Riemann surfaces of genus $g \geq 1$. This space is defined as follows. First, fix a compact connected orientable topological surface S of genus g. Second, consider the space $\mathscr{C}_g$ of all complex structures on S. Finally, say that two complex structures are equivalent if there exists an orientation preserving homeomorphism of S carrying one structure to the other. We obtain, thus, the moduli space

$$\mathcal{M}_g = \mathscr{C}_g/\mathrm{Diff}^+(S),$$

where $\mathrm{Diff}^+(S)$ is the group of orientation-preserving homeomorphisms of S acting on $\mathscr{C}_g$ by pullback.

If M is a compact connected Riemann surface of genus $g \geq 1$, then the vector space $\Omega(M)$ of holomorphic 1-forms on M (also called *Abelian differentials*) has dimension g over $\mathbb{C}$. The moduli space of Abelian differentials, denoted by $\Omega\mathcal{M}_g$, forms a natural vector bundle over the space $\mathcal{M}_g$. A point (M, ω) of $\Omega\mathcal{M}_g$ consists of a Riemann surface $M \in \mathcal{M}_g$ equipped with a holomorphic 1-form $\omega \in \Omega(M)$. Such a pair (M, ω) is called a *connected translation surface* if $\omega \neq 0$. An arbitrary, not necessarily connected, *translation surface* is just a finite disjoint union of connected translation surfaces.

We are going to explain the term 'translation' involved here. Let $\Sigma = \{Z_1, \ldots, Z_s\}$ be the set of zeros of the 1-form ω. In local coordinates, outside Σ, this form can be written as $\omega = dz$. Indeed, if $\omega = f(v)dv$ in a chart (U, v) on M with $U \cap \Sigma = \emptyset$, then for a point $P_0 \in U$ we take

$$z(P) := \int_{P_0}^{P} \omega$$

for any $P \in U$. Furthermore, defining in such a way local coordinates z_0 and z_1 on two charts (U_0, v_0) and (U_1, v_1) for some base points $P_0 \in U_0$ and $P_1 \in U_1$, we will have

$$z_0(P) - z_1(P) = \int_{P_0}^{P} \omega - \int_{P_1}^{P} \omega = \int_{P_0}^{P_1} \omega = c \in \mathbb{C}$$

constantly, for any point $P \in U_0 \cap U_1$. Therefore, the transition maps are just *translations*.

A graphic way of constructing translation surfaces consists in taking a finite set of polygons in the real plane $\mathbb{R}^2$ and gluing pairs of their sides: every side is identified by translation to another one.

As for a neighbourhood of a zero, in an appropriate local coordinate z the holomorphic 1-form ω can be written as $\omega = z^d dz$, where d is the multiplicity (or *order*) of the zero. Since $z^d dz = d\left(\frac{z^{d+1}}{d+1}\right)$, the zero is a conical point with cone angle $2\pi(d+1)$. For example, the vertices of the polygon in

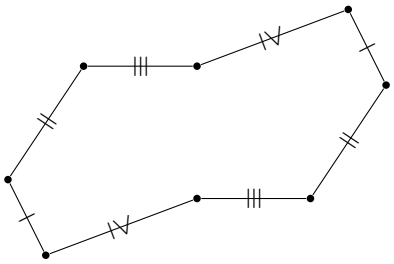


Figure 2.1: A translation surface as a polygon with identification of pairs of sides.

FIGURE 2.1 after gluing the pairs of sides with the same marking will turn into one conical singularity of angle $\pi(8-2) = 2\pi(2+1)$.

By the Gauss-Bonnet formula we have

$$\sum_{i=1}^{s} d_i = 2g - 2,$$

where d_i is the multiplicity of the zero Z_i.

The connected translation surfaces (M, ω) such that ω has zeros of orders $d_1, \ldots, d_s$ form a stratum $\mathcal{H}(d_1, \ldots, d_s)$ in $\Omega\mathcal{M}_g$. This stratum may be naturally endowed with a structure of complex-analytic orbifold of dimension

$$\dim_{\mathbb{C}} \mathcal{H}(d_1, \ldots, d_s) = 2g + s - 1,$$

while $\dim_{\mathbb{C}} \mathcal{M}_g = 3g - 3$.

For example, in genus 2, we have a decomposition of the moduli space of Abelian differentials into $\Omega\mathcal{M}_2 = \mathcal{H}(1,1) \sqcup \mathcal{H}(2)$, where $\dim_{\mathbb{C}} \mathcal{H}(1,1) = 5$ and $\dim_{\mathbb{C}} \mathcal{H}(2) = 4$.

2.2 Square-tiled surfaces and their monodromy groups

A special 'integer' case of translation surfaces is that of the surfaces which can be tiled by squares.

To every translation surface (M, ω) corresponds a class $[\omega] \in H^1(M, \Sigma; \mathbb{C})$ in the relative cohomology group, where $\Sigma = \{Z_1, \ldots, Z_s\}$ is the set of zeros of the holomorphic 1-form ω. The cohomology space $H^1(M, \Sigma; \mathbb{C})$ contains a natural integer lattice $H^1(M, \Sigma; \mathbb{Z} \oplus \sqrt{-1}\,\mathbb{Z})$. In the case where $[\omega] \in H^1(M, \Sigma; \mathbb{Z} \oplus \sqrt{-1}\,\mathbb{Z})$, all relative periods of ω are integer-valued, that is, $\int_{Z_j}^{Z_k} \omega \in \mathbb{Z} \oplus \sqrt{-1}\,\mathbb{Z}$ for any $j, k \in \{1, \ldots, s\}$. Consider then the map f from M to the standard torus $\mathbb{T}^2 = \mathbb{C}/(\mathbb{Z} \oplus \sqrt{-1}\,\mathbb{Z})$ set by

$$f : P \mapsto \left(\int_{Z_1}^{P} \omega \right) \mod \mathbb{Z} \oplus \sqrt{-1}\,\mathbb{Z},$$

where $P \in M$. Since f is holomorphic and onto, it is a ramified covering. Moreover, it has exactly s ramification points – the zeros $Z_1, \ldots, Z_s$ of ω, they project to $0 \in \mathbb{T}^2$.

Conversely, a covering $M \to \mathbb{T}^2$ ramified only above the origin gives rise to a translation surface (M, ω) whose cohomology class $[\omega]$ belongs to $H^1(M, \Sigma; \mathbb{Z} \oplus \sqrt{-1}\,\mathbb{Z})$, and we suggest the following definition:

Definition 2.1. A *square-tiled surface*, or else an *origami*, is a translation surface corresponding to a covering of the torus $\mathbb{T}^2$ unramified everywhere except, possibly, above the origin[1].

[1]Note that, by definition, it is not compulsory for an origami to be a connected surface.

The torus itself is obtained from a unit square by identifying the opposite sides, and the preimages of that square under the covering $f : M \to \mathbb{T}^2$ provide a tiling of M. Therefore, an origami can be viewed as a finite collection of copies of the unit square $\{z \in \mathbb{C} \mid 0 \le \Re(z), \Im(z) \le 1\}$ together with a gluing of edges: the right edge of each square is identified to the left edge of some square and the top edge of each square is identified to the bottom edge of some square. Examples of origamis represented in such a way are shown in FIGURE 2.2, where **any boundary edge without marking is identified with its opposite boundary edge** (in the horizontal or the vertical direction).

Let $O = (M, \omega)$ be an origami with n squares. This origami can be encoded by a pair of permutations $(\sigma, \tau) \in S_n \times S_n$, where S_n denotes the symmetric group on the set $\{1, \ldots, n\}$. Indeed, number the squares by integers $1, \ldots, n$, and define the permutations as follows[2]:

$\sigma(i) = j$, if the right edge of the ith square is glued to the left edge of the jth one;
$\tau(i) = k$, if the top edge of the ith square is glued to the bottom edge of the kth one.

Since renumbering of the squares causes conjugation of σ and τ by the same permutation, an n-square-tiled surface corresponds to the diagonal conjugacy class of (σ, τ), that is, to an element of the set $(S_n \times S_n)/\mathrm{Inn}(S_n)$ of orbits under the diagonal action of the group of inner automorphisms.

Obviously, the origami O represented by a pair (σ, τ) is connected if only if the permutation subgroup $\mathtt{gp}\{\sigma, \tau\}$ generated by the permutations σ and τ is transitive. Besides, it is the commutator $[\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1}$ that indicates to which stratum the origami belongs: if $[\sigma, \tau]$ is a product of s nontrivial disjoint cycles of lengths $(d_1 + 1)$, …, $(d_s + 1)$, then we have $O \in \mathcal{H}(d_1, \ldots, d_s)$.

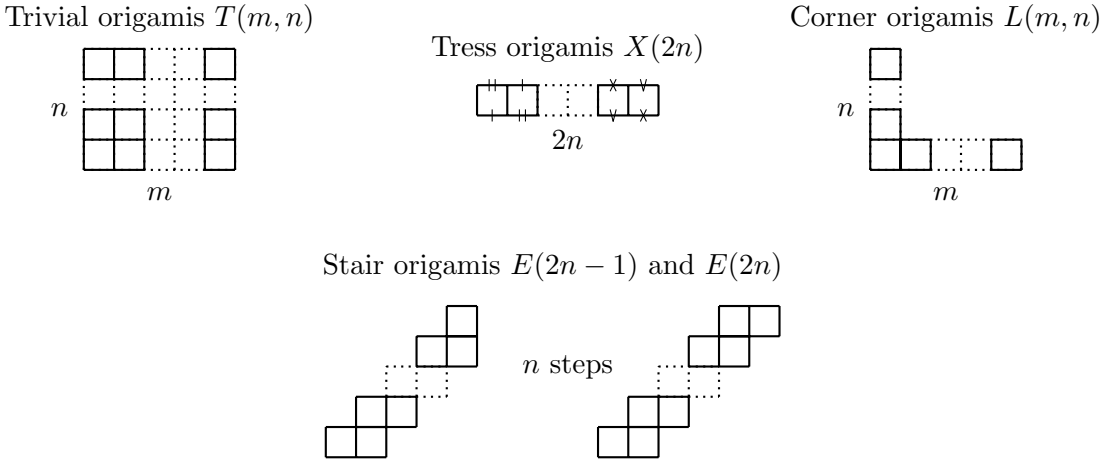


Figure 2.2: Some well-known series of origamis.

Definition 2.2. We call a *monodromy group* of an origami O the group $\mathtt{gp}\{\sigma, \tau\}$ generated by two permutations representing O, and denote it by $\mathcal{M}on(O)$.

In fact, for a given n-square-tiled surface O such a definition does not determine its monodromy group uniquely, but only up to conjugation in S_n. However, what we really mean here is that $\mathcal{M}on(O)$ is being regarded as an abstract group (isomorphism class), and also we keep in mind an embedding into the symmetric group S_n. More precisely, if we have

- a finite two-generator group G,
- a pair of generators (g, h) of G,
- a faithful representation $\rho : G \hookrightarrow S_n$,

[2] If ν is a permutation on a set V, then $\nu(x)$, or $\nu \cdot x$, denotes the image of $x \in V$ under ν.

then the pair of permutations $(\rho(g), \rho(h))$ gives an n-square origami O with $\mathcal{M}on(O) \simeq G$. Furthermore, two triples $(G, (g, h), \rho)$ and $(G, (g, h), \eta)$ correspond to the same origami if and only if the representations ρ and η are equivalent[3].

The monodromy groups of well-known square-tiled surfaces are listed in TABLE 2.1, where C_n is the cyclic group of order n and D_n is the dihedral group of order $2n$. Let us, for example, explain how we found the group of the corner origami $L(m, n)$, where $m, n > 1$. This origami is represented by the permutations $\sigma = (1\ 2\ \ldots\ m)$ and $\tau = (m\ \ m{+}1\ \ \ldots\ \ m{+}n{-}1)$. It is a matter of direct verification (see also [50] for a proof using Jordan's theorem), that $\mathtt{gp}\{\sigma, \tau\}$ is the whole symmetric group S_{m+n-1}, unless both m and n are odd, in which case we get the alternating group A_{m+n-1}.

Table 2.1: Characteristics of some origamis.

Origami	Genus	Stratum	Monodromy group	Primitivity[4]
$T(m, n)$	1	$\mathcal{H}(0)$	$C_m \times C_n$	no, if mn is composite
$X(2n)$	n	$\mathcal{H}(n{-}1, n{-}1)$	$C_n \times D_n$ for n odd	no, if $n > 1$
$L(m, n)$ for $m, n > 1$	2	$\mathcal{H}(2)$	A_{m+n-1} for m, n odd, S_{m+n-1} otherwise	yes
$E(2n{-}1)$	n	$\mathcal{H}(2n{-}2)$	D_{2n-1}	no, if $2n-1$ is composite
$E(2n)$	n	$\mathcal{H}(n{-}1, n{-}1)$	D_{2n}	no, if $n > 1$

The word 'monodromy' is not used by chance. Let $O = (M, \omega)$ be the square-tiled surface corresponding to a covering $f : M \to \mathbb{T}^2$ ramified above 0. If we puncture the origin 0 of the torus and the points on the surface M belonging to the fiber $f^{-1}(0)$, we will obtain an unramified covering $f_0 : M_0 \to \mathbb{T}^2_0$. Consider a point $x \in \mathbb{T}^2_0$, let $\Lambda = f^{-1}(x)$ be the fiber over x, so that $|\Lambda|$ is the number of squares of M. For any loop $\gamma : [0, 1] \to \mathbb{T}^2_0$ based at x and any point $\tilde{x} \in \Lambda$, denote by $\gamma \cdot \tilde{x}$ the endpoint $\tilde{\gamma}(1)$, where $\tilde{\gamma}$ is the lift of γ starting at $\tilde{x}$. This gives a well-defined action of the fundamental group $\pi_1(\mathbb{T}^2_0, x) \simeq F_2$ on the set Λ, that is, a homomorphism $\pi_1(\mathbb{T}^2_0, x) \hookrightarrow Sym(\Lambda)$ into the symmetric group on Λ. The image of this homomorphism is known as the *monodromy group of the covering* f_0 with base point x, and it is isomorphic to $\mathcal{M}on(O)$. Choosing another base point results in conjugating the group.

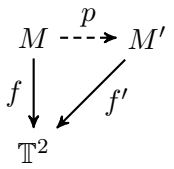
2.3 Primitivity

Let $O = (M, \omega)$ be a connected origami, and $f : M_0 \to \mathbb{T}^2_0$ the corresponding unramified covering of the punctured torus. The preimage $M_0 = f^{-1}(\mathbb{T}^2_0)$ is a finite union of open squares whose closure tile O. Denote by $\mathrm{Sq}(O)$ the set of these squares. The origami O is encoded by two permutations $\sigma, \tau \in Sym(\mathrm{Sq}(O))$ corresponding to gluing to the right and to the top respectively. We say that O

[3] Permutation representations $\rho : G \to Sym(V)$ and $\eta : G \to Sym(V')$ are *equivalent* if there exists a bijection $\lambda : V \to V'$ such that $\lambda(\rho(u) \cdot x) = \eta(u) \cdot \lambda(x)$ for all $u \in G$ and $x \in V$. In the case that $V = V'$ this means the following: for some $\alpha \in Sym(V)$ we have $\eta(u) = \alpha\rho(u)\alpha^{-1}$.

[4] See the definition of primitivity in Section 2.3.

covers an origami $O' = (M', \omega')$ if the following diagram



(2.1)

commutes for a ramified covering p. Moreover, we say that O is a *proper ramified covering* of O' if the degrees of the ramified coverings p and f' are greater than 1. Interpreting the former definition in terms of permutations, we have:

Proposition 2.1. *Consider two connected square-tiled surfaces O and O' represented by permutations $\sigma, \tau \in Sym(\mathrm{Sq}(O))$ and $\sigma', \tau' \in Sym(\mathrm{Sq}(O'))$. The origami O covers the origami O' if and only if there exists a function*

$$\pi : \mathrm{Sq}(O) \to \mathrm{Sq}(O') \text{ such that } \pi \circ \sigma = \sigma' \circ \pi \text{ and } \pi \circ \tau = \tau' \circ \pi.$$

Proof. $(\Longleftarrow)$ Suppose such a function π exists, then it must be surjective since the origami O' is connected (that is, the group $\mathtt{gp}\{\sigma', \tau'\}$ is transitive). Let $\mathrm{Sq}(O) = \{\mathcal{D}_1, \ldots, \mathcal{D}_n\}$. If two squares $\mathcal{D}_i$ and $\mathcal{D}_j$ are glued in one direction, say $\sigma(\mathcal{D}_i) = \mathcal{D}_j$, then so are the squares $\pi(\mathcal{D}_i)$ and $\pi(\mathcal{D}_j)$, as $\pi(\mathcal{D}_j) = \sigma'(\pi(\mathcal{D}_i))$. Therefore, define p to be a mapping from O to O' projecting a square $\mathcal{D}_i$ to $\pi(\mathcal{D}_i)$. This is a ramified covering and we have the commutative diagram (2.1).
$(\Longrightarrow)$ Suppose the diagram (2.1) commutes. If the right (top) edge of a square $\mathcal{D}_i$ of O is glued to the left (bottom) edge of a square $\mathcal{D}_j$, then obviously the same is true for the squares $p(\mathcal{D}_i)$ and $p(\mathcal{D}_j)$ of the origami O'. Therefore, we can take $\pi : \mathcal{D}_i \mapsto p(\mathcal{D}_i)$. □

Definition 2.3. A connected square-tiled surface (M, ω) is called *primitive*[5] if it is not a proper ramified covering of another square-tiled surface.

Let us see what it means in terms of permutations. A nonempty subset Δ of $\Lambda_n = \{1, \ldots, n\}$ is called a *block* for a permutation group $G \subseteq S_n$ if, for each $\alpha \in G$, either $\alpha(\Delta) = \Delta$ or $\alpha(\Delta) \cap \Delta = \emptyset$. In particular, the singletons $\{x\}$ and the whole set Λ_n are blocks, which are called *trivial*. A permutation group G is said to be *primitive* if it has no nontrivial blocks.

It is easy to see that a primitive permutation group is automatically transitive. The inverse is not always true when n is composite: a transitive group can have a nontrivial block Δ, and, if it does, the images $\alpha(\Delta)$ form a G-invariant partition of Λ_n in which all parts have equal size $1 < |\Delta| < n$. In this case $|\Delta|$ must divide n. This observation can also be stated as:

Lemma 2.2. *Let G be a transitive permutation group on V, and $x \in V$. Then G is primitive if and only if the only blocks containing x are $\{x\}$ and V.*

The following lemma and proposition are useful criteria for a group and an origami, respectively, to be primitive:

Lemma 2.3. *A transitive permutation group G on a set V is primitive if and only if the point stabilizers G_x ($x \in V$) are maximal subgroups of G.*

Proof. Recall that in a transitive permutation group all point stabilizers are conjugate.
$(\Longleftarrow)$ If G is not primitive and $\Delta \subset V$ is a nontrivial block, then for any $x \in \Delta$ the subgroup G_x is not maximal, since it is properly contained in the subgroup

$$G_\Delta := \{\alpha \in G \mid \alpha(y) \in \Delta \text{ for any } y \in \Delta\} \neq G.$$

[5] In some articles the notion of primitivity stands for a different property. We will also introduce *reduced* origamis in Section 2.6.

$\Longrightarrow$ Conversely, suppose that a subgroup G_x is not maximal, $G_x \lneq H \lneq G$. Let us show that the orbit $\Delta = H \cdot x$ is a nontrivial block for G. First, $\Delta \neq \{x\}$ and $\Delta \neq G$, since $H \neq G_x$ and $H \neq G$ respectively. Second, if for some $\alpha \in G$ and $\beta, \gamma \in H$ we have $\alpha(\beta(x)) = \gamma(x) \in \Delta$ then $\gamma^{-1}\alpha\beta \in G_x$. Therefore, $\alpha \in H$ and $\alpha(\Delta) = \Delta$. Thus Δ is a nontrivial block for G, and G is not primitive. □

Proposition 2.4. *A connected n-square-tiled surface O is primitive if and only if its monodromy group $\mathcal{M}on(O) \subseteq S_n$ is primitive.*

Proof. Let $(\sigma, \tau) \in S_n \times S_n$ be a pair of permutations corresponding to the n-square-tiled surface O, so that we have $\mathcal{M}on(O) = \mathtt{gp}\{\sigma, \tau\}$.
$\Longrightarrow$ Suppose that the permutation group $G = \mathcal{M}on(O)$ is not primitive, *i.e.* that it has a nontrivial block $\Delta \subset \Lambda_n = \{1, \ldots, n\}$. Denote by $B = \{\Delta_1, \ldots, \Delta_k\}$ the G-orbit of the block Δ, it gives a G-invariant partition of Λ_n, since G is transitive. The action of σ and τ on the set B induces two permutations σ' and τ' from $Sym(B) \simeq S_k$ respectively. Let O' be the origami represented by (σ', τ'). We affirm that the ramified covering $f' : O' \to \mathbb{T}^2$ factorizes the ramified covering $f : O \to \mathbb{T}^2$ (see an example in FIGURE 2.3).

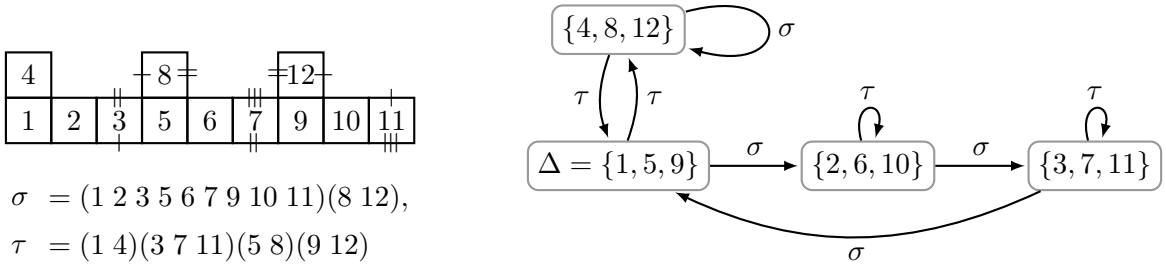
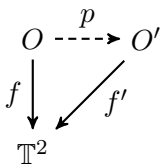


Figure 2.3: The left origami covers the origami induced by the graph on the right.

Indeed, define a map $p : O \to O'$ such that, for all $1 \leq i \leq k$, the squares of O enumerated by integers from the block $\Delta_i \subset \Lambda_n$ project to the Δ_i-th square of O' (*i.e.* the one enumerated by $\Delta_i \in B$). By construction of the origami O', if the right (resp. top) edge of the a-th square of O is identified with the left (resp. bottom) edge of the b-th square of O, then the same is true for the Δ_i-th and Δ_j-th squares of the origami O', where $a \in \Delta_i$ and $b \in \Delta_j$. Thus, the map p is a well-defined ramified covering, and O is not primitive.
$\Longleftarrow$ Conversely, suppose that the following diagram of ramified coverings



commutes for some origami O' different from O and $\mathbb{T}^2$. Let $\mathcal{D} \subset O'$ be the interior of one of the squares by which the surface O' is tiled (the open square $\mathcal{D}$ is projected by f' onto the torus $\mathbb{T}^2$ deprived of two loops). Consider the preimage $p^{-1}(\mathcal{D})$, it is a disjoint union of open squares from the tiling of O. Denote by $\Delta_{\mathcal{D}} \subset \Lambda_n = \{1, \ldots, n\}$ the subset of integers enumerating these squares. Obviously, the set $B = \{\Delta_{\mathcal{D}} \mid \mathcal{D} \text{ is an open square of } O'\}$ forms a nontrivial partition of Λ_n. We want to show that this partition is invariant under the action of the permutations σ and τ and, thus, is G-invariant, where $G = \mathcal{M}on(O) = \mathtt{gp}\{\sigma, \tau\}$. Indeed, for any open square $\mathcal{D}_i \subset O'$, the integers from the set $\sigma(\Delta_{\mathcal{D}_i}) \cup \tau(\Delta_{\mathcal{D}_i})$ correspond to the squares which are glued to the squares of O enumerated

by integers from $\Delta_{\mathcal{D}_i}$. Therefore, we have $\sigma(\Delta_{\mathcal{D}_i}) = \Delta_{\mathcal{D}_j}$ and $\tau(\Delta_{\mathcal{D}_i}) = \Delta_{\mathcal{D}_k}$, where $\mathcal{D}_j$ is the square glued to the right edge of $\mathcal{D}_i$ and $\mathcal{D}_k$ is the one glued to the top edge of $\mathcal{D}_i$. So, the partition B is G-invariant, and the permutation group G is not primitive. □

It is evident that the alternating and symmetric groups of degree $n > 2$ are transitive and primitive. An old conjecture of Eugen Netto [72, 1892], which is now a theorem of John D. Dixon proved in [24, 1969], states that the probability that a random pair of permutations from A_d generates the entire A_d tends to 1 as $d \to \infty$. As László Babai showed in [6, 1989], the probability has the asymptotic form $1 - 1/n + O(1/n^2)$.

Question 2.1. Let p_n be the probability that a random pair (σ, τ) of permutations from S_n, such that the commutator $[\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1}$ is conjugate to a given even permutation, generate S_n or A_n. Is it true that p_n tends to 1 as $n \to \infty$? (For instance, is the following limit

$$\lim_{n\to\infty} \frac{\#\left\{(\sigma,\tau) \in S_n \times S_n \mid [\sigma,\tau] \text{ is a 3-cycle and } \mathrm{gp}\{\sigma,\tau\} = S_n \text{ or } A_n\right\}}{\#\left\{(\sigma,\tau) \in S_n \times S_n \mid [\sigma,\tau] \text{ is a 3-cycle}\right\}}$$

equal to 1, where $\#M$ denotes the cardinal of a set M?)

The following classical theorem will be of interest to us:

Theorem 2.5 (Jordan [52], 1873)**.** *Let G be a primitive subgroup of S_n.*

1. *If G contains a transposition then $G = S_n$.*
2. *If G contains a 3-cycle then $G \supseteq A_n$.*
3. *In general, if G contains a cycle of prime order $p \leqslant n - 3$, then either $G = A_n$ or $G = S_n$.*

We refer the reader to Helmut Wielandt's textbook [98, 1964] for a proof (*e.g.* Theorem 13.9). See also the article [50, 1995] giving an elementary proof in the cases $p = 2$ and 3.

Since the result of Camille Jordan, several generalisations have been achieved. One of them is the theorem below (that can be found in the book [25], see Theorems 5.3A and 5.4A). For a permutation $\sigma \in G$ acting on a set V denote by $\mathrm{supp}(\sigma)$ its *support*, *i.e.* the set of moved points, and let $m(G)$ be the *minimal degree* of G defined as the minimum of $|\mathrm{supp}(\sigma)|$ over all nontrivial elements in G:

$$\mathrm{supp}(\sigma) := \{v \in V \mid \sigma(v) \neq v\} \quad \text{and} \quad m(G) := \min_{\sigma\in G,\, \sigma\neq 1} |\mathrm{supp}(\sigma)|.$$

Theorem 2.6 (Babai [4]-[5], 1981-1982, and Pyber [80], 1991)**.** *For every primitive permutation group G of degree n which does not contain the alternating group, we have $n < 4(m(G))^2$. Moreover, if G is 2-transitive, then $n \leq (m(G) - 1)^2$ and $n \leq 8m(G)$.*

Corollary 2.7. *In the stratum $\mathcal{H}(d_1, \ldots, d_s)$ the monodromy group of any primitive origami with at least $4(s + \sum_{i=1}^{s} d_i)^2$ squares is equal to A_n or S_n.*

The corollary follows from the fact that the commutator of two permutations representing an origami from $\mathcal{H}(d_1, \ldots, d_s)$ is a product of s cycles of orders $(d_1 + 1)$, …, $(d_s + 1)$, and therefore its support contains exactly

$$s + \sum_{i=1}^{s} d_i = s + 2g - 2 = \dim_{\mathbb{C}} \mathcal{H}(d_1, \ldots, d_s) - 1$$

points, where g is the genus of the origami.

Within a fixed stratum, the corollary tells us that for n large enough, all primitive n-square-tiled surfaces will have the monodromy group A_n or S_n. An estimation of the starting moment for n to

have such a property is given by the corollary in an effective way but not optimally. For instance, in the stratum $\mathcal{H}(1,1)$, we have $4(s+\sum_{i=1}^{s} d_i)^2 = 4(2+1+1)^2 = 64$, however, as we shall establish in Section 3.4, the monodromy group of a primitive origami with $n \geqslant 7$ squares must be A_n or S_n (and $7 < 64$).

2.4 Nielsen equivalence and T-systems

An important technical tool of the combinatorial group theory are Nielsen transformations (see [62] or [61]). Recall the definition. Let G be a group and let $(g_1, \ldots, g_k)$ be an ordered k-tuple of its elements. The following operations are called *elementary Nielsen moves*:

(N1) interchange g_i and g_j, where $i \neq j$;

(N2) replace g_i by g_i^{-1};

(N3) replace g_i by $g_i g_j$ or $g_j g_i$, where $i \neq j$.

A composition of such elementary operations is a *Nielsen transformation*. The set of Nielsen transformations of $G^k = \underbrace{G \times \ldots \times G}_{k}$ is denoted by $\mathrm{NT}(G^k)$. One has a well-defined equivalence relation on G^k: two k-tuples $\mathfrak{g}$ and $\mathfrak{g}'$ of elements of G are said to be *Nielsen equivalent* if there exists a Nielsen transformation mapping one tuple to another. Write $\mathfrak{g} \overset{\mathrm{N}}{\sim} \mathfrak{g}'$. Notice that the set $\mathrm{NT}(G^k)$ forms a subgroup of permutations on G^k, and the Nielsen equivalence classes are the transitivity sets for this subgroup.

Besides, a Nielsen transformation carries any *generating vector* (that is, a tuple of elements which generates G) to a generating vector. In particular, a Nielsen transformation of a free basis of the free group F_k defines an automorphism of F_k: with a Nielsen transformation sending $(x_1, \ldots, x_k)$ to $(y_1, \ldots, y_k)$ we associate the automorphism $(x_1, \ldots, x_k) \mapsto (y_1, \ldots, y_k)$. Let $x_1, \ldots, x_k$ be a free basis of F_k, the following automorphisms are called *elementary*:

(A1) $x_i \mapsto x_j,\ x_j \mapsto x_i,\ x_l \mapsto x_l\ (l \neq i, j)$;

(A2) $x_i \mapsto x_i^{-1},\ x_l \mapsto x_l\ (l \neq i)$;

(A3) $x_i \mapsto x_i x_j$ or $x_j x_i,\ x_l \mapsto x_l\ (l \neq i)$.

The classical results of Jacob Nielsen give us valuable information about the free group $F_2 = \langle x, y \rangle$ of rank two:

Theorem (Nielsen [75], 1917)**.**

1. *The automorphism group* $\mathrm{Aut}(F_2)$ *is generated by the elementary automorphisms on* x, y*, and all pairs of generators of* F_2 *form a single Nielsen equivalence class.*

2. (Nielsen's commutator test) *A pair* (a, b) *of elements of* F_2 *is Nielsen equivalent to* (x, y) *if and only if* $[a, b]$ *is conjugate to* $[x, y]^{\pm 1}$.

3. *One has an exact sequence*

$$0 \to \mathrm{Inn}(F_2) \longrightarrow \mathrm{Aut}(F_2) \xrightarrow{\Phi} \mathrm{GL}(2, \mathbb{Z}) \to 0,$$

for the homomorphism

$$\Phi : \gamma \longmapsto \begin{pmatrix} e_x(\gamma(x)) & e_x(\gamma(y)) \\ e_y(\gamma(x)) & e_y(\gamma(y)) \end{pmatrix},$$

where $e_x(w)$ and $e_y(w)$ are the sums of the exponents of x and y, respectively, in the word $w \in F_2$.

The first statement of this theorem holds for a free group of any finite rank (also proved by Nielsen, see [76]): the group $\mathrm{Aut}(F_k)$ is generated by the elementary automorphisms on a free basis. We would like to make three important remarks, of which the reader should be aware:

1– It is easy to check that if an elementary Nielsen move sends a pair (g, h) of elements of a group G to (g', h'), then $[g, h]$ is conjugate to $[g', h']^{\pm 1}$. This observation gives us the first invariant of the Nielsen equivalence classes, namely, the union of two conjugacy classes $[g, h]^G \cup [h, g]^G$, where u^G stands for the set $\{g^{-1}ug \mid g \in G\}$. For instance, in the alternating group A_5 the commutator of a generating pair is either a 3-cycle or a 5-cycle. Since both can occur, for $[(1\ 2\ 3), (1\ 2\ 3\ 4\ 5)] = (1\ 2\ 4)$ and $[(1\ 3\ 4\ 2\ 5), (1\ 2\ 3\ 4\ 5)] = (1\ 4\ 5\ 2\ 3)$, there are at least two nontrivial Nielsen equivalence classes in A_5.

   Using the commutator invariant, Robert Guralnick and Igor Pak [34] showed that the number of Nielsen classes in $\mathrm{PSL}(2, \mathbb{F}_p)$ is unbounded as $p \to \infty$. Such a result was generalised by Shelly Garion and Aner Shalev [30] to other families of finite simple groups. As for the case that G is infinite, in particular we know that the group of a torus knot $G(p, q) = \langle g, h \mid g^p = h^q \rangle$, where $p, q > 1$ and $p + q > 4$, has infinitely many distinct Nielsen classes of generating pairs (Heiner Zieschang [100]).

   In contrast to the case of F_2, the commutator invariant is not always complete. For example, in the alternating group A_6 the permutations $\sigma = (1\,3\,6)$, $\tau = (1\,2\,3\,4\,5)$ and $\sigma' = (1\,3)(2\,6)$, $\tau' = (1\,2\,6\,4\,5)$ satisfy $[\sigma, \tau] = [\sigma', \tau'] = (1\,3\,6\,4\,2)$. However, the generating pairs (σ, τ) and (σ', τ') belong to distinct Nielsen classes (and even to distinct T-systems, a consequence of calculations by Daniel Stork [89]).

2– Let us illustrate an easy criterion for two tuples to be Nielsen equivalent (confining ourselves to the case $k = 2$). Consider a two-generator group G, and let (g, h) and (g', h') be two generating pairs of G (see FIGURE 2.4). By Nielsen's theorem, given free bases (x, y) and (x', y') of F_2, there always is a sequence $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_m$ of elementary Nielsen moves carrying the pair (x, y) to (x', y'). Applying analogous moves to (g, h) we will get another generating pair (g_m, h_m), and

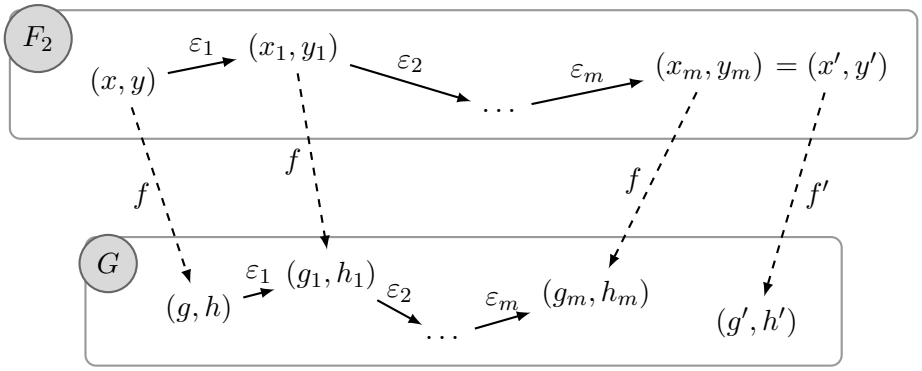


Figure 2.4: Nielsen equivalence classes.

it will coincide with (g', h') if and only if the epimorphism $f : F_2 \twoheadrightarrow G, x \mapsto g, y \mapsto h$ also sends the pair (x', y') to (g', h').

3– We already mentioned that a Nielsen transformation of a free basis of F_k gives rise to an element of $\mathrm{Aut}(F_k)$. We are going to give a generalisation to this, as a corollary to an easy but fundamental theorem of Walther Dyck (see [20], page 8).

Theorem (Dyck [26], 1882)**.** *Let $H = \langle X;\, R\rangle$ and K be groups. Given a mapping $\psi : X \to K$ there exists a homomorphism $\Psi : H \to K$ such that*

$$\Psi(x) = \psi(x) \quad \textit{for any } x \in X$$

if and only if the set $\psi(X) \subset K$ satisfies the relations R. Moreover, the homomorphism Ψ is uniquely determined.

Proof. $(\Longleftarrow)$ For any $x_1, \ldots, x_k \in X$ and $\epsilon_1, \ldots, \epsilon_k \in \{-1, 1\}$, we put $\Psi(x_1^{\epsilon_1} \cdot \ldots \cdot x_k^{\epsilon_k}) = \psi(x_1)^{\epsilon_1} \cdot \ldots \cdot \psi(x_k)^{\epsilon_k}$. As soon as ψ preserves the relations R, the mapping Ψ is well-defined and a homomorphism. It is unique, because X generates H. $(\Longrightarrow)$ Obvious. □

Since an action of a group H on a set V is given by a homomorphism from H to the symmetric group $Sym(V)$, we immediately obtain:

Corollary 2.8. *Let $H = \langle X \mid (R_k(X))_{k\in K}\rangle$ be a presentation of H with $X = (x_i)_{i\in I}$. Suppose that to each generator $x_i \in X$ corresponds a permutation α_i of a finite set V. Then these permutations determine (uniquely) an action of the group H on the set V if and only if $R_k((\alpha_i)_{i\in I})$ is the identity permutation of V for all $k \in K$.*

We have the following corollary (*cf.* [62], p. 134):

Corollary 2.9. *Let $G = \langle g_1, \ldots, g_k;\, R\rangle$ be a hopfian[6] group, and let $\psi : G^k \to G^k$ be a Nielsen transformation sending the tuple $(g_1, \ldots, g_k)$ to $(h_1, \ldots, h_k)$. There exists an automorphism Ψ of G such that*

$$\Psi(g_i) = h_i \quad \textit{for any } 1 \le i \le k$$

if and only if the tuple $(h_1, \ldots, h_k)$ satisfies the relations R.

Proof. $(\Longleftarrow)$ Suppose that the tuple $(h_1, \ldots, h_k)$ satisfies the relations R. Then, according to Dyck's theorem, there exists a homomorphism $\Psi : G \to G$ with the property that $\Psi(g_i) = h_i$ for any $1 \le i \le k$. It is surjective, because $(h_1, \ldots, h_k)$ is a generating vector of G. Since the group G is hopfian, the epimorphism Ψ must be automorphism.
$(\Longrightarrow)$ Conversely, if there exists such an automorphism $\Psi \in \mathrm{Aut}(G)$, then for any relation $W(g_1, \ldots, g_k) = 1$ we automatically have $W(h_1, \ldots, h_k) = \Psi(W(g_1, \ldots, g_k)) = 1$. □

Let G be a finite group, let $d(G)$ be the minimal number of generators in G, and for $k \ge d(G)$ denote by $\mathcal{G}_k(G)$ the set of k-tuples generating G. The group $\mathrm{Aut}(F_k)$ acts on this set by Nielsen transformations, and the orbits are just the Nielsen equivalence classes. More accurately, if we fix a free basis $(x_1, \ldots, x_k)$ of F_k, then $\mathcal{G}_k(G)$ can be identified with the set of epimorphisms $\mathrm{Epi}(F_k, G) = \{f : F_k \twoheadrightarrow G\}$. Indeed, a surjective homomorphism f sends $(x_1, \ldots, x_k)$ to a generating k-tuple of the group G, and any generating k-tuple of G is obtained in such a way due to the universal property of the free groups. From this point of view, the *left* action of $\mathrm{Aut}(F_k)$ on $\mathcal{G}_k(G)$ is given by composition

$$\gamma \cdot f = f \circ \gamma^{-1} \quad \text{for } \gamma \in \mathrm{Aut}(F_k) \text{ and } f \in \mathrm{Epi}(F_k, G).$$

[6] A group is called *hopfian* if it is not isomorphic to any of its proper quotients. For instance, finite groups and finitely-generated free groups are hopfian. In 1951, Graham Higman discovered a non-hopfian group G and a Nielsen transformation $\psi : (g_1, \ldots, g_k) \mapsto (h_1, \ldots, h_k)$ such that the tuple $(h_1, \ldots, h_k)$ satisfies the relations of G but an automorphism Ψ as in Corollary 2.9 does not exist.

This action defines the same permutation subgroup on the set $\mathcal{G}_k(G)$ that the left action of $\mathrm{NT}(G^k)$ does. Take, for instance, the automorphisms $\gamma_1 : x \mapsto x,\ y \mapsto yx^{-1}$ and $\gamma_2 : x \mapsto xy^{-1},\ y \mapsto y$ of the free group F_2, and compare them to the Nielsen transformations $\varepsilon_1 : (g,h) \mapsto (g,hg)$ and $\varepsilon_2 : (g,h) \mapsto (gh,h)$. Since we have

$$(x,y) \overset{\gamma_1^{-1}}{\longmapsto} (x,yx) \overset{\gamma_2^{-1}}{\longmapsto} (xy,yxy),$$

$$\begin{array}{ccccc} \gamma_1\gamma_2 \cdot [\,(x,y) \overset{f}{\longmapsto} (g,h)\,] & = & \gamma_1 \cdot [\,(x,y) \overset{f\circ\gamma_2^{-1}}{\longmapsto} (gh,h)\,] & = & [\,(x,y) \overset{f\circ\gamma_2^{-1}\circ\gamma_1^{-1}}{\longmapsto} (gh,hgh)\,] \\ \varepsilon_1\varepsilon_2 \cdot (g,h) & = & \varepsilon_1 \cdot (gh,h) & = & (gh,hgh), \end{array},$$

the permutations of $\mathcal{G}_k(G)$ induced by $\gamma_1, \gamma_2, \gamma_1\gamma_2$ and $\varepsilon_1, \varepsilon_2, \varepsilon_1\varepsilon_2$ respectively are the same.

In fact, extending this reasoning to the action of $\mathrm{Aut}(F_k)$ on the set G^k by considering the set of all homomorphisms $\mathrm{Hom}(F_k, G)$ instead of $\mathrm{Epi}(F_k, G)$, we obtain an epimorphism

$$\mathrm{Aut}(F_k) \twoheadrightarrow \mathrm{NT}(G^k). \tag{2.2}$$

And also we have $\mathrm{Aut}(F_k) \twoheadrightarrow \mathrm{NT}(\mathcal{G}_k(G))$ as a restriction of (2.2).

Now, consider the diagonal action of the group $\mathrm{Aut}(G)$ on $\mathcal{G}_k(G)$. This action commutes with that of the group $\mathrm{Aut}(F_k)$, as we have

$$\varphi \cdot (\gamma \cdot f) = \varphi \circ f \circ \gamma^{-1} \quad \text{for } \varphi \in \mathrm{Aut}(G),\ \gamma \in \mathrm{Aut}(F_k) \text{ and } f \in \mathrm{Epi}(F_k, G).$$

The orbits of the product $\mathrm{Aut}(F_k) \times \mathrm{Aut}(G)$ acting on the set $\mathcal{G}_k(G)$ are called the *systems of transitivity* (or *T_k-systems*) of G. As a result, we have got new equivalence classes, larger than the Nielsen ones: two generating vectors $\mathfrak{g} = (g_1, \ldots, g_k)$ and $\mathfrak{g}' = (g'_1, \ldots, g'_k)$ lie in the same T_k-system if and only if there exist an automorphism γ of F_k and an automorphism φ of G such that $\mathfrak{g}' = \varphi \cdot (\gamma \cdot \mathfrak{g})$.

We denote the set of $\mathrm{Aut}(G)$-orbits on $\mathcal{G}_k(G)$ by $\widehat{\mathcal{G}}_k(G)$.

Another way to obtaining the systems of transitivity comes from the action of $\mathrm{Aut}(F_k)$ on the set of G-defining subgroups of F_k. A *G-defining subgroup* of F_k is a normal subgroup N such that F_k/N is isomorphic to G. Clearly such subgroups are in one-to-one correspondence with the $\mathrm{Aut}(G)$-orbits of $\mathcal{G}_k(G)$, and the action of $\mathrm{Aut}(F_k)$ on $\widehat{\mathcal{G}}_k(G)$ is equivalent to its action on G-defining subgroups. For if we have an exact sequence

$$1 \to N \longrightarrow F_k \xrightarrow{f} G \to 1,$$

then, for any automorphism $\gamma \in \mathrm{Aut}(F_k)$,

$$1 \to \gamma(N) \longrightarrow F_k \xrightarrow{f\circ\gamma^{-1}} G \to 1$$

is an exact sequence as well.

Systems of transitivity were introduced by Bernhard H. Neumann and Hanna Neumann in [73], where they also discuss the significance of T-systems. A connection with the product replacement algorithm and an overview of results can be found in Igor Pak's article [79].

2.5 Real Veech groups

There is a natural action of $\mathrm{GL}^+(2, \mathbb{R})$ on the moduli space $\Omega\mathcal{M}_g$. Let A be a real matrix and (M, ω) a translation surface. The new surface $A \cdot (M, \omega) = (M, A \cdot \omega)$ is defined in local coordinates as follows:

$$\text{if } (U, v) \text{ is a chart for } \omega, \text{ then } (U, A \circ v) \text{ is a chart for } A \cdot \omega,$$
$$\text{where } v : U \to \mathbb{C} \text{ and } A \circ v : U \xrightarrow{v} \mathbb{C} \simeq \mathbb{R}^2 \xrightarrow{A} \mathbb{R}^2 \simeq \mathbb{C}.$$

If the translation surface is presented as a polygon in the real plane, then the action is effectuated in a common way (see FIGURE 2.5). The orientation of M being induced by the complex structure, any matrix $A \in \mathrm{GL}^+(2, \mathbb{R})$ preserves it.

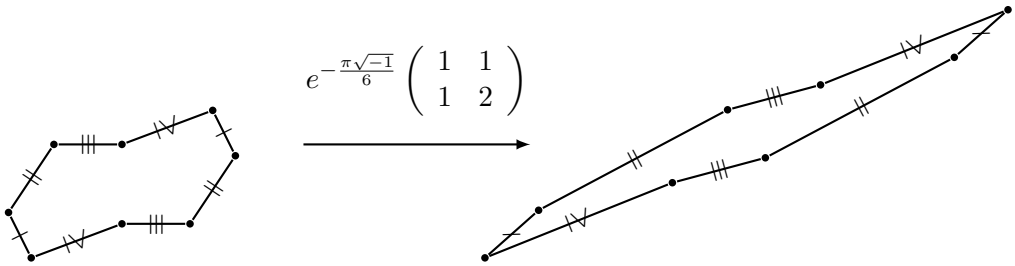


Figure 2.5: Action of a matrix on a translation surface.

As is easy to check, the $\mathrm{GL}^+(2, \mathbb{R})$-action on $\Omega\mathcal{M}_g$ doesn't change orders of the zeros of holomorphic 1-forms, and thus descents to an action on each stratum. The stabilizer of a translation surface (M, ω) is called its (*real*) *Veech group*. We will denote it by

$$\Gamma(M, \omega) := \mathrm{Stab}_{\mathrm{GL}^+(2,\mathbb{R})}(M, \omega).$$

Note that translation surfaces are endowed with a choice of vertical direction. For instance, the origamis $\square\square$ and $\begin{smallmatrix}\square\\\square\end{smallmatrix}$ differ while isomorphic as Riemann surfaces.

Let us mention the action of some subgroups of $\mathrm{GL}^+(2, \mathbb{R})$:

- ▷ the special linear group $\mathrm{SL}(2, \mathbb{R})$ preserves area;
- ▷ the diagonal group $\left\{ \begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix}, t \in \mathbb{R} \right\}$ rescales the surface;
- ▷ the special orthogonal group $\mathrm{SO}(2, \mathbb{R})$ rotates the surface (or else its vertical direction), and corresponds to multiplying the holomorphic 1-form by a complex number of norm one;
- ▷ the diagonal group $\left\{ \begin{pmatrix} e^t & 0 \\ 0 & e^{-t} \end{pmatrix} \right\}$ acts continuously on each stratum and induces a natural flow, which is called the *Teichmüller geodesic flow*. A theorem of Howard Masur and William A. Veech states that both actions of this group and the group $\mathrm{SL}(2, \mathbb{R})$ are ergodic on connected components of normalized strata with respect to a well-defined measure (see [65], [94], and also the survey [102] of Anton Zorich, pp. 464-465). Moreover, Artur Avila, Sébastien Gouëzel and Jean-Christophe Yoccoz [3] proved the exponential rate of mixing for the Teichmüller geodesic flow.
- ▷ the parabolic groups $\left\{ \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \right\}$ and $\left\{ \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} \right\}$ shear the charts of the surface horizontally and vertically, respectively, and determine the *horocycle flows* in strata.

Veech groups have been intensively studied since the late 1980s (*e.g.* [95]), in particular, with the purpose of classifying closures of orbits of translation surfaces in a given stratum. Recently, the closures of the $\mathrm{SL}(2, \mathbb{R})$-orbits of elements $(M, \omega) \in \Omega\mathcal{M}_g$ were fully described by Curtis T. McMullen (see [68]) for genus $g = 2$. In the general case, this is an open problem.

In fact, the Veech group of a translation surface (M,ω) is the derivative of its affine group. The *affine group* $\mathrm{Aff}^+(M,\omega)$ is defined to be the subgroup of orientation-preserving homeomorphisms of the surface M which keep the set Σ of zeros of ω invariant and which are given by affine maps in the charts $(U, z : P \mapsto \int_{P_0}^{P} \omega)$ outside Σ. So, an element $f \in \mathrm{Aff}^+(M,\omega)$ can be locally written as

$$f : z \mapsto A \circ z + c \quad \text{for some } A \in \mathrm{SL}(2,\mathbb{R}) \text{ and } c \in \mathbb{C},$$

where the matrix A is independent of the charts, since all transition maps are translations. This provides a homomorphism

$$D : \mathrm{Aff}^+(M,\omega) \to \mathrm{SL}(2,\mathbb{R}),$$

and the Veech group of the surface is just the image of D. One has an exact sequence

$$1 \to \mathrm{Aut}(M,\omega) \longrightarrow \mathrm{Aff}^+(M,\omega) \xrightarrow{D} \Gamma(M,\omega) \to 1,$$

where $\mathrm{Aut}(M,\omega)$ is the *automorphism group* of (M,ω), consisting of those homeomorphisms of M which preserve Σ and induce translations in the charts.

Martin Möller shows in [70] that the affine group of a generic surface of genus $g \geq 2$ is trivial or isomorphic to $\mathbb{Z}/2$, where 'genericity' (in a stratum) means 'all outside a countable union of real codimension one submanifolds'. Therefore, the real Veech group of a translation surface from a stratum $\mathcal{H}(d_1,\ldots,d_s) \neq \mathcal{H}(0)$ almost surely is trivial or $\{\pm I\}$.

Special attention has been paid to investigation of several properties of the Veech group of a connected translation surface:

- $\Gamma(M,\omega)$ is always a *discrete* subgroup of $\mathrm{SL}(2,\mathbb{R})$, this fact is originally due to Veech [95], an easy proof can be found in the article [96] of Yaroslav Vorobets;

- $\Gamma(M,\omega)$ is *never cocompact*, that is, in the natural quotient topology the space $\mathrm{SL}(2,\mathbb{R})/\Gamma(M,\omega)$ is not compact (see [46]);

- if $\Gamma(M,\omega)$ is a *lattice* in $\mathrm{SL}(2,\mathbb{R})$, that is, the quotient $\mathrm{SL}(2,\mathbb{R})/\Gamma(M,\omega)$ is of finite volume, then (M,ω) is called a *Veech surface*. A theorem of John Smillie states that in this case and only this case the $\mathrm{GL}^+(2,\mathbb{R})$-orbit of (M,ω) is closed in its stratum (for a proof, see the paper [69] of Yair Minsky and Barak Weiss).

  Speaking of the geometry of Veech surfaces, let us first recall some notions. By a *direction* δ on a given translation surface we mean the pullback of the straight lines of slope δ from $\mathbb{R}^2 \simeq \mathbb{C}$ using the charts. A *linear flow* $\mathcal{F}_\delta$ on (M,ω) is the map from $M \times \mathbb{R}^+$ to M sending a pair (P,t) to the point P_t such that the line segment from P to P_t has direction δ and length t. A *saddle connection* is a geodesic segment for the flat metric $|\omega|$ joining a zero of ω to another one (or to itself), and not containing any zero in its interior. The saddle connections lie on orbits of the flows $\mathcal{F}_\delta$ and bound *cylinders*, that is, maximal connected sets of homotopic simple closed geodesics. The *modulus* of a cylinder equals $\mu = h/l$, where h is its height and l is its circumference.

  The linear flow $\mathcal{F}_\delta$ is called *periodic* if in the direction δ the surface decomposes into a finite number of cylinders. The following important result is referred to as the Veech dichotomy or alternative (see also [96]):

  Theorem (**Veech dichotomy** [95]). *If (M,ω) is a Veech surface, then for each direction δ the flow $\mathcal{F}_\delta$ is either uniquely ergodic or periodic with commensurable moduli of cylinders (i.e. the ratio of any two moduli is rational).*

- if $\Gamma(M,\omega)$ is *arithmetic*, that is, commensurable[7] to $\mathrm{SL}(2,\mathbb{Z})$, then the translation surface (M,ω) is in the $\mathrm{SL}(2,\mathbb{R})$-orbit of an origami. This fact together with the converse statement, which is true, compose the well-known theorem of Eugene Gutkin and Chris Judge, see the papers [35] and more detailed [36]. A proof different from the original one is given in [45].

2.6 Actions of $\mathrm{GL}(2,\mathbb{Z})$ on origamis

The action of the real special linear group $\mathrm{SL}(2,\mathbb{R})$ on translation surfaces descends to an action of $\mathrm{SL}(2,\mathbb{Z})$ on square-tiled surfaces. This comes from the following fact: if all relative periods of ω are integer-valued (*i.e.* $\int_{Z_j}^{Z_k}\omega \in \mathbb{Z}\oplus\sqrt{-1}\,\mathbb{Z}$ for any $Z_j, Z_k \in \Sigma$), then so are those of $A\circ\omega$ for any $A\in\mathrm{SL}(2,\mathbb{Z})$. In the real plane one applies a 'cut-and-glue' procedure to picture how an integer matrix acts on an origami (see FIGURE 2.6, where parallel edges with the same marking are identified).

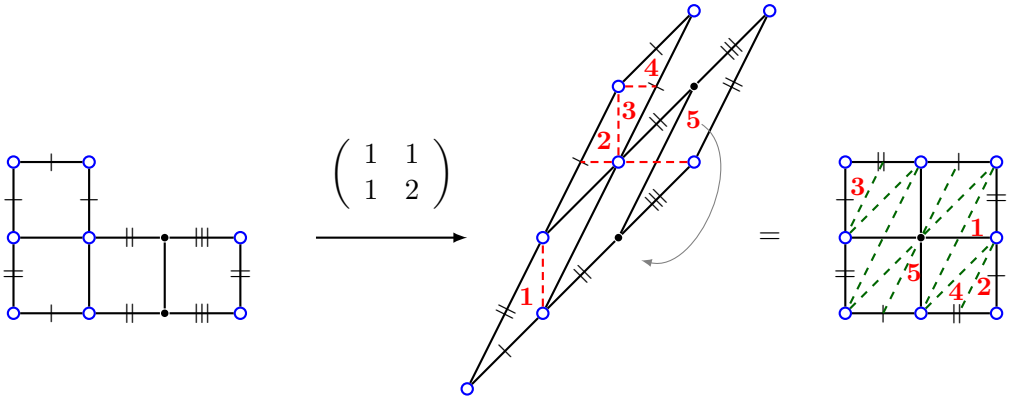


Figure 2.6: Action of a matrix on an origami.

Given a connected square-tiled surface (M,ω), the linear combinations of the relative periods $\int_{Z_j}^{Z_k}\omega$ with integer coefficients form a subgroup of $\mathbb{Z}\oplus\sqrt{-1}\,\mathbb{Z}$, which is called the *lattice of periods* of ω and denoted by $\mathrm{Per}(\omega)$. The map p from M to the torus $\mathbb{C}/\mathrm{Per}(\omega)$ defined by

$$p : P \mapsto \left(\int_{Z_1}^{P}\omega\right) \mod \mathrm{Per}(\omega), \qquad \text{for any } P\in M \text{ and a fixed zero } Z_1 \text{ of } \omega,$$

is a covering ramified over 0. We have a commutative diagram

$$\begin{array}{ccc} (M,\omega) & \overset{p}{\longrightarrow} & (\mathbb{C}/\mathrm{Per}(\omega),\, dz) \\ {\scriptstyle f}\downarrow & \swarrow_{f'} & \\ (\mathbb{T}^2, dz) & & \end{array}$$

where the degree of f' equals $[\mathbb{Z}\oplus\sqrt{-1}\,\mathbb{Z} : \mathrm{Per}(\omega)]$.

[7] In a group G two subgroups H and K are *commensurable* when for some G-conjugate H^g the intersection $H^g\cap K$ has finite index both in H^g and K.

A connected origami will be called *reduced* when $\mathrm{Per}(\omega) = \mathbb{Z} \oplus \sqrt{-1}\,\mathbb{Z}$. Thus, reduced square-tiled surfaces are exactly those surfaces which do not cover a torus of area > 1 with one branch point. For example, all primitive origamis are automatically reduced.

In theory, classification of square-tiled surfaces is brought to that of reduced surfaces. This is explained by the first of the following properties:

a) *Any origami belongs to the* $\mathrm{GL}^+(2, \mathbb{Q})$*-orbit of a reduced one.* Indeed, for a square-tiled surface (M, ω) let (e_1, e_2) be a basis of the lattice $\mathrm{Per}(\omega)$ over $\mathbb{Z}$ and let A be the rational matrix sending this basis to $(1, \sqrt{-1})$. Then the origami $A \cdot (M, \omega)$ is reduced, because $\mathrm{Per}(A \cdot \omega) = A \cdot \mathrm{Per}(\omega) = \mathbb{Z} \oplus \sqrt{-1}\,\mathbb{Z}$.

b) *For any reduced origami* (M, ω)*, its real Veech group is a subgroup of* $\mathrm{SL}(2, \mathbb{Z})$. Indeed, if a matrix A preserves the origami, then it sends a saddle connection to a saddle connection and, thus, preserves the lattice $\mathrm{Per}(\omega) = \mathbb{Z} \oplus \sqrt{-1}\,\mathbb{Z}$. (One just has $A \cdot \mathrm{Per}(\omega) = \mathrm{Per}(A \cdot \omega) = \mathrm{Per}(\omega) = \mathbb{Z} \oplus \sqrt{-1}\,\mathbb{Z}$.)

c) *The* $\mathrm{SL}(2, \mathbb{Z})$*-orbit of a reduced origami* (M, ω) *consists of all reduced origamis in its* $\mathrm{SL}(2, \mathbb{R})$*-orbit.* Indeed, another square-tiled surface $(M, A \cdot \omega)$ with $A \in \mathrm{SL}(2, \mathbb{R})$ is reduced if and only if $A \cdot \mathrm{Per}(\omega) = \mathbb{Z} \oplus \sqrt{-1}\,\mathbb{Z} = \mathrm{Per}(\omega)$, that is, $A \in \mathrm{SL}(2, \mathbb{Z})$.

In view of the property b), one is interested in finding *integer Veech groups* of square-tiled surfaces, namely, the following groups

$$\mathrm{SL}(M, \omega) := \mathrm{Stab}_{\mathrm{SL}(2,\mathbb{Z})}(M, \omega) \quad \text{and} \quad \mathrm{GL}(M, \omega) := \mathrm{Stab}_{\mathrm{GL}(2,\mathbb{Z})}(M, \omega).$$

We are now going to describe two actions of the integer linear group $\mathrm{GL}(2, \mathbb{Z})$, having the presentation (2.3) below, on the set $(S_n \times S_n)^*$ of conjugacy classes of pairs, that is, on the set of n-square origamis. The first one – the natural (or else direct) action '$\cdot$' – is the restriction of the natural action of $\mathrm{GL}(2, \mathbb{R})$ on the moduli space $\Omega\mathcal{M}_g$, it will be given by (2.4). The second one – the dual action '$\times$' – corresponds to Nielsen transformations through the isomorphism $\mathrm{GL}(2, \mathbb{Z}) \simeq \mathrm{Aut}(F_2)/\mathrm{Inn}(F_2)$, it will be defined by the diagram (2.5). Stabilizers for the two actions will be related by (2.6). An important property of the actions, as we will see, is that they don't change the monodromy group of an origami.

The natural action of $\mathrm{GL}(2, \mathbb{Z})$**.** Moving towards the description of a $\mathrm{GL}(2, \mathbb{Z})$-action, let us introduce the matrices

$$J = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} - \text{ axial symmetry}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} - \text{ horizontal shear},$$

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} - \text{ rotation by } \pi/2, \quad U = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} - \text{ vertical shear}.$$

As is well-known, the group $\mathrm{GL}(2, \mathbb{Z})$ is generated by J and any two of the other three matrices. Consider the following presentations:

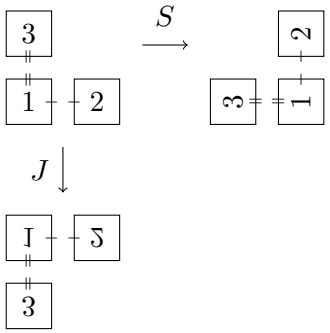
$$\begin{array}{rcl} \mathrm{SL}(2, \mathbb{Z}) & = & \langle T, U \mid TUT = UTU,\ (TUT)^4 \rangle, \\ \mathrm{GL}(2, \mathbb{Z}) & = & \langle T, U, J \mid TUT = UTU,\ (TUT)^4,\ J^2,\ (JT)^2,\ (JU)^2 \rangle. \end{array} \tag{2.3}$$

We already mentioned that the natural action of the group $\mathrm{SL}(2, \mathbb{R})$ on the moduli spaces gives an action of the group $\mathrm{SL}(2, \mathbb{Z})$ on the square-tiled surfaces. Defining in the standard manner an orientation-reversing action of the matrix J, one gets an action of the general linear group $\mathrm{GL}(2, \mathbb{Z})$ on the origamis. We call this action *direct* and write it as $A \cdot (M, \omega)$.

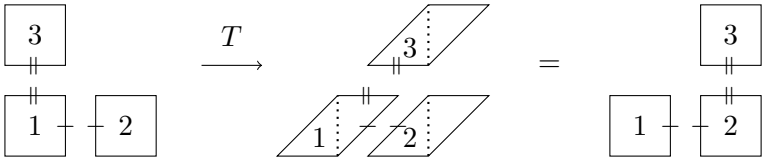
Let O be a square-tiled surface encoded by a pair of permutations $(\sigma, \tau) \in S_n \times S_n$, we write $O = (\sigma, \tau)^*$, where $(\sigma, \tau)^* = \left\{(\mu^{-1}\sigma\mu, \mu^{-1}\tau\mu) \mid \mu \in S_n\right\}$ denotes the conjugacy class of (σ, τ). Our affirmation is that the matrices above act on the origami O in the following way:

$$\begin{aligned} J \cdot (\sigma, \tau)^* &= (\sigma, \tau^{-1})^* \\ S \cdot (\sigma, \tau)^* &= (\tau^{-1}, \sigma)^* \\ T \cdot (\sigma, \tau)^* &= (\sigma, \tau\sigma^{-1})^* \\ U \cdot (\sigma, \tau)^* &= (\sigma\tau, \tau)^*. \end{aligned} \tag{2.4}$$

This can be rapidly checked by considering a geometric presentation of the origami $O = (\sigma, \tau)^*$ in the real plane. The matrix J reflects the squares with respect to the first coordinate axis, the matrix S performs a counterclockwise rotation around the origin by angle $\pi/2$ as shown in the figure.



The matrix T shears the squares horizontally, and we have to apply a cut-and-glue procedure: the new ith square will contain the image of the bottom left triangle of the old ith square. Likewise we do for U, which is a vertical shear.



Therefore, the equalities (2.4) are correct. Moreover, just by looking at the actions of J, T and U, we draw an important conclusion[8]:

the monodromy group $\mathcal{M}on(O)$ ***is an invariant of the*** $\mathrm{GL}(2, \mathbb{Z})$***-orbit of*** O***.***

To be specific, $\mathcal{M}on(O) = \mathtt{gp}\{\sigma, \tau\}$ gets conjugated inside S_n when another conjugacy class representative (σ, τ) for the origami O is chosen, but it does not change whatsoever as an abstract group.

Generalities: direct and dual actions of $\mathrm{GL}(2, \mathbb{Z})$**.** Recall that, for any group G, we have a left action of $\mathrm{Aut}(F_2)$ on the set $G \times G$ by Nielsen transformations. It is given by

$$\gamma \cdot (g, h) := (w_1(g, h), w_2(g, h)), \quad \text{for any } \gamma \in \mathrm{Aut}(F_2), \text{ such that } \gamma^{-1} : \begin{pmatrix} x \mapsto w_1(x, y) \\ y \mapsto w_2(x, y) \end{pmatrix}, \quad \text{and any } (g, h) \in G \times G.$$

Since generators of the linear groups satisfy non-redundant relations, one cannot define a non-trivial model action of $\mathrm{GL}(2, \mathbb{Z})$ on $G \times G$ as we did for $\mathrm{Aut}(F_2)$. However, we shall introduce a $\mathrm{GL}(2, \mathbb{Z})$-action on the set $(G \times G)^* = (G \times G)/\mathrm{Inn}(G)$ of conjugacy classes of pairs, by means of a commutative diagram

[8] Announced by the author during his talk at the workshop *Dynamics in the Teichmüller space*, Roscoff, France, June 2008.

$$\begin{array}{ccc} \mathrm{Aut}(F_2) \times (G \times G) & \longrightarrow & G \times G \\ \downarrow & & \downarrow \\ \mathrm{GL}(2,\,\mathbb{Z}) \times (G \times G)^* & \longrightarrow & (G \times G)^* \end{array} \tag{2.5}$$

It is constructed in details as follows:

$$\begin{array}{ccc} (\gamma,\,(g,h)) & \longmapsto & (g',h') \\ \downarrow & & \downarrow \\ (A,\,(g,h)^*) & \longmapsto & (g',h')^* \end{array}$$

where $(g,h)^*$ denotes the conjugacy class of a pair (g,h), and

- γ is an automorphism of $F_2 = \langle x, y\rangle$ such that $\gamma^{-1} : \begin{pmatrix} x \mapsto w_1(x,y) \\ y \mapsto w_2(x,y) \end{pmatrix}$,
- (g',h') is equal to $\gamma \cdot (g,h) = (w_1(g,h), w_2(g,h))$,
- A is the matrix such that $A = \Phi(\gamma)$, where Φ is the epimorphism from Nielsen's theorem giving the exact sequence

$$0 \to \mathrm{Inn}(F_2) \to \mathrm{Aut}(F_2) \xrightarrow{\Phi} \mathrm{GL}(2,\,\mathbb{Z}) \to 0, \quad \Phi : \gamma \longmapsto \begin{pmatrix} e_x(\gamma(x)) & e_x(\gamma(y)) \\ e_y(\gamma(x)) & e_y(\gamma(y)) \end{pmatrix},$$

  $e_x(w)$ and $e_y(w)$ denote the sums of the exponents of x and y, respectively, in the word $w \in F_2$.

  For instance, if $\gamma : \begin{pmatrix} x \mapsto xy \\ y \mapsto y \end{pmatrix}$ then

$$\gamma^{-1} : \begin{pmatrix} x \mapsto xy^{-1} \\ y \mapsto y \end{pmatrix}, \quad \gamma \cdot (g,h) = (gh^{-1}, h), \quad A = \Phi(\gamma) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

  and so $(A,\ (g,h)^*) = (gh^{-1}, h)^*$.

The action of GL(2, $\mathbb{Z}$) on the set $(G \times G)^*$ defined by the diagram (2.5) will be called ***direct*** and written as $A \cdot (g,h)^*$. Remark that, in the case where $G = S_n$, the direct action coincides with the natural action of GL(2, $\mathbb{Z}$) on the origamis.

If we replace in the definition above the equality $A = \Phi(\gamma)$ by the equality $A = \left(\Phi(\gamma^{-1})\right)^t$, then we will obtain another GL(2, $\mathbb{Z}$)-action on $(G \times G)^*$. We will call that action ***dual***, and write $A \times (g,h)^*$. For instance, we have

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot (g,h)^* = (gh^{-1}, h)^*, \quad \text{but} \quad \begin{array}{l} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \times (g,h)^* = (g, gh)^*, \\ \\ \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \times (g,h)^* = (gh^{-1}, h)^*. \end{array}$$

Let us give several examples for the dual action (checking, by the way, that the relators in the presentations (2.3) induce the identity permutation on the set $(G \times G)^*$):

$$\begin{aligned}
J{\times}(g,h)^* &= (g,h^{-1})^*,\\
T{\times}(g,h)^* &= (gh,h)^*,\\
U{\times}(g,h)^* &= (g,g^{-1}h)^*,\\
TUT{\times}(g,h)^* &= TU{\times}(gh,h)^* = T{\times}(gh,h^{-1}g^{-1}h)^* = T{\times}(hg,g^{-1})^* = (h,g^{-1})^*,\\
UTU{\times}(g,h)^* &= UT{\times}(g,g^{-1}h)^* = U{\times}(h,g^{-1}h)^* = (h,h^{-1}g^{-1}h)^* = (h,g^{-1})^*,\\
(TUT)^4{\times}(g,h)^* &= (TUT)^2{\times}(g^{-1},h^{-1})^* = (g,h)^*,\\
J^2{\times}(g,h)^* &= (g,h)^*,\\
(JT)^2{\times}(g,h)^* &= JT{\times}(gh,h^{-1})^* = (g,h)^*,\\
(JU)^2{\times}(g,h)^* &= JU{\times}(g,h^{-1}g)^* = (g,g^{-1}hg)^* = (g,h)^*,
\end{aligned}$$

The stabilizers of a conjugacy class $(g,h)^*$ for the direct and dual actions will be denoted respectively by

$$\begin{aligned}
\mathrm{GL}(g,h) &:= \{A \in \mathrm{GL}(2,\mathbb{Z}) \mid A \cdot (g,h)^* = (g,h)^*\},\\
\mathrm{GL}^{\times}(g,h) &:= \{A \in \mathrm{GL}(2,\mathbb{Z}) \mid A{\times}(g,h)^* = (g,h)^*\}.
\end{aligned}$$

In particular, when $G = S_n$, the elements of the set $(S_n \times S_n)^*$ encode the n-square-tiled surfaces. The stabilizer $\mathrm{GL}(O)$ of an origami $O = (\sigma, \tau)^*$ for the direct action is the integer Veech group, the stabilizer $\mathrm{GL}^{\times}(O)$ for the dual action will be called the *dual* (*integer*) *Veech group*.

In general, the direct and dual stabilizers are not the same thing. We shall see how they are related. One may notice that

$$\begin{aligned}
J \cdot (g,h)^* = J{\times}(g,h)^* &= (J^{-1})^t{\times}(g,h)^*,\\
T \cdot (g,h)^* = U{\times}(g,h)^* &= (T^{-1})^t{\times}(g,h)^*,\\
U \cdot (g,h)^* = T{\times}(g,h)^* &= (U^{-1})^t{\times}(g,h)^*.
\end{aligned}$$

By these relations and the fact that $\mathrm{GL}(2,\mathbb{Z})$ is generated by the matrices J, T and U, we conclude that the stabilizer $\mathrm{GL}(g,h)$ is obtained from the stabilizer $\mathrm{GL}^{\times}(g,h)$ by transposing its elements:

$$\mathrm{GL}(g,h) = \left(\mathrm{GL}^{\times}(g,h)\right)^t.$$

And so we have

$$\mathrm{GL}(O) = \left(\mathrm{GL}^{\times}(O)\right)^t, \tag{2.6}$$

in the case where $G = S_n$.

2.7 Labeled digraphs

By a *labeled digraph* we mean a triple $(V,E,\mathcal{L})$ consisting of a set V, a totally ordered alphabet $\mathcal{L}$ and a subset $E \subset V \times V \times \mathcal{L}$. The elements of V are called *vertices*, those of E *edges* and those of $\mathcal{L}$ *labels*. If the alphabet $\mathcal{L} = \{l_1,\ldots,l_k\}$ has k letters and for any i from 1 to k there is an edge with label l_i, then the digraph is also called *k-labeled*. We say that a finite sequence of edges (v_0,v_1,l_{i_1}), (v_1,v_2,l_{i_2}), $\ldots$, (v_{p-1},v_p,l_{i_p}) is a *directed path from $v_0 \in V$ to $v_p \in V$*. A path is *closed* if $v_0 = v_p$.

An *isomorphism between two labeled digraphs* $(V,E,\mathcal{L})$ and $(V',E',\mathcal{L}')$ is a pair of bijections $f : V \to V'$ and $\phi : \mathcal{L} \to \mathcal{L}'$, such that ϕ respects order and we have $(u,v,l) \in E$ if and only if $(f(u),f(v),\phi(l)) \in E'$.

Along with $\mathcal{L}$ and E, we consider the set of *inverse labels* $\mathcal{L}^{-1} = \{l_1^{-1}, \dots, l_k^{-1}\}$ and the set of *inverse edges* $E^{-1} = \{(v, u, l^{-1}) \mid (u, v, l) \in E\}$. It allows us to introduce an *undirected path* as a sequence of edges $(v_0, v_1, l_{i_1}^{\epsilon_1})$, $(v_1, v_2, l_{i_2}^{\epsilon_2})$, $\dots$, $(v_{p-1}, v_p, l_{i_p}^{\epsilon_p})$ from $E \cup E^{-1}$, where $\epsilon_1, \epsilon_2, \dots, \epsilon_p \in \{1, -1\}$.

Definition 2.4. Let V be a finite set and let O be an origami corresponding to a pair of permutations $(\sigma_1, \sigma_2) \in Sym(V) \times Sym(V)$. We define a *digraph of the square-tiled surface* O, or else an *origamal digraph of* O, to be a 2-labeled digraph $(V, E, \mathcal{L})$ with the set of vertices V, an ordered alphabet $\mathcal{L} = \{l_1, l_2\}$, $l_1 \prec l_2$, and the set of edges

$$E = \bigcup_{i=1,2} \{(v, \sigma_i(v), l_i) \mid v \in V\}.$$

The labels l_1 and l_2 correspond to the horizontal and vertical directions respectively. For any vertex $v \in V$ and any label $l_i \in \mathcal{L}$ of an origamal digraph $(V, E, \mathcal{L})$, there is exactly one edge with label l_i beginning at v and one edge with label l_i ending at v. Therefore any path $(v_0, v_1, l_{i_1}^{\epsilon_1})$, $(v_1, v_2, l_{i_2}^{\epsilon_2})$, $\dots$, $(v_{p-1}, v_p, l_{i_p}^{\epsilon_p})$ is uniquely determined by the initial point $v_0 \in V$ and the labels $l_{i_m}^{\epsilon_m} \in \mathcal{L} \cup \mathcal{L}^{-1}$. We denote such a path by $l_{i_p}^{\epsilon_p} \dots l_{i_2}^{\epsilon_2} l_{i_1}^{\epsilon_1}[v_0]$, and by $l_{i_p}^{\epsilon_p} \dots l_{i_2}^{\epsilon_2} l_{i_1}^{\epsilon_1} \cdot v_0$ its endpoint v_p.

Two 2-labeled digraphs stand for the same origami if and only if they are isomorphic. The digraph of the origami defined by the permutations $\sigma_1 = (1\ 2\ 3)$ and $\sigma_2 = (1\ 4)$ is shown in FIGURE 2.7, where $V = \{1, 2, 3, 4\}$, the edges with label l_1 are solid, and those with label l_2 are dashed.

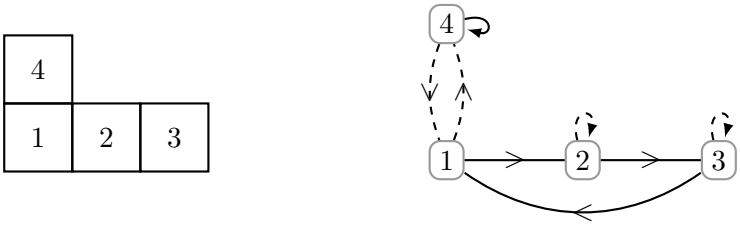


Figure 2.7: A digraph of the origami $L(3, 2)$.

2.8 The main idea of construction

Given a two-generator[9] group G acting on a finite set V, we can construct origamis associated to this action. Indeed, we have a permutation representation $\rho : G \to Sym(V)$, and for any generating set $\{g, h\}$ of G the pair $(\rho(g), \rho(h))$ defines an n-square origami O, where $n = |V|$. The number of connected components of O is equal to the number of orbits under the action of G, so that O is connected if and only if this action is transitive.

Whenever the representation ρ is faithful (*i.e.* $\ker \rho = \{1\}$), the monodromy group of the square-tiled surface O is isomorphic to G: $\mathcal{M}on(O) = \mathtt{gp}\{\rho(g), \rho(h)\} \simeq G$.

Among the most curious choices of the group G are classical groups. For instance, this can be a finite nonabelian simple group (as Gunter Malle, Jan Saxl and Thomas Weigel proved in [63], such a group is generated by two elements, one of which is an involution).

We will focus our attention, first, on the regular representation ρ_{reg} corresponding to the left action of G on the set of its elements, and, second, on coset representations ρ_H corresponding to the action of G on the set of left cosets modulo a subgroup H.

[9] We consider that cyclic groups are particular cases of two-generator groups.

Proposition 2.10 (**Classification of transitive representations**). *Every transitive representation of a group G is equivalent to its coset representation ρ_H for some $H \subseteq G$. It is faithful if and only if*

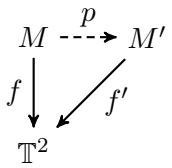
$$\bigcap_{g \in G} gHg^{-1} = 1.$$

Moreover, two coset representations ρ_H and $\rho_{H'}$ are equivalent exactly when H and H' are conjugate in G.

For a proof, see Lemma 1.6B of the book [25] by John D. Dixon and Brian Mortimer.

Chapter 3
The moduli space $\Omega\mathcal{M}_2$ and beyond

Consider a connected square-tiled surface (M, ω) of genus 2. Suppose that it is not primitive, and let (M', ω') be an intermediate square-tiled surface, so that we have a commutative diagram of ramified coverings:



Denote by g' the genus of M' and by k the degree of the ramified covering p. Since the surface M topologically is a pretzel, its Euler characteristic is equal to $\chi(M) = -2$, and by the Riemann-Hurwitz formula we have

$$-2 = \chi(M) = k \cdot \chi(M') - \sum(r_i - 1) \leqslant k \cdot \chi(M') = k(2 - 2g').$$

where r_i are ramification indices: at some conical points $P \in M$ the cone angle is $r_i \cdot 2\pi(d_i + 1)$ whilst the angle at $p(P) \in M'$ equals $2\pi(d_i + 1)$. The only possibilities to satisfy the inequality $k \cdot (g' - 1) \leq 1$ are either $k = 1$ or $g' = 1$. In the first case M' coincides with M, and in the second case M' is a torus.

We conclude that in order to verify the primitivity of a square-tiled surface of genus 2, it suffices to check that it is not a covering of any torus of area greater than 1.

Recall that by definition, a *reduced* square-tiled surface must not cover a torus of area > 1 with one branch point. Therefore, in the stratum $\mathcal{H}(2)$, all reduced origamis are automatically primitive (there is a unique branch point). In general, it is not prohibited for a reduced surface to be a proper covering of a torus ramified over two points. Thus,

Lemma 3.1. *In the stratum $\mathcal{H}(1,1)$, the reduced origamis which are not primitive correspond to coverings of tori with two ramification indices $r_1 = r_2 = 2$.*

In the next sections (see Proposition 3.3, Theorems 3.12 and 3.21), we will investigate the following question: given a stratum $\mathcal{H}$ and a positive integer n, is there a primitive n-square-tiled surface in $\mathcal{H}$ with monodromy group different from the alternating and symmetric groups of degree n?

Minimal number of squares in a given stratum

We have the following statement:

Theorem 3.2. *The minimal number $N = N(d_1, \ldots, d_s)$, for which there exists an N-square-tiled surface in the stratum $\mathcal{H}(d_1, \ldots, d_s)$, is equal to $s + d_1 + \cdots + d_s$.*

Moreover, for any $n \geq N$, there exists an n-square-tiled surface in $\mathcal{H}(d_1, \ldots, d_s)$ consisting of one horizontal cylinder of height 1.

Proof. First of all, an n-square origami O encoded by two permutations $\sigma, \tau \in S_n$ belongs to $\mathcal{H}(d_1, \ldots, d_s)$ if and only if the commutator $[\sigma, \tau]$ is a product of s disjoint cycles of lengths $d_1 + 1$, $\ldots$, $d_s + 1$ respectively. Therefore, we have $N \geq s+d_1+\cdots+d_s$.

Conversely, let $n \geq s+d_1+\cdots+d_s$ and let $\mu \in S_n$ be a permutation that decomposes into a product of s disjoint cycles of lengths $d_1 + 1$, $\ldots$, $d_s + 1$. Obviously, μ is even as $d_1 + \cdots + d_s = 2g - 2$, where g is the genus of the origamis in $\mathcal{H}(d_1, \ldots, d_s)$. Our goal is to show that the permutation μ is a commutator of two permutations $\sigma, \tau \in S_n$ such that σ is an n-cycle.

A. M. Gleason proved in 1962 that any permutation $\mu \in A_n$ is a product of two n-cycles, *cf.* [49, Proposition 4]. Since two n-cycles are conjugate, this means that $\mu = \sigma(\tau\sigma\tau^{-1}) = [\sigma, \tau]$ for some $\sigma, \tau \in S_n$, where σ is an n-cycle. Such permutations σ and τ obviously generate a transitive subgroup of S_n, and so $(\sigma,\, \tau)^*$ is a connected origami belonging to the stratum $\mathcal{H}(d_1, \ldots, d_s)$. We conclude that $N = s+d_1+\cdots+d_s$.

Moreover, since σ is an n-cycle, for any $n \geq N$, an n-square origami $O \in \mathcal{H}(d_1, \ldots, d_s)$ encoded by the pair of permutations $(\sigma,\, \tau)$ consists of one horizontal cylinder of height 1. □

Remark. Preceding Gleason's result, a theorem of Øystein Ore [78, 1951] states that each even permutation is a commutator of permutations. Thus, the famous Ore conjecture arose: any element of a finite non-abelian simple group is a commutator. In his Ph.D. thesis [10, 1972, Corollary 2.1] Edward Bertram generalized the Gleason's result by showing that any element of A_n, $n \neq 4$, is a product of two l-cycles if and only if $\left[\frac{3n}{4}\right] \leq l \leq n$.

$\mathrm{SL}_2(\mathbb{Z})$-orbits versus $\mathrm{GL}_2(\mathbb{Z})$-orbits

Let O be an origami. Denote its stabilizers for the $\mathrm{SL}_2(\mathbb{Z})$- and $\mathrm{GL}_2(\mathbb{Z})$-actions respectively by $\Gamma := \mathrm{SL}(O)$ and $\widetilde{\Gamma} := \mathrm{GL}(O)$. Since the special linear group is a normal subgroup of the general one, we may apply the second isomorphism theorem: the product $\widetilde{\Gamma}\cdot\mathrm{SL}_2(\mathbb{Z}) = \left\{ AB \;\middle|\; A \in \widetilde{\Gamma},\ B \in \mathrm{SL}_2(\mathbb{Z}) \right\}$ is a subgroup of $\mathrm{GL}_2(\mathbb{Z})$, the intersection $\widetilde{\Gamma} \cap \mathrm{SL}_2(\mathbb{Z}) = \Gamma$ is a normal subgroup of $\widetilde{\Gamma}$, and

$$\widetilde{\Gamma}/(\widetilde{\Gamma} \cap \mathrm{SL}_2(\mathbb{Z})) = (\widetilde{\Gamma} \cdot \mathrm{SL}_2(\mathbb{Z}))/\mathrm{SL}_2(\mathbb{Z}).$$

This implies the following inequalities:

$$1 \leq |\widetilde{\Gamma}/\Gamma| \leq 2.$$

- In the case that $|\widetilde{\Gamma}/\Gamma| = 2$, the $\mathrm{SL}_2(\mathbb{Z})$- and $\mathrm{GL}_2(\mathbb{Z})$-orbits of the origami O coincide.
- In the case that $|\widetilde{\Gamma}/\Gamma| = 1$, the $\mathrm{GL}_2(\mathbb{Z})$-orbit is twice bigger and consists of the $\mathrm{SL}_2(\mathbb{Z})$-orbits of the origamis O and $J \cdot O$, where $J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

In other words, we have

$$\begin{cases} \mathrm{GL}_2(\mathbb{Z}) \cdot O = \mathrm{SL}_2(\mathbb{Z}) \cdot O & \text{if } J \cdot O \in \mathrm{SL}_2(\mathbb{Z}) \cdot O, \\ \mathrm{GL}_2(\mathbb{Z}) \cdot O = \mathrm{SL}_2(\mathbb{Z}) \cdot O \ \cup\ \mathrm{SL}_2(\mathbb{Z}) \cdot (J \cdot O) & \text{else,} \end{cases} \tag{3.1}$$

because $\mathrm{GL}_2(\mathbb{Z}) = \langle J,\, \mathrm{SL}(2,\, \mathbb{Z})\rangle$.

3.1 The stratum $\mathcal{H}(2)$

The number $\mathcal{N}_n^{\mathrm{pr}}(2)$ of primitive n-square-tiled surfaces in the stratum $\mathcal{H}(2)$ is given by the formula

$$\mathcal{N}_n^{\mathrm{pr}}(2) = \frac{3}{8} n^2 (n-2) \prod_{\substack{p \mid n \\ p \text{ prime}}} \left(1 - \frac{1}{p^2}\right), \tag{3.2}$$

as indicated in the paper [28] by Alex Eskin, Howard Masur and Martin Schmoll.

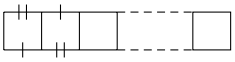
As for the monodromy group of a primitive origami in $\mathcal{H}(2)$, we have the following statement:

Proposition 3.3. *Let $p > 2$ be a prime number and let $n \geqslant p+3$ be a positive integer. Then for any* primitive *n-square origami O from the stratum $\mathcal{H}(p-1)$, the monodromy group $\mathcal{M}on(O)$ is either alternating (A_n) or symmetric (S_n).*

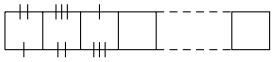
In $\mathcal{H}(2)$, the monodromy group of any primitive origami is either alternating or symmetric.

Proof. For the square-tiled surface O from $\mathcal{H}(p-1)$ represented by a pair (σ, τ), we have that the commutator $[\sigma, \tau]$ is a cycle of prime order p belonging to the group $\mathcal{M}on(O) = \mathtt{gp}\{\sigma, \tau\}$. If now the origami O is primitive, then the permutation group $\mathcal{M}on(O)$ is primitive (see Proposition 2.4) and, thus, must be equal to A_n or S_n by Jordan's theorem (Theorem 2.5). □

So, we have $\mathcal{M}on(O) = A_n$ or S_n for every primitive n-square-tiled surface belonging to $\mathcal{H}(2)$. If for some n both groups are realized, then we obtain at least two $\mathrm{GL}(2, \mathbb{Z})$-orbits, because the monodromy group is $\mathrm{GL}(2, \mathbb{Z})$-invariant. On the other hand, due to the work [67] of Curtis T. McMullen and the work [45] of Pascal Hubert and Samuel Lelièvre we know that the primitive n-square origamis in $\mathcal{H}(2)$ constitute at most two $\mathrm{GL}(2, \mathbb{Z})$-orbits. Precisely, if $n \geqslant 4$ is even, then there is only one orbit: it is represented by the origami

$P_n =$  encoded by $\sigma_n = (1\ 2\ \ldots\ n)$, $\tau_2 = (1\ 2)$.

If $n \geqslant 5$ is odd, then besides the orbit of P_n there is another orbit represented by

$Q_n =$  encoded by $\sigma_n = (1\ 2\ \ldots\ n)$, $\tau_3 = (1\ 2\ 3)$.

Remark. For even n, the origamis P_n and Q_n are in the same $\mathrm{GL}(2, \mathbb{Z})$-orbit.

We obviously have $\mathcal{M}on(P_n) = \mathtt{gp}\{\sigma_n, \tau_2\} = S_n$ for any n and

$$\mathcal{M}on(Q_n) = \mathtt{gp}\{\sigma_n, \tau_3\} = \begin{cases} S_n & \text{if } n \text{ is even;} \\ A_n & \text{if } n \text{ is odd.} \end{cases}$$

Therefore, we have just described a complete invariant of the orbits of primitive origamis in the stratum $\mathcal{H}(2)$: one has $\mathcal{M}on(O) = \mathcal{M}on(O')$ if and only if O and O' are in the same $\mathrm{GL}(2, \mathbb{Z})$-orbit.

It does not take long to determine in which orbit the origami O defined by (σ, τ) falls: if at least one of the permutations σ and τ is odd, then O is in the orbit of P_n, otherwise both permutations are even and O is in the orbit of Q_n.

As a consequence of the paper [44] by P. Hubert – S. Lelièvre and the paper [58] by S. Lelièvre – E. Royer, we have the following result:

Theorem 3.4 (Hubert, Lelièvre, Royer, 2005)**.** *For any $k \geqslant 2$, the Veech groups* $\mathrm{GL}(P_{2k})$, $\mathrm{GL}(P_{2k+1})$ *and* $\mathrm{GL}(P_{2k+1})$ *are noncongruence subgroups of* $\mathrm{GL}(2,\mathbb{Z})$ *of indices*

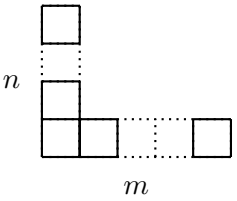
$$[\mathrm{GL}(2,\mathbb{Z}) : \mathrm{GL}(P_{2k})] = 3(k-1)k^2 \prod_{p|2k}\left(1-\frac{1}{p^2}\right),$$

$$[\mathrm{GL}(2,\mathbb{Z}) : \mathrm{GL}(P_{2k+1})] = \frac{3}{8}k(2k+1)^2 \prod_{p|2k+1}\left(1-\frac{1}{p^2}\right),$$

$$[\mathrm{GL}(2,\mathbb{Z}) : \mathrm{GL}(Q_{2k+1})] = \frac{3}{8}(k-1)(2k+1)^2 \prod_{p|2k+1}\left(1-\frac{1}{p^2}\right),$$

where p stands for a prime number.

For instance, consider the corner origami $L(m,n)$, where $m,n>1$ and $(m,n)\neq(2,2)$. It has $N = m+n-1$ squares, belongs to $\mathcal{H}(2)$ and is primitive. If both m and n are odd, then $\mathcal{M}on(L(m,n)) = A_N$

$L(m,n) =$ 

with $\sigma = (1\ 2\ \ldots\ m)$, $\tau = (m\ \ m{+}1\ \ \ldots\ \ m{+}n{-}1)$,

and so $L(m,n)$ is in the $\mathrm{GL}(2,\mathbb{Z})$-orbit of Q_N. If at least one of m and n is even, then $\mathcal{M}on(L(m,n)) = S_N$ and the origami is in the $\mathrm{GL}(2,\mathbb{Z})$-orbit of P_N. Therefore, the integer Veech groups $\mathrm{GL}(L(m,n))$ are noncongruence subgroups.

3.2 A generalization: the strata $\mathcal{H}(m)$

Given a set Ω, denote by $\Omega^{(k)}$ the set of k-tuples with distinct entries. If $|\Omega| = n$, then $|\Omega^{(k)}| = \frac{n!}{(n-k)!}$. A permutation group G acting on Ω is called *k-transitive* if the diagonal action of G on the set $\Omega^{(k)}$ is transitive, that is, for any two k-tuples $(x_1,\ldots,x_k)$ and $(y_1,\ldots,y_k)\in\Omega^{(k)}$ there exists a permutation $\sigma\in G$ such that $(\sigma(x_1),\ldots,\sigma(x_k)) = (y_1,\ldots,y_k)$. In this definition, requiring uniqueness of the permutation σ brings the notion of a *sharply k-transitive* permutation group.

Lemma 3.5. *Let G be a transitive permutation group on a set Ω, and $x\in\Omega$. Then G is k-transitive if and only if the stabilizer G_x is $(k-1)$-transitive on the set $\Omega\setminus\{x\}$.*

As a corollary of the lemma, the order of a k-transitive subgroup G of S_n is a multiple of

$$n(n-1)\ldots(n-k+1) = \frac{n!}{(n-k)!},$$

or else the index $[S_n : G]$ divides the number $(n-k)!$.

Obviously, the symmetric group S_n is sharply n-transitive. The fact that the alternating group A_n is $(n-2)$-transitive follows by induction from Lemma 3.5. We also have:

Lemma 3.6. *A permutation group of degree n, which is neither alternating nor symmetric, can be at most $\left(\left[\frac{n}{3}\right]+1\right)$-transitive.*

Proof. This is the statement of Theorem IV, §138 in the book [14] by William Burnside. □

Lemma 3.7 (Otto Hölder [43], 1895)**.** *If n is a positive integer different from 2 and 6, then $\mathrm{Aut}(S_n) = S_n$, that is, all automorphisms of the symmetric group of degree n are inner. Else, $\mathrm{Aut}(S_2) = 1$ and $\mathrm{Aut}(S_6) = S_6 \rtimes C_2$.*

Proof. See Theorem 8.2A in the book [25], Theorem 7.5 in the book [81] by Joseph J. Rotman or the original paper [43] by Otto Hölder. □

Lemma 3.8. *Let $n > 2$ be a positive integer.*

1. *If $n \neq 4$ then the alternating group A_n is the only subgroup in S_n of index less than n.*
2. *If $n \neq 6$ then S_n has exactly n subgroups of index n, which are the symmetric groups of degree $n-1$ fixing one of the letters $1, 2, \ldots, n$.*

Proof. 1. Suppose that $H \neq A_n$ is a subgroup of S_n of index k, where $2 \leq k < n$. The group S_n acts transitively on the set of left cosets S_n/H, and we have a homomorphism $\rho_H : S_n \to S_k$. The kernel $\ker \rho_H = \cap_{g \in S_n} gHg^{-1}$ is a normal subgroup of S_n of index at least 2, and so is trivial (when $n \neq 4$, the only proper normal subgroup of S_n is A_n). In other words, we obtain an isomorphic copy of S_n in the group S_k, which is impossible, since $k! < n!$.

For $n = 4$, the Klein four-group $C_2 \times C_2 = \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ is an index 3 subgroup of S_4.

2. If H is a subgroup of index n in S_n, then the action on the left cosets gives a homomorphism $\rho_H : S_n \to Sym(S_n/H) \simeq S_n$. The kernel of ρ_H is a normal subgroup of index at least n, and so is trivial (for $n \neq 4$, S_n does not have proper normal subgroups except of A_n, as for $n = 4$, the Klein four-group and A_4 are the only proper normal subgroups of S_4). Therefore, we obtain an automorphism $S_n \xrightarrow{\simeq} S_n$, for which the image of H is the stabilizer $\mathrm{Stab}_{S_n}(i) \simeq S_{n-1}$ of the letter $i \in \{1, 2, \ldots, n\}$ corresponding to the coset H through ρ_H. According to Lemma 3.7, all automorphisms of S_n where $n \neq 6$, are inner, that is, H is conjugate to the stabilizer of a letter, and so it is the stabilizer of a letter itself. □

Given a group G acting on a set Ω and a subset $\Delta \subseteq \Omega$, denote by G_Δ the subgroup of G stabilizing all elements $x \in \Delta$. We say that a subset $\Gamma \subseteq \Omega$ is a *Jordan set* for G if $|\Gamma| > 1$ and the group $G_{\Omega \setminus \Gamma}$ acts transitively on Γ. In this case, the set $\Delta = \Omega \setminus \Gamma$ is called a *Jordan complement*.

Theorem 3.9 (Bernhard Marggraf [64], 1892)**.** *Let G be a primitive permutation group of degree n.*

1. *If the group G contains an m-cycle with $1 < m < n$, then it is $(n-m+1)$-transitive.*
2. *If the group G contains an m-cycle with $1 < m < n - \left[\frac{n}{3}\right]$, then $G \supseteq A_n$.*
3. *If G has a Jordan set of size m with $1 < m < \frac{n}{2}$, then $G \supseteq A_n$.*
4. *If the group G has a Jordan set Γ of size m with $1 < m < n - \left[\frac{n}{3}\right]$ and the group $G_{\Omega \setminus \Gamma}$ acts primitively on Γ, then G contains the alternating group.*

Proof. 1. See Theorem 13.8 in the textbook [98] by Helmut Wielandt,
2. By the first part of the theorem, the group G is $(n-m+1)$-transitive. If G does not contain A_n, then according to Lemma 3.6, we have $n - m + 1 \leq \left[\frac{n}{3}\right] + 1$, that is, $n - \left[\frac{n}{3}\right] \leq m$.
3. See Theorem 13.5 in [98] or Proposition 7.4B in the textbook [25].
4. See Theorem I, §160 in Burnside's textbook [14]. □

The theorem stated below is another refinement of Jordan's theorem (see Theorem 2.5), in which the cases $n = p, p+1, p+2$ are accomplished.

Theorem 3.10 (Thilo E. Zieschang [101], 1995)**.** *Let G be a primitive permutation group of degree n containing a p-cycle, where p is prime. Then one of the following situations occurs (see the remark below for the notation):*

1) $G = A_n$ *or* $G = S_n$*;*

2) $n = p + 2 = 2^k + 1$ *and* $G \simeq \mathrm{PSL}(2, 2^k)$ *or* $G \simeq \mathrm{P\Gamma L}(2, 2^k)$*;*

3) $n = p + 1$ *and* $G \simeq \mathrm{PSL}(2, p)$ *or* $G \simeq \mathrm{PGL}(2, p)$*;*

4) $n = p$ *and* $G \subseteq \mathrm{AGL}(1, p)$ *such that* $G \simeq \mathbb{F}_p \rtimes H$*, where*[1] $H \subseteq \mathbb{F}_p^\times$*;*

5.a) $n = p + 1 = 12$ *and* $G \simeq M_{11}$ *or* $G \simeq M_{12}$*;*

5.b) $n = p + 1 = 24$ *and* $G \simeq M_{24}$*;*

5.c) $n = p + 1 = 2^m$ *and* $G \subseteq \mathrm{ASL}(m, 2)$ *such that* $G = \mathbb{F}_2^m \rtimes H$*, where*[2] $\mathbb{Z}_p \subseteq H \subseteq \mathrm{SL}(m, 2)$*;*

6.a) $n = p = 11$ *and* $G \simeq \mathrm{PSL}(2, 11)$ *or* $G \simeq M_{11}$*;*

6.b) $n = p = 23$ *and* $G \simeq M_{23}$*;*

6.c) $n = p$ *and* $\mathrm{PSL}(m, q) \subseteq G \subseteq \mathrm{P\Gamma L}(m, q)$*, where* $n = \frac{q^m - 1}{q - 1}$.

Remark. The following mostly standard notation is used:

- $q = p_0^k$ is a power of a prime number p_0 (not to be confused with p).
- $Tr(m, q)$ denotes the group of translations on an m-dimensional vector space over the field $\mathbb{F}_q$, so $Tr(m, q) \simeq \mathbb{F}_q^m$.
- $\mathrm{GL}(m, q)$ and $\mathrm{SL}(m, q)$ are the general and special linear groups of degree m over $\mathbb{F}_q$ with orders

$$|\mathrm{GL}(m, q)| = q^{m(m-1)/2}(q - 1)(q^2 - 1)\dots(q^m - 1) \text{ and } |\mathrm{SL}(m, q)| = \frac{1}{q - 1}|\mathrm{GL}(m, q)|. \tag{3.3}$$

- $\mathrm{AGL}(m, q)$ and $\mathrm{ASL}(m, q)$ are the *general* and *special affine groups* of degree m over $\mathbb{F}_q$, that is,

$$\mathrm{AGL}(m, q) = \mathbb{F}_q^m \rtimes \mathrm{GL}(m, q) \text{ and } \mathrm{ASL}(m, q) = \mathbb{F}_q^m \rtimes \mathrm{SL}(m, q), \tag{3.4}$$

  where $\mathrm{GL}(m, q)$ acts on $\mathbb{F}_q^m$ in the natural manner.

  The group $\mathrm{AGL}(m, q)$ acts faithfully on the space $\mathbb{F}_q^m$ by $\mathbf{x} \mapsto A \cdot \mathbf{x} + \mathbf{y}$, where $A \in \mathrm{GL}(m, q)$ and $\mathbf{y} \in \mathbb{F}_q^m$. The groups $\mathrm{ASL}(m, q)$, $Tr(m, q)$, $\mathrm{GL}(m, q)$, $\mathrm{SL}(m, q)$ can be viewed as subgroups of $\mathrm{AGL}(m, q)$ corresponding to the additional conditions $\det A = 1$, $A = 1$, $\mathbf{y} = 0$, $\mathbf{y} = 0 \wedge \det A = 1$, respectively. Hence, all these groups constitute subgroups of S_{q^m}.

- $\mathrm{PGL}(m, q)$ and $\mathrm{PSL}(m, q)$ are the *projective general* and *special linear groups* of degree m over the field $\mathbb{F}_q$ with orders

$$|\mathrm{PGL}(m, q)| = \frac{1}{q - 1}|\mathrm{GL}(m, q)| \text{ and } |\mathrm{PSL}(m, q)| = \frac{1}{\gcd(m, q - 1)}|\mathrm{PGL}(m, q)|, \tag{3.5}$$

  since we have $\mathrm{PGL}(m, q) = \mathrm{GL}(m, q)/Z$ and $\mathrm{PSL}(m, q) = \mathrm{SL}(m, q)/SZ$, where Z consists of all nonzero scalar transformations of $\mathbb{F}_q^m$ and SZ consists of those with unit determinant. In particular, we have $|\mathrm{PGL}(2, q)| = q(q^2 - 1)$ and $|\mathrm{PSL}(2, q)| = \begin{cases} q(q^2 - 1) & \text{if } q = 2^k, \\ \frac{1}{2}q(q^2 - 1) & \text{else.} \end{cases}$

[1] The affine group $\mathrm{AGL}(m, q)$ contains the subgroup of translations $Tr(m, q) \simeq \mathbb{F}_q^m$ and the diagonal subgroup $\{\lambda I \mid \lambda \in \mathbb{F}_q^\times\} \simeq \mathbb{F}_q^\times$. In the case that $m = 1$, we have $\mathrm{AGL}(1, q) \simeq \mathbb{F}_q \rtimes \mathbb{F}_q^\times$.

[2] The stabilizer U of 0 for the action of $\mathrm{SL}(m, q)$ on the vector space $\mathbb{F}_q^m$ is a group of order $q^m - 1$, since U acts regularly on $\mathbb{F}_q^m - \{0\}$. In our case, $q = 2$ and $p = 2^m - 1$ is prime, so $U \simeq \mathbb{Z}_p$. See also the textbook [48] by Bertram Huppert and Norman Blackburn.

The group $\mathrm{PGL}(m,q)$ acts faithfully and transitively on the projective space $\mathbb{P}^{m-1}(\mathbb{F}_q)$, which has $n = \frac{q^m-1}{q-1}$ points. This gives faithfull representations of $\mathrm{PGL}(m,q)$ and $\mathrm{PSL}(m,q)$ in S_n. Moreover, as Évariste Galois showed in 1832, the groups $\mathrm{PSL}(2,p)$ have exceptional faithful transitive actions of degree p when $p = 5, 7$ and 11.

- $\Gamma\mathrm{L}(m,q)$ is the *general semilinear group* of degree m over $\mathbb{F}_q$, that is, the semidirect product

$$\Gamma\mathrm{L}(m,q) = \mathrm{GL}(m,q) \rtimes \mathrm{Gal}(\mathbb{F}_q), \tag{3.6}$$

  where $\mathrm{Gal}(\mathbb{F}_q)$ is the Galois group of the field $\mathbb{F}_q = \mathbb{F}_{p_0^k}$ over $\mathbb{F}_{p_0}$, acting componentwise on the vectors from $\mathbb{F}_q^m$. Recall also that $\mathrm{Gal}(\mathbb{F}_q)$ is cyclic of order k.

- $\mathrm{A}\Gamma\mathrm{L}(m,q)$ is the *affine semilinear group* of degree m over $\mathbb{F}_q$,

$$\mathrm{A}\Gamma\mathrm{L}(m,q) = \mathbb{F}_q^m \rtimes \Gamma\mathrm{L}(m,q). \tag{3.7}$$

  The group $\mathrm{A}\Gamma\mathrm{L}(m,q)$ acts faithfully on the space $\mathbb{F}_q^m$ by $\mathbf{x} \mapsto A \cdot \mathbf{x}^\sigma + \mathbf{y}$, where $A \in \mathrm{GL}(m,q)$, $\mathbf{y} \in \mathbb{F}_q^m$ and $\sigma \in \mathrm{Gal}(\mathbb{F}_q)$. Thus, we have embeddings of $\mathrm{A}\Gamma\mathrm{L}(m,q)$ and $\Gamma\mathrm{L}(m,q)$ in S_{q^m}.

- $\mathrm{P}\Gamma\mathrm{L}(m,q)$ is the *projective semilinear group* of degree m over $\mathbb{F}_q$,

$$\mathrm{P}\Gamma\mathrm{L}(m,q) = \mathrm{PGL}(m,q) \rtimes \mathrm{Gal}(\mathbb{F}_q). \tag{3.8}$$

  The faithfull action of the group $\mathrm{P}\Gamma\mathrm{L}(m,q)$ on the projective space $\mathbb{P}^{m-1}(\mathbb{F}_q)$ corresponds to the permutations $[x_1 : \ldots : x_m] \mapsto A \cdot [x_1^\sigma : \ldots : x_m^\sigma]$, where $A \in \mathrm{PGL}(m,q)$ and $\sigma \in \mathrm{Gal}(\mathbb{F}_q)$. This gives an embedding of $\mathrm{P}\Gamma\mathrm{L}(m,q)$ in S_n for $n = {}^{(q^m-1)}/_{(q-1)}$. Notice that the elements of $\mathrm{P}\Gamma\mathrm{L}(m,q)$ are *semilinear transformations* of $\mathbb{P}^{m-1}(\mathbb{F}_q)$, *i.e.* bijections preserving the property of points to be collinear. If $m \geq 3$, then the projective semilinear group $\mathrm{P}\Gamma\mathrm{L}(m,q)$ is the full collineation group of the projective space $\mathbb{P}^{m-1}(\mathbb{F}_q)$, *cf.* Theorem 2.26 in the textbook [2] by Emil Artin.

- $M_{11}, M_{12}, M_{23}, M_{24}$ are Mathieu groups, which are the first sporadic simple groups discovered (we will not explicit these groups here).

Linear groups play a special role here, and we shall give more information.

Fact 1. The commutator $[A,B]$ of two elements $A, B \in \mathrm{PSL}(2,q)$ is well-defined in $\mathrm{SL}(2,q)$.

Fact 2. If $[A,B] = \pm I$, then A and B don't generate the group $\mathrm{PSL}(2,q)$, since it is non-abelian.

Fact 3. If $\mathrm{tr}([A,B]) = 2$, then A and B don't generate $\mathrm{PSL}(2,q)$. Indeed, we can assume by conjugation that $[A,B] = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$. For $\lambda = 0$, use Fact 2. Otherwise, we have $ABA^{-1} = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \cdot B = \begin{pmatrix} a+\lambda c & b+\lambda d \\ c & d \end{pmatrix}$, and equating the traces shows that $c = 0$. Therefore, the matrices B and A (by symmetry argument) are upper-triangular, and so they don't generate $\mathrm{PSL}(2,q)$.

Fact 4. Let $A, B \in \mathrm{SL}(2,q)$ be two matrices such that $\mathrm{tr}(A) = \mathrm{tr}(B) \neq \pm 2$. Then the matrix A is conjugate to B. For each of the traces 2 and -2, there are:

- two conjugacy classes if q is even: the class of $-I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ and the class containing all other matrices with trace -2;

– three conjugacy classes if q is odd: the class $\{-I\}$ and two classes represented by $\begin{pmatrix} -1 & z \\ 0 & -1 \end{pmatrix}$ and $\begin{pmatrix} -1 & z' \\ 0 & -1 \end{pmatrix}$, where $z, z' \in \mathbb{F}_q^\times$ such that z is a square and z' is a non-square. The last two classes are conjugated by $\begin{pmatrix} u & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}(2,q)$, where $u \in \mathbb{F}_q$ is a non-square.

We will need the following theorem:

Theorem 3.11 (Darryl J. McCullough and Marcus Wanderley [66], 2008)**.** *When $q \geq 13$ is an odd prime power, every non-identity element of $\mathrm{PSL}(2,q)$ is the commutator of a generating pair. When $q = 2^k$, an element of $\mathrm{PSL}(2,q)$ is the commutator of a generating pair if and only if its trace is distinct from 0.*

When $q < 13$, necessary and sufficient conditions for a matrix $A \in \mathrm{SL}(2,q) \setminus \{-I\}$ to be the commutator of a generating pair of $\mathrm{SL}(2,q)$ are:

- $\mathrm{tr}(A) \neq 2$*, for* $q = 2, 4, 8$*;*
- $\mathrm{tr}(A) \notin \{1, 2\}$*, for* $q = 3, 9, 11$*;*
- $\mathrm{tr}(A) \notin \{0, -1, 2\}$*, for* $q = 5$*;*
- $\mathrm{tr}(A) \notin \{0, 1, 2\}$*, for* $q = 7$*.*

Sketch of proof. For $q < 13$, the statement of the theorem can be checked by direct calculations.

We assume from now on that $q \geq 13$. Let $x, y \in \mathbb{F}_q^\times$ such that x generates $\mathbb{F}_q^\times$. Consider the matrices

$$H_x = \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \quad \text{and} \quad J_y = \begin{pmatrix} y+1 & 1 \\ y & 1 \end{pmatrix}.$$

It can be shown that these matrices generate $\mathrm{SL}(2,q)$, using the following points (it suffices to prove that the images of H_x and J_y in $\mathrm{PSL}(2,q)$ generate the whole group):

Point 1. Let $q = p^k$ with p prime and denote $d = \gcd(2, q-1)$. Then every subgroup of $\mathrm{PSL}(2,q)$ is isomorphic to one of the following groups[3]:

(a) (small subgroups) The dihedral groups of orders $2(q \pm 1)/d$ and their subgroups;

(b) (triangular subgroups) A group H of order $q(q-1)/d$ and its subgroups;

(c) (exceptional subgroups) A_4, S_4 or A_5;

(d) (linear subgroups) $\mathrm{PSL}(2, p^r)$ or $\mathrm{PGL}(2, p^r)$, where r divides k.

Point 2. The orders of nonparabolic[4] elements of $\mathrm{PSL}(2,q)$ are exactly the divisors of $(q \pm 1)d$, as is shown in the paper [32] by Henry Glover and Denis Sjerve. So, the maximum order of a nonparabolic element of $\mathrm{PSL}(2,q)$ is $(q+1)/d$.

Point 3. One has the commutator $[H_x, J_y] = \begin{pmatrix} 1 - Dxy & Dx(y+1) \\ -Dx^{-1}y & 1 + Dx^{-1}y \end{pmatrix}$ and the trace $\mathrm{tr}([H_x, J_y]) = 2 - D^2 y$, where $D = x - x^{-1}$.

Point 4. As $q > 7$, the elements $[H_x, J_y]$ and $[H_x^{-1}, J_y]$ do not commute in $\mathrm{PSL}(2,q)$.

[3] *cf.* Theorem 6.25 (Chapter 3) in the textbook [91] by Michio Suzuki.

[4] An element of $\mathrm{PSL}(2,q)$ is called *parabolic* if its trace is ± 2.

Point 5. Let G be the group generated by H_x and J_y. Since small and triangular subgroups of $\mathrm{PSL}(2,q)$ have abelian commutator subgroups, Point 4 implies that G is neither of type (a) nor of type (b). The order of H_x is $\frac{q-1}{2} \geq 6$, and so G is not of type (c). Furthermore, the matrix H_x is not parabolic: its trace $x + x^{-1}$ is not ± 2 as x generates $\mathbb{F}_q - \{0\}$. The linear groups $\mathrm{PSL}(2,p^r)$ and $\mathrm{PGL}(2,p^r)$ with $r < k$ are ruled out by Point 2, because the inequality $\frac{p^k-1}{2} \leq p^r+1$ doesn't hold for $p^k \geq 13$.

Therefore, we have $\mathrm{SL}(2,q) = \langle H_x, J_y \rangle$. Remark that, for a fixed generator $x \in \mathbb{F}_q^\times$, the trace $\mathrm{tr}([H_x, J_y]) = 2 - D^2 y$ runs over all elements of $\mathbb{F}_q - \{2\}$ as y runs over $\mathbb{F}_q^\times$.

Let $A \in \mathrm{SL}(2,q)$ be a matrix with $\mathrm{tr}(A) \neq 2$. Consider a generating pair (H_x, J_y) such that $\mathrm{tr}(A) = \mathrm{tr}([H_x, J_y])$. Evidently, $[H_x, J_y]$ is not $-I$, since the images of H_x and J_y generate $\mathrm{PSL}(2,q)$.

When $\mathrm{tr}(A) \neq -2$ or q is even, it follows from Fact 4 above that $[H_x, J_y] = C^{-1}AC$ for some $C \in \mathrm{SL}(2,q)$, and so the generating pair (CH_xC^{-1}, CJ_yC^{-1}) has commutator A.

When $\mathrm{tr}(A) = -2$ and q is odd, by Fact 4 there exists $D \in \mathrm{GL}(2,q)$ such that $[H_x, J_y] = D^{-1}AD$, and the generating pair (DH_xD^{-1}, DJ_yD^{-1}) of $\mathrm{SL}(2,q)$ has commutator A. □

Now, we are able to establish the main result of the section (recall that by Theorem 3.2 the number of squares of an origami from $\mathcal{H}(m)$ can be equal to $m+1, m+2, \dots$):

Theorem 3.12. *Let m be an even positive integer. Denote by $a(m)$ the minimal natural number greater than m such that, for any primitive n-square-tiled surface in the stratum $\mathcal{H}(m)$ with $n \geq a(m)$, the monodromy group is either A_n or S_n. We have*

1. *$a(2) = 3$;*
2. *if $p = m+1 \geq 5$ is a prime but not Mersenne[5], then $a(m) = m+3$, and for $n \in \{m+1, m+2\}$ there are primitive n-square origamis in $\mathcal{H}(m)$ with monodromy group not containing A_n;*
3. *if $p = m+1 \geq 7$ is a Mersenne prime, then $a(m) = m+4$, and for $n \in \{m+1, m+2, m+3\}$ there are primitive n-square origamis in $\mathcal{H}(m)$ with monodromy group not containing A_n;*
4. *$a(m) \leq \frac{3}{2}m + 2$ for all even $m \in \mathbb{N}$.*

Proof. Consider an n-square primitive origami $O \in \mathcal{H}(m)$ corresponding to a pair $(\sigma, \tau) \in S_n \times S_n$. The monodromy group $G = \mathcal{M}on(O) = \mathtt{gp}\{\sigma, \tau\}$ is primitive and contains $[\sigma, \tau]$, which is an $(m+1)$-cycle.

1. We saw in Section 3.1 that the monodromy group of any primitive n-square origami from the stratum $\mathcal{H}(2)$ is either A_n or S_n.

2. Let $p = m+1$ be a prime but not Mersenne. If $n \geq p+3 = m+4$, then by Proposition 3.3 the group G contains A_n. For $n = p+2 = m+3$, due to Theorem 3.10 case 2) we have that either G contains A_n or $p+2 = 2^k+1$. Since the latter is false (p is not Mersenne), we obtain $a(m) \leq m+3$.

Let us now show that, for $n = p+1$ and p, primitive groups distinct from A_n and S_n occur as monodromy groups of n-square origamis in the stratum $\mathcal{H}(m)$:

→ Case $n = p+1 = m+2 \geq 8$. Corresponding to Theorem 3.10 case 3), the natural action of $\mathrm{PSL}(2,p)$ on the projective line $\mathbb{P}^1(\mathbb{F}_p)$ is faithful and primitive, that is, we have a primitive permutation group $G \subset S_{p+1}$ isomorphic to $\mathrm{PSL}(2,p)$. When $p \geq 7$, we know from Theorem 3.11 that there exist two elements A and B generating $\mathrm{PSL}(2,p)$ such that

$$[A,B] = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix},$$

[5] A *Mersenne prime* is a prime of the form $2^k - 1$. In this case, it is easy to show that a number k must also be prime.

which is an element of order p. Translating to G, we obtain a generating pair (σ, τ) such that $[\sigma, \tau]$ is a p-cycle. Hence, the $(p+1)$-square origami O encoded by this pair belongs to $\mathcal{H}(p-1)$ and has primitive monodromy group $G \simeq \mathrm{PSL}(2, p)$ of order $\frac{1}{2}p(p^2-1) < \frac{1}{2}(p+1)!$.

→ Case $n = p + 1 = m + 2 = 6$. When $p = 5$, the 6-square origami given by the permutations $\sigma = (1\ 2)(5\ 6)$ and $\tau = (1\ 3\ 4)(2\ 5\ 6)$ belongs to the stratum $\mathcal{H}(4)$, and its monodromy group is $\mathrm{PSL}(2, 5) \simeq A_5$, see Table B.1.

→ Case $n = p = m + 1$. Corresponding to Theorem 3.10 case 4), the action of $\mathrm{AGL}(1, p)$ on the space $\mathbb{F}_p$ is faithful and primitive, that is, we have a primitive permutation group $G \subset S_{p+1}$ isomorphic to $\mathrm{AGL}(1, p)$. Let $a \in \mathbb{F}_p^\times$ and $b \in \mathbb{F}_p$ such that $ab - b \neq 0$. Consider the elements f, g of $\mathrm{AGL}(1, p)$ such that

$$f(x) = ax \quad \text{and} \quad g(x) = x + b \quad \text{for any } x \in \mathbb{F}_p.$$

Then the commutator $h = [f, g]$ satisfies $h(x) = x + ab - b$, and so it's an element of order p. Translating to G, we obtain a generating pair (σ, τ) such that $[\sigma, \tau]$ is a p-cycle. Hence, the $(p+1)$-square origami O given by this pair belongs to $\mathcal{H}(p-1)$ and has primitive monodromy group $G \simeq \mathrm{AGL}(1, p)$ of order $p(p-1) < \frac{1}{2}(p+1)!$, when $p \geq 5$.

3. Let $p = m + 1 = 2^k - 1$ be a Mersenne prime. If $n \geq p + 3 = m + 4$, then by Proposition 3.3 the group G contains A_n.

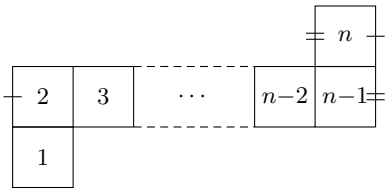
If $n = p + 2 = m + 3 = 2^k + 1$, then Theorem 3.10 case 2) and Theorem 3.11 provide a primitive origami in $\mathcal{H}(p-1)$ with monodromy group $\mathrm{PSL}(2, 2^k)$. For $n = p+1 = m+2 \geq 8$ and $n = p = m+1$, we also construct primitive origamis in $\mathcal{H}(p-1)$ with monodromy group not containing A_n, as in the part 2 of the proof.

4. Let $n \geq \frac{3}{2}m + 2$. Then we have the following inequality

$$m + 1 \leq \frac{2}{3}(n-2) + 1 < \frac{2}{3}n \leq n - \left[\frac{n}{3}\right].$$

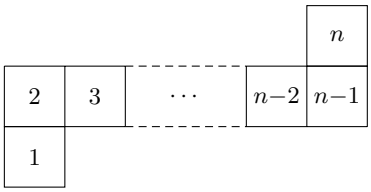
By Theorem 3.9, the monodromy group of O contains the alternating group A_n. □

Example 1 (**the stratum $\mathcal{H}(4)$**)**.** Let us give a list of the primitive monodromy groups which can occur in the stratum $\mathcal{H}(4)$. The minimal number of squares of an origami in $\mathcal{H}(4)$ is 5, so take $n \geq 5$. Consider the following n-square origamis:

$O_n =$ 

encoded by $\sigma_n = (2\ 3\ \ldots\ n{-}1\ \ n)$, $\tau_n = (1\ 2)(n{-}1\ \ n)$

and

$O'_n =$ 

encoded by $\sigma'_n = (2\ 3\ \ldots\ n{-}1)$, $\tau_n = (1\ 2)(n{-}1\ \ n)$.

We have $[\sigma_n, \tau_n] = [\sigma'_n, \tau_n] = (1\ n\ \ n{-}1\ \ 2\ 3)$, so these origamis belong to $\mathcal{H}(4)$. Moreover, their monodromy groups are primitive. Indeed, let Δ and Δ' be some blocks for $\mathcal{M}on(O_n)$ and $\mathcal{M}on(O'_n)$, respectively, containing 1 and another integer $x \neq 1$. Since σ_n and σ'_n don't move 1, we have that $(\sigma_n)^k(\Delta) = \Delta$ and $(\sigma'_n)^k(\Delta') = \Delta'$ for any $k \in \mathbb{N}$. Therefore, the block Δ contains all integers from 1 to n, and Δ' contains the integers from 1 to $n{-}1$, as well as the integer n, because $|\Delta'|$ divides n. By Lemma 2.2, the groups $\mathcal{M}on(O_n)$ and $\mathcal{M}on(O'_n)$ are primitive.

According to Theorem 3.12 part 2, for all primitive n-square origamis in $\mathcal{H}(4)$ with $n \geq 7$, the monodromy group must be A_n or S_n. Therefore, when $n \geq 7$, we obtain

$$\mathcal{M}on(O_n) = \begin{cases} S_n & \text{if } n \text{ is odd,} \\ A_n & \text{if } n \text{ is even.} \end{cases} \quad \text{and} \quad \mathcal{M}on(O'_n) = \begin{cases} S_n & \text{if } n \text{ is even,} \\ A_n & \text{if } n \text{ is odd,} \end{cases} \tag{3.9}$$

which depends on the parities of σ_n and σ'_n. This shows that both A_n and S_n are realized as monodromy groups in $\mathcal{H}(4)$.

The cases of $n = 5$ and 6 are brought in Table B.1, and we are going to display them. Let $O(\sigma, \tau)^*$ be an n-square-tiled surface in $\mathcal{H}(4)$ with monodromy group $G = \mathcal{M}on(O)$ containing a 5-cycle $[\sigma, \tau]$.

Suppose that $n = 5$ and G doesn't contain A_5. By Theorem 3.10 (*cf.* the cases 4 and 6.c), either $G \simeq \mathbb{F}_5 \rtimes H$ for a subgroup $H \subseteq \mathbb{F}_5^\times$, or $\mathrm{PSL}(m, q) \subseteq G \subseteq \mathrm{P\Gamma L}(m, q)$, where m is a natural number and q is a prime power satisfying the equality $\frac{q^m-1}{q-1} = 5$. For the first case, since G has a 5-cycle which is a commutator of two elements, the subgroup H cannot be $\{1\}$, and so it is either $\{1, 4\}$ or $\mathbb{F}_5^\times$. For the second case, the equality $q(5 - q^{m-1}) = 4$ implies that $m = 2$ and $q = 4$. However, the order of $\mathrm{PSL}(2, 4)$ is $4(4^2 - 1) = 60 = {}^{5!}\!/2$, and so if $G \supseteq \mathrm{PSL}(2, 4)$, then G contains A_5 by Lemma 3.8. Thus the second case is excluded.

Suppose that $n = 5{+}1 = 6$ and G doesn't contain A_6. Then Theorem 3.10 (*cf.* case 3) implies that either $G = \mathrm{PSL}(2, 5)$ or $G = \mathrm{PGL}(2, 5)$. (See Table B.1 classifying the 5- and 6-square $\mathrm{SL}_2(\mathbb{Z})$-orbits in $\mathcal{H}(4)$. It turns out that all 5- and 6-square origamis in this stratum are primitive.)

3.3 Background: orbitals and their graphs

Let G be a transitive permutation group on a set Ω (possibly infinite). An *orbital* of G is an orbit of G for its usual action on the cartesian product $\Omega \times \Omega$. The cardinal $r = r(G)$ of the set of orbitals is called the *rank* of G. We have the following extremal cases:

- $r = 1$ if and only if $G = \{1\}$,
- $r = 2$ if and only if G is 2-transitive,
- $r = |\Omega|$ for a finite Ω if and only if G is regular[6] (there is a one-to-one correspondence between the orbitals and the orbits of a point stabilizer G_x acting on the set Ω, see below).

The orbital $\{(x, x) \mid x \in \Omega\}$ is called *diagonal*, the others are *nondiagonal*. The orbital *paired* with an orbital Θ is the following set (denoted by Θ^*)

$$\Theta^* := \{(y, x) \mid (x, y) \in \Theta\}.$$

We say that Θ is *self-paired* if $\Theta = \Theta^*$.

[6] that is, $G_x = 1$ for any $x \in \Omega$.

For each orbital Θ, the *orbital graph* Graph(Θ) is the digraph with vertex set Ω and edge set Θ: there is a directed edge from x to y if and only if $(x, y) \in \Theta$. For instance, the orbital graph of the diagonal orbital has one loop at each vertex. None of the other orbital graphs have loops. The digraph Graph(Θ^*) is obtained from Graph(Θ) by reversing the directions of the edges.

The orbital graphs for the cyclic group $C_4 = \mathtt{gp}\{(1\ 2\ 3\ 4)\}$ and the dihedral group $D_5 = \mathtt{gp}\{(1\ 2\ 3\ 4\ 5), (1\ 4)(2\ 3)\}$ are shown in Figure 3.1.

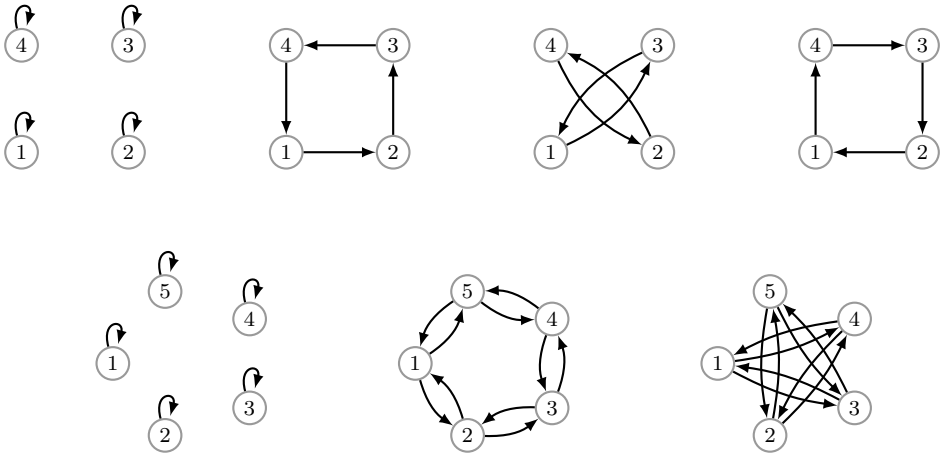


Figure 3.1: Orbital graphs for the groups C_4 and D_5.

Recall that, by definition, an *automorphism* of a digraph (Ω, E) is a permutation $\sigma \in Sym(\Omega)$ of its set of vertices such that, for any edge $e = (x, y) \in E$, the pair $\sigma(e) = (\sigma(x), \sigma(y))$ is also an edge. Clearly, the automorphism group of each orbital graph for the group G contains G:

$$G \subseteq \mathrm{Aut}(\mathrm{Graph}(\Theta)), \quad \text{for any orbital } \Theta. \tag{3.10}$$

Other properties of orbital graphs:

- the orbital graphs are *vertex-transitive* digraphs: for any two vertices x and y of Graph(Θ), there is an automorphism of the digraph that sends the vertex x to the vertex y (it is given by a permutation $\sigma \in G$ such that $\sigma(x) = y$);
- each vertex has the same indegree, as well as outdegree[7] (this follows from vertex-transitivity);
- if G is finite, then the indegree and outdegree of each vertex are equal to each other (since the sums of the indegrees and outdegrees are equal).

Thus, all finite nondiagonal orbital graphs are *regular* digraphs (*i.e.* there are no loops, each vertex has the same indegree and outdegree that are equal to each other).

There is a natural bijection between the orbitals of G and the orbits of a point stabiliser G_x (recall that since G is transitive, the point stabilizers are conjugate in G). To the orbital Θ corresponds the following G_x-orbit

$$\Theta(x) := \{y \in \Omega \mid (x, y) \in \Theta\} = G_x \cdot y_0, \quad \text{for an arbitrary } y_0 \in \Omega \text{ such that } (x, y_0) \in \Theta.$$

In other words, $\Theta(x)$ is the set of vertices lying on an edge from x in the digraph Graph(Θ). The bijection $\Theta \mapsto \Theta(x)$ in particular tells us that the number of G_x-orbits is equal to the rank r of G.

[7] The *indegree* of a vertex x is the number of edges to x, its *outdegree* is the number of edges from x.

The G_x-orbits are called *suborbits*, and their cardinalities are the *subdegrees* of G. If the transitive permutation group G is of finite degree n, then the list of its subdegrees

$$1 = n_1 \leq n_2 \leq \ldots \leq n_r, \quad \text{where } n = n_1 + n_2 + \ldots + n_r,$$

is an invariant of G (that is, of the equivalence class of representations $G \to Sym(\Omega)$). The first subdegree $n_1 = 1$ corresponds to the trivial orbit $\{x\}$, or else to the diagonal orbital. As for the second subdegree, remark that the set $\Delta = \mathrm{fix}(G_x) = \{y \in \Omega \mid G_x \cdot y = \{y\}\}$ is a block for G:

if $y \in \Delta$ then $G_x \subseteq G_y$, and so $G_x = G_y$ due to transitivity of G,

if also $\sigma(y) \in \Delta$ for some $\sigma \in G$, then $G_x = G_{\sigma(y)} = \sigma G_y \sigma^{-1} = \sigma G_x \sigma^{-1}$, and so $\sigma(\Delta) = \Delta$.

Therefore, in the case where G is primitive, there are two possibilities:

- either $\mathrm{fix}(G_x) = \{x\}$ implying the inequality $n_2 > 1$,
- or $\mathrm{fix}(G_x) = \Omega$, that is, $G_x = \{1\}$ and the group G is regular of prime degree (in a primitive group, the point stabilizers are maximal subgroups). In this case, we have $r = n$ and $n_1 = n_2 = \ldots = n_r = 1$.

Recall that a digraph is *connected* if for any two vertices x and y there exists an undirected path from x to y (that is, a sequence of vertices $x = v_0, v_1, \ldots, v_m = y$ such that, for each i, the vertices v_i and v_{i+1} are adjacent). The digraph is called *strongly connected* if such a path can always be chosen directed (for each i, there is an edge from v_i to v_{i+1}).

A graph-theoretic test of primitivity is provided by the following theorem.

Theorem 3.13 (Higman)**.** *A transitive permutation group G is primitive if and only if all its nondiagonal orbital graphs are connected.*

Proof. $\boxed{\Longrightarrow}$ Let Θ be a nondiagonal orbital. The set Δ of vertices of a connected component of the graph $\mathrm{Graph}(\Theta)$ is a block for G. This is due to (3.10) and the fact that the automorphisms of a graph permute its connected components. Therefore, if G is primitive, then $\mathrm{Graph}(\Theta)$ is connected. $\boxed{\Longleftarrow}$ Let $\mathrm{Graph}(\Theta)$ be a connected orbital graph and Δ be a block for G. For any point $x \in \Delta$, the set $N(x)$ of the neighbours of the vertex x in the orbital graph satisfies the condition:

$$\text{either } \; N(x) \cap \Delta = \emptyset \quad \text{or} \quad N(x) \subset \Delta.$$

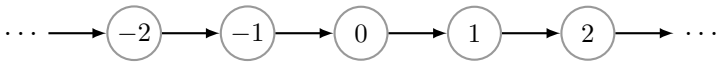
Indeed, if $y \in N(x) \cap \Delta$ and $z \in N(x)$ then, by definition of $\mathrm{Graph}(\Theta)$, there exists a permutation $\sigma \in G$ such that $\sigma^{-1} \cdot \{x, z\} = \{x, y\} \subset \Delta$. Since Δ is a block for G and $x \in \sigma(\Delta) \cap \Delta$, it follows that $\sigma(\Delta) = \Delta$ and so $z \in \Delta$.

Suppose now that Δ has at least two points x_0 and y, and let Θ be the orbital which contains the pair (x_0, y). Then $y \in N(x_0) \cap \Delta$ implies that $N(x_0) \subset \Delta$. Furthermore, for any neighbour x_1 of the vertex x_0, we have $x_0 \in N(x_1) \cap \Delta$ and thus $N(x_1) \subset \Delta$. By recurrence on k, we prove that any undirected path $\{x_0, x_1, \ldots, x_k\}$ of length k in the orbital graph is a subset of Δ. Since the graph $\mathrm{Graph}(\Theta)$ is connected, we obtain $\Delta = \Omega$, that is, the block Δ must be trivial. □

Proposition 3.14. *If a finite vertex-transitive digraph is connected, then it is strongly connected. In particular, each nondiagonal orbital graph for a finite primitive permutation group G is strongly connected.*

Proof. Let x be a vertex of the connected digraph, and denote by $D(x)$ the set of vertices which can be reached by directed paths from x. For any vertex $y \in D(x)$, we have the evident inclusion $D(y) \subseteq D(x)$. Moreover, if σ is an automorphism of the graph such that $\sigma \cdot x = y$, then $\sigma \cdot D(x) = D(y)$. Thus $D(x)$ and $D(y)$ have the same (finite) cardinality, and so are equal. As a conclusion: if there is a directed path from x to y, then there is a directed path from y to x as well. Since the digraph is connected, it is strongly connected. □

The proposition above is false in the infinite case: let $G = \langle\sigma\rangle$ be an infinite cyclic group acting on $\mathbb{Z}$ by the shift $\sigma \cdot n = n + 1$. Then the graph of the orbital $\Theta = \{(n, n+1) \mid n \in Z\}$ is connected but not strongly connected (see the figure).



Proposition 3.15. *Let G be a primitive permutation group of finite degree n and rank $1 < r < n$. The following inequalities for the subdegrees $1 = n_1 < n_2 \le \ldots \le n_r$ of the group G are satisfied:*

$$n_{i+1} \le n_i(n_2 - 1) \quad \text{for all } i > 1.$$

In particular, we have the following upper bound

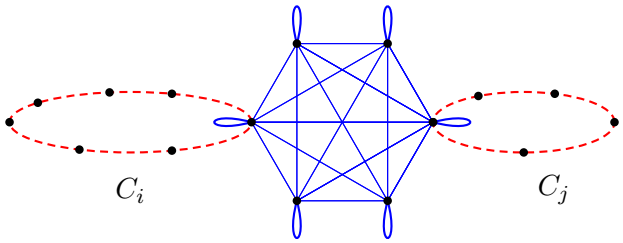
$$n \le 1 + n_2 + n_2(n_2 - 1) + \cdots + n_2(n_2 - 1)^{r-2} = \frac{n_2(n_2 - 1)^{r-1} - 2}{n_2 - 2}.$$

Proof. See Theorem 3.2B and Lemma 3.2B in the book [25] by John D. Dixon and Brian Mortimer, or Theorem 3.14 in the book [15] by Peter J. Cameron. □

Remark. Recall that for $r = 1$ and $r = n$, we have $n_1 = n_2 = \ldots = n_r = 1$.

Lemma 3.16. *Let (V, E) be a connected graph with edges colorod blue and red. Suppose that the subgraph induced by the blue edges has r connected components and that the subgraph induced by the red edges has s connected components and m vertices. Then one has the inequality $r + s \le m + 1$.*

Proof. Denote by C_1, C_2, …, C_s the red connected components. Since the graph (V, E) is connected, through each blue connected component passes at least one C_i.



Let us compress the vertices from every blue connected component into one point and erase the blue edges – we will obtain a connected graph (V', E') with r vertices and only red edges (more accurately, (V', E') will be a *multigraph*, that is, it may contain multiple edges). Such a graph is also a union of the s red connected components, in which some vertices are identified. Identifications of vertices from distinct components can be performed in order. Namely, if $s > 1$, then the graph C_1 is glued to another red component, let it be C_2. (We say that two graphs X and Y are *glued* if a vertex x of X is identified with a vertex y of Y, giving a graph of cardinal $|X| + |Y| - 1$, that we will denote by $X \underset{x=y}{\star} Y$ or simply by $X \star Y$.) If $s > 2$, then another component, for instance C_3, is glued to $C_1 \star C_2$. And so on, the graph C_k is glued to $C_1 \star C_2 \star \ldots \star C_{k-1}$ for k from 2 to s, due to the connectivity of (V', E'). Since the graph (V', E') is the result of $s - 1$ such gluings plus possibly other identifications of vertices, and since after each gluing the number of vertices is decreased by 1, we get

$$r \le m - (s - 1) = m - s + 1,$$

where $m = |C_1| + |C_2| + \ldots + |C_s|$. □

Proposition 3.17. *Let $G \subseteq S_n$ be a primitive permutation group containing a permutation σ with s nontrivial disjoint cycles and $|\mathrm{supp}(\sigma)| = m$. Then the rank of G is bounded from above by:*

$$r(G) \leq m - s + 1.$$

Proof. Let $u \in \mathrm{supp}(\sigma)$. Since the group G is primitive, the stabilizer G_u is a maximal subgroup and so $G = \mathsf{gp}\{\sigma, G_u\}$. Construct an undirected graph (V, E) with edges colored blue and red as follows: the set of vertices is $V = \{1, 2, \ldots, n\}$, two vertices $x, y \in V$ are connected by a blue edge if there is a permutation $\tau \in G_u$ such that $\tau(x) = y$, and they are connected by a red edge if $x \neq y$ and $\sigma(x) = y$. The subgraph of (V, E) induced by the blue edges has n vertices and $r(G)$ connected components. The subgraph induced by the red edges has m vertices and consists of s disjoint cycles, denote them by C_1, C_2, …, C_s. Since the group G is transitive and $G = \mathsf{gp}\{\sigma, G_u\}$, the graph (V, E) is connected. By Lemma 3.16, we obtain

$$r(G) \leq m - s + 1,$$

where $m = |C_1| + |C_2| + \ldots + |C_s|$ as required. □

Lemma 3.18. *Let $G \subseteq S_n$ be an arbitrary permutation group, and let Δ_1 and Δ_2 be two subsets of $\{1, 2, \ldots, n\}$. If we have $\sigma(\Delta_1) \cap \Delta_2 \neq \emptyset$ for all $\sigma \in G$, then there exists $x_0 \in \Delta_1$ such that*

$$|G \cdot x_0| \leq |\Delta_1| \cdot |\Delta_2|.$$

Proof. We will use the following classical lemma of Bernhard Hermann Neumann (see [74, 1954]): if a group G is a finite union of left cosets

$$G = \bigcup_{i=1}^{m} g_i H_i$$

for some subgroups $H_i \subseteq G$ and some elements $g_i \in G$, then $|G : H_i| \leq m$ for at least one i.

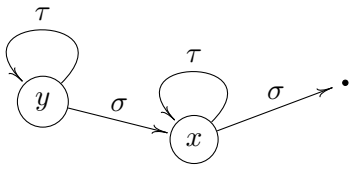
Delegate to every $x \in \Delta_1$ and $y \in (G \cdot x) \cap \Delta_2$ a permutation $\sigma_{xy} \in G$ sending x to y. By the hypothesis, for any $\sigma \in G$ there exists $x \in \Delta_1$ such that $\sigma(x) \in \Delta_2$. Hence, the permutation σ lies in the coset $\sigma_{xy} G_x$, where $y = \sigma(x)$. Since there are at most $|\Delta_1| \cdot |\Delta_2|$ of these cosets, Neumann's lemma shows that $|G : G_{x_0}| \leq |\Delta_1| \cdot |\Delta_2|$ for some $x_0 \in \Delta_1$ as required. □

Lemma 3.19. *Let σ, $\tau \in S_n$ be two permutations, and denote $\Delta = \mathrm{supp}(\sigma) \cap \mathrm{supp}(\tau)$. Then*

$$\mathrm{supp}([\sigma, \tau]) \subseteq \Delta \cup \sigma(\Delta) \cup \tau(\Delta).$$

In particular, if the supports of σ and τ have exactly one point in common, then $[\sigma, \tau]$ is a 3-cycle.

Proof. A point $x \in \mathrm{supp}([\sigma, \tau])$ belongs to the union $\mathrm{supp}(\sigma) \cup \mathrm{supp}(\tau)$, say $\sigma(x) \neq x$. Let us suppose that $x \notin \Delta \cup \sigma(\Delta) \cup \tau(\Delta)$.



Then it follows from $x \notin \Delta$ and $\sigma(x) \neq x$ that $\tau^{-1}(x) = x$. Furthermore, from $\sigma^{-1}(x) \notin \Delta$ and $\sigma(\sigma^{-1}(x)) \neq \sigma^{-1}(x)$ we have that $\tau(\sigma^{-1}(x)) = \sigma^{-1}(x)$. This gives

$$[\sigma, \tau] \cdot x = \sigma\tau\sigma^{-1}\tau^{-1}(x) = \sigma\tau(\sigma^{-1}(x)) = x,$$

which contradicts the assumption that $x \in \mathrm{supp}([\sigma, \tau])$. Therefore, $x \in \Delta \cup \sigma(\Delta) \cup \tau(\Delta)$ as required. □

Theorem 3.20. *Let G be a primitive permutation group of degree n not containing A_n. Suppose that the group G has an element σ with $|\mathrm{supp}(\sigma)| = m$, where $m \geq 4$. Then*

$$n < (m-1)^{2m}.$$

Moreover, if G is 2-transitive, then necessarily $n \leq 1 + (m-1)^2$.

Proof. Consider the set $\Delta = \mathrm{supp}(\sigma) \setminus \{x\}$ for some point $x \in \mathrm{supp}(\sigma)$. Suppose that there exists a permutation $\tau \in G_x$ such that $\tau(\Delta) \cap \Delta = \emptyset$. Then

$$\begin{aligned} \text{for any } y \in \mathrm{supp}(\sigma) \setminus \{x\} \quad & \text{one has } \tau(y) \notin \mathrm{supp}(\sigma) \setminus \{x\}, \\ & \text{that is, either } \sigma(\tau(y)) = \tau(y) \text{ or } \tau(y) = x, \\ & \text{and so } y \notin \mathrm{supp}(\tau^{-1}\sigma\tau) \setminus \{x\}. \end{aligned}$$

Therefore, the supports of the permutations σ and $\tau^{-1}\sigma\tau$ have exactly one point in common, namely $\mathrm{supp}(\sigma) \cap \mathrm{supp}(\tau^{-1}\sigma\tau) = \{x\}$, and so Lemma 3.19 shows that G contains a 3-cycle. By Jordan's theorem, the group G must be A_n or S_n, which is not the case.

Now, we have that $\tau(\Delta) \cap \Delta \neq \emptyset$ for any $\tau \in G_x$. According to Lemma 3.18, the group G_x has an orbit $G_x \cdot x_0$, where $x_0 \in \Delta$, of length

$$|G_x \cdot x_0| \leq |\Delta| \cdot |\Delta| = (m-1)^2.$$

In particular, the second subdegree n_2 of the permutation group G is not greater than $(m-1)^2$. Using Proposition 3.15 and the fact that the rank $r = r(G)$ of G is at most m (see Proposition 3.17), we get:

$$n \leq 1 + n_2 + n_2^2 + \ldots + n_2^{r-1} < n_2^r \leq (m-1)^{2m}.$$

When G is 2-transitive, we have $r = 2$ and $n \leq 1 + n_2 \leq 1 + (m-1)^2$ as required. □

3.4 The stratum $\mathcal{H}(1,1)$

The total number $\mathscr{N}_n^{\mathrm{pr}}(1,1)$ of primitive n-square-tiled surfaces in the stratum $\mathcal{H}(1,1)$,

$$\mathscr{N}_n^{\mathrm{pr}}(1,1) = \frac{1}{6} n^2 (n-2)(n-3) \prod_{\substack{p \mid n \\ p \text{ prime}}} \left(1 - \frac{1}{p^2}\right), \tag{3.11}$$

that can be derived from the results of the papers [11] by Spencer Bloch and Andrei Okounkov and [23] by Robbert Dijkgraaf.

Table 3.1: The number of primitive n-square-tiled surfaces in the stratum $\mathcal{H}(1,1)$ for $4 \leq n \leq 17$.

n	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$\mathscr{N}_n^{\mathrm{pr}}(1,1)$	4	24	48	160	240	504	672	1440	1440	3080	3168	4992	5824	10080

The theorem below is based on results of Camille Jordan going back to 1875 (see [53]). The proof, that we are going to present, mostly follows Example 3.3.1 of the textbook [25] by John D. Dixon and Brian Mortimer.

Theorem 3.21. *For each integer $n \neq 6$, the monodromy group of any primitive n-square-tiled surface from $\mathcal{H}(1,1)$ is either A_n or S_n.*

Proof. By Theorem 3.2, the smallest origamis in the stratum $\mathcal{H}(1,1)$ have 4 squares. The $\mathrm{SL}(2,\mathbb{Z})$-orbits of n-square-tiled surfaces with $n \in \{4,5,6\}$ are given in Table B.2 (the data is obtained using mathematics software systems Sage and GAP). As we see in the table, when $n=4$, only one primitive group occurs, namely A_4. When $n=5$, there is only S_5. An exception for $n=6$: besides A_6, we have another primitive monodromy group, which is an index 6 subgroup of S_6.

When $7 \leq n \leq 17$, there are two orbits of primitive origamis in $\mathcal{H}(1,1)$ – they correspond to the monodromy groups A_n and S_n. This is illustrated in Table B.3, obtained using a program in Sage. An algorithm for such a program is quite simple:

- ▷ for a given n from 11 to 17, pick an origami O_A with monodromy group A_n, and an origami O_S with monodromy group S_n,
- ▷ find the lengths l_A and l_S of the $\mathrm{SL}_2(\mathbb{Z})$-orbits of the origamis O_A and O_S, respectively,
- ▷ check that $l_A + l_S = \mathscr{N}_n^{\mathrm{pr}}(1,1)$, see Table 3.1, and conclude that there are only two orbits of primitive n-square origamis.

This is closely related to Conjecture 1 stated at the end of the section.

Now, assume that $n \geq 18$ and consider a primitive n-square-tiled surface $O = (\sigma, \tau)^*$ from the stratum $\mathcal{H}(1,1)$. The monodromy group $G = \mathcal{M}on(O)$ is a primitive permutation subgroup of S_n containing the following element (up to conjugation of σ and τ):

$$\mu = [\sigma, \tau] = (1\ 2)(3\ 4).$$

Note that $|\mathrm{supp}(\mu)| = 4$. According to Proposition 3.17, the rank r of G is not greater than $4-2+1 = 3$. Suppose that G is distinct from A_n and S_n. Then by Theorem 3.20, when G is 2-transitive (the case that $r=2$), we have the upper bound $n \leq 1+(4-1)^2 = 10$, which is false. Thus, the rank of G is 3.

Denote by $H \subset G$ the stabilizer of 1 for the action on the set $\{1,2,\ldots,n\}$, and let $\Delta_1 = \{1\}$, Δ_2 and Δ_3 be the orbits of H. The respective lengths $1 = n_1 \leq n_2 \leq n_3$ of these orbits are the subdegrees of the group G. Due to Proposition 3.15, we obtain

$$18 \leq n = n_1 + n_2 + n_3 \leq 1 + n_2 + n_2(n_2-1) = 1 + (n_2)^2,$$

from where $n_2 \geq 5$.

By the primitivity of G, the subgroup H is maximal (see Lemma 2.3), and so $G = \mathtt{gp}\{H, \mu\}$. Hence, neither Δ_2 nor Δ_3 contains all the numbers 2, 3 and 4.

Define the following subsets of H:

$$B_{xy} = \{\lambda \in H \mid \lambda(x) = y\}, \quad \text{where } 2 \leq x, y \leq 4.$$

Let us show that the union of these subsets is the whole H,

$$H = \bigcup_{2 \leq x,y \leq 4} B_{xy}.$$

Indeed, for any permutation $\delta \in H$ such that

$$\begin{array}{rl} \delta: & 2 \mapsto a \\ & 3 \mapsto b \\ & 4 \mapsto c \end{array}$$

we must have $\{a,b,c\}\cap\{2,3,4\}\neq\emptyset$. Otherwise, the commutator of the permutations $\mu=(1\ 2)(3\ 4)$ and $\delta\mu\delta^{-1}=(1\ a)(b\ c)$ would be a 3-cycle $(1\ 2\ a)$, and by Jordan's theorem G would contain A_n.

Furthermore, let us find the cardinals of B_{xy}. If x and y belong to the same orbit Δ_i for $i\in\{2,3\}$, then B_{xy} is a coset of the point stabilizer B_{xx} in the group H acting transitively on Δ_i, and we have

$$|B_{xy}|=|B_{xx}|=|B_{yy}|=|B_{yx}|=\frac{|H|}{|\Delta_i|}=\frac{|H|}{n_i}.$$

If x and y belong to distinct orbits, then B_{xy} is empty, $|B_{xy}|=0$.

Since a Δ_p, where $p\in\{2,3\}$, contains exactly two of the numbers $2,3,4$ and another Δ_q, where $q\in\{2,3\}\setminus\{p\}$, contains the third one, we get

$$|H|=\left|\bigcup_{2\leq x,y\leq 4}B_{xy}\right|\leq\bigcup_{2\leq x,y\leq 4}|B_{xy}|=4\cdot\frac{|H|}{n_p}+\frac{|H|}{n_q}.$$

However, the lower bounds $5\leq n_2\leq n_3$ and $18\leq 1+n_2+n_3$ imply that $\frac{4}{n_p}+\frac{1}{n_q}<\frac{4}{5}+\frac{1}{5}=1$. This contradiction shows that the primitive group G is either A_n or S_n. □

Let us give, for $n\geq 4$, two families of n-square-tiled surfaces from $\mathcal{H}(1,1)$ with monodromy groups containing the alternating group of degree n. Consider the following n-square-tiled surfaces ("*panties*"), where $1\leq l<h\leq n/2$:

$P_n^{l,h}=$

1	⋯	l	$l+1$	⋯	h
$h+1$	⋯	$h+l$	$h+l+1$	⋯	$n-1$	n

encoded by $\sigma_n=(1\ 2\ \ldots\ h)(h+1\ h+2\ \ldots\ n)$, $\tau_n=(1\ h+1)(2\ h+2)\ldots(l\ h+l)$

and

$Q_n^{l,h}=$

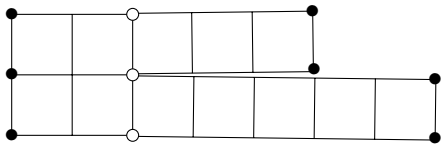
1	⋯	l	$l+1$	⋯	h
$h+1$	⋯	$h+l$	$h+l+1$	⋯	$n-1$	n

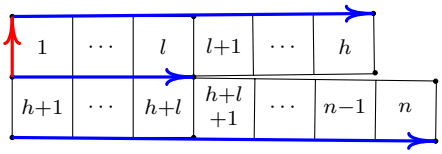
encoded by $\upsilon_n=(1\ 2\ \ldots\ n)=(1\ h+1)\,\sigma_n$, $\tau_n=(1\ h+1)(2\ h+2)\ldots(l\ h+l)$.

We have $[\sigma_n,\tau_n]=[\upsilon_n,\tau_n]=(1\ h+1)(l+1\ h+l+1)$, so these origamis belong to $\mathcal{H}(1,1)$.

Proposition 3.22. *The origamis $P_n^{l,h}$ and $Q_n^{l,h}$ are reduced if and only if $\gcd(l,h,n)=1$. They are primitive if and only if $\gcd(h,n)=1$.*

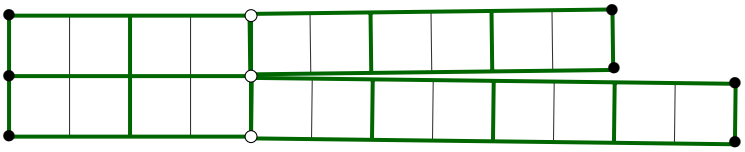
Proof. (*Reducibility*) $\boxed{\Longleftarrow}$ Consider an origami $P_n^{l,h}$, the case of $Q_n^{l,h}$ being analogous. It has two ramification points, indicated at the picture below by $\bullet$ and $\circ$:





The lattice of periods $\mathrm{Per}(\omega)\subseteq\mathbb{Z}\oplus\sqrt{-1}\,\mathbb{Z}$ of the square-tiled surface $P_n^{l,h}=(M,\omega)$ is the set of linear combinations of the relative periods $\int_{Z_j}^{Z_k}\omega$ with integer coefficients, and thus contains the vectors $1+0\sqrt{-1}$, $\mathfrak{l}=0+l\sqrt{-1}$, $\mathfrak{h}=0+h\sqrt{-1}$ and $\mathfrak{n}=0+n\sqrt{-1}$. Suppose that $\gcd(l,h,n)=1$, then there exist integers $a,b,c\in\mathbb{Z}$ for which $a\mathfrak{l}+b\mathfrak{h}+c\mathfrak{n}=0+1\sqrt{-1}$. Hence, we have $\mathrm{Per}(\omega)=\mathbb{Z}\oplus\sqrt{-1}\,\mathbb{Z}$, and the origami $P_n^{l,h}$ is reduced.

$\Longrightarrow$ Conversely, if $\gcd(l,h,n) = m > 1$, then the origami $P_n^{l,h}$ is a one branch point covering of the torus obtained from the rectangle $1 \times m$ by gluing its opposite sides (see the picture below). In this case, the origami is not reduced.



(*Primitivity*) $\Longleftarrow$ Suppose that the integers h and n are coprime, where $1 \leq l < h < n/2$. Let us show that the monodromy group $G = \mathcal{M}on(P_n^{l,h}) = \mathtt{gp}\{\sigma_n, \tau_n\}$ is primitive. Indeed, take a block Δ for G, containing 1 and another integer $x \neq 1$. Consider the case where $h \leq x \leq n$. Since $\gcd(h, n-h) = 1$, for any integer c there exists $a \in \mathbb{Z}$ such that $ah \equiv c \bmod (n-h)$. Then the permutation $(\sigma_n)^{ah} = (h{+}1 \;\; h{+}2 \;\; \ldots \;\; n)^c$ stabilizes 1, and, for a suitable c, sends x to any integer from $h+1$ to n. Therefore, we have $(\sigma_n)^{ah}(\Delta) = \Delta$, and so the block Δ contains the integers $1, h+1, h+2, \ldots, n$, which is more than $n/2$ elements. As the cardinal $|\Delta|$ divides n, it must be n, and Lemma 2.2 implies that the group G is primitive. In the case where $1 < x \leq h$, let k be a positive integer such that $(1\;2\;\ldots\;h)^k \cdot 1 > l$ but $(1\;2\;\ldots\;h)^k \cdot x \leq l$. Then we have

$$\sigma_n^{-k}\tau_n\sigma_n^k \cdot 1 = 1 \quad \text{and} \quad \sigma_n^{-k}\tau_n\sigma_n^k \cdot x = y \quad \text{with} \quad h \leq y \leq n.$$

This means that $\sigma_n^{-k}\tau_n\sigma_n^k(\Delta) = \Delta$ and the block Δ contains 1 and y, which allows us to use the previous argument to conclude that the group G is primitive.

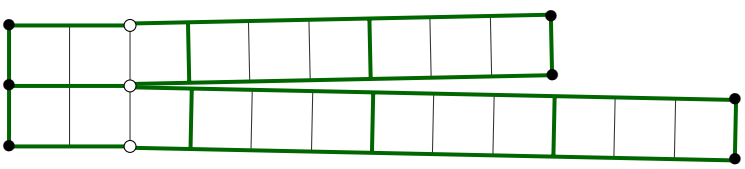
Let us now show that the monodromy group $H = \mathcal{M}on(Q_n^{l,h}) = \mathtt{gp}\{\upsilon_n, \tau_n\}$ is primitive too. Consider a block Δ for H containing 1 and another integer $x \neq 1$. Denote $\lambda = \tau(\upsilon_n)^h$. Since υ_n is an n-cycle and $\gcd(h,n) = 1$, the permutation $(\upsilon_n)^h$ is also an n-cycle. Each integer $a \in [1,l]$ is sent by $(\upsilon_n)^h$ to the integer $h{+}a \in [h{+}1, h{+}l]$. As $(a \;\; h{+}a)(\ldots\; s\; a\; h{+}a\; t\; \ldots) = (\ldots\; s\; h{+}a\; t\; \ldots)$, the permutation

$$\lambda = \tau{\cdot}\upsilon_n^h = (1\;\; h{+}1)(2\;\; h{+}2)\ldots(l\;\; h{+}l){\cdot}\upsilon_n^h$$

is an $(n{-}l)$-cycle fixing the integers $1, 2, \ldots, l$. In particular λ stabilizes 1, implying that $\lambda(\Delta) = \Delta$ and $\lambda^k \cdot x \in \Delta$ for any $k \in \mathbb{Z}$. Therefore, if $l < x \leq n$, then the integers from $l{+}1$ to n belong to the block Δ, that is $|\Delta| > n/2$ and so $|\Delta| = n$. By Lemma 2.2, the group H is primitive. In the case where $1 < x \leq l$, we have

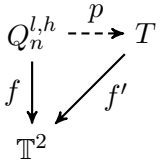
$$\tau(\upsilon_n)^{h+1-x} \cdot x = 1 \quad \text{and} \quad \tau(\upsilon_n)^{h+1-x} \cdot 1 = y, \quad \text{where} \quad y = \begin{cases} h+1-x & \text{if } \; h+1-x > l, \\ 2h+1-x & \text{if } \; h+1-x \leq l. \end{cases}$$

Hence, $\tau(\upsilon_n)^{h+1-x}(\Delta) = \Delta$ and the block Δ also contains an integer y such that $l < y \leq n$, allowing us to apply the previous argument for the primitivity of H.

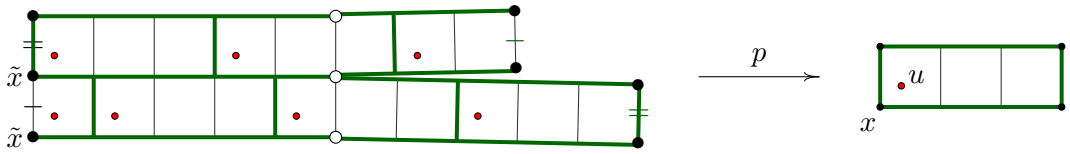


$\Longrightarrow$ Conversely, if $\gcd(h,n) = m > 1$, then the origamis $P_n^{l,h}$ and $Q_n^{l,h}$ are ramified coverings of the torus obtained from the rectangle $1 \times m$ by gluing its opposite sides (see the picture above). $\square$

Remark. Let us sketch another proof of the fact that the condition $\gcd(h,n)=1$ implies the primitivity of $P_n^{l,h}$ and $Q_n^{l,h}$. By the first part of the proposition, we obtain that the origamis $P_n^{l,h}$ and $Q_n^{l,h}$ are reduced. Suppose that they are not primitive. Then they must be ramified coverings of tori with two branch points (see Lemma 3.1). Therefore, $P_n^{l,h}$ and $Q_n^{l,h}$ are paved by horizontal rectangles $1\times m$ with $m>1$. For the origami $P_n^{l,h}$, this means that m is a common divisor of h and n, which is impossible, and so $P_n^{l,h}$ is primitive. As for $Q_n^{l,h}$, we have a commutative diagram:



where T is a trivial origami of area m (rectangle $1\times m$ with glued opposite sides) and $p: Q_n^{l,h}\to T$ is a covering with two branch points. The ramification point $\tilde{x}\in Q_n^{l,h}$ (corresponding to $\bullet$ at the picture) is projected by the map p to one of the branch points, denote it by $x\in T$. The conditions $\gcd(h,n)=1$ and $m|n$ imply that $\gcd(h,m)=1$, and so $\tilde{x}$ occurs at vertices and in the interior of sides of the pavement rectangles, as shown at the picture below:



Namely, the preimage $p^{-1}(u)$ of a point u from a neighbourhood of $x\in T$ has at least $n/m+1$ points, whilst the degree of the covering p is n/m. This contradiction proves that the origami $Q_n^{l,h}$ is primitive.

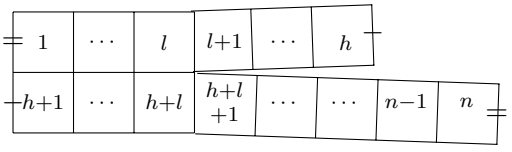
Lemma 3.23. *Let l,h,l',h' be positive integers such that $1\le l<h\le n/2$, $1\le l'<h'\le n/2$ and $(l,h)\ne(l',h')$. Then the origamis $P_n^{l,h}$, $Q_n^{l,h}$, $P_n^{l',h'}$ and $Q_n^{l',h'}$ are distinct.*

Proof. The square-tiled surfaces in question are encoded by the following permutations:

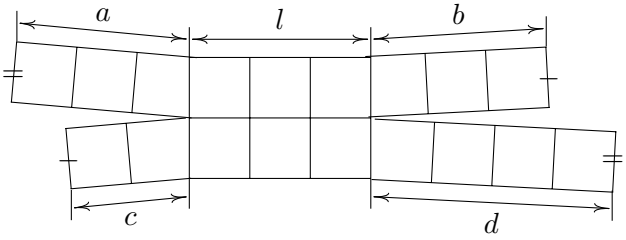
$$\begin{aligned}
\sigma_n &= (1\ 2\ \dots\ h)(h+1\ \ h+2\ \dots\ n),\\
\tau_n &= (1\ \ h+1)(2\ \ h+2)\dots(l\ \ h+l),\\
\upsilon_n &= (1\ 2\ \dots\ n),\\
\sigma'_n &= (1\ 2\ \dots\ h')(h'+1\ \ h'+2\ \dots\ n),\\
\tau'_n &= (1\ \ h'+1)(2\ \ h'+2)\dots(l'\ \ h'+l'),
\end{aligned}$$

namely, $P_n^{l,h}=(\sigma_n,\tau_n)^*$, $Q_n^{l,h}=(\upsilon_n,\tau_n)^*$, $P_n^{l',h'}=(\sigma'_n,\tau'_n)^*$ and $Q_n^{l',h'}=(\upsilon_n,\tau'_n)^*$. Remark at once that $P_n^{l,h}\ne Q_n^{l,h}$ and $P_n^{l,h}\ne Q_n^{l',h'}$, since the permutations σ_n and υ_n are not conjugate.

If $l\ne l'$, then we have $P_n^{l,h}\ne P_n^{l',h'}$ and $Q_n^{l,h}\ne Q_n^{l',h'}$, because τ_n and τ'_n are not conjugate. When $l=l'$ but $h\ne h'$, we also have $P_n^{l,h}\ne P_n^{l,h'}$, since the permutations σ_n and σ'_n are not conjugate. Finally, the origamis $Q_n^{l,h}$ and $Q_n^{l,h'}$ are distinct as well. Indeed, the only connected figures with a $2\times l$ rectangle, that can be obtained from the figure

$Q_n^{l,h}=$ 

by re-gluing squares, are



where $\{a+d,\, b+c\} = \{h-l,\, n-h-l\}$. Since either b or d must be less than $h'-l \le n-h'-l$, we have $Q_n^{l,h} \neq Q_n^{l,h'}$. □

Let $1 = d_1 < d_2 < \ldots < d_{\varphi(n)} = n-1$ be the numbers less than n that are coprime to n. Denote by $\vartheta_1(n)$ and $\vartheta_2(n)$ the following sums

$$\vartheta_1(n) := \sum_{i=1}^{\varphi(n)} d_i \quad \text{and} \quad \vartheta_2(n) := \sum_{i=1}^{\varphi(n)/2} d_i. \tag{3.12}$$

By $\vartheta_1'(n)$ and $\vartheta_2'(n)$ we denote the following sums

$$\vartheta_1'(n) := \sum_{i=1}^{\varphi(n)} \left[\frac{d_i}{2}\right] \quad \text{and} \quad \vartheta_2'(n) := \sum_{i=1}^{\varphi(n)/2} \left[\frac{d_i}{2}\right]. \tag{3.13}$$

Lemma 3.24. a) *For any positive integer $n > 1$, one has*[8] $\vartheta_1(n) = \dfrac{n\varphi(n)}{2}$.

b) *In the case that n is a multiple of 4, one has* $\vartheta_2(n) = \dfrac{n\varphi(n)}{8}$.

c) *If $n > 1$ is odd, then* $\vartheta_1'(n) = \dfrac{\vartheta_1(n)}{2} - \dfrac{\varphi(n)}{4}$, *else* $\vartheta_1'(n) = \dfrac{\vartheta_1(n)}{2} - \dfrac{\varphi(n)}{2}$.

d) *If $n > 1$ is even, then* $\vartheta_2'(n) = \dfrac{\vartheta_2(n)}{2} - \dfrac{\varphi(n)}{4}$.

Proof. a) From the relations

$$d_1 + d_{\varphi(n)} = n, \quad d_2 + d_{\varphi(n)-1} = n, \quad \ldots \quad , \quad d_{\varphi(n)/2} + d_{\varphi(n)/2+1} = n, \tag{3.14}$$

we obtain $\vartheta_1(n) = n \cdot \frac{\varphi(n)}{2}$ that shows the first part of the lemma.

b) If n is divisible by 4, then we have $\gcd(\frac{n}{2} + d_i, n) = 1$ and the sets $\{d_1, d_2, \ldots, d_{\varphi(n)}\}$ and $\{d_1, \ldots, d_{\varphi(n)/2}, \frac{n}{2} + d_1, \ldots, \frac{n}{2} + d_{\varphi(n)/2}\}$ coincide. Therefore,

$$\vartheta_1(n) = \sum_{i=1}^{\varphi(n)} d_i = \sum_{i=1}^{\varphi(n)/2} d_i + \sum_{i=1}^{\varphi(n)/2} \left(\frac{n}{2} + d_i\right) = 2 \cdot \sum_{i=1}^{\varphi(n)/2} d_i + \frac{n}{2} \cdot \frac{\varphi(n)}{2},$$

and so $\vartheta_2(n) = \frac{1}{2}\left(\vartheta_1(n) - \frac{n\varphi(n)}{4}\right) = \frac{n\varphi(n)}{8}$ as required.

c) If n is odd, then all numbers d_i and $d_{\varphi(n)-i+1} = n - d_i$ have opposite parities for all $1 \le i \le \frac{\varphi(n)}{2}$. Thus $\left[\frac{d_i}{2}\right] + \left[\frac{d_{\varphi(n)-i+1}}{2}\right] = \frac{d_i}{2} + \frac{d_{\varphi(n)-i+1}}{2} - \frac{1}{2}$, and so

$$\vartheta_1'(n) = \sum_{i=1}^{\varphi(n)} \left[\frac{d_i}{2}\right] = \sum_{i=1}^{\varphi(n)} \frac{d_i}{2} - \frac{1}{2} \cdot \frac{\varphi(n)}{2} = \frac{\vartheta_1(n)}{2} - \frac{\varphi(n)}{4}.$$

[8] Here φ is Euler's totient function, $\varphi(n) = n \prod\limits_{\substack{p \mid n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right)$.

If n is even, then all d_i are odd and $\left[\frac{d_i}{2}\right] = \frac{d_i}{2} - \frac{1}{2}$. Therefore,

$$\vartheta_1'(n) = \sum_{i=1}^{\varphi(n)} \left[\frac{d_i}{2}\right] = \sum_{i=1}^{\varphi(n)} \left(\frac{d_i}{2} - \frac{1}{2}\right) = \frac{\vartheta_1(n)}{2} - \frac{\varphi(n)}{2}. \tag{3.15}$$

d) For even n, we obtain that $\vartheta_2'(n) = \frac{\vartheta_2(n)}{2} - \frac{\varphi(n)}{4}$ if we replace $\varphi(n)$ by $\varphi(n)/2$ in (3.15). □

Proposition 3.25. *Let $n \geq 4$ be a positive integer. If n is odd, then one has the following $2\vartheta_2(n)-\varphi(n)$ distinct primitive n-square-tiled surfaces in the stratum $\mathcal{H}(1,1)$:*

$$\vartheta_2(n) - \tfrac{\varphi(n)}{2} \text{ origamis } P_n^{l,h} \text{ such that } \mathcal{M}on(P_n^{l,h}) = S_n,$$

$$\vartheta_2'(n) \text{ origamis } Q_n^{l,h} \text{ such that } \mathcal{M}on(Q_n^{l,h}) = S_n,$$

$$\vartheta_2(n) - \vartheta_2'(n) - \tfrac{\varphi(n)}{2} \text{ origamis } Q_n^{l,h} \text{ such that } \mathcal{M}on(Q_n^{l,h}) = A_n.$$

If n is even, then one has the following $2\vartheta_2(n) - \varphi(n)$ distinct primitive n-square-tiled surfaces in the stratum $\mathcal{H}(1,1)$:

$$\tfrac{\vartheta_2(n)}{2} - \tfrac{\varphi(n)}{4} \text{ origamis } P_n^{l,h} \text{ such that } \mathcal{M}on(P_n^{l,h}) = S_n,$$

$$\tfrac{\vartheta_2(n)}{2} - \tfrac{\varphi(n)}{4} \text{ origamis } P_n^{l,h} \text{ such that } \mathcal{M}on(P_n^{l,h}) = A_n,$$

$$\vartheta_2(n) - \tfrac{\varphi(n)}{2} \text{ origamis } P_n^{l,h} \text{ such that } \mathcal{M}on(P_n^{l,h}) = S_n.$$

Proof. According to Proposition 3.22, for any pair (l,h) of positive integers such that $1 \leq l < h \leq n/2$ and $\gcd(h,n) = 1$, the square-tiled surfaces $P_n^{l,h}$ and $Q_n^{l,h}$ are primitive. By Theorem 3.21 for $n \geq 7$, the monodromy group of such a surface is either the alternating A_n or symmetric S_n, which depends on the parities of σ_n, υ_n and τ_n. We obtain Table 3.2.

Table 3.2: The monodromy groups of $P_n^{l,h}$ and $Q_n^{l,h}$, when $\gcd(h,n) = 1$.

n	l	τ_n	σ_n	υ_n	$\mathcal{M}on(P_n^{l,h})$	$\mathcal{M}on(Q_n^{l,h})$
odd	odd	odd	odd	even	S_n	S_n
	even	even				A_n
even	odd	odd	even	odd	S_n	S_n
	even	even			A_n	

Due to Lemma 3.23, all square-tiled surfaces $P_n^{l,h}$ and $Q_n^{l,h}$ are distinct. Among them, there are

$$2 \cdot \sum_{\substack{1 \leq l < h \leq n/2 \\ \gcd(h,n)=1}} 1 = 2 \cdot \sum_{i=1}^{\varphi(n)/2} \sum_{1 \leq l < d_i} 1 = 2 \cdot \sum_{i=1}^{\varphi(n)/2} (d_i - 1) = 2\vartheta_2(n) - \varphi(n)$$

primitive ones, where $1 = d_1 < d_2 < \ldots < d_{\varphi(n)} = n-1$ denote the positive integers less than n and coprime to n (we have $d_{\varphi(n)/2} < n/2$ and $d_{\varphi(n)/2+1} > n/2$ by (3.14)). The number of distinct primitive origamis $P_n^{l,h}$ and the number of distinct primitive origamis $Q_n^{l,h}$ coincide and are equal to

$$\sum_{\substack{1 \leq l < h \leq n/2 \\ \gcd(h,n)=1}} 1 = \vartheta_2(n) - \frac{\varphi(n)}{2}.$$

• If n is odd, then the number of distinct n-square origamis $Q_n^{l,h}$ with $\mathcal{M}on(Q_n^{l,h}) = S_n$ is given by

$$\sum_{\substack{1\leq l<h\leq n/2\\ \gcd(h,n)=1\\ l \text{ odd}}} 1 = \sum_{i=1}^{\varphi(n)/2} \sum_{\substack{1\leq l<d_i\\ l \text{ odd}}} 1 = \sum_{i=1}^{\varphi(n)/2} \left[\frac{d_i}{2}\right] = \vartheta_2'(n).$$

So, the number of distinct n-square origamis $Q_n^{l,h}$ with $\mathcal{M}on(Q_n^{l,h}) = A_n$ equals $\vartheta_2(n) - \vartheta_2'(n) - \frac{\varphi(n)}{2}$.

• If n is even, then the number of distinct n-square origamis $P_n^{l,h}$ with $\mathcal{M}on(P_n^{l,h}) = S_n$ is given by

$$\sum_{\substack{1\leq l<h\leq n/2\\ \gcd(h,n)=1\\ l \text{ odd}}} 1 = \sum_{i=1}^{\varphi(n)/2} \sum_{\substack{1\leq l<d_i\\ l \text{ odd}}} 1 = \sum_{i=1}^{\varphi(n)/2} \left[\frac{d_i}{2}\right] = \vartheta_2'(n) = \frac{\vartheta_2(n)}{2} - \frac{\varphi(n)}{4}, \quad \text{due to Lemma 3.24-d.}$$

This is also half of the number of all primitive n-square origamis $P_n^{l,h}$. □

Remark. Compare the statement of Proposition 3.25 with the total number $\mathcal{N}_n^{\mathrm{pr}}(1,1)$ of primitive n-square-tiled surfaces in the stratum $\mathcal{H}(1,1)$, see (3.11).

We end the section by formulating a conjecture:

Conjecture 1. *For any $n \geq 7$, there are exactly two orbits of primitive n-square-tiled surfaces in the stratum $\mathcal{H}(1,1)$. Moreover, when n is odd, the positive integers*

$$\mathscr{A}_n(1,1) = \frac{1}{24} n^2 (n-3)(n-5) \prod_{\substack{p\mid n\\ p \text{ prime}}} \left(1 - \frac{1}{p^2}\right),$$

$$\mathscr{S}_n(1,1) = \frac{1}{8} n^2 (n-1)(n-3) \prod_{\substack{p\mid n\\ p \text{ prime}}} \left(1 - \frac{1}{p^2}\right)$$

are the cardinals of the orbits of n-square-tiled surfaces with monodromy group A_n and S_n, respectively. When n is even, the positive integers

$$\mathscr{A}_n(1,1) = \frac{1}{24} n^3 (n-2) \prod_{\substack{p\mid n\\ p \text{ prime}}} \left(1 - \frac{1}{p^2}\right),$$

$$\mathscr{S}_n(1,1) = \frac{1}{8} n^2 (n-2)(n-4) \prod_{\substack{p\mid n\\ p \text{ prime}}} \left(1 - \frac{1}{p^2}\right)$$

are the cardinals of the orbits of n-square-tiled surfaces with monodromy group A_n and S_n, respectively.

Chapter 4
Regular representations

4.1 General theory

Suppose here that G is finite, and consider the action of the group G on the set $V = G$ induced by left multiplication: $u \cdot v = uv$, where $u \in G$ and $v, uv \in V$. The corresponding representation $\rho_{\text{reg}} : G \hookrightarrow Sym(G)$ is called (*left*) *regular*. It is always faithful, in particular any finite group can be embedded into a symmetric group.

Recall that for any generating set $\{g, h\}$ of G one constructs a labeled digraph, called *Cayley diagram*, that illustrates the multiplicative structure of G in terms of generators. The set of vertices of such a digraph is the set of elements of G and the directed edges are labeled by g and h: there is an edge with label g (resp. h) from a vertex $u \in G$ to a vertex $v \in G$ if and only if $v = gu$ (resp. $v = hu$). FIGURE 4.1 shows the diagram of the group $G = \langle g, h \mid g^3, h^2, (gh)^2 \rangle$, the edges with label h being dashed.

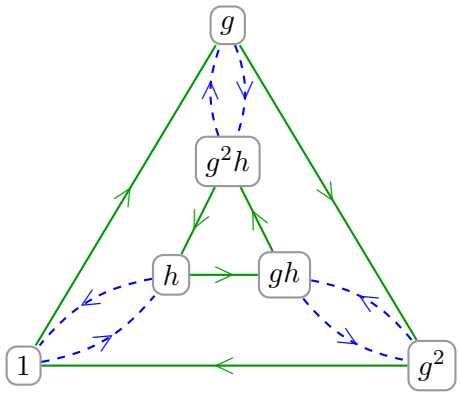


Figure 4.1: The Cayley diagram of $S_3 = \langle g, h \mid g^3, h^2, (gh)^2 \rangle$.

The Cayley diagram of a group $G = \langle X \mid R \rangle$ with a set of generators X and a set of defining relators R is denoted by $C(X; R)$ (or simply by $C(G)$, once X and R are fixed).

Remark that the Cayley diagram of a finite two-generator group $G = \langle g, h \mid R \rangle$ is isomorphic to the graph of the origami O defined by $(\rho_{\text{reg}}(g), \rho_{\text{reg}}(h)) \in Sym(G) \times Sym(G)$, and the monodromy group $\mathcal{M}on(O) = \mathtt{gp}\{\rho_{\text{reg}}(g), \rho_{\text{reg}}(h)\} \simeq G$ is a regular[1] subgroup of $Sym(G)$. Here in purpose to distinguish directions on the origami, we order the set of generators $X = \{g, h\}$, say $g \prec h$, attaching g to the horizontal direction and h to the vertical one (or else we consider the ordered pair (g, h) that indicates '$g \prec h$').

[1] A permutation group is called *regular* if none of its elements, except the identity, fixes a point.

Conversely, we would like to understand when a graph of an origami is isomorphic to a Cayley diagram of a group. The answer to this is given by the following proposition (see [62], Theorem 1.6, for a proof).

Proposition 4.1. *An origamal digraph $(V, E, \mathcal{L})$ is isomorphic to the Cayley diagram of a group if and only if for any vertices $v, v' \in V$ and any sequence of labels $l_{i_1}^{\epsilon_1}, l_{i_2}^{\epsilon_2}, \ldots, l_{i_p}^{\epsilon_p} \in \mathcal{L} \cup \mathcal{L}^{-1}$ the path $l_{i_p}^{\epsilon_p} \ldots l_{i_2}^{\epsilon_2} l_{i_1}^{\epsilon_1}[v]$ is closed whenever the path $l_{i_p}^{\epsilon_p} \ldots l_{i_2}^{\epsilon_2} l_{i_1}^{\epsilon_1}[v']$ is closed.*

Using this criterion, we can in a finite number of steps verify whether an origamal digraph $(V, E, \mathcal{L})$, where $\mathcal{L} = \{l_1, l_2\}$, is isomorphic to the Cayley diagram of a given group $G = \langle X \mid R \rangle$, where $X = \{g_1, g_2\}$ and R is a finite set of relators (the method is not effective though):

- check that $|V| = |G|$,
- check that there is a bijection $\lambda : X \to \mathcal{L}$ such that for any word[2] $W(g_1, g_2)$ from R and any vertex $v \in V$ the path $W(\lambda(g_1), \lambda(g_2))[v]$ is closed.

Further, for a finite group $G = \langle g, h \mid R \rangle$ we will denote the corresponding origami by $O_{G,g,h}$, or implicitely by O_G or O_{reg}, and call such an origami *regular*. To make it clear: the origami $O_{G,g,h}$ is defined by the group G together with the choice of a generating pair (g, h). Then, we would like to know when two different generating pairs of a group give rise to the same origami:

Lemma 4.2. *Let (g, h) and (g', h') be two pairs of generators of a finite group G. The origamis $O_{G,g,h}$ and $O_{G,g',h'}$ coincide if and only if there exists an automorphism $\alpha \in \mathrm{Aut}(G)$ such that $\alpha(g) = g'$ and $\alpha(h) = h'$.*

Proof. $(\Longleftarrow)$ If an automorphism $\alpha \in \mathrm{Aut}(G)$ sends (g, h) to (g', h'), then the induced set bijection $\alpha : G \to G$ determines an isomorphism of the labeled digraphs $C(g, h; R)$ and $C(g', h'; R')$ of G. Indeed, for any vertices $u, v \in G$ there is an edge from u to v with label g, resp. h, if and only if there is an edge from $\alpha(u)$ to $\alpha(v)$ with label $g' = \alpha(g)$, resp. $h' = \alpha(h)$, that is,

$$g \cdot u = v \iff \alpha(g) \cdot \alpha(u) = \alpha(v) \quad \text{and} \quad h \cdot u = v \iff \alpha(h) \cdot \alpha(u) = \alpha(v).$$

$(\Longrightarrow)$ Conversely, if the origamis $O_{G,g,h}$ and $O_{G,g',h'}$ coincide, then the labeled digraphs $(G, E, \{g, h\})$ and $(G, E', \{g', h'\})$, *i.e.* the corresponding Cayley diagrams of G, are isomorphic. Thus, by Proposition 4.1 for any word W the path $W(g, h)[1]$ is closed if and only if the path $W(g', h')[1]$ is closed, that is, $W(g, h) = 1$ if and only if $W(g', h') = 1$. Due to Dyck's theorem there exists an automorphism $\alpha \in \mathrm{Aut}(G)$ such that $\alpha(g) = g'$ and $\alpha(h) = h'$. □

Besides, if $\alpha : G \to G'$ is a group isomorphism then the origamis $O_{G,g,h}$ and $O_{G',\alpha(g),\alpha(h)}$ are the same. In other words, we have a one-to-one correspondence between regular origamis and isomorphism classes of finite two-generator *marked groups*.

Lemma 4.3. *Let (g, h) and (g', h') be two pairs of generators of a group G. If for a matrix A from $\mathrm{GL}(2, \mathbb{Z})$ we have $(g', h')^* = A \cdot (g, h)^*$ then $O_{G,g',h'} = A \cdot O_{G,g,h}$.*

[2] Let $\widehat{\mathcal{L}}$ be a system of letters. A *word over* $\widehat{\mathcal{L}}$ is a formal expression

$$W \equiv W(\widehat{\mathcal{L}}) \equiv L_1^{\epsilon_1} L_2^{\epsilon_2} \ldots L_m^{\epsilon_m}, \quad \text{where } L_i \in \widehat{\mathcal{L}} \text{ and } \epsilon_i = \pm 1.$$

Given a generating system X for a group G such that there is a bijection $\widehat{\mathcal{L}} \to X$, it is convenient to identify $\widehat{\mathcal{L}}$ with X. Care must be taken to distinguish a word $W(\widehat{\mathcal{L}})$ from the element $W(X)$ it represents – this should always be clear from the context.

Proof. Consider the regular representation $\rho_{\text{reg}} : G \to Sym(G)$. By the description of the $\mathrm{GL}(2, \mathbb{Z})$-actions on origamis, the condition $(g', h')^* = A \cdot (g, h)^*$ signifies that there exist an automorphism $\eta_A \in \mathrm{Aut}(F_2)$ and an element $u \in G$ such that

$$u(g', h')u^{-1} = \eta_A \cdot (g, h),$$

where $(\eta_A \cdot (g, h))^* = A \cdot (g, h)^*$.

Recall that, for any group H, the group $\mathrm{Aut}(F_2)$ acts on $H \times H$ by Nielsen transformations (see Section 2.4). We have $\sigma\,(\rho_{\text{reg}}(g'), \rho_{\text{reg}}(h'))\,\sigma^{-1} = \eta_A \cdot (\rho_{\text{reg}}(g), \rho_{\text{reg}}(h))$, where $\sigma = \rho_{\text{reg}}(u) \in Sym(G)$. Therefore, $(\rho_{\text{reg}}(g'), \rho_{\text{reg}}(h'))^* = A \cdot (\rho_{\text{reg}}(g), \rho_{\text{reg}}(h))^*$, that is, $O_{G,g',h'} = A \cdot O_{G,g,h}$. □

The following theorem is a useful tool for finding the Veech group of an origami, given a presentation of its monodromy group. Hereafter, if a pair $(a, b) \in G \times G$ satisfies a relation $W(a, b) = 1$, then we also say that the conjugacy class $(a, b)^* = \{c(a, b)c^{-1} \mid c \in G\}$ *satisfies the relation* W.

Theorem 4.4. *Let $\langle g, h \mid R\rangle$ be a presentation of a finite group G. The integer Veech group of the square-tiled surface $O_{G,g,h}$ consists of the matrices which preserve R, namely,*

$$A \in \mathrm{GL}(O_{G,g,h}) \iff \textit{the conjugacy class } A \cdot (g, h)^* \textit{ satisfies the relations } R.$$

Moreover, the number of $\mathrm{GL}(2, \mathbb{Z})$*-orbits of regular origamis $O_{G,g,h}$ over all pairs of generators (g, h) is equal to the number of T_2-systems of the group G.*

Remark 1 (The dual version of the theorem). Remind that there are two $\mathrm{GL}(2, \mathbb{Z})$-actions on origamis, the natural and dual ones. The orbits for these actions coincide and the stabilizers are related by (2.6). Thus, we could replace GL by $\mathrm{GL}^{\times}$ and '$\cdot$' by '$\times$' in the statement above.

Remark 2. The first part of the theorem (the direct version) can be viewed as a special case of a result by Gabriela Schmithüsen, see [83, Proposition 2.1].

Proof. Let $(g', h')^* = A \cdot (g, h)^*$ for a matrix $A \in \mathrm{GL}(2, \mathbb{Z})$, then by the previous Lemma 4.3 we have $O_{G,g',h'} = A \cdot O_{G,g,h}$. The matrix A belongs to the Veech group $\mathrm{GL}(O_{G,g,h})$ if and only if the square-tiled surfaces $O_{G,g,h}$ and $O_{G,g',h'}$ coincide. By Lemma 4.2 it is equivalent to say that there exists an automorphism $\alpha \in \mathrm{Aut}(G)$ such that $\alpha(g) = g'$ and $\alpha(h) = h'$. As we know from the definition of the natural $\mathrm{GL}(2, \mathbb{Z})$-action (2.4), the mapping $(g, h) \mapsto (g', h')$, up to conjugation by an element of G, is a Nielsen transformation. By Corollary 2.9 we conclude that a necessary and sufficient condition of the inclusion $A \in \mathrm{GL}(O_{G,g,h})$ is for the pair (g', h') to satisfy the relations R.

Moreover, due to Lemma 4.2 for a given group G, the regular origamis $O_{G,g,h}$ are in bijection with the $\mathrm{Aut}(G)$-orbits of pairs (g, h), that is, in bijection with the G-defining subgroup of F_2 (see Section 2.4). The dual action of $\mathrm{GL}(2, \mathbb{Z})$ on origamis $O_{G,g,h}$ corresponds to the action of $\mathrm{Aut}(F_2)$ on G-defining subgroups. Therefore, the number of $\mathrm{GL}(2, \mathbb{Z})$-orbits in question equals the number of T_2-systems of the group G. □

Corollary 4.5. *Let G be a finite group generated by two elements g and h such that the origami $O_{G,g,h}$ is stabilized by* $\mathrm{GL}(2, \mathbb{Z})$*. Then, for any pair (u, v) Nielsen equivalent to the pair (g, h), the four elements g, h, u and v are of the same order in the group G.*

First proof. Consider a presentation $\langle g, h \mid R\rangle$ of the group G. Let k, l, m and n be orders of the elements g, h, gh and gh^{-1} respectively, and let us add the corresponding four relations to the set R (if there are not already in) so that

$$G = \left\langle g, h \;\middle|\; R, g^k = 1, h^l = 1, (gh)^m = 1, (gh^{-1})^n = 1 \right\rangle. \tag{4.1}$$

The Veech group of the origami $O_{G,g,h}$ is the whole group $\mathrm{GL}(2,\mathbb{Z})$. Then by Theorem 4.4 the following conjugacy classes

$$\begin{aligned}(h^{-1},g)^* &= S{\times}(g,h)^*,\\ (gh^{-1},h)^* &= T^{-1}{\times}(g,h)^*,\\ (gh,h)^* &= T{\times}(g,h)^*\end{aligned}$$

satisfy the new relations. In particular we have $h^k = g^l = 1$, $(gh^{-1})^k = g^m = 1$ and $(gh)^k = g^n = 1$, that is, $l|k$, $k|l$, $n|k$, $k|m$ and $m|k$, $k|n$. Hence, $k = l = m = n$.

We conclude that for any pair $(u,v) = \varepsilon_1 \cdot (g,h)$, where ε_1 is an elementary Nielsen move, the elements g, h, u and v are of the same order in G. Suppose that the same is true for $(u,v) = \varepsilon_{N-1}\cdot\ldots\varepsilon_1\cdot(g,h)$, $N \geq 2$, and prove it for $(u',v') = \varepsilon_N\cdot(u,v)$, where $\varepsilon_N, \varepsilon_{N-1},\ldots,\varepsilon_1$ are elementary Nielsen moves. Indeed, by definition of the $\mathrm{GL}(2,\mathbb{Z})$-action there exists a matrix $A \in \mathrm{GL}(2,\mathbb{Z})$ such that $(u,v)^* = A{\times}(g,h)^*$, and so $O_{G,u,v} = A{\times}O_{G,g,h}$. The origami $O_{G,g,h}$ is stabilized by $\mathrm{GL}(2,\mathbb{Z})$, we have $O_{G,u,v} = O_{G,g,h}$, and according to what was already shown the four elements u, v, u' and v' are of the same order in $G = \langle u, v \mid \ldots \rangle$, as $(u',v') = \varepsilon_N \cdot (u,v)$. We are done by induction. □

Second proof. The origami $O_{G,g,h}$ is defined by the pair of permutations $(\rho_{\mathrm{reg}}(g), \rho_{\mathrm{reg}}(h))$. For any pair (u,v) Nielsen equivalent to the pair (g,h) there exists a matrix $A \in \mathrm{GL}(2,\mathbb{Z})$ such that $(u,v)^* = A{\times}(g,h)^*$. The origami $O_{G,g,h}$ coincides with the origamis $O_{G,u,v} = A{\times}O_{G,g,h}$, and so the pairs of permutations $(\rho_{\mathrm{reg}}(g), \rho_{\mathrm{reg}}(h))$ and $(\rho_{\mathrm{reg}}(u), \rho_{\mathrm{reg}}(v))$ are conjugate. Since $\rho_{\mathrm{reg}} : G \hookrightarrow Sym(G)$ is an injective homomorphism the elements g and u must have the same order in G, as well as h and v. Applying this argument to the pair (v^{-1},u), where $(v^{-1},u)^* = (SA){\times}(g,h)^*$, we conclude that g, h, u and v are of the same order in G. □

Definition 4.1. A faithful permutation representation $\rho : G \to S_m$ is called *structural* if for each automorphism $\phi \in \mathrm{Aut}(\rho(G))$ there exists $\sigma \in S_m$ such that

$$\phi(\tau) = \sigma\tau\sigma^{-1}, \quad \text{for all } \tau \in \rho(G).$$

Proposition 4.6. *The regular representation $\rho = \rho_{\mathrm{reg}} : G \hookrightarrow Sym(G)$ is structural.*

Proof. Indeed, an automorphism $\phi \in \mathrm{Aut}(\rho(G))$ is a composition $\rho\circ\alpha\circ\rho^{-1}$ for some $\alpha \in \mathrm{Aut}(G)$ (consequently $\alpha \in Sym(G)$). Let us show that $\phi(\rho(g)) = \alpha\rho(g)\alpha^{-1}$ for any $g \in G$, that is, $\rho(\alpha(g)) = \alpha\rho(g)\alpha^{-1}$. Recall that the permutation $\rho(g) \in Sym(G)$ is defined by $\rho(g) : h \to g\cdot h$, and so one has $\alpha\rho(g)\alpha^{-1} : h \to \alpha(g\cdot\alpha^{-1}(h))$. In other words, we want to show that $\alpha(g)\cdot h = \alpha(g\cdot\alpha^{-1}(h))$ for any $g,h \in G$, which is obviously true, since α is an automorphism of G. □

Note that for any subgroup $H \subseteq S_m$ and any permutation σ from the normalizer of H in S_m, the mapping $\phi_\sigma : \mu \mapsto \sigma\mu\sigma^{-1}$, where $\mu \in H$, is an automorphism of H. Hence, if $\rho : G \to S_m$ is a faithful structural representation, then we have

$$\mathrm{Aut}(G) \simeq {}^{N_{S_m}(\rho(G))}\!/_{C_{S_m}(\rho(G))},$$

where $N_{S_m}(\rho(G))$ and $C_{S_m}(\rho(G))$ are the normalizer and the centralizer of $\rho(G)$ in S_m respectively.

Theorem 4.7. *Consider a finite group G generated by two elements g and h. Let $\rho_{\mathrm{reg}} : G \hookrightarrow Sym(G)$ be its regular representation, and $\rho : G \hookrightarrow S_m$ another faithful permutation representation. Denote by O_{reg} and O_ρ the origamis defined by the pairs $(\rho_{\mathrm{reg}}(g), \rho_{\mathrm{reg}}(h))$ and $(\rho(g),\rho(h))$ respectively. Then*

$$\mathrm{GL}(O_\rho) \subseteq \mathrm{GL}(O_{\mathrm{reg}}).$$

Moreover, if the representation ρ is structural, then one has the equality $\mathrm{GL}(O_\rho) = \mathrm{GL}(O_{\mathrm{reg}})$.

Remark. In her Ph.D. thesis [84, Corollary 5.2], Gabriela Schmithüsen showed that the Veech group of an origami O is related (by inclusion) to the Veech groups of three regular origamis naturally associated to O.

Proof. Let $A \in \mathrm{GL}(2,\mathbb{Z})$ be a matrix which stabilizes the origami $O_\rho = (\sigma,\tau)^*$, where $\sigma = \rho(g)$ and $\tau = \rho(h)$. Then, by the definition of the direct $\mathrm{GL}(2,\mathbb{Z})$-action (see Section 2.6), there exist $\gamma_A \in \mathrm{Aut}(F_2)$ and $\delta \in S_m$ such that

$$\gamma_A \cdot (\sigma,\tau) = \delta(\sigma,\tau)\delta^{-1},$$

where γ_A is actually a preimage of A in the exact sequence

$$0 \to \mathrm{Inn}(F_2) \to \mathrm{Aut}(F_2) \xrightarrow{\Phi} \mathrm{GL}(2,\mathbb{Z}) \to 0, \quad \text{that is, } \Phi(\gamma_A) = A$$

We have $\gamma_A \cdot (\sigma,\tau) = (w_1(\sigma,\tau), w_2(\sigma,\tau))$, where $\gamma_A^{-1} : \begin{pmatrix} x \mapsto w_1(x,y) \\ y \mapsto w_2(x,y) \end{pmatrix}$, implying

$$\gamma_A \cdot (\sigma,\tau) = (w_1(\rho(g),\rho(h)),\, w_2(\rho(g),\rho(h))) = (\rho\times\rho)(w_1(g,h), w_2(g,h)) = (\rho\times\rho)(\gamma_A \cdot (g,h)),$$

and also

$$\gamma_A \cdot (\sigma,\tau) = \delta(\sigma,\tau)\delta^{-1} = \delta(\rho(g),\rho(h))\delta^{-1} = \phi_\delta \circ (\rho\times\rho)(g,h).$$

Here $\phi_\delta : \mu \mapsto \delta\mu\delta^{-1}$ is an automorphism of $\rho(G)$, since the pair (σ,τ) generates the group $\rho(G)$ and $\delta(\sigma,\tau)\delta^{-1} = (w_1(\sigma,\tau), w_2(\sigma,\tau)) \in \rho(G)\times\rho(G)$. Therefore, the mapping $\rho^{-1}\circ\phi_\delta\circ\rho$ is an automorhism of G such that

$$(\rho^{-1}\circ\phi_\delta\circ\rho)(g,h) = \gamma_A \cdot (g,h),$$

and so by Lemma 4.2 we have $A \in \mathrm{GL}(O_{\mathrm{reg}})$. This proves the inclusion $\mathrm{GL}(O_\rho) \subseteq \mathrm{GL}(O_{\mathrm{reg}})$.

Now, suppose that ρ is a structural representation, and let $A \in \mathrm{GL}(O_{\mathrm{reg}})$. We have the following logical order:

$$\begin{aligned}
A \in \mathrm{GL}(O_{\mathrm{reg}}) &\overset{\text{Lemma } 4.2}{\Longrightarrow} \exists \alpha \in \mathrm{Aut}(G) \text{ such that } (\alpha\times\alpha)(g,h) = \gamma_A \cdot (g,h), \\
&\qquad \text{where } \gamma_A \in \mathrm{Aut}(F_2) \text{ with } \Phi(\gamma_A) = A \\
&\Longrightarrow \quad \phi = \rho\circ\alpha\circ\rho^{-1} \in \mathrm{Aut}(\rho(G)) \text{ and } (\phi\times\phi)(\sigma,\tau) = \gamma_A \cdot (\sigma,\tau), \\
&\qquad \text{where } \sigma = \rho(g) \text{ and } \tau = \rho(h) \\
&\overset{\rho \text{ is structural}}{\Longrightarrow} \exists \delta \in S_m \text{ such that } \gamma_A \cdot (\sigma,\tau) = \delta(\sigma,\tau)\delta^{-1} \\
&\Longrightarrow \quad A \in \mathrm{GL}(O_\rho).
\end{aligned}$$

Thus, together with the first part of the proof, we obtain the equality $\mathrm{GL}(O_\rho) = \mathrm{GL}(O_{\mathrm{reg}})$. □

Rephrasing the statement of the theorem gives an immediate

Corollary 4.8. *Let $O = (\sigma,\tau)^*$ be an m-square origami, and $G = \mathcal{M}on(O) = \mathrm{gp}\{\sigma,\tau\} \subset S_m$ its monodromy group, then $\mathrm{GL}(O) \subseteq \mathrm{GL}(O_{G,\sigma,\tau})$.*

Proposition 4.9. *A regular square-tiled surface $O_{G,g,h}$ is primitive if and only if G is a cyclic group of prime order or trivial.*

Proof. $(\Longrightarrow)$ Due to Proposition 2.4, if the square-tiled surface O_G is primitive then its monodromy group $\mathcal{M}on(O_G) = \rho_{\mathrm{reg}}(G) \simeq G$ is a primitive permutation group on the set $V = G$, and so any point stabilizer G_x ($x \in V$) is a maximal subgroup (see Lemma 2.3). On the other hand, the stabilizer of 1 for the action of G on itself by left multiplication trivially equals $\{1\}$. Thus $\{1\}$ is a maximal subgroup of G, that is, G has prime order or trivial.
$(\Longleftarrow)$ Conversely, if $|G| = p$ is prime then the origami O_G has p squares and is primitive. □

In order to find out the stratum of a regular origami $O_{G,g,h}$, we shall look at the cycle pattern of the permutation $\rho_{\text{reg}}([g,h])$. Let n be the order of the group G, and k the order of its element $[g,h] = ghg^{-1}h^{-1}$. For the action of the commutator $[g,h]$ by left multiplication on G, we get n/k orbits of length k. Therefore,

$$O_{G,g,h} \in \mathcal{H}(\underbrace{k-1,\ldots,k-1}_{n/k}) \quad \text{and} \quad \text{genus}(O_{G,g,h}) = \frac{k-1}{2} \cdot \frac{n}{k} + 1, \tag{4.2}$$

with the regular origami $O_{G,g,h}$ having n squares.

Before we proceed to the examples of regular square-tiled surfaces, we shall point out that much work was done in that direction by Frank Herrlich and Gabriela Schmithüsen. Also in a similar with ours spirit, that is, from the point of view of monodromy groups, Karsten Kremer studies families of origamis in his Ph.D. thesis [56].

4.2 Examples

4.2.1 Trivial or abelian origamis

Consider a finite group G generated by two elements g and h, and let $\rho_{\text{reg}} : G \hookrightarrow Sym(G)$ be its regular representation. We affirm that G ia abelian if and only if the origami O_G is a torus. Indeed, the origami O_G belongs to the stratum $\mathcal{H}(0)$ if and only if the commutator $[\rho_{\text{reg}}(g), \rho_{\text{reg}}(h)]$ is the identity pemutation, *i.e.* $[g, h] = 1$.

Any finite two-generator abelian group is a product of two cyclic groups and has the following presentation in terms of generators and relators:

$$G = \mathbb{Z}_m \times \mathbb{Z}_n = \langle g, h \mid g^m = h^n = [g, h] = 1 \rangle ,$$

where one takes $g = (1, 0)$ and $h = (0, 1)$. Remark that for m and n coprime the group $\mathbb{Z}_m \times \mathbb{Z}_n$ is generated by (s, r), where $mr + ns = 1$, and thus it is isomorphic to $\mathbb{Z}_{mn}$.

The corresponding regular origami is the trivial origami $T(m, n)$, see FIGURE 4.2 where the solid edges are labeled by g and the dashed ones by h.

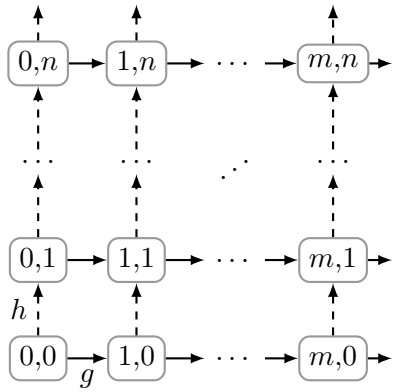


Figure 4.2: The Cayley diagram of $\mathbb{Z}_m \times \mathbb{Z}_n$.

For the dual action of GL(2, $\mathbb{Z}$) we have

$$J\times(g, h)^* = (g, -h)^*,\ T\times(g, h)^* = (g + h, h)^* \ \text{ and } \ U\times(g, h)^* = (g, h - g)^*,$$

$$\text{where } \ J = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},\ T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \ \text{ and } \ U = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}.$$

Since an action of a group is *uniquely* defined by the action of its generating system (cf. Corollary 2.8), we conclude that

$$A\times(g, h)^* = (ag + bh, cg + dh)^* = ((a, b), (c, d))^* \quad \text{for any } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}(2, \mathbb{Z}).$$

According to Theorem 4.4, a matrix A preserves the origami O_G if and only if

$$m \cdot (a, b) = (ma, mb) = (0, 0) \quad \text{and} \quad n \cdot (c, d) = (nc, nd) = (0, 0),$$

that is, we obtain

$$\text{GL}^{\times}(T(m, n)) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}(2, \mathbb{Z}) \mid b \equiv 0 \bmod \frac{n}{\gcd(m, n)}, \quad c \equiv 0 \bmod \frac{m}{\gcd(m, n)} \right\}.$$

4.2.2 Dihedral origamis

A regular polygon with $m \geq 3$ sides has $2m$ symmetries: m rotations and m reflections. These symmetries form a group denoted by D_m and called *dihedral group*. It is non-abelian and has the following presentation:

$$D_m = \langle s, t \mid s^2 = t^2 = (st)^m = 1 \rangle \simeq \mathbb{Z}_n \rtimes \mathbb{Z}_2, \tag{4.3}$$

where s and t are two reflections as shown in Figure 4.3.

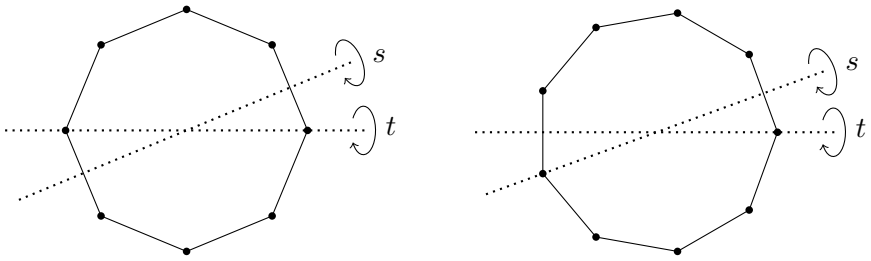


Figure 4.3: Symmetries of regular polygons.

The corresponding regular origami $O_{D_m,s,t}$ will be called *dihedral*. The commutator $[s,t] = (st)^2$ has order m if the number m is odd, and $m/2$ else. Thus, by the formulas (4.2), we have

$$O_{D_m} \text{ belongs to } \begin{cases} \mathcal{H}(m-1, m-1) \text{ and has genus } m & \text{if } m \text{ is odd,} \\ \mathcal{H}(\frac{m}{2}-1, \frac{m}{2}-1, \frac{m}{2}-1, \frac{m}{2}-1) \text{ and has genus } m-1 & \text{if } m \text{ is even.} \end{cases}$$

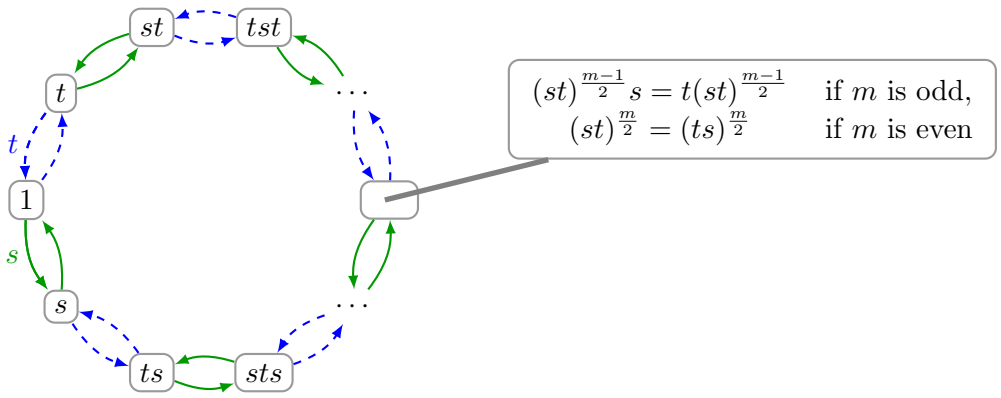


Figure 4.4: The Cayley diagram of D_m.

Proposition 4.10. *The dual Veech group of the dihedral origami O_{D_m} is*

$$\mathrm{GL}^{\times}(O_{D_m}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2,\mathbb{Z}) \mid a+b \text{ and } c+d \text{ are odd} \right\},$$

which is an index three subgroup of $\mathrm{GL}(2,\mathbb{Z})$.

Proof. For the dual action of $\mathrm{GL}(2,\mathbb{Z})$ we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \times (s,t)^* = (w_1(s,t), w_2(s,t))^*,$$

and words w_1 and w_2 can be chosen such that

$$\begin{aligned} e_s(w_1) &= a, \quad e_t(w_1) = b, \\ e_s(w_2) &= c, \quad e_t(w_2) = d, \end{aligned}$$

where $e_s(w)$ and $e_t(w)$ denote the sums of the exponents of s and t in the word w respectively.

Since $s^2 = t^2 = 1$, there are three types of elements in the group D_m:

$$(st)^k s,\ t(st)^l \ \text{ and } (st)^r, \ \text{ where } k, l \in \mathbb{N} \cup \{0\},\ r \in \mathbb{Z}.$$

According to Theorem 4.4 a matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ stabilizes the regular origami O_{D_m} if and only if

$$w_1^2 = 1,\ w_2^2 = 1 \ \text{ and } \ (w_1 w_2)^m = 1.$$

Remark that if the integers $a+b$ and $c+d$ are both odd then the three equalities are satisfied in D_m, because in this case each of the words w_1 and w_2 is of the form $(st)^k s$ or $t(st)^l$ with $k, l \in \mathbb{N} \cup \{0\}$. Thus, the group Γ consisting of the matrices A with $a+b$ and $c+d$ odd is a subgroup of $\mathrm{GL}^\times(O_{D_m})$. Since Γ is exactly the stabilizer of the point $[1:1]$ for the transitive action of $\mathrm{GL}(2, \mathbb{Z})$ on the projective line $\mathbb{P}^1(\mathbb{F}_2)$, it is an index three subgroup of $\mathrm{GL}(2, \mathbb{Z})$.

Taking into account the fact that the origami O_{D_m} is not preserved by the matrix T,

$$T \notin \mathrm{GL}^\times(O_{D_m}) \ \text{ as } T \times (s,t)^* = (st, t)^* \text{ and } (st)^2 = [s,t] \neq 1,$$

we conclude that $\mathrm{GL}^\times(O_{D_m}) = \Gamma$. □

4.2.3 Heisenberg origamis

Let $p > 2$ be an odd prime number. The Heisenberg group modulo p is the following non-abelian subgroup of $\mathrm{SL}(3, \mathbb{F}_p)$ of upper-triangular matrices:

$$H_p = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{SL}(3, \mathbb{F}_p) \mid a, b, c \in \mathbb{F}_p \right\}.$$

It has order p^3 and can be presented as

$$H_p = \langle s, t \mid s^p = t^p = [s,t]^p = 1,\ s[s,t] = [s,t]s,\ t[s,t] = [s,t]t \rangle,$$

where

$$s = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad t = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad [s,t] = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

The Heisenberg group H_p is periodic of period p, since

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^k = \begin{pmatrix} 1 & ka & kb + \frac{k(k-1)}{2}ac \\ 0 & 1 & kc \\ 0 & 0 & 1 \end{pmatrix}.$$

The corresponding regular origami O_{H_p} is called a *Heisenberg origami* (they were first studied by Frank Herrlich in [40]).

Proposition 4.11. *The dual Veech group of O_{H_p} is the entire* $\mathrm{GL}(2, \mathbb{Z})$,

$$\mathrm{GL}^\times(O_{H_p}) = \mathrm{GL}(2, \mathbb{Z}).$$

Proof. By Theorem 4.4, it follows that

$$\begin{aligned} J \in \mathrm{GL}^\times(O_{H_p}) &\quad \text{as } J\times(s,t)^* = (s,t^{-1})^* \text{ and } [s,t^{-1}] = t^{-1}(tst^{-1}s^{-1})t = t^{-1}[s,t]^{-1}t = [s,t]^{-1}; \\ T \in \mathrm{GL}^\times(O_{H_p}) &\quad \text{as } T\times(s,t)^* = (st,t)^* \text{ and } [st,t] = [s,t]; \\ U \in \mathrm{GL}^\times(O_{H_p}) &\quad \text{as } U\times(s,t)^* = (s,s^{-1}t)^* \text{ and } [s,s^{-1}t] = s^{-1}[s,t]s = [s,t], \end{aligned}$$

and so O_{H_p} is stabilized by $\mathrm{GL}(2, \mathbb{Z})$, □

By the formulas (4.2), the square-tiled surface belongs to the stratum $\mathcal{H}(\underbrace{p-1, \ldots, p-1}_{p^2})$ and is of genus $\frac{1}{2}p^2(p-1)+1$.

For $p = 3$ the Heisenberg origami O_{H_3} coinsides with the Burnside origami $O_{B(2,3)}$. Indeed, by Dyck's theorem there is an homomorphism $\Psi : H_3 \to B(2,3)$, $s \mapsto g, t \mapsto h$, since the orders of the elements of H_3 divide 3 and thus the relations (4.6) are also satisfied in H_3. Moreover, Ψ is an isomorphism in view of the fact that $|H_3| = |B(2,3)| = 27$.

4.2.4 The quaternion origami

The quaternion group Q_8 is a non-abelian group of order 8. It has the following presentations:

$$\begin{aligned} Q_8 &= \langle -1, i, j, k \mid (-1)^2 = 1,\, i^2 = j^2 = k^2 = ijk = -1 \rangle \\ &= \langle x, y \mid x^2 = y^2,\, xy = yx^{-1} \rangle, \end{aligned}$$

where, for instance, $i = x$, $j = y$, $k = xy$, and we have $x^4 = y^4 = 1$.

The regular origami $O_{Q_8,x,y}$, called the *quaternion origami*, has a lot of interesting properties (see, for instance, the paper [41] by Frank Herrlich and Gabriela Schmithüsen). In particular it is stabilized by $\mathrm{GL}(2, \mathbb{Z})$, what we are going to establish.

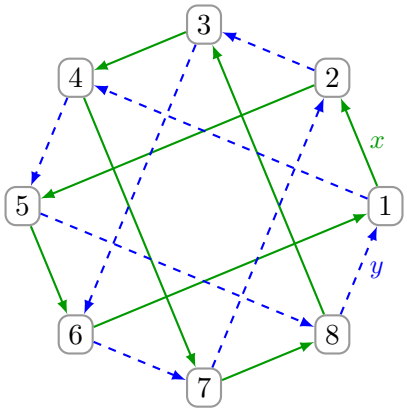


Figure 4.5: An origamal digraph for O_{Q_8}.

Let us verify the invariance of the relations $x^2 = y^2$, $xy = yx^{-1}$ under each of the three substitutions $y \to y^{-1}$, $x \to xy$, $y \to x^{-1}y$. We have

$$\begin{aligned} (y^{-1})^2 = y^2 = x^2 \quad &\text{and} \quad xy^{-1} = x(x^{-1}y^{-1}x^{-1}) = y^{-1}x^{-1}, \\ (xy)^2 = (xyx)y = y^2 = x^2 \quad &\text{and} \quad (xy)y = xy^2 = x^3 = x^{-1} = y(xy)^{-1}, \\ (x^{-1}y)^2 = x^{-1}(yx^{-1})y = x^{-1}(xy)y = y^2 = x^2 \quad &\text{and} \quad x(x^{-1}y) = y = (x^{-1}y)x^{-1}. \end{aligned}$$

Therefore, by Theorem 4.4 the quaternion origami is preserved by the matrices J, T, U, and so

$$\mathrm{GL}^{\times}(O_{Q_8}) = \mathrm{GL}(2, \mathbb{Z}).$$

Since the commutator $[x, y] = x(yx^{-1}y^{-1}) = x^2$ is of order 2, the origami lies in the stratum $\mathcal{H}(1, 1, 1, 1)$ and has genus 3 by the formulas (4.2).

4.2.5 Generalized quaternion origamis

The *generalized quaternion group* Q_{4n}, where $n \geq 2$, is the group of order $4n$ given by the presentation

$$Q_{4n} = \left\langle x, y \;\middle|\; x^{2n} = 1,\, x^n = y^2,\, xy = yx^{-1} \right\rangle. \tag{4.4}$$

The case that $n = 2$ corresponds to the classical quaternion group Q_8 considered above. The generalized quaternion group is di-cyclic, that is, an extension of a cyclic group by a cyclic group,

$$1 \longrightarrow C_{2n} \longrightarrow Q_{4n} \longrightarrow C_2 \longrightarrow 1.$$

The group Q_{4n} can be realized as the subgroup of $\mathrm{GL}_2(\mathbb{C})$ generated by

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} e^{\,i\pi/n} & 0 \\ 0 & e^{-\,i\pi/n} \end{pmatrix}.$$

The generalized quaternion group has a close connection with the dihedral group:

$$Q_{4n} \big/ \mathtt{gp}\left\{y^2\right\} \simeq D_n.$$

Indeed, the set $\{1, y^2\} = \mathtt{gp}\left\{y^2\right\}$ is the center of Q_{4n}, and if we add the relation $y^2 = 1$ to (4.4) we will obtain the presentation (4.3) of the dihedral group, where $s = xy^{-1}$ and $t = y$.

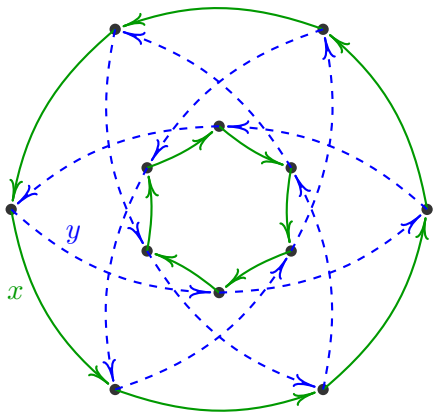


Figure 4.6: An origamal digraph for $O_{Q_{12}}$.

The regular origami $O_{Q_{4n},x,y}$ will be called a *generalized quaternion origami*. By the formulas (4.2), since the commutator $[x, y] = x(yx^{-1}y^{-1}) = x^2$ is of order n, the origami belongs to the stratum $\mathcal{H}(n-1, n-1, n-1, n-1)$ and has genus $2n - 1$.

Let m be a positive integer, introduce the following notation

$$\Gamma^0(m) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2,\, \mathbb{Z}) \;\middle|\; b \equiv 0 \bmod m \right\},$$

which is a congruence subgroup of $\mathrm{GL}(2, \mathbb{Z})$.

Let us establish a known result:

Proposition 4.12. *The index of the subgroup* $\Gamma^0(m)$ *of* $\mathrm{GL}(2, \mathbb{Z})$ *is equal to*

$$m \prod_{\substack{p \,|\, m \\ p \text{ prime}}} \left(1 + \frac{1}{p}\right).$$

Proof. Denote by $\psi(m)$ the index $|\mathrm{GL}(2,\mathbb{Z}):\Gamma^0(m)|$. For a prime number p, the subgroup $\Gamma^0(p)$ is exactly the stabilizer of the point $[0:1]$ for the transitive action of $\mathrm{GL}(2,\mathbb{Z})$ on the projective line[3] $\mathbb{P}^1(\mathbb{F}_p)$, and so $\psi(p)=p+1$. Further, the index $|\Gamma^0(p):\Gamma^0(p^k)|$ of the subgroup $\Gamma^0(p^k)$ in $\Gamma^0(p)$ is equal to p^{k-1}, since $\{I,T^p,T^{2p},\dots,T^{(p^{k-1}-1)p}\}$ is a complete list of representatives of the cosets $\Gamma^0(p)/\Gamma^0(p^k)$. Indeed, for any matrix

$$\begin{pmatrix} a & b\\ c & d\end{pmatrix}\in\Gamma^0(p),\quad \text{where}\quad \begin{array}{ll} b=b'p^k+xp, & 0\le x<p^{k-1},\\ d=d'p^k+y, & 0<y<p^k,\ p\nmid y,\end{array}$$

there exists an integer $0\le z<p^{k-1}$ such that $zy\equiv x \bmod p^{k-1}$, and

$$\begin{pmatrix} 1 & zp\\ 0 & 1\end{pmatrix}\begin{pmatrix} a & b\\ c & d\end{pmatrix}=\begin{pmatrix} a+zcp & b+zdp\\ c & d\end{pmatrix}\in\Gamma^0(p^k).$$

Therefore, we have $\psi(p^k)=|\Gamma^0(p):\Gamma^0(p^k)|\cdot|\mathrm{GL}(2,\mathbb{Z}):\Gamma^0(p)|=p^{k-1}(p+1)$.

Now, let us show that ψ is a multiplicative function (in terms of number theory), that is,

$$\psi(mn)=\psi(m)\cdot\psi(n)\quad\text{for any coprime positive integers } m,n.$$

First, recall that for any subgroup H and K of a group G, there is a natural bijection

$$H/(H\cap K)\longleftrightarrow HK/K,\quad h(H\cap K)\leftrightarrow hK,$$

where HK denotes the set of products hu with $h\in H$, $u\in K$. Second, any matrix $A=\begin{pmatrix} a & b\\ c & d\end{pmatrix}$ from $\mathrm{GL}(2,\mathbb{Z})$ can be presented in the form

$$A=B\cdot C\quad\text{for some } B\in\Gamma^0(m) \text{ and } C\in\Gamma^0(n). \tag{4.5}$$

Indeed, if $\gcd(d,n)=1$ then there exist $x,y\in\mathbb{Z}$ such that $xmd+yn=b$, and so

$$\begin{pmatrix} a & b\\ c & d\end{pmatrix}=\begin{pmatrix} 1 & xm\\ 0 & 1\end{pmatrix}\begin{pmatrix} a-xmc & yn\\ c & d\end{pmatrix}.$$

Else, if d and n are not coprime then, as $\gcd(b,d)=1$ for $ad-bc=\pm1$, there is an integer z such that $\gcd(zb+d,n)=1$, for instance we can choose z to be the greatest divisor of n coprime to d. Thus, by what we have just seen, one gets a presentation (4.5) for the matrix

$$U^{-z}A=\begin{pmatrix} 1 & 0\\ z & 1\end{pmatrix}\begin{pmatrix} a & b\\ c & d\end{pmatrix}=\begin{pmatrix} a & b\\ za+c & zb+d\end{pmatrix}=B\cdot C,\ \text{where } B\in\Gamma^0(m) \text{ and } C\in\Gamma^0(n),$$

implying $A=(U^zB)\cdot C$, where $U^zB\in\Gamma^0(m)$ and $C\in\Gamma^0(n)$.

Hence, we have $\Gamma^0(m)\Gamma^0(n)=\mathrm{GL}(2,\mathbb{Z})$, and finally

$$\begin{aligned}|\Gamma^0(m):\Gamma^0(mn)|=|\Gamma^0(m):\Gamma^0(m)\cap\Gamma^0(n)|&=|\Gamma^0(m)\Gamma^0(n):\Gamma^0(n)|\\ &=|\mathrm{GL}(2,\mathbb{Z}):\Gamma^0(n)|=\psi(n).\end{aligned}$$

This proves that $\psi(mn)=\psi(m)\cdot\psi(n)$. In particular, we conclude that if $m=p_1^{k_1}\cdots p_s^{k_s}$ then $\psi(m)=\psi(p_1^{k_1})\cdots\psi(p_s^{k_s})=m(1+1/p_1)\cdots(1+1/p_s)$. □

[3] A *projective line* over an (associative, with 1) ring $\mathscr{R}$ is the space of equivalence classes of pairs from $\mathscr{R}^2$ such that

$$(a,b)\sim(c,d)\quad\text{if and only if}\quad a=uc,\ b=ud \text{ for some } u\in\mathscr{U},$$

where $\mathscr{U}$ is the group of units (*i.e.* invertible elements) of the ring $\mathscr{R}$. The projective line over $\mathscr{R}$ is denoted by $\mathbb{P}^1(\mathscr{R})$, and its points by $[a:b]$. If $\mathscr{R}$ is a field then $\mathbb{P}^1(\mathscr{R})$ consists of the points $[a:1]$, where $a\in\mathscr{R}$, and the point $\infty=[1:0]$.

Proposition 4.13. *For $n > 2$, the dual Veech groups of the generalized quaternion origamis are*

$$\mathrm{GL}^{\times}(O_{Q_{4n}}) = \begin{cases} \Gamma^0(4) & \text{if } n \text{ is odd,} \\ \Gamma^0(2) & \text{if } n \text{ is even,} \end{cases}$$

which are congruence subgroups of $\mathrm{GL}(2,\mathbb{Z})$ *of index 6 and 3 respectively.*

Proof. Recall, as usual, that for the dual action of $\mathrm{GL}(2,\mathbb{Z})$ we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \times (x,y)^* = (w_1(x,y), w_2(x,y))^*,$$

and words w_1 and w_2 can be chosen such that

$$\begin{aligned} e_x(w_1) &= a, \quad e_y(w_1) = b, \\ e_x(w_2) &= c, \quad e_y(w_2) = d, \end{aligned}$$

where $e_x(w)$ and $e_y(w)$ denote the sums of the exponents of x and y in the word w respectively.

Moreover, using the relation $xy = yx^{-1}$, it is easy to see that

$$\begin{aligned} w_1(x,y) &= x^k y^b, \quad \text{where } k \equiv a \bmod 2, \\ w_1(x,y) &= x^l y^d, \quad \text{where } l \equiv c \bmod 2. \end{aligned}$$

According to Theorem 4.4, a matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ stabilizes the regular origami $O_{Q_{4n}}$ if and only if

$$w_1^{2n} = 1, \ w_1^n = w_2^2 \ \text{ and } \ w_1 w_2 = w_2 w_1^{-1}.$$

Let us show that the three relations are satisfied if $2 \mid b$ and $4 \mid bn$. Indeed, if b is even then $y^{2b} = 1$, x commutes with y^b and the integers k and d are odd, as $ad - bc = \pm 1$. In particular, $x^{kn} = x^n$ and $y^{2d} = y^2$. Also, $y^{bn} = 1$ when bn is divisible by 4. Therefore, we have:

$$\begin{aligned} &w_1^{2n} = (x^k y^b)^{2n} = (x^{2n})^k y^{2bn} = 1, \\ &w_1^n = (x^k y^b)^n = x^{kn} y^{bn} = x^n \quad \text{and} \quad w_2^2 = (x^l y^d)^2 = x^{l-l} y^{2d} = y^2 = x^n, \\ &w_1 w_2 = (x^k y^b)(x^l y^d) = x^{k+l} y^{b+d} \quad \text{and} \quad w_2 w_1^{-1} = (x^l y^d)(y^{-b} x^{-k}) = x^{k+l} y^{d-b} = x^{k+l} y^{b+d}. \end{aligned}$$

One concludes that $\Gamma^0(4) \leq \mathrm{GL}^{\times}(O_{Q_{4n}})$ for any n, and $\Gamma^0(2) \leq \mathrm{GL}^{\times}(O_{Q_{4n}})$ if n is even. We know from Proposition 4.12 that the congruence subgroups $\Gamma^0(4)$ and $\Gamma^0(2)$ are of indices 6 and 3 in $\mathrm{GL}(2,\mathbb{Z})$ respectively. By Theorem 4.4, there are at least 4 (resp. 2) different cosets in $\mathrm{GL}(2,\mathbb{Z})/\mathrm{GL}^{\times}(O_{Q_{4n}})$ when $n > 2$ is odd (resp. even):

$$\begin{aligned} &T \notin \mathrm{GL}^{\times}(O_{Q_{4n}}) && \text{as } T\times(x,y)^* = (xy,y)^* \text{ and } (xy)y = xy^2 = x^{n+1} \neq x^{-1} = y(xy)^{-1}; \\ &T^2 \notin \mathrm{GL}^{\times}(O_{Q_{4n}}) \text{ if } 2 \nmid n && \text{as } T\times(x,y)^* = (xy^2,y)^* \text{ and } (xy^2)^n = x^n y^{2n} = y^{2(n+1)} = 1 \neq y^2; \\ &T^3 \notin \mathrm{GL}^{\times}(O_{Q_{4n}}) && \text{as } T\times(x,y)^* = (xy^3,y)^* \text{ and } (xy^3)y = xy^4 = x \neq x^{-n-1} = y(xy^3)^{-1}. \end{aligned}$$

So, the dual Veech group $\mathrm{GL}^{\times}(O_{Q_{4n}})$ is exactly $\Gamma^0(4)$ and $\Gamma^0(2)$ respectively for n odd and even. □

4.2.6 The tetrahedral origami

The group of orientation-preserving symmetries of a regular tetrahedron has 12 elements (identity, 8 rotations by 120° and 3 rotations by 180°). It can be presented as

$$Tet = \langle s, t \mid s^2 = t^3 = (st)^3 = 1 \rangle \simeq A_4,$$

where s is a rotation by 180° with respect to an axis connecting the midpoints of two opposite edges, and t is a rotation by 120° with respect to an axis passing through a vertex and the center of the opposite face (see Figure 4.7).

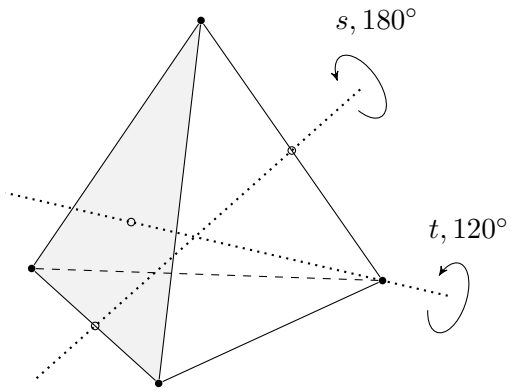


Figure 4.7: Symmetries of a regular tetrahedron.

The corresponding regular origami $O_{Tet,s,t}$ is called *tetrahedral*. Since $[s,t] = (sts)t^2 = t^{-1}s^{-1}t$ has order 2, from the formulas (4.2) follows that the regular origami O_{Tet} belongs to $\mathcal{H}(1,1,1,1,1,1)$ and has genus 4.

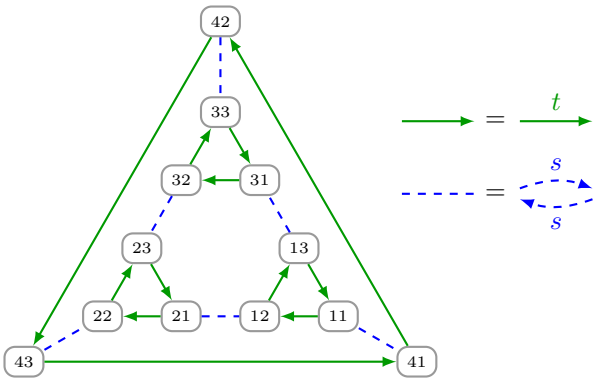


Figure 4.8: An origamal digraph for O_{Tet}.

Proposition 4.14. *The dual Veech group* $\mathrm{GL}^{\times}(O_{Tet})$ *of the tetrahedral origami is* $\Gamma^0(3)$.

Proof. Since $Tet \simeq A_4$, the order of any element in Tet is 1, 2 or 3. Moreover, by Dyck's theorem we have a homomorphism

$$\varphi : Tet \twoheadrightarrow \mathbb{Z}_3, \quad s \mapsto 0,\ t \mapsto 1,$$

which is surjective, so that an element $w(s,t)$ is sent to $e_t(w)$ mod 3, where $e_t(w)$ denotes the sum of the exponents of t in the word w. The kernel $\ker\varphi$ consist of the identity and three elements of order 2, namely s, tst^{-1} and $t^{-1}st$ – the three rotations by 180°. This gives a criterion: $w^2 = 1$ in the group Tet if and only if $e_t(w)$ is a multiple of 3. (In particular if $3 \nmid e_t(w)$ then w has order 3.)

Now, for the dual action of $\mathrm{GL}(2,\mathbb{Z})$ we have

$$A\times(s,t)^* = (w_1(s,t), w_2(s,t))^*, \quad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

where words w_1 and w_2 can be chosen such that

$$\begin{aligned} e_s(w_1) &= a, \quad e_t(w_1) = b, \\ e_s(w_2) &= c, \quad e_t(w_2) = d. \end{aligned}$$

According to Theorem 4.4 a matrix A stabilizes the regular origami O_{Tet} if and only if

$$w_1^2 = 1,\ w_2^3 = 1 \ \text{ and } \ (w_1 w_2)^3 = 1.$$

By the argument above, $w_1^2 = 1$ implies $3 \mid b$. Conversely, if $3 \mid b$ then $w_1^2 = 1$. Besides, $3 \nmid d$, as $ad - bc = \pm 1$, and so $w_2^3 = 1$, $(w_1 w_2)^3 = 1$. Therefore, according to Theorem 4.4,

$$\mathrm{GL}^{\times}(O_{Tet}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2,\mathbb{Z}) \mid b \equiv 0 \bmod 3 \right\},$$

which is an index 4 congruence subgroup (see Proposition 4.12). □

4.2.7 An octahedral origami

The *octahedral group Oct* is the group of orientation-preserving symmetries of a regular octahedron (or a cube, which is its dual). It has 24 elements (identity, 6 rotations by 90°, 8 rotations by 120°, 3 rotations by 180° about a 4-fold axis and 6 rotations by 180° about a 2-fold axis). The octahedral group is isomorphic to S_4 and can be presented as

$$Oct = \langle s, t \mid s^2 = t^3 = (st)^4 = 1 \rangle \simeq S_4,$$

where s is a rotation by 180° with respect to an axis connecting the midpoints of two opposite edges (a 2-fold axis), and t is a rotation by 120° with respect to an axis passing through the centers of two opposite faces (see the figure below).

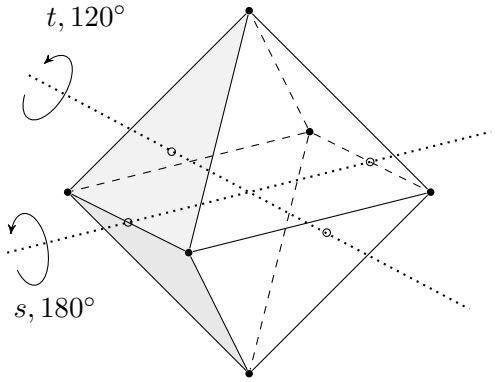


Figure 4.9: A regular octahedron.

The corresponding regular origami $O_{Oct} = O_{Oct,s,t}$ is called *octahedral*. By the formulas (4.2), the regular origami O_{Oct} belongs[4] to the stratum $\mathcal{H}(2_8)$ and has genus 9, since the commutator $[s,t] = (sts)t^2 = t^{-1}s^{-1}t^{-1}s^{-1}t = (st)^{-1}t^{-1}(st)$ has order 3 in Oct.

Proposition 4.15. *The direct Veech group of the octahedral origami O_{Oct} is*

$$\mathrm{GL}(O_{Oct}) = \mathtt{gp}\left\{ \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -5 & -2 \\ 3 & 1 \end{pmatrix}, \begin{pmatrix} -3 & -2 \\ 5 & 3 \end{pmatrix} \right\},$$

which is a noncongruence subgroup of $\mathrm{GL}(2,\mathbb{Z})$ *of index* 9.

Proof. The symmetries from Oct permute the four pairs of opposite sides of the octahedron, and there is an enumeration of the pairs providing an isomorphism

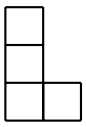
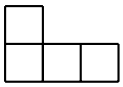
$$\rho : Oct \xrightarrow{\simeq} S_4 \quad \text{such that } \rho(s) = (1\ 2) \text{ and } \rho(t) = (2\ 3\ 4).$$

Since all automorphisms of the group $\rho(Oct) = S_4$ are inner (cf. Lemme 3.7), the representation ρ is structural and by Theorem 4.7 we have

$$\mathrm{GL}(O_\rho) = \mathrm{GL}(O_{Oct}),$$

where O_ρ is the 4-square-tiled surface encoded by the permutations (1 2) and (2 3 4), or else it is the corner origami $L(2,3)$.

[4] The abbreviation $\mathcal{H}(a_b) = \mathcal{H}(\underbrace{a, \ldots, a}_{b})$ is employed.

$L(2,3) =$  $\xrightarrow{S=\left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)}$ $L(3,2) =$ 

According to Gabriela Schmithüsen [85], the $\mathrm{SL}(2,\mathbb{Z})$-stabilizer of $L(3,2)$ is

$$\mathrm{SL}(L(3,2)) = \mathtt{gp}\left\{\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 2 & 1\end{pmatrix}, \begin{pmatrix}1 & 3\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & -3\\ 2 & -5\end{pmatrix}, \begin{pmatrix}3 & -5\\ 2 & -3\end{pmatrix}\right\},$$

where the generator $\begin{pmatrix}1 & 3\\ 0 & 1\end{pmatrix}$ is actually redundant. The group $\mathrm{SL}(L(3,2))$ is a noncongruence subgroup of $\mathrm{SL}(2,\mathbb{Z})$ of index $9 = 3(2-1)2^2(1-\frac{1}{2^2})$, due to [85] or by Theorem 3.4.

We have $\mathrm{SL}(O_\rho) = S \cdot \mathrm{SL}(L(3,2)) \cdot S^{-1}$, and

$$S\begin{pmatrix}a & b\\ c & d\end{pmatrix}S^{-1} = \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} = \begin{pmatrix}-c & -d\\ a & b\end{pmatrix}\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} = \begin{pmatrix}d & -c\\ -b & a\end{pmatrix}.$$

Finally, the matrix $J = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$ belongs to $\mathrm{GL}(O_\rho)$, since

$$J \cdot O_\rho = J \cdot ((1\ 2),(2\ 3\ 4))^* = ((1\ 2),(2\ 4\ 3))^* = (\delta(1\ 2)\delta^{-1}, \delta(2\ 3\ 4)\delta^{-1})^* = O_\rho, \quad \text{where } \delta = (3\ 4).$$

Therefore, the statement of the proposition is verified. □

4.2.8 Two icosahedral origamis

A regular icosahedron has 20 identical equilateral triangular faces, 30 edges and 12 vertices (see the picture below). The *icosahedral group* Ico is the group of orientation-preserving symmetries of a regular icosahedron (or its dual – a regular dodecahedron). The group Ico consists of 60 elements:

- the identity,
- the rotations by $k \cdot 72^\circ$ with $k = 1, 2, 3, 4$ about the axes passing through two opposite vertices (*i.e.* $4 \times \frac{12}{2} = 24$ rotations),
- the rotations by 180° about the axes passing through the midpoints of two opposite edges (*i.e.* $\frac{30}{2} = 15$ rotations),
- the rotations by $k \cdot 120^\circ$ with $k = 1, 2$ about the axes passing through the centers of two opposite faces (*i.e.* $2 \times \frac{20}{2} = 20$ rotations).

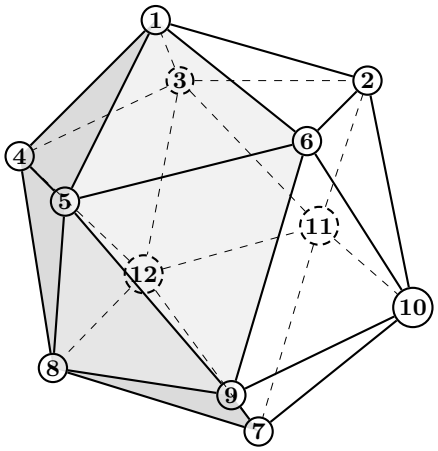


Figure 4.10: A regular icosahedron.

The icosahedral group is isomorphic to A_5 and $\mathrm{PSL}(2, \mathbb{F}_5)$, and can be presented as

$$Ico = \left\langle s, t \;\middle|\; s^2 = t^3 = (st)^5 = 1 \right\rangle \simeq A_5 \simeq \mathrm{PSL}(2, \mathbb{F}_5).$$

An isomorphism $\rho_1 : Ico \xrightarrow{\simeq} A_5$ is constructed as follows[5]. Let us divide the 30 edges of the icosahedron into 5 disjoint subsets, containing six edges parallel or perpendicular to each other:

$$\begin{aligned} a &= \{\text{1-2, 7-8, 4-5, 10-11, 6-9, 3-12}\}, \\ b &= \{\text{1-3, 7-9, 5-6, 11-12, 4-8, 2-10}\}, \\ c &= \{\text{1-4, 7-10, 2-6, 8-12, 5-9, 3-11}\}, \\ d &= \{\text{1-5, 7-11, 2-3, 8-9, 6-10, 4-12}\}, \\ e &= \{\text{1-6, 7-12, 3-4, 9-10, 5-8, 2-11}\}. \end{aligned}$$

Define s to be the rotation by 180° about the axis passing through the midpoints of the opposite edges 1-6 and 7-12. Then in the alternating group $Alt(\{a, b, c, d, e\})$, it is represented by the permutation

[5]There are several distinct ways to obtain such an isomorphism. A peculiar one lies in the fact that the centers of the faces of the icosahedron form the 20 vertices of a regular dodecahedron, which is, in its turn, the compound of five tetrahedra (the convex hull of the compound is the dodecahedron), or else the compound of five cubes. Each rotational symmetry of the icosahedron permutes these five tetrahedra.

$(a\ b)(c\ d)$. Further, define t to be the counterclockwise rotation by 240° about the axis passing through the centers of the opposite faces 1-6-2 and 7-12-8. Then t is represented by the permutation $(a\ c\ e)$. Since Ico is generated by the rotations s and t, we obtain an isomorphism

$$\rho_1 : Ico \xrightarrow{\simeq} \mathtt{gp}\left\{(a\ b)(c\ d),\ (a\ c\ e)\right\} = Alt(\{a,b,c,d,e\}) \simeq A_5.$$

The corresponding regular square-tiled surface $O_{Ico,s,t}$ is called the *first icosahedral origami*. By the formulas (4.2), the origami $O_{Ico,s,t}$ belongs to the stratum $\mathcal{H}(4_{12})$ and has genus 25, since the commutator

$$[s,t] = (sts)t^2 = t^{-1}s^{-1}t^{-1}s^{-1}t^{-1}s^{-1}t = (tst)^{-1}(st)(tst)$$

is of order 5 in Ico.

Proposition 4.16. *Let O_1 be the 5-square origami encoded by the permutations* (1 2)(3 4) *and* (1 3 5). *Then* $\mathrm{GL}(O_{Ico,s,t}) = \mathrm{GL}(O_1)$.

Proof. The composition of the isomorphism $\rho_1 : Ico \xrightarrow{\simeq} A_5$ defined above and the inclusion $A_5 \hookrightarrow S_5$ gives a faithful permutation representation $\rho : Ico \hookrightarrow S_5$. This representation is structural, since all automorphisms of the alternating group of degree 5 are conjugations by a permutation from S_5, that is, $\mathrm{Aut}(A_5) = S_5$. By Theorem 4.7, we have $\mathrm{GL}(O_1) = \mathrm{GL}(O_\rho) = \mathrm{GL}(O_{Ico,s,t})$. □

The origami O_1 in the proposition belongs to the stratum $\mathcal{H}(4)$ and is of genus 3.

$$O_1 = \begin{array}{|c|c|c|}\hline & 5 & \\ \hline 4 & 3 & \\ \hline & 1 & 2 \\ \hline \end{array}$$

Using the mathematics software system Sage, we found its Veech group

$$\mathrm{GL}(O_1) = \mathtt{gp}\left\{\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}, \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}, \begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 3 & 0\end{pmatrix}, \begin{pmatrix}-4 & 3\\ -7 & 5\end{pmatrix}\right\}$$

which is a subgroup of $\mathrm{GL}(2,\mathbb{Z})$ of index 10.

The icosahedral group has another presentation

$$Ico = \left\langle u, v \;\middle|\; u^3 = v^3 = (uv)^5 = (uv^{-1}uv)^2 = 1 \right\rangle,$$

where u the counterclockwise rotation by 120° about the axis passing through the midpoints of the faces 5-9-6 and 11-3-12, and v is the counterclockwise rotation by 240° about the axis passing through the midpoints of the faces 5-8-9 and 11-2-3. The rotations u and v correspond to the permutations $(a\ b\ c)$ and $(c\ d\ e)$. Thus, we obtain an isomorphism

$$\rho_2 : Ico \xrightarrow{\simeq} \mathtt{gp}\left\{(a\ b\ c),\ (c\ d\ e)\right\} = Alt(\{a,b,c,d,e\}) \simeq A_5.$$

The regular square-tiled surface $O_{Ico,u,v}$ is called the *second icosahedral origami.* We have

$$(uv)^{-1} \cdot [u,v] \cdot (uv) = u^{-1}v^{-1}uv = u(uv^{-1}uv) = u(uv^{-1}uv)^{-1} = uv^{-1}(u^{-1})vu^{-1},$$

i.e. the commutator $[u,v]$ is of order 3 in the group Ico. Hence, by the formulas (4.2), the origami $O_{Ico,u,v}$ belongs to the stratum $\mathcal{H}(2_{20})$ and has genus 21.

Proposition 4.17. *Let O_2 be the 5-square origami encoded by the permutations* (1 2 3) *and* (3 4 5). *Then* $\mathrm{GL}(O_{Ico,u,v}) = \mathrm{GL}(O_2)$.

Proof. Analogous to the proof of the previous proposition. □

The origami O_2 belongs to the stratum $\mathcal{H}(2)$ and has genus 2.

$$O_2 = L(3,3) = \begin{array}{|c|c|c|}\hline 5 & & \\ \hline 4 & & \\ \hline 3 & 1 & 2 \\ \hline \end{array}$$

Using Sage, we found that its Veech group is generated by the following matrices

$$\mathrm{GL}(O_2) = \mathtt{gp}\left\{\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}, \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}, \begin{pmatrix}3 & -1\\ 1 & 0\end{pmatrix}, \begin{pmatrix}5 & -9\\ 4 & -7\end{pmatrix}\right\}$$

and is a subgroup of $\mathrm{GL}(2, \mathbb{Z})$ of index 9.

4.2.9 Burnside origamis

Consider the Burnside group $B(m,k)$, $m>1$, defined as the largest m-generator group in which the identity $x^k=1$ holds for all elements x. Burnside's famous problem asks whether the group $B(m,k)$ is finite. For instance, the group $B(m,2)$ is elementary abelian of order 2^m, since $xyx^{-1}y^{-1} = x^2(x^{-1}y)^2y^{-2}$. In the historical 1902 paper [13], William Burnside himself showed that the order of $B(m,3)$ is bounded by 3^{2^m-1}, and also $|B(2,4)|\le 2^{12}$. Only almost 40 years later Ivan N. Sanov [82] proved that $B(m,4)$ is finite, and in 1958 Marshall Hall Jr. [54] established finiteness of $B(m,6)$. The particular case of $B(2,5)$ remains open: it is not known whether this group is finite. In a series of fundamental articles published in 1968, Petr S. Novikov and Sergei I. Adjan [77] gave the negative answer to the question of Burnside for odd $k\ge 4381$. Afterwards, Adjan [1, 1975] improved the result by showing that already for odd $k\ge 665$ the group $B(m,k)$ is infinite.

Proposition 4.18. *Let $B(2,k)$ be a finite two-generator Burnside group. The integer Veech group of the regular origami $O_{B(2,k)}$ is the whole group* $\mathrm{GL}(2,\mathbb{Z})$.

Proof. By presenting the Burnside group $B(2,k)$ as follows

$$B(2,k) = \left\langle g,h \;\middle|\; (W(g,h))^k = 1 \text{ for any word } W \right\rangle, \tag{4.6}$$

and by applying Theorem 4.4, we immediately conclude. □

Case $k=3$. Let us show that any Burnside group $B(m,3)$ is finite. First, introduce two definitions. A group is called *periodic* if all its elements have finite orders (not necessary the same). A group G is called *locally finite* if any finitely generated subgroup of G is finite.

Proposition 4.19. *If some normal subgroup N and the quotient G/N of a group G are locally finite, then G is locally finite as well.*

Proof. Let $S=\{s_1,\dots,s_p\}$ be a finite subset of G. By assumption, the cosets s_iN generate a finite group $H=\{t_1N,\dots,t_qN\}$, $q\ge p$. The set of representatives $T=\{t_1,\dots,t_q\}$ can be chosen such that all s_i and s_i^{-1} belong to it. For any $1\le i,j\le q$ we have

$$t_i\cdot t_j = t_r n_{ij}, \qquad \text{where } 1\le r\le q \text{ and } n_{ij}\in N.$$

Therefore, any word $t_{i_1}\cdots t_{i_r}$ is equal to a word $t\cdot n$, where $t\in T$ and n is a product of n_{ij}'s (for instance, $t_1t_2t_3 = t_1t_an_{23} = t_b\cdot n_{1a}n_{23}$). Since the finite set $\{n_{ij}\}$ generates a finite subgroup of N, the subgroup of G generated by the set $S\subset T$ is finite as well. □

Corollary 4.20. *Any periodic solvable group G is locally finite.*

Proof. An abelian periodic group is locally finite because any elements $a_1,\cdots,a_p$ with orders $k_1,\dots,k_p$ generate a subgroup of order at most $k_1\cdots k_p$. The corollary follows by induction on the length of a subnormal series of G using Proposition 4.19. □

Remark that in a periodic group G of period[6] 3, any element commutes with its conjugates, that is, $x(yxy^{-1}) = (yxy^{-1})x$ for any $x,y\in G$. Indeed, we have $(xy)^3 = y^3 = (x^{-1}y)^3 = 1$, and so

$$(xyx)(y^{-1})(x^{-1}yx^{-1})(y^{-1}) = (y^{-1}x^{-1}y^{-1})(y^2)(y^{-1}xy^{-1})(y^2) = 1.$$

Let now $\{g_1,\dots,g_m\}$ be a generating system of $G=B(m,3)$. Take the subgroup N_1 generated by all conjugates of g_1. Obviousely, it is normal in $B(m,3)$, and by the remark we made N_1 is abelian. Further, consider the group G/N_1 which is also periodic with period 3. Let N_2/N_1, where

[6] A *period* of a group G is a positive integer n such that $x^n=1$ for all $x\in G$.

$N_1 \lhd N_2 \leq G$, be the subgroup of G/N_1 generated by the conjugates of $g_2 N_1$. Again, it is normal and abelian. Continue this procedure recursively on i from 1 to $m-1$ by defining N_{i+1}/N_i, where $N_i \lhd N_{i+1} \leq G$, to be the subgroup of $G/N_i \simeq {}^{(G/N_{i-1})}\big/_{(N_i/N_{i-1})}$ generated by the conjugates of $g_{i+1}N_i$. We will get a subnormal series

$$\{1\} \lhd N_1 \lhd N_2 \lhd \cdots \lhd N_m = G,$$

whose factor groups are abelian. Thus, the group $B(m,3)$ is solvable. By Corollary 4.20 it is locally finite, and so finite.

Friedrich Levi and B. L. van der Waerden [59, 1933] showed that

$$|B(m,3)| = 3^{m+\binom{m}{2}+\binom{m}{3}}.$$

In particular, the Burnside group $B(2,3)$ has order 27 and is given by the following presentation:

$$B(2,3) = \langle g, h \mid g^3 = h^3 = (gh)^3 = (gh^{-1})^3 = 1 \rangle \tag{4.7}$$

By Proposition 4.18, the corresponding regular origami is invariant under the action of $\mathrm{GL}(2,\mathbb{Z})$,

$$\mathrm{GL}^{\times}(O_{B(2,3)}) = \mathrm{GL}(2,\mathbb{Z}).$$

Further, the order of the commutator $[g,h]$ is 3, thus by the formulas (4.2) this Burnside origami belongs to the stratum $\mathcal{H}(\underbrace{2,\ldots,2}_{9})$ and is a surface of genus 10.

Case $k=4$. In his Ph.D. thesis [93, 1954], Sean Tobin proved that $B(2,4)$ has order 2^{12} and can be presented in the following way (see also [55]):

$$B(2,4) = \langle g, h \mid g^4 = h^4 = (gh)^4 = (g^{-1}h)^4 = (g^2h)^4 = (gh^2)^4 = 1,\ (g^{-1}h^{-1}gh)^4 = (g^{-1}hgh)^4 = 1 \rangle.$$

The corresponding regular origami $O_{B(2,4)}$ is also stabilized by $\mathrm{GL}(2,\mathbb{Z})$. It belongs to the stratum $\mathcal{H}(\underbrace{3,\ldots,3}_{2^{10}})$ and has genus $3\cdot 2^9 + 1$.

Case $k=6$. Marshall Hall Jr. showed in [54] that the group $B(m,6)$ has order

$$2^a 3^{b+\binom{b}{2}+\binom{b}{3}}, \quad \text{where } a = 1+(m-1)3^{m+\binom{m}{2}+\binom{m}{3}},\ b = 1+(m-1)2^m.$$

In particular, we have $|B(2,6)| = 2^{28}3^{25}$. The square-tiled surface $O_{B(2,6)}$ corresponding to the presentation (4.6) is stabilized by $\mathrm{GL}(2,\mathbb{Z})$, lies in the stratum $\mathcal{H}(\underbrace{5,\ldots,5}_{2^{27}3^{24}})$ and has genus $5\cdot 2^{26}3^{24}+1$.

4.2.10 Polynomial origamis

The following set of polynomials over a finite field $\mathbb{F}_p$, where p is prime,

$$G_n(p) = \left\{ x + a_2x^2 + \cdots + a_nx^n \mid a_i \in \mathbb{F}_p \right\}$$

forms a group under the binary operation of composition of functions modulo x^{n+1}. This is a two-generator group of order p^{n-1}, see the textbook [51, p. 68] by D. L. Johnson. The corresponding regular origamis $O_{G_n(p)}$ are called *polynomial*.

• When $n = 3$, wa have a group of order p^2:

$$G_3(p) = \left\{ x + ax^2 + bx^3 \mid a, b \in \mathbb{F}_p \right\}.$$

Take an element $R = x + ax^2 + bx^3$ and calculate its powers. Denote

$$R^k = x + a_kx^2 + b_kx^3,$$

where $a_1 = a$ and $b_1 = b$. Then

$$\begin{aligned} R^{k+1} = R \circ R^k &= (x + a_kx^2 + b_kx^3) + a(x + a_kx^2 + b_kx^3)^2 + b(x + a_kx^2 + b_kx^3)^3 \\ &= x + (a_k + a)x^2 + (b_k + 2aa_k + b)x^3, \end{aligned}$$

that is, $a_{k+1} = a_k + a$ and $b_{k+1} = b_k + 2aa_k + b$, from where

$$\begin{aligned} a_k &= ka, \\ b_k &= kb + 2aa_1 + 2aa_2 + \ldots + 2aa_{k-1} = kb + 2a^2(1 + 2 + \ldots + k - 1) \\ &= kb + k(k-1)a^2, \end{aligned}$$

for any $k \geq 1$. Therefore, one has $R^p = x$, which is the identity element.

Recall that any group of order p^2 is abelian[7], *i.e.* isomorphic to $C_p \times C_p$ or C_{p^2}. Since $R^p = x$ for any element $R \in G_3(p)$, we conclude that

$$G_3(p) \simeq C_p \times C_p.$$

In particular, according to the subsection 4.2.1 we get the following proposition:

Proposition 4.21. *The origami $O_{G_3(p)}$ is trivial and* $\mathrm{GL}(O_{G_3(p)}) = \mathrm{GL}(2, \mathbb{Z})$.

• When $n = 4$, we are dealing with a group of order p^3:

$$G_4(p) = \left\{ x + ax^2 + bx^3 + cx^4 \mid a, b, c \in \mathbb{F}_p \right\}.$$

[7] Indeed, let G be a group of order p^2 and Z its center. The group G acts on its elements by conjugation, each orbit has length $[G : G_g]$ for some $g \in G$ and $G_g = \left\{ h \in G \mid hgh^{-1} = g \right\}$. Denote by $g_1, g_2, \ldots, g_l$ representatives of the conjugacy classes of G. Then we obtain that

$$p^2 = |G| = \sum_{i=1}^{l} [G : G_{g_i}] = \sum_{g_i \in Z} 1 + \sum_{g_i \notin Z} [G : G_{g_i}].$$

Since the first sum equals $|Z|$ and the second one is a multiple of p, the order of the center $|Z|$ is a multiple of p as well (for the same reason, the center of a nontrivial p-group is never trivial). If $|Z| = p^2$, then the group $G = Z$ is abelian. Else $|Z| = p$, implying that both Z and G/Z are cyclic groups of order p. Suppose that Z is generated by u and G/Z by vZ, where $u, v \in G$. Then the group G is generated by u and v that do commute as $u \in Z$.

The group $G_4(p)$ is never abelian. Indeed, the elements $V = x + x^2$ and $W = x + x^3$ don't commute:

$$V \circ W = (x + x^3) + (x + x^3)^2 = x + x^2 + x^3 + 2x^4,$$
$$W \circ V = (x + x^2) + (x + x^2)^3 = x + x^2 + x^3 + 3x^4.$$

Consider an arbitrary element $F = x + ax^2 + bx^3 + cx^4$ of the group $G_4(p)$, and let

$$F^k = x + a_k x^2 + b_k x^3 + c_k x^4$$

with $a_1 = a$, $b_1 = b$ and $c_1 = c$. Then

$$\begin{aligned} F^{k+1} = F \circ F^k &= (x + a_k x^2 + b_k x^3 + c_k x^4) + a(x + a_k x^2 + b_k x^3 + c_k x^4)^2 \\ &\qquad + b(x + a_k x^2 + b_k x^3 + c_k x^4)^3 + c(x + a_k x^2 + b_k x^3 + c_k x^4)^4 \\ &= (x + a_k x^2 + b_k x^3 + c_k x^4) + (ax^2 + 2aa_k x^3 + 2ab_k x^4 + aa_k^2 x^4) + (bx^3 + 3ba_k x^4) + cx^4 \\ &= x + (a_k + a)x^2 + (b_k + b + 2aa_k)x^3 + (c_k + c + 2ab_k + 3ba_k + aa_k^2)x^4. \end{aligned}$$

This means that $a_{k+1} = a_k + a$, $b_{k+1} = b_k + b + 2aa_k$ and $c_{k+1} = c_k + c + 2ab_k + 3ba_k + aa_k^2$, from where we find that

$$\begin{aligned} a_k &= ka, \\ b_k &= kb + 2a\sum_{i=1}^{k-1} a_i = kb + 2a^2 \sum_{i=1}^{k-1} i = kb + k(k-1)a^2, \\ c_k &= kc + 2a\sum_{i=1}^{k-1} b_i + 3b\sum_{i=1}^{k-1} a_i + a\sum_{i=1}^{k-1} a_i^2 \\ &= kc + 2a\sum_{i=1}^{k-1} \big(ib + i(i-1)a^2\big) + 3b\sum_{i=1}^{k-1} ia + a\sum_{i=1}^{k-1} (ia)^2 \\ &= kc + 5ab\sum_{i=1}^{k-1} i + a^3 \sum_{i=1}^{k-1} \big(2i(i-1) + i^2\big) = kc + 5ab\,\frac{k(k-1)}{2} + a^3 \sum_{i=1}^{k-1} \big(3i^2 - 2i\big) \\ &= kc + 5ab\,\frac{k(k-1)}{2} + a^3\Big(3\frac{(k-1)k(2k-1)}{6} - 2\frac{k(k-1)}{2}\Big) \\ &= kc + 5ab\,\frac{k(k-1)}{2} + a^3\,\frac{k(k-1)(2k-3)}{2} \end{aligned}$$

for any $k \geq 1$. Therefore, one has

$$F^p = \begin{cases} x + (ab + a^3)x^4 & \text{if } p = 2, \\ x & \text{if } p \geq 3. \end{cases} \tag{4.8}$$

It is known (see Exercise 7.5.2 of the textbook [7] by Homer Bechtell) that up to isomorphism there are exactly 5 distinct groups of order p^3:

the abelian groups $C_p \times C_p \times C_p$, $C_{p^2} \times C_p$ and C_{p^3};

(for $p = 2$) the dihedral group $D_4 = \langle s, t \mid s^2 = t^2 = (st)^4 = 1 \rangle$ of order 8 and the quaternion group $Q_8 = \langle s, t \mid s^2 = t^2, st = ts^{-1} \rangle$;

(for $p \geq 3$) the Heisenberg group

$$\begin{aligned} H_p &= \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{SL}(3, \mathbb{F}_p) \mid a, b, c \in \mathbb{F}_p \right\} \\ &= \langle s, t \mid s^p = t^p = [s,t]^p = 1,\ s[s,t] = [s,t]s,\ t[s,t] = [s,t]t \rangle \end{aligned}$$

$$\text{and the group } L_p = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a, b \in \mathbb{F}_{p^2},\ a \equiv 1 \bmod p \right\} = \left\langle s, t \;\middle|\; t^{-1}st = s^{1+p},\ s^{p^2} = t^p = 1 \right\rangle.$$

The polynomial group $G_4(p)$ is a non-abelian group of order p^3. For $p = 2$, it follows from (4.8) that $G_4(2)$ has exactly 6 involutions corresponding to

$$(a, b, c) \in \{(0,0,0), (0,0,1), (0,1,0), (0,1,1), (1,1,0), (1,1,1)\}.$$

Since in the quaternion group there are exactly two involutions 1 and -1 and all other elements have order 4, we obtain $G_4(2) \simeq D_4$. For $p \geq 3$, the equation $F^p = x$ is satisfied for each $F \in G_4(3)$, and so $G_4(3) \simeq H_p$.

Denote by (X, Y) the generating pair of the group $G_4(p)$ that is sent by an isomorphism to the generating pair (s, t) of D_4 and H_p respectively for $p = 2$ and $p \geq 3$ (see the presentations of D_4 and H_p above). Consider the origami $O_{G_4(p)} = O_{G_4(p),X,Y}$. According to the subsections 4.2.2 and 4.2.3, the following proposition takes place:

Proposition 4.22. *The origami $O_{G_4(2)}$ is dihedral and its Veech group is*

$$\mathrm{GL}(O_{G_4(2)}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z}) \mid a + c \text{ and } b + d \text{ are odd} \right\}.$$

For any prime $p \geq 3$, the origami $O_{G_4(p)}$ is Heisenberg, and $\mathrm{GL}(O_{G_4(p)}) = \mathrm{GL}(2, \mathbb{Z})$.

• Now, let us study the case that $n = 5$ and $p = 2$ corresponding to the group $G_5(2)$ of order 16. It has the following presentation:

$$G_5(2) = \left\langle P, Q \;\middle|\; P^4 = Q^4 = (PQ)^2 = (PQ^{-1})^2 = 1 \right\rangle,$$

where $P = x + x^2$, $Q = x + x^3$ and the identity 1 stands for the polynomial x, see [51, p. 68]. For instance,

$$\begin{aligned} P^2 &= (x + x^2) + (x + x^2)^2 = x + x^4, \\ P^3 &= (x + x^4) + (x + x^4)^2 = x + x^2 + x^4, \\ Q^2 &= (x + x^3) + (x + x^3)^2 = x + x^5, \\ Q^3 &= (x + x^5) + (x + x^5)^3 = x + x^3 + x^5. \end{aligned}$$

Using the relations $PQ = Q^{-1}P^{-1}$ and $PQ^{-1} = QP^{-1}$, one concludes that any element $w(P, Q)$ of the group $G_5(2)$ can be *uniquely* presented in the form

$$P^i Q^j, \quad \text{for some } 0 \leq i, j \leq 3.$$

Moreover, such integers i and j have the same parities as $e_P(w)$ and $e_Q(w)$ respectively, where $e_P(w)$ and $e_Q(w)$ are sums of the exponents of P and Q in the word w. Denoting $\chi(k) = 1 + (-1)^k \in \{0, 2\}$, one has

$$\begin{aligned} P^i Q^j &= Q^{(-1)^i j} P^{(-1)^j i}, \\ (P^i Q^j)^2 &= P^{\chi(j)i} Q^{\chi(i)j}, \end{aligned}$$

and so $(P^i Q^j)^2 = 1$ if and only if $(i - j)$ is even (if i is odd and j is even then $\chi(j)i$ is not a multiple of 4). Also, since $\chi(k)$ is always even,

$$(P^i Q^j)^4 = P^{\chi(j)i} Q^{\chi(i)j} P^{\chi(j)i} Q^{\chi(i)j} = P^{2\chi(j)i} Q^{2\chi(i)j} = 1,$$

that is, the order of any nontrivial element in $G_5(2)$ is either 2 or 4.

The order of the commutator $[P, Q] = P(QP^{-1})Q^{-1} = P^2 Q^{-2} = P^2 Q^2$ is 2. Therefore, by the formulas (4.2), the origami $O_{G_5(2),P,Q}$ is of genus 5 and belongs to the stratum $\mathcal{H}(1_8)$.

Proposition 4.23. *The dual Veech group of the polynomial origami $O_{G_5(2),P,Q}$ is*

$$\mathrm{GL}^{\times}(O_{G_5(2),P,Q}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2,\,\mathbb{Z}) \;\middle|\; a+b \text{ and } c+d \text{ are odd} \right\},$$

which is an index three subgroup of $\mathrm{GL}(2,\,\mathbb{Z})$.

Proof. The dual action of $\mathrm{GL}(2,\,\mathbb{Z})$ on the conjugacy classes of pairs is given by

$$A{\times}(P,Q)^* = (w_1(P,Q), w_2(P,Q))^*, \quad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

where words w_1 and w_2 can be chosen such that

$$\begin{aligned} e_P(w_1) &= a, \quad e_Q(w_1) = b, \\ e_P(w_2) &= c, \quad e_Q(w_2) = d. \end{aligned}$$

According to Theorem 4.4, a matrix A stabilizes the regular origami $O_{G_5(2),P,Q}$ if and only if

$$w_1^4 = 1,\ w_2^4 = 1,\ (w_1 w_2)^2 = 1 \ \text{ and } \ (w_1 w_2^{-1})^2 = 1.$$

The first two relations are automatically satisfied, since the group $G_5(2)$ has only elements of order 1, 2 and 4. For the third relation, we shall present the element $w_1 w_2$ in the form $P^i Q^j$, where i and j have the same parities as $a+c$ and $b+d$ respectively. Thus, $(w_1 w_2)^2 = 1$ if and only if $(i-j)$ is even, that is, $k = (a+c)-(b+d)$ is even. By analogy, $(w_1 w_2^{-1})^2 = 1$ if and only if $(a-c)-(b-d) = k+2(d-c)$ is even.

For integers a, b, c, d such that $ad - bc = \pm 1$, the condition $2 \mid (a+c)-(b+d)$ is equivalent to the condition that both $a+c$ and $b+d$ are odd (as $ad-bc = d(a+c) - c(b+d)$), or else that $a+b$ and $c+d$ are odd. This proves the proposition. □

Remark that the groups $G_5(2)$ and D_8 are both of order 16, and the corresponding regular origamis have the same Veech groups (*cf.* Propositions 4.10 and 4.23). However, the group $G_5(2)$ is not isomorphic to the dihedral group, since the order of any of its elements is at most 4, meanwhile D_8 has an element of order 8 (rotation by $\pi/4$).

Question 4.1. Study the polynomial origamis $O_{G_n(p)}$ with $n \geq 5$. For instance, is it true that the Veech group of such an origami is a congruence subgroup?

4.2.11 Projective origamis

Let p be a prime number. The projective special linear group $\mathrm{PSL}(2,p) = \mathrm{PSL}(2,\mathbb{F}_p)$ over the field $\mathbb{F}_p$ is a quotient of the special linear group $\mathrm{SL}(2,p)$,

$$\mathrm{PSL}(2,p) = \mathrm{SL}(2,p)/SZ,$$

where SZ consists of nonzero scalar transformations of $\mathbb{F}_p^2$ with unit determinant, that is,

$$SZ = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{F}_p,\ a^2 = 1 \right\}.$$

Since $SZ = \{\pm I\} = \{I\}$ for $p = 2$ and $SZ = \{\pm I\} = \{I\}$ for $p \geq 3$, where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, we obtain

$$n := |\mathrm{PSL}(2,p)| = \frac{1}{\gcd(2,p-1)}|\mathrm{SL}(2,p)| = \frac{p(p^2-1)}{\gcd(2,p-1)} = \begin{cases} 6 & \text{if } p = 2, \\ \frac{1}{2}p(p^2-1) & \text{if } p \geq 3. \end{cases}$$

The regular square-tiled surfaces with monodromy group $\mathrm{PSL}(2,p)$ will be called *projective*, and denoted by $O_{\mathrm{PSL}(2,p)}$, or explicitely by $O_{\mathrm{PSL}(2,p),\bar{A},\bar{B}}$ with $(\bar{A},\bar{B})$ a generating pair of $\mathrm{PSL}(2,p)$.

Proposition 4.24. *The number of distinct* $\mathrm{GL}(2,\mathbb{Z})$*-orbits of projective* n*-square origamis* $O_{\mathrm{PSL}(2,p)}$*, where* $p > 2$ *is prime and* $n = p(p^2-1)/2$*, tends to infinity as* $p \to \infty$*.*

Proof. By Theorem 4.4, the number of $\mathrm{GL}(2,\mathbb{Z})$-orbits of regular origamis $O_{\mathrm{PSL}(2,p)}$ is equal to the number of T_2-systems in the group $\mathrm{PSL}(2,p)$. Due to a result of Martin J. Evans [29], the number of T_2-systems in $\mathrm{PSL}(2,p)$ tends to infinity as $p \to \infty$. (See also the paper [34] by Robert Guralnick and Igor Pak.) □

Remark. As Darryl J. McCullough and Marcus Wanderley showed in [66], the number of T_2-systems in $\mathrm{PSL}(2,p^s)$, for $p = 2$ or $p^s \geq 13$, is greater than

$$\frac{1}{s}\sum_{r|s} \varphi\left(\frac{s}{r}\right) p^r, \quad \text{where } \varphi \text{ is the Euler totient function.}$$

• When $p = 2$, an isomorphism $\mathrm{PSL}(2,2) \simeq S_3$ is easily observed though the faithful action of $\mathrm{PSL}(2,2)$ on the projective line $\mathbb{P}^1(\mathbb{F}_2) = \mathbb{F}_2 \cup \{\infty\}$. In the symmetric group

$$S_3 \simeq Sym(\mathbb{P}^1(\mathbb{F}_2)) = \{\mathrm{id}, (0\ 1), (0\ \infty), (1\ \infty), (0\ 1\ \infty), (0\ \infty\ 1)\},$$

there are exactly $2 \cdot \binom{5}{2} - 2 = 18$ generating pairs:

$$\mathcal{G}_2(S_3) = \{(\sigma,\tau) \mid \sigma,\tau \in S_3 \setminus \{\mathrm{id}\},\ \sigma \neq \tau\} \setminus \{((0\ 1\ \infty),(0\ \infty\ 1)),\ ((0\ \infty\ 1),(0\ 1\ \infty))\}.$$

The commutator of any generating pair is a 3-cycle. Moreover, the elements of $\mathcal{G}_2(S_3)$ form a single T_2-system. Therefore, by Theorem 4.4 all 6-square projective origamis $O_{\mathrm{PSL}(2,2)}$ belong to the same $\mathrm{GL}(2,\mathbb{Z})$-orbit (*cf.* also below).

• When $p \geq 3$, the projective group $\mathrm{PSL}(2,p)$ is a two-generator group with the following presentation[8]:

$$\mathrm{PSL}(2,p) = \left\langle t, u \;\middle|\; t^p = 1,\ tut = utu,\ (u^4 t^{(p+1)/2})^2 = 1 \right\rangle, \tag{4.9}$$

[8] This presentation was obtained in the dissertation of J. H. Renshaw (1982). He applied the results of the paper [90] by J. G. Sunday and the paper [8] by H. Behr and J. L. Mennicke. See also the paper [17] by Colin M. Campbell and Peter P. Campbell, the Ph.D. thesis [99] by P. D. Williams and the paper [16] by Colin M. Campbell.

where t and u are the images of the matrices $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $U = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$ from $\mathrm{SL}(2,p)$.

The commutator of two elements from $\mathrm{PSL}(2,p)$ being well-defined in $\mathrm{SL}(2,p)$, we have

$$[t,u] = [T,U] = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}\cdot\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}\cdot\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

It follows by induction on $m \geq 1$ that the positive powers of the integer matrix

$$C = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^2 \in \mathrm{SL}(2,\,\mathbb{Z})$$

$$\text{are} \quad C^m = \begin{pmatrix} f_{2m-1} & f_{2m} \\ f_{2m} & f_{2m+1} \end{pmatrix},$$

where (f_m) is the Fibonacci sequence defined recurrently via

$$f_0 = 0,\ f_1 = 1 \quad \text{and} \quad f_{m+1} = f_m + f_{m-1} \quad \text{for any} \ \ m \in \mathbb{N}.$$

Denote by $\bar{C}$ the image of the matrix C in the projective group $\mathrm{PSL}(2,p)$. Let k be the order of $\bar{C}$, that is, the minimal integer greater than 1 such that

$$\begin{cases} f_{2k-1} \equiv f_{2k+1} \equiv \pm 1 \mod p, \\ f_{2k} \equiv 0 \mod p. \end{cases}$$

• When $p = 2$, we have $n = 6$ and $k = 3$, so according to (4.2),

$$O_{\mathrm{PSL}(2,2),t,u} \in \mathcal{H}(2,2) \quad \text{and} \quad \mathrm{genus}(O_{\mathrm{PSL}(2,2),t,u}) = 3.$$

Under the isomorphism $\mathrm{PSL}(2,2) \simeq Sym(\mathbb{P}^1(\mathbb{F}_2))$ described above, the elements x and y correspond to the permutations $\sigma = (0\ 1)$ and $\tau = (1\ \infty)$ respectively, since $T : x \mapsto x{+}1$ and $U : x \mapsto x/(-x{+}1)$ for any $x \in \mathbb{P}^1(\mathbb{F}_2)$. Hence, the regular origamis $O_{\mathrm{PSL}(2,2),t,u}$ and $O_{S_3,\sigma,\tau}$ are the same. The latter is also the dihedral origami O_{D_3}, and by Proposition 4.10 we find that the Veech group

$$\mathrm{GL}(O_{\mathrm{PSL}(2,2),t,u}) = \mathrm{GL}(O_{D_3})$$

is an index three subgroup of $\mathrm{GL}(2,\,\mathbb{Z})$.

• When $p \geq 3$, the order k of $\bar{C}$ divides $(p \pm 1)/2$ due to the following lemma:

Lemma 4.25. *Let $A \in \mathrm{SL}(2,p)$ be a nonparabolic[9] matrix, and $\bar{A}$ its image in $\mathrm{PSL}(2,p)$. Then the order of $\bar{A}$ is a divisor of $\frac{p-1}{2}$ or $\frac{p+1}{2}$.*

Proof. Let $\lambda_1, \lambda_2 \in \mathbb{F}_{p^2}$ be the eigenvalues of $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ – we have $\lambda_1\lambda_2 = 1$ and $\lambda_1 \neq \lambda_2$. Take $z = \lambda_1/\lambda_2 = (\lambda_1)^2$. The cyclic group $\mathtt{gp}\left\{\bar{A}\right\}$ acts *faithfully* on the projective line $\mathbb{P}^1(\mathbb{F}_p) = \mathbb{F}_p \cup \{\infty\}$ via

$$\bar{A}\cdot x = \frac{ax+b}{cx+d} \ \text{ for any } x \in \mathbb{F}_p \text{ and } \bar{A}\cdot\infty = \frac{a}{c}.$$

If the eigenvalues of A belong to $\mathbb{F}_p$, then this action is equivalent to the multiplication by $z \in \mathbb{F}_p$, since the matrix A is conjugate to $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$. The equivalence means that the actions of $\mathtt{gp}\left\{\bar{A}\right\}$ and $\mathtt{gp}\left\{z\right\}$ on $\mathbb{P}^1(\mathbb{F}_p)$ correspond to conjugate subgroups in the symmetric group $Sym(\mathbb{P}^1(\mathbb{F}_p)))$. Thus the

[9] that is, with trace distinct from ± 2.

order of $\bar{A}$ is equal to the order of $z = (\lambda_1)^2$ in the multiplicative group $\mathbb{F}_p^\times$, and so it must divide the integer $\frac{p-1}{2}$ as $(\lambda_1^2)^{\frac{p-1}{2}} = \lambda_1^{p-1} = 1$.

If the eigenvalues of A don't belong to $\mathbb{F}_p$, then we also consider the faithful action of $\mathtt{gp}\left\{\bar{A}\right\}$ on the projective line $\mathbb{P}^1(\mathbb{F}_{p^2}) = \mathbb{F}_{p^2} \cup \{\infty\}$. Again, it is equivalent to the multiplication by $z \in \mathbb{F}_{p^2}$, implying that the lengths of the respective orbits for the actions of the cyclic groups $\mathtt{gp}\left\{\bar{A}\right\}$ and $\mathtt{gp}\{z\}$ on $\mathbb{P}^1(\mathbb{F}_{p^2})$ are the same. Let k be the order of z in $\mathbb{F}_{p^2}^\times$. Multiplying the elements of $\mathbb{P}^1(\mathbb{F}_{p^2})$ by z, there are exactly two orbits of length 1 and p^2-1 orbits of length k. Since A is not parabolic, the element $\bar{A}$ has no fixed points in $\mathbb{P}^1(\mathbb{F}_p)$. Therefore, all orbits of $\mathtt{gp}\left\{\bar{A}\right\}$ on $\mathbb{P}^1(\mathbb{F}_p) \subset \mathbb{P}^1(\mathbb{F}_{p^2})$ have length k. In particular, k divides $p+1$, that is, $z^{p+1} = 1$. Since $\lambda_1^2 - (a+d)\lambda_1 + 1 = 0$, we obtain

$$\begin{aligned} 1 = (\lambda_1^2)^{p+1} &= (\lambda_1^2)^p \cdot \lambda_1^2 = ((a+d)\lambda_1 - 1)^p \cdot \lambda_1^2 = ((a+d)\lambda_1^p - 1) \cdot \lambda_1^2 \\ &= (a+d)\lambda_1^{p+2} - (a+d)\lambda_1 + 1, \\ &\text{and so} \quad (a+d)\lambda_1^{p+1} = (a+d). \end{aligned}$$

When $(a+d) \neq 0$, we have $\lambda_1^{p+1} = 1$. When $(a+d) = 0$, we have $\lambda_1^2 = -1$. Moreover, $p \equiv 3 \bmod 4$: otherwise, $\lambda_1 \in \mathbb{F}_p$ as -1 is a quadratic residue modulo p if and only if $p \equiv 1 \bmod 4$ (a nonzero $a \in \mathbb{F}_p$ is a square if and only if $a^{\frac{p-1}{2}} = 1$). Hence, $\lambda_1^{p+1} = (-1)^{\frac{p+1}{2}} = 1$. In any case, we obtain $\lambda_1^{p+1} = 1$, and so $(\lambda_1)^{\frac{p+1}{2}} = \pm 1 = (\lambda_2)^{\frac{p+1}{2}}$. This gives the relation $A^{\frac{p+1}{2}} = \pm I$ as required. □

In particular, the lemma implies that $k \leq \frac{p+1}{2}$. According to (4.2), we have $O_{\mathrm{PSL}(2,p),t,u} \in \mathcal{H}((k-1)_{n/k})$ and

$$\begin{aligned} \mathrm{genus}(O_{\mathrm{PSL}(2,p),t,u}) &= \left(1 - \frac{1}{k}\right) \cdot \frac{n}{2} + 1 \\ &\leq \left(1 - \frac{2}{p+1}\right) \cdot \frac{p(p^2-1)}{4} + 1 = \frac{1}{4}p(p-1)^2 + 1. \end{aligned}$$

Note that k is equal to $\widehat{k}$ or $\widehat{k}/2$, where $\widehat{k}$ is the order of the image of the integer matrix C in the finite group $\mathrm{SL}(2,p)$. As easy to show, the integer $2\widehat{k} > 1$ is the period of the Fibonacci sequence (f_m) modulo p. There are several papers on the subject, see for instance [97] by Donald D. Wall.

Finding a general formula for the order k, that depends on the prime p, seems to be a hard problem. To solve this problem, one should be able to determine the orders of the golden ratio $\frac{1+\sqrt{5}}{2}$ in the fields $\mathbb{F}_{p^2}$ for all prime numbers $p > 2$. The degree of difficulty is comparable with that of Artin's conjecture on primitive roots[10]. We also refer the reader to the subsection 5.2.1.

Recall, by the way, some well-known isomorphisms for groups $\mathrm{PSL}(2,q)$, where q is a power of p:

$$\mathrm{PSL}(2,3) \simeq A_4, \quad \mathrm{PSL}(2,4) \simeq \mathrm{PSL}(2,5) \simeq A_5, \quad \mathrm{PSL}(2,9) \simeq A_6.$$

[10] A famous conjecture of Emil Artin states that, given a non-square integer $a \neq -1$, there are infinitely many prime numbers p, for which a is a primitive root. See Problem F9 in the book [37] by Richard K. Guy.

4.2.12 Alternating origamis

Let $d \geq 3$ be a positive integer. The alternating group A_d is a two-generator group of order $n := |A_d| = d!/2$. For any generating pair (α, β) of A_d, the regular n-square-tiled surface $O_{A_d,\alpha,\beta}$ will be called *alternating of degree d*.

Due to Øystein Ore [78, 1951], any element of the alternating group A_d with $d \geq 5$ is a commutator of two elements. Shelly Garion and Aner Shalev showed in [30, 2009, Theorem 1.7] that almost all elements of A_d are commutators of generating pairs of A_d. We are going to establish the following strong and apparently new result:

Theorem 4.26. *Let d be a positive integer, and let p be a prime number such that $\left[\frac{3d}{4}\right] \leq p \leq d-3$. Then every permutation $\mu \in A_d$ moving at least $p+2$ points can be presented as a commutator $[\sigma, \tau]$, where (σ, τ) generates A_d and σ is a p-cycle.*

Proof. First, let us show that for any permutation $\mu \in A_d$ moving at least $p+2$ points, there are two permutations σ, $\tau \in A_d$ such that

$$1)\ \mu = [\sigma, \tau], \quad 2)\ \sigma \text{ is a } p\text{-cycle} \quad \text{and} \quad 3)\ \sigma, \tau \text{ generate a transitive subgroup of } A_d.$$

According to Edward Bertram [10, 1972], every even permutation is a commutator $[\sigma, \tau]$, where σ is an l-cycle and $\tau \in S_d$, if and only if $\left[\frac{3d}{4}\right] \leq l \leq d$. So, this is true if one takes $l = p$: we have $\mu = [\sigma, \tau]$ for a p-cycle $\sigma \in A_d$. We may suppose that $\sigma = (1\ 2\ \ldots\ p)$, otherwise conjugate σ, τ, μ by a suitable permutation. We have to prove two things:

- *The permutation $\tau \in S_d$ can be chosen so that $\mathtt{gp}\{\sigma, \tau\}$ is a transitive subgroup of S_d.* Indeed, consider the decomposition of τ into disjoint cycles:

$$\tau = \gamma_1 \gamma_2 \ldots \gamma_r. \tag{4.10}$$

Lemma 4.27. *Two permutations $\sigma = (1\ 2\ \ldots\ p)$ and $\tau \in S_d$ generate a transitive subgroup if and only if τ fixes no integer in the interval $[p+1, d]$ and each disjoint cycle of τ moves at least one integer in the interval $[1, p]$, that is,*

$$\{p+1, p+2, \ldots, d\} \subseteq \mathrm{supp}(\tau) \quad \textit{and} \quad [1,p] \cap \mathrm{supp}(\gamma_i) \neq \emptyset \ \textit{ for any } 1 \leq i \leq r.$$

Proof. $(\Longleftarrow)$ The integer 1 can be moved by cycle σ to any integer $a \in [1, p]$, afterwards it can be moved to any integer $b \in \{p+1, \ldots, d\} \subseteq \mathrm{supp}(\gamma_1 \gamma_2 \ldots \gamma_r)$ by means of a cycle γ_i:

$$\text{if } \gamma_i^m(a) = b, \text{ then } (\tau')^m(a) = b.$$

$(\Longrightarrow)$ If some interger from $p+1$ to d is not in the support of τ, then it can't be sent to 1 by means of the permutations σ and τ. If there is a cycle γ_i containing only integers from the interval $[p+1, d]$, then again those integers don't lie in the orbit of 1 for the action of $\mathtt{gp}\{\sigma, \tau\}$. □

We may suppose that each cycle γ_i of τ moves at least one integer in the interval $[1, p]$, otherwise remove all cycles permuting only integers from $p+1$ to d, this will not affect the commutator $[\sigma, \tau]$. Since

$$\mu = \sigma(\tau\sigma^{-1}\tau^{-1}) = (1\ 2\ \ldots\ p) \cdot (\tau(p)\ \ldots\ \tau(2)\ \tau(1)) \tag{4.11}$$

and $|\mathrm{supp}(\mu)| > p$, there is an integer $x \in [1, p]$ which is sent by τ to an integer $y \in [p+1, d]$, say $\gamma_1(x) = y$. Denote by $y_1, y_2, \ldots, y_s$ the integers from $p+1$ to d which are fixed by τ,

$$\{y_1, y_2, \ldots, y_s\} = \mathrm{fix}(\tau) \cap [p+1, d],$$

and let $\tau' = \tau \cdot (y\ y_1\ y_2\ \ldots\ y_s) = (A\ x\ y\ y_1\ \ldots\ y_s) \cdot \gamma_2 \ldots \gamma_r$, where $\gamma_1 = (A\ x\ y)$. Then we have

$$[\sigma, \tau'] = \sigma\tau \cdot (y\ y_1\ \ldots\ y_s)\sigma^{-1}(y\ y_1\ \ldots\ y_s)^{-1} \cdot \tau^{-1} = \sigma\tau\sigma^{-1}\tau^{-1} = [\sigma, \tau],$$

and the group $\mathtt{gp}\{\sigma, \tau'\}$ is transitive by Lemma 4.27.

- *Moreover, τ can be chosen even.* We have just obtained two permutations $\sigma \in A_d$ and $\tau \in S_d$ satisfying 1), 2) and 3). It follows from (4.11) and $|\mathrm{supp}(\mu)| \geq p+2$ that at least two distinct integers $x, x' \in [1,p]$ are sent by τ to some integers $y, y' \in [p+1,d]$. In terms of a cycle decomposition (4.10), we are dealing with situations of two kinds:

$$\begin{array}{lll} \text{either} & \gamma_1(x) = y \quad \text{and} & \gamma_1(x') = y' \\ \text{or} & \gamma_1(x) = y \quad \text{and} & \gamma_2(x') = y' \end{array}$$

  In the first situation, we have $\gamma_1 = (A\ x\ y\ B\ x'\ y')$ and so

$$\tau \cdot (y\ y') = (A\ x\ y)(B\ x'\ y') \cdot \gamma_2\gamma_3 \dots \gamma_s.$$

  In the second situation, we have $\gamma_1 = (A\ x\ y)$, $\gamma_2 = (B\ x'\ y')$ and so

$$\tau \cdot (y\ y') = (A\ x\ y\ B\ x'\ y') \cdot \gamma_3 \dots \gamma_s.$$

  So far, the commutator hasn't changed,

$$[\sigma, \tau(y\ y')] = \sigma\tau \cdot (y\ y')\sigma^{-1}(y\ y') \cdot \tau^{-1} = \sigma\tau\sigma^{-1}\tau^{-1} = [\sigma,\tau],$$

  and $\mathtt{gp}\{\sigma, \tau(y\ y')\}$ is still a transitive subgroup of S_d due to Lemma 4.27. Since the permutations τ and $\tau(y\ y')$ have distinct parities, one of them is even, as required.

Second, let us show that permutations $\sigma,\ \tau \in A_d$ satisfying the conditions 2) and 3) above, actually generate the entire alternating group A_d. By Jordan's theorem, we know that a primitive group containing a p-cycle with $p \leq d-3$ is either alternating or symmetric. So, it is enough to check that the group $G = \mathtt{gp}\{\sigma, \tau\}$ is primitive, which is true due to

Lemma 4.28. *If a transitive permutation group G of degree d contains a p-cycle, where $p > d/2$ is prime, then it is primitive.*

Proof. Let $\Delta \subseteq \{1, \dots, p, p+1, \dots, d\}$ be a block for the transitive group G such that $1 \in \Delta$. If this block contains an integer $x > p$, then $\sigma^m(\Delta) \cap \Delta \neq \emptyset$ for any $m \in \mathbb{Z}$, and so $\{1, 2, \dots, p\} \subset \Delta$. Thus $|\Delta| = d$, because $|\Delta|$ divides d and $|\Delta| \geq p > d/2$. Now, If $\Delta \subseteq \{1, 2, \dots, p\}$ then it is a block for the subgroup $\mathtt{gp}\{\sigma\} \subseteq G$ acting transitively on the set $\{1, \dots, p\}$, and so either $\Delta = \{1\}$ or $|\Delta| = p$, which is impossible as $p \nmid d$. In all cases we obtained that $|\Delta| = 1$ or d. By Lemma 2.2 the group G is primitive. □

Therefore, the group $G = \mathtt{gp}\{\sigma, \tau\}$, where σ, τ are even and σ is a p-cycle with $p \geq [3d/4]$, is primitive, and by Jordan's theorem $G = A_d$. We conclude that any even permutation μ moving at least $p+2$ points is the commutator of a generating pair of A_d, one of the elements being a p-cycle. □

Remark. When $d \geq 14$, except for $d = 19$, there exists a prime p such that $\left[\frac{3d}{4}\right] \leq p \leq d-3$. Indeed, Jitsuro Nagura [71, 1952] proved that, for any $m \geq 25$, the interval between m and $\frac{6}{5}m$ contains a prime number. Therefore, for $\left[\frac{3d}{4}\right] \geq 25$, or else for all $d \geq 34$, there exits a prime p such that

$$\begin{array}{rcl} \left[\dfrac{3d}{4}\right] & \leq & p \quad \leq \dfrac{6}{5}\left[\dfrac{3d}{4}\right] \leq \dfrac{9d}{10}, \\ \text{and so} \quad \left[\dfrac{3d}{4}\right] & \leq & p \quad \leq \left[\dfrac{9d}{10}\right] = d + \left[-\dfrac{d}{10}\right]. \end{array} \tag{4.12}$$

For $d \in [14, 33] \setminus \{19\}$, a prime p is given in Table 4.1.

Table 4.1: A prime number p such that $\left[\frac{3d}{4}\right] \le p \le d-3$, where $d \in [14,33] \setminus \{19\}$.

d	14	15	16	17	18	20	21	22	23	24	25	26	27	28	29	30	31	32	33
$\left[\frac{3d}{4}\right]$	10	11	12	12	13	15	15	16	17	18	18	19	20	21	21	22	23	24	24
p	11	11	13	13	13	17	17	17	17	19	19	19	23	23	23	23	23	29	29

Corollary 4.29. a) *When $d \ge 20$, except maybe for $d = 32$, every permutation $\mu \in A_d$ that fixes at most $\left[\frac{d}{10}\right] - 1$ points is the commutator of a generating pair of A_d.*

b) *Given a real number $r > 4$, there exists an integer $D(r)$ such that for all $d \ge D(r)$, any permutation $\mu \in A_d$ fixing at most $\left[\frac{d}{r}\right]$ points is the commutator of a generating pair of A_d.*

Proof. a) Take an integer $d \ge 20$ not equal to 32. It follows from (4.12) and Table 4.1 that there exists a prime p such that $\left[\frac{3d}{4}\right] \le p \le d - \left[\frac{d}{10}\right] - 1$. If a permutation $\mu \in A_d$ fixes at most $\left[\frac{d}{10}\right] - 1$ points, then it moves at least $d - \left[\frac{d}{10}\right] + 1 \ge p + 2$ points. The required statement is, thus, a consequence of Theorem 4.26.

b) If $r > 4$ then the number $h = \frac{4}{3} \cdot \frac{r-1}{r}$ is greater than 1. Take a real $\varepsilon > 0$ satisfying $h - \varepsilon > 1$. For any integer d large enough, there exists a prime p between $\left[\frac{3d}{4}\right]$ and $(h-\varepsilon)\left[\frac{3d}{4}\right]$. Indeed, for each $k > 1$ and n large enough there is always a prime between n and kn: due to the asymptotic estimate $\pi(n) \sim {}^{n}\!/\!_{\ln n}$ of the prime-counting function, we have $\pi(kn) - \pi(n) \underset{n\to\infty}{\longrightarrow} \infty$. Therefore,

$$\left[\frac{3d}{4}\right] \le p \le \left(\frac{4}{3} \cdot \frac{r-1}{r} - \varepsilon\right)\left[\frac{3d}{4}\right] \le \frac{r-1}{r}d - \varepsilon\left[\frac{3d}{4}\right] = d - \frac{d}{r} - \varepsilon\left[\frac{3d}{4}\right].$$

In particular, $p \le d - \left[\frac{d}{r}\right] - 2$ when $[3d/4] \ge 2/\varepsilon$. Thus for sufficiently large d, any permutation $\mu \in A_d$ that fixes at most $\left[\frac{d}{r}\right]$ points, moves at least $d - \left[\frac{d}{r}\right] \ge p + 2$ points. According to Theorem 4.26, such a permutation μ is the commutator of a generating pair of A_d. □

Corollary 4.30. *The probability that a random element of the alternating group A_d is the commutator of a generating pair tends to 1 as $d \to \infty$.*

Proof. The number of permutations in S_d that fix at least k points doesn't exceed $\binom{n}{k}(d-k)! = \frac{d!}{k!}$. Indeed, for given k points there are $(d-k)!$ permutations fixing them, and there are $\binom{n}{k}$ ways to choose k points among d.

The number of permutations in A_d fixing at most $k-1$ points is not less than $\frac{d!}{2} - \frac{d!}{k!}$. Therefore, due to Corollary 4.29a, the probability p_d that a random element of the group A_d is the commutator of a generating pair is bounded by

$$p_d \ge \frac{\frac{d!}{2} - \frac{d!}{[d/10]!}}{d!/2} = 1 - \frac{2}{[d/10]!} \quad \text{for } d \ge 33.$$

This implies that $\lim\limits_{d\to\infty} p_d = 1$, as required. □

Remark. It is well known and easy to prove by inclusion-exclusion principle, that the number of permutations in S_d fixing no point (such permutations are called *derangements*) is equal to

$$a_d = d! \sum_{m=0}^{d} \frac{(-1)^m}{m!} = \left[\frac{d!}{e} + \frac{1}{2}\right]. \tag{4.13}$$

Moreover, denote by b_d and c_d the numbers of even and odd derangements respectively. Then[11]

$$b_d - c_d = (-1)^{d-1}(d-1). \tag{4.14}$$

Indeed, let $A = (x_{ij})_{i,j=1}^{d}$ be the $d \times d$ matrix with zeroes on the diagonal and ones elsewhere, that is, $x_{ii} = 0$ and $x_{ij} = 1$ for any $1 \le i \ne j \le d$. We have

$$\det A = \sum_{\lambda \in S_d} \operatorname{sign}(\lambda) \cdot x_{1\lambda(1)} x_{2\lambda(2)} \dots x_{d\lambda(d)},$$

where each even derangement contributes 1, each odd derangement contributes -1 and the permutations that fix a point contribute 0. It is easy to show that the eigenvalues of the symmetric matrix A are -1 with multiplicity $d-1$ and $d-1$ with multiplicity 1. Thus, we obtain that $\det A = (-1)^{d-1}(d-1)$, implying the relation (4.14).

From (4.13), (4.14) and $a_d = b_d + c_d$ follows the formula

$$b_d = \frac{1}{2}\left[\frac{d!}{e} + \frac{1}{2}\right] + \frac{(-1)^{d-1}(d-1)}{2}.$$

So, the number of even permutations fixing at most k points is equal to

$$\binom{d}{0} b_d + \binom{d}{1} b_{d-1} + \ldots + \binom{d}{k} b_{d-k} = \frac{1}{2}\sum_{i=0}^{k} \binom{d}{i} \left[\frac{(d-i)!}{e} + \frac{1}{2}\right] + \frac{1}{2}\sum_{i=0}^{k} (-1)^{d-1-i} \binom{d}{i} (d-1-i).$$

Corollary 4.31. *For any real $r > 4$ and sufficiently large integer d, the number of different strata containing an alternating origami of degree d is greater than*

$$\frac{1}{2}P(d) - \frac{1}{2}P\big(d - [d/r]\big),$$

where $P(m)$ denotes the number of unrestricted partitions[12] of a positive integer m.

Proof. By Theorem 4.4, the number of $\mathrm{GL}(2, \mathbb{Z})$-orbits of regular origamis with monodromy group A_d is equal to the number of T_2-systems in A_d. If a pair of even permutations (σ, τ) is a representative of a T_2-system, then the conjugacy class of the commutator $[\sigma, \tau]$ is an invariant of the T_2-systems. Hence, the number of T_2-systems in A_d is not less than than the number of conjugacy classes of the commutators $[\sigma, \tau]$, where (σ, τ) generate A_d. Due to Corollary 4.29b, this includes all conjugacy classes of even permutations fixing at most $\left[\frac{d}{r}\right] - 1$ points for sufficiently large d.

According to József Dénes, Paul Erdős and Paul Turán [22, 1969], the number $c(d)$ of conjugacy classes in the alternating group A_d is equal to[13]

$$c(d) = \frac{1}{2}P(d) + \frac{3}{2}Q(d), \tag{4.15}$$

where $Q(d)$ denotes the number of partitions of d into distinct odd summands (see also [31, 1980] by Robert D. Girse). Notice that the number of conjugacy classes in A_d containing permutations that fix at least k points is clearly $c(d-k)$. Therefore, the number of conjugacy classes in A_d of permutations fixing at most $k-1$ points is equal to $c(d) - c(d-k)$. For $k = \left[\frac{d}{r}\right]$ this gives

$$c(d) - c\big(d - [d/r]\big) \text{ classes.}$$

[11] See, for instance, the note [9, 2005] by Arthur T. Benjamin, Curtis T. Bennett and Florence Newberger.

[12] that is, the number of ways of writing m as a sum of positive integers; two sums that differ only in the order of their summands are considered to be the same partition.

[13] from this equation they derived the expansion $c(d) \sim \frac{1}{2}P(d) \sim \frac{1}{8d\sqrt{3}} e^{\pi\sqrt{\frac{2d}{3}}}$ as $d \to \infty$.

It is easy to see that $Q(d) > Q\big(d-[d/r]\big)$ for sufficiently large d. From this and the relation (4.15), we deduce a lower bound for the number of conjugacy classes of permutations in A_d fixing at most $[d/r]-1$ points:

$$c(d)-c(d-[d/r]) = \frac{1}{2}\Big(P(d)-P(d-[d/r])\Big)+\frac{3}{2}\Big(Q(d)-Q(d-[d/r])\Big) > \frac{1}{2}\Big(P(d)-P(d-[d/r])\Big),$$

when d is large enough, as required. □

Remark 1. A famous result of Godfrey H. Hardy and Srinivasa Ramanujan [39, 1918] states that

$$P(d) \sim \frac{1}{4d\sqrt{3}} e^{\pi\sqrt{\frac{2d}{3}}} \quad \text{as } d\to\infty.$$

From this asymptotic behaviour follows that

$$\lim_{d\to\infty}\frac{P\big(d-[d/r]\big)}{P(d)} = \frac{r}{r-1}\lim_{d\to\infty} e^{\pi\sqrt{\frac{2}{3}}\left(\sqrt{d-[d/r]}-\sqrt{d}\right)} = 0,$$

$$\text{and so} \quad P(d)-P\big(d-[d/r]\big) \sim \frac{1}{4d\sqrt{3}} e^{\pi\sqrt{\frac{2d}{3}}} \quad \text{as } d\to\infty.$$

Therefore, we obtain a lower bound

$$\frac{1}{2}\Big(P(d)-P\big(d-[d/r]\big)\Big) \geq \frac{C}{d} e^{\pi\sqrt{\frac{2d}{3}}},$$

for any $d > r$ and some real constant $C > 0$ small enough.

Remark 2. In the proof of the corollary above we used the fact that $Q(d) - Q\big(d-[d/r]\big) > 0$ for sufficiently large d. Actually, we even have

Lemma 4.32. *For $m \geq 3$, the function Q is non-decreasing: $Q(m) \geq Q(m-1)$.*

Proof. The generating function for the sequence $(Q(m))_{m\in\mathbb{N}}$ is

$$f(x) = \prod_{l=1}^{\infty}(1+x^{2l-1}) = (1+x)(1+x^3)\dots(1+x^{2l-1})\dots = 1+\sum_{m\in\mathbb{N}} Q(m)x^m.$$

Denote by $R(m)$ the number of partitions of m into distinct odd summands greater than 2. Then

$$\prod_{l=2}^{\infty}(1+x^{2l-1}) = 1+\sum_{m\in\mathbb{N}} R(m)x^m,$$

and so we obtain

$$1+\sum_{m=2}^{\infty}\big(Q(m)-Q(m-1)\big)x^m = (1-x)f(x)$$

$$= (1-x^2)\prod_{l=2}^{\infty}(1+x^{2l-1}) = 1-x^2+\sum_{m=3}^{\infty}\big(R(m)-R(m-2)\big)x^m,$$

as $Q(1) = 1$ and $R(1) = R(2) = 0$. Therefore, the relation $Q(m)-Q(m-1) = R(m)-R(m-2)$ is satisfied for any $m \geq 3$. Let us show that $R(m) \geq R(m-2)$. Indeed, if

$$m-2 = a_1+a_2+\dots+a_r$$

is a partition of $m-2$ with all a_i's odd and such that $a_1 > a_2 > \ldots > a_r \geq 3$, then we get a partition of m having the same property:

$$m = (a_1 + 2) + a_2 + \ldots + a_r.$$

This gives an injection from the set of partitions for $m-2$ with distinct odd summands ≥ 3 into the set of such partitions for m. As a result, $Q(m) - Q(m-1) = R(m) - R(m-2) \geq 0$. □

The number of $\mathrm{GL}(2, \mathbb{Z})$-orbits of regular origamis with monodromy group A_d is equal to the number of T_2-systems in A_d. Thus, we obtain Table 4.2, by using the following papers, where the T_2-systems in the alternating group were calculated:

[73, 1951] by Bernhard H. Neumann and Hanna Neumann, and [38, 1936] by Philip Hall (for $d = 5$),

[89, 1972] by Daniel Stork (for $d = 6$),

[42, 1998] by Osamu Higuchi and Izumi Miyamoto (for $d = 7, 8, 9$).

Table 4.2: Alternating n-square-tiled surfaces of degree d with $3 \leq d \leq 9$.

$n = \lvert A_d \rvert$	**Monodromy group** (A_d)	**Number of strata**	**Number of** $\mathrm{GL}(2, \mathbb{Z})$**-orbits**	**Number of origamis**
3	A_3	1	1	4
12	A_4	1	1	4
60	A_5	2	2	19
360	A_6	3	4	53
2520	A_7	6	16	916
20160	A_8	7	18	7448
181440	A_9	10	38	77004

• When $d > 3$ is odd, we have the following presentation:

$$A_d = \left\langle \sigma, \tau \;\middle|\; \sigma^{d-2} = \tau^2 = (\sigma\tau)^d = 1, \quad (\tau\sigma^{-k}\tau\sigma^k)^2 = 1 \text{ for any } 1 \leq k \leq \frac{d-3}{2} \right\rangle, \qquad (4.16)$$

$$\text{where} \quad \sigma = (3\ 4\ \ldots\ d), \quad \tau = (1\ 2\ 3).$$

The commutator $[\sigma, \tau] = (1\ 3\ 4)$ is of order 3. According to the formulas (4.2), the alternating origami $O_{A_d,\sigma,\tau}$ belongs to the stratum $\mathcal{H}(2_{d!/6})$ and has genus $d!/6 + 1$.

• When $d > 3$ is even, we have the following presentation:

$$A_d = \left\langle \sigma, \tau \;\middle|\; \sigma^{d-2} = \tau^2 = (\sigma\tau)^{d-1} = 1, \quad (\tau^{(-1)^k}\sigma^{-k}\tau\sigma^k)^2 = 1 \text{ for any } 1 \leq k \leq \frac{d-2}{2} \right\rangle, \qquad (4.17)$$

$$\text{where} \quad \sigma = (1\ 2)(3\ 4\ \ldots\ d), \quad \tau = (1\ 2\ 3).$$

The commutator $[\sigma, \tau] = (1\ 3)(2\ 4)$ is of order 2. According to the formulas (4.2), the alternating origami $O_{A_d,\sigma,\tau}$ belongs to the stratum $\mathcal{H}(1_{d!/4})$ and has genus $d!/8 + 1$.

The presentations (4.16) and (4.17) were found by Carmichael in [19, 1923, p.262], they are also given in the classical textbook [21] by Harold S. M. Coxeter and William O. J. Moser. The complexity of these presentations, as for finding Veech groups using Theorem 4.4, is that the number of relations grows together with d. The existence of presentations with uniformly bounded number of generators and relations was established by several mathematicians (*e.g.* [12, 2011] and [33, 2008]). For instance, R. M. Guralnick, W. M. Kantor, M. Kassabov and A. Lubotzky showed in the paper [33, Lemma 2.2 and Theorem 3.17] that, for any natural d, the group A_d has a presentation with at most 35 generators and 116 relators.

However, we are interested only in two-generator presentations, because the alternating origamis are given by the choice of a pair of elements generating A_d.

Definition 4.2. Let G be a finite group, and let $\widehat{G}$ be a *covering group* of G, that is, a group of maximal order for which there exists a subgroup $A \subseteq \widehat{G}$ with the properties[14]

$$A \subseteq Z(\widehat{G}) \cap [\widehat{G}, \widehat{G}] \quad \text{and} \quad \widehat{G}/A \simeq G.$$

In general, $\widehat{G}$ is not uniquely defined, but A is unique up to isomorphism and is called the *Schur multiplier of* G – it is denoted by $M(G)$.

Consider a presentation $G = \langle X \mid R \rangle$. It is known that the Schur multiplier $M(G)$ is isomorphic to the second homology group $H_2(G, \mathbb{Z})$, or else to the second cohomology group $H^2(G, \mathbb{C}^\times)$, and satisfies the formula

$$M(G) = \frac{\overline{R} \cap [F, F]}{[\overline{R}, F]},$$

where $F = F(X)$ is the free group on X, and $\overline{R}$ is the normal closure of R in F. In the important paper [87, 1907], Issai Schur proved that

(i) the group $M(G)$ is an invariant of G, that is, independent of the finite presentation $\langle X \mid R \rangle$,

(ii) the group $M(G)$ is *finite* abelian,

(iii) the inequality $|R| - |X| \geq \mathrm{rg}(M(G))$ holds for any presentation $G = \langle X \mid R \rangle$, where $\mathrm{rg}(M(G))$ is the cardinal of a minimal generating system for the abelian group $M(G)$.

When G has a finite presentation for which the equality $|R| - |X| = \mathrm{rg}(M(G))$ takes place, we say that the group G is *efficient* (after D. B. A. Epstein [27]). For instance, the projective groups $\mathrm{PSL}(2, p)$, where p is an odd prime, are efficient due to (4.9) and the fact that $M(\mathrm{PSL}(2, p)) = \mathbb{Z}_2$ according to the textbook [47, Theorem 25.7] by Bertram Huppert.

In the case of the alternating group $G = A_d$, Issai Schur [88, 1911] found that

$$M(A_d) = \begin{cases} 0 & \text{for } d < 4, \\ \mathbb{Z}_6 & \text{for } d = 6, 7, \\ \mathbb{Z}_2 & \text{for } d = 4, 5 \text{ and } d \geq 8. \end{cases}$$

The group A_d is efficient for $d \leq 9$. However, it is not known whether A_d is efficient for all d, see the paper [18, 2004] by C. M. Campbell, G. Havas, C. Ramsay and E. F. Robertson. Moreover, a much weaker question appears to be open:

Question 4.2. Does there exist a *two-generator* presentation $A_d = \langle X \mid R \rangle$ such that the number of relations $|R|$ is independent of d?

[14] As usual $Z(H)$ and $[H, H]$ stand for the center and the commutator subgroup of H:

$$Z(H) = \{ g \in H \mid ghg^{-1} = h \text{ for any } h \in H \}, \qquad [H, H] = \mathtt{gp}\{ [g, h] \mid g, h \in H \}.$$

Chapter 5
Coset representations

5.1 General theory

For any group G and any subgroup $H \subseteq G$ of finite index, the action of G by left multiplication on the set of left cosets $\{g_1H, \ldots, g_nH\}$ defines a representation $\rho_H : G \to Sym(G/H)$. It will be called a *coset representation* of G. Obviously, it is transitive but not necessary faithful.

If an element $u \in G$ lies in the kernel of ρ_H then $ugH = gH$ for any $g \in G$, that is $u \in gHg^{-1}$, and we have

$$\ker \rho_H = \bigcap_{g \in G} gHg^{-1}.$$

Thus, the kernel of ρ_H is the largest normal subgroup of G contained in H.

Let $G = \langle X \mid R \rangle$ be a presentation of the group G, where the system X is finite. The ideas used for constructing Cayley diagrams now lead to their generalization – to coset diagrams. More precisely, it is a labeled digraph: the set of its vertices is $\{g_1H, \ldots, g_nH\}$ and its directed edges are labeled by generators from X, so that an edge with label $g \in X$ from g_iH to g_jH means that $g \cdot g_iH = g_jH$. We suppose that the finite set X is endowed with a total order.

We will denote the coset diagram of G by $C(X; R/H)$, or if it is clear simply by $C(G/H)$. In the trivial case we have $C(G) = C(G/\{1\})$. An example for the free group $F_2 = \langle x, y \mid - \rangle$ and its subgroup $H = \mathtt{gp}\left\{x^2, y^2, xyx, yxy\right\}$ is given in FIGURE 5.1.

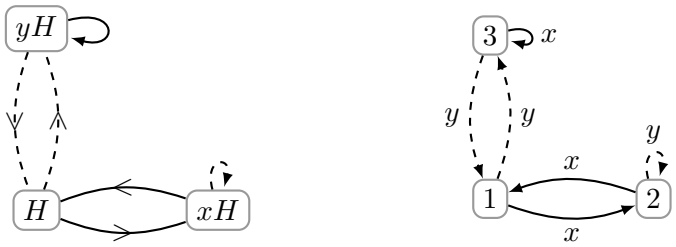


Figure 5.1: The coset diagram $C(F_2/\mathtt{gp}\left\{x^2, y^2, xyx, yxy\right\})$.

In a coset diagram $C(G/H)$ the subgroup H is exactly the stabilizer of the vertex $v =$'H', that is, consists of all words $W(X)$ such that the path $W(X)[v]$ is closed. The stabilizer of the vertex 'gH', for $g \in G$, obviousely is gHg^{-1}.

By definition, for a two-generator group $G = \langle g, h \mid R \rangle$ and a finite index subgroup $H \subseteq G$, the coset diagram $C(g, h; R/H)$ is an origamal digraph (say, with $g \prec h$). The corresponding square-tiled surface will be denoted by $O_{G/H}$ or explicitely by $O_{G/H,g,h}$. It will also be called a *coset origami*. By construction we have $\mathcal{M}on(O_{G/H}) \simeq \rho_H(G)$.

Proposition 5.1. *Given a finite two-generator group G, let O be a square-tiled surface with monodromy group $\mathcal{M}on(O) \simeq G$. Then there exist a generating pair $(g, h) \in G \times G$ and a subgroup $H \subseteq G$ such that $O = O_{G/H,g,h}$.*

Proof. The statement is an immediate consequence of the classification of the transitive permutation representations $G \to S_n$, see Proposition 2.10. □

Now, a natural question arises: *given a connected origami O, what are the groups G such that*

$$O = O_{G/H} \quad \textit{for a subgroup} \quad H \subseteq G? \tag{5.1}$$

For example, we always can assign $G = F_2$ (the construction that follows is due to Gabriela Schmithüsen, see [83]). Indeed, take a look at an origamal digraph Υ of O, let x and y be its labels with $x \prec y$. Fix a vertex v_0 and consider the set S_0 of all words $W(x, y)$ over the letters $\{x, y\} \cup \{x^{-1}, y^{-1}\}$ such that the path $W(x, y)[v_0]$ is closed. Endowed with the standard formalism (concatenation of pathes, inverse path and empty path), the set S_0 is a group with two-generators x and y. It is a subgroup of the free group $F(x, y) = \langle x, y \mid - \rangle$, and the origamal digraph Υ is isomorphic to $C(F(x, y)/S_0)$. For there is a bijection between the vertices of Υ and the cosets $F(x, y)/S_0$: if v is a vertex and $W_v(x, y)[v_0]$ a path from v_0 to v then

$$v \mapsto W_v(x, y) \cdot S_0.$$

Thus the group F_2 satisfies the property (5.1).

In general case we have:

Proposition 5.2. *Let $G = \langle g, h \mid R \rangle$ be a group, and Υ a connected origamal digraph with n vertices and two labels $\{l_1, l_2\}$, $l_1 \prec l_2$. The digraph Υ is isomorphic to a coset diagram $C(G/H)$ for some subgroup $H \subseteq G$ of index n if and only if for any vertex v of Υ and any relator $W(g, h) \in R$ the path $W(l_1, l_2)[v]$ is closed.*

Proof. ($\Longleftarrow$) Suppose that the path $W(g, h)[v]$ is closed for any vertex v of Υ and any $W(g, h) \in R$. For a fixed vertex v_0 construct its stabilizer S_0 as above so that $\Upsilon \simeq C(F(l_1, l_2)/S_0)$, where the group $F(l_1, l_2)$ is free of rank 2. Consider the epimorphism $f : F(l_1, l_2) \twoheadrightarrow G$, $l_1 \mapsto g$, $l_2 \mapsto h$, and take $H = f(S_0)$, which of course is a subgroup of G. By assumption a word $W(l_1, l_2)$ belongs to S_0 whenever $W(g, h) = 1$ in G, that is, the subgroup S_0 contains the kernel $\ker f$. Therefore, S_0 is the full preimage of the subgroup H (if $f(s) = f(t) \in H$ for some $s \in S_0$ and $t \in F(l_1, l_2)$, then $s^{-1}t \in \ker f$ and $t \in S_0 \cdot \ker f = S_0$).

We have a mapping from the cosets $F(l_1, l_2)/S_0$ onto the cosets G/H :

$$wS_0 \mapsto f(w)H,$$

which is also injective, since $f(w_1)H = f(w_2)H$ implies $w_1^{-1}w_2 \in f^{-1}(H) = S_0$. At the same time, in the coset diagram $C(F(l_1, l_2)/S_0)$ there is an edge labeled by l_i from wS_0 to $w'S_0$ if and only if there is an edge labeled by $f(l_i)$ from $f(w)H$ to $f(w')H$ in the diagram $C(G/H)$. Indeed, $l_i wS_0 = w'S_0$ implies $f(l_i)f(w)H = f(w')H$, and the converse is true because only one edge with label $f(l_i)$ starts at $f(w)H$. This shows that $\Upsilon \simeq C(F(l_1, l_2)/S_0) \simeq C(G/H)$ for the subgroup $H = f(S_0)$, which is of index n in G since the diagram $C(G/H)$ has n vertices.

($\Longrightarrow$) Conversely, suppose $\Upsilon \simeq C(G/H)$. For any relation $W(g, h) = 1$ in G and any coset uH, we have $W(g, h) \cdot uH = uH$. Thus, the path $W(g, h)[v]$ is closed in Υ, where the vertex v corresponds to uH under the bijection between the sets of vertices of Υ and $C(G/H)$. □

Corollary 5.3. *The monodromy group $\mathcal{M}on(O)$ is the smallest group satisfying the property (5.1).*

Proof. Let (σ, τ) be a pair of permutations encoding the origami O. Consider an origamal digraph Υ for O with labels $\{l_1, l_2\}$. By the definition of an origamal digraph, a path $W(l_1, l_2)[v]$ is closed in the digraph Υ whenever $W(\sigma, \tau) = 1$ holds in the monodromy group $\mathcal{M}on(O) = \mathtt{gp}\{\sigma, \tau\}$. It follows from Proposition 5.2 that $\mathcal{M}on(O)$ satisfies the property (5.1).

On the other hand, for any group G such that $O = O_{G/H}$ for some $H \subseteq G$ we have by construction of the coset origami that $\rho_H(G) \simeq \mathcal{M}on(O)$. Therefore, $|\mathcal{M}on(O)| = |G/\ker \rho_H| \leq |G|$. □

Given an origamal digraph Υ with two labels $\{l_1, l_2\}$, we can use this proposition to describe in terms of presentations all groups G such that, for some $H \subseteq G$, the coset diagram $C(G/H)$ is isomorphic to Υ. Denote by $\mathcal{R}(\Upsilon)$ the set of formal words W over two letters such that the path $W(l_1, l_2)[v]$ is closed for any vertex v of Υ. We will call $\mathcal{R}(\Upsilon)$ the *realizer* of the origamal digraph Υ. If we consider the words in $\mathcal{R}(\Upsilon)$ as elements of the free group $F_2 = F(l_1, l_2)$ then for any vertex stabilizer S_0 we have $\mathcal{R}(\Upsilon) = \cap_{w \in F_2} w S_0 w^{-1}$ being a finite index subgroup of F_2.

Let $\langle g, h \mid R \rangle$ be a presentation of a group G. We obtain that

$$\Upsilon \simeq C(G/H) \text{ for a subgroup } H \text{ of } G \iff R \subseteq \mathcal{R}(\Upsilon).$$

The following is a generalisation of Lemma 4.2:

Lemma 5.4. *Let (g, h) and (g', h') be two pairs of generators of a group G, and H a finite index subgroup of G. The origamis $O_{G/H,g,h}$ and $O_{G/H,g',h'}$ coincide if there exists an automorphism $\alpha \in \mathrm{Aut}(G)$ such that*

$$\alpha(g) = g',\ \alpha(h) = h' \ \text{ and } \ \alpha(H) = H.$$

Proof. Let us show that an automorphism $\alpha \in \mathrm{Aut}(G)$ satisfying the above conditions determines an isomorphism of the labeled digraphs $C(g, h; R/H)$ and $C(g', h'; R'/H)$. First of all, we have a bijection $uH \mapsto \alpha(u)H$ between their sets of vertices. Secondly, for any two vertices uH and vH, there is an edge from uH to vH with label g (analogically for the label h) if and only if there is an edge with label $g' = \alpha(g)$ from $\alpha(u)H$ to $\alpha(v)H$. Indeed,

$$\begin{aligned} g \cdot uH = vH \implies \alpha(g) \cdot \alpha(u)H = \alpha(v)H \quad &\text{and} \\ \alpha(g) \cdot \alpha(u)H = \alpha(v)H \implies \alpha(gu) = \alpha(v) \cdot w \implies gu = v \cdot \alpha^{-1}(w), \end{aligned}$$

where w and $\alpha^{-1}(w)$ belong to H. Therefore, the origamal digraphs of $O_{G/H,g,h}$ and $O_{G/H,g',h'}$ are isomorphic. □

Proposition 5.5. *Let $G = \langle g, h \mid R \rangle$ be a two-generator group, and H a finite index subgroup of G. The origami $O_{G/H,g,h}$ is primitive if and only if H is a maximal subgroup.*

First proof. $(\Longrightarrow)$ Let $H \subseteq H_1$ be two subgroups of G. Then the origami $O_{G/H,g,h}$ covers the origami $O_{G/H_1,g,h}$. Indeed, for the natural mapping $\pi : G/H \to G/H_1$, sending uH to uH_1, we have

$$\pi(w \cdot uH) = wuH_1 = w \cdot \pi(uH) \quad \text{for any } w, u \in G.$$

Thus Proposition 2.1 can be applied. In particular, if $O_{G/H,g,h}$ is a primitive square-tiled surface, then the subgroup H must be a maximal in G.

$(\Longrightarrow)$ Suppose that the origami $O = O_{G/H,g,h}$ is not primitive, that it covers properly another origami O_1 by means of $p : O \to O_1$. Let us draw origamal digraphs of O and O_1 directely on the square-tiled surfaces by choosing for the vertices the centers of the squares, and for the edges (labeled by g and h) geodesics connecting these vertices. Further, pick such a vertex v on O, and let $v_1 = p(v)$. Then for any word W such that $W(g, h)[v]$ is a closed path on O, the path $p(W(g, h)[v])$ will be closed as well. Therefore, by Proposition 5.2 the origamal digraph of O_1 is isomorphic to a coset diagram $C(G/H_1)$. Assuming without loss of generality that the subgroups H and H_1 are the stabilizers of the vertices v and $v_1 = p(v)$ respectively, we obtain $H \subsetneq H_1 \subsetneq G$. So, H is not a maximal subgroup of G. □

Second proof. By Proposition 2.4 the origami $O_{G/H,g,h}$ is primitive whenever the permutation group $\mathcal{M}on(O_{G/H,g,h}) = \rho_H(G)$ is primitive. The permutation group $\rho_H(G)$ on the set $V = G/H$ is primitive if and only if all point stabilizers G_x ($x \in V$) are maximal subgroups of G (see Lemma 2.3). On the other hand, the stabilizer of a coset uH for the left action of G is the subgroup uHu^{-1}. It is maximal if and only if H is a maximal subgroup of G. □

5.2 Examples

5.2.1 Projective coset origamis

Let p be a prime number, and $q = p^m$ for some $m \in \mathbb{N}$. Consider the projective general linear group $\mathrm{PGL}(2,q)$ and the projective special linear group $\mathrm{PSL}(2,q)$ over the finite field $\mathbb{F}_q$. By definition,

$$\mathrm{PGL}(2,q) = \mathrm{GL}(2,q)/Z \quad \text{and} \quad \mathrm{PSL}(2,q) = \mathrm{SL}(2,q)/\{\pm I\},$$

where I is the 2×2 identity matrix and Z is the subgroup of nonzero scalar matrices aI with $a \in \mathbb{F}_q^\times$. It is well known that $\mathrm{PSL}(2,q)$ is a simple two-generator group, with two exceptions: $\mathrm{PSL}(2,2) \simeq S_3$ and $\mathrm{PSL}(2,3) \simeq A_4$. Note that $\mathrm{PSL}(2,q)$ is not necessary a subgroup of $\mathrm{PGL}(2,q)$. However, $\mathrm{PSL}(2,q)$ is isomorphic to a normal subgroup of $\mathrm{PGL}(2,q)$ via

$$\mathrm{PGL}(2,q) = \frac{\mathrm{GL}(2,q)}{Z} \supseteq \frac{\mathrm{SL}(2,q)\cdot Z}{Z} \simeq \frac{\mathrm{SL}(2,q)}{\mathrm{SL}(2,q)\cap Z} = \mathrm{PSL}(2,q),$$

$$\text{where } \mathrm{SL}(2,q)\cdot Z = \{A\cdot B \mid A \in \mathrm{SL}(2,q),\ B \in Z\},$$

so we shall ignore the subtle distinction.

For a matrix $A \in \mathrm{GL}(2,q)$ we will denote by $\bar{A}$ its image in $\mathrm{PGL}(2,q)$. Consider the projective line over the field $\mathbb{F}_q$,

$$\mathbb{P}^1(\mathbb{F}_q) = \{[x:y] \mid x,y \in \mathbb{F}_q\}\big/\big([x:y] \sim [ax:ay] \text{ for any } a \in \mathbb{F}_q^\times\big) = \mathbb{F}_q \cup \{\infty\} \quad \text{with } \infty = [1:0].$$

The group $\mathrm{PGL}(2,q)$ acts on $\mathbb{P}^1(\mathbb{F}_q)$ in the following way:

$$\text{if } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2,q), \text{ then } \bar{A}\cdot[x:y] = [ax+by : cx+dy] = \frac{a\,x/y + b}{c\,x/y + d}.$$

This action is faithful and transitive, giving a permutation representation of degree $q+1$,

$$\rho : \mathrm{PGL}(2,q) \hookrightarrow Sym(\mathbb{P}^1(\mathbb{F}_q)) \simeq S_{q+1}. \tag{5.2}$$

For instance, the images of the matrices $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $U = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$ permute the elements $x \in \mathbb{P}^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}$ by the rule

$$\bar{T}\cdot x = x+1 \quad \text{and} \quad \bar{U}\cdot x = \frac{x}{-x+1} = \frac{1}{x^{-1}-1}, \text{ or else } \bar{U}\cdot\frac{1}{x} = \frac{1}{x-1}.$$

If p is odd, there are three types of elements in the group $\mathrm{PGL}(2,q)$ according to the number of distinct eigenvalues, or else to the action on the projective line, as shown in Table 5.1.

The automorphisms of the group $\mathrm{PSL}(2,q)$ are well-understood. Let $\mathrm{P\Gamma L}(2,q)$ be the projective semilinear group over $\mathbb{F}_q$, that is, a semidirect product

$$\mathrm{P\Gamma L}(2,q) = \mathrm{PGL}(2,q) \rtimes \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p).$$

This group acts on $\mathrm{PSL}(2,q)$ via $\bar{A} \mapsto \bar{B}\,\overline{A^\phi}\,\bar{B}^{-1}$, where $\bar{B} \in \mathrm{PGL}(2,q)$ and A^ϕ is the matrix obtained by applying an automorphism ϕ of $\mathbb{F}_q$ to each entry of $A \in \mathrm{SL}(2,q)$. This gives a homomorphism

$$f : \mathrm{P\Gamma L}(2,q) \longrightarrow \mathrm{Aut}(\mathrm{PSL}(2,q)), \tag{5.3}$$

which is onto as the following theorem states.

Table 5.1: Three types of elements in the groups $\mathrm{PGL}(2,q)$ and $\mathrm{PSL}(2,q)$.

Number of distinct eigenvalues in $\mathbb{F}_q$	**Action on $\mathbb{P}^1(\mathbb{F}_q)$**	**Order in $\mathrm{PGL}(2,q)$**	**Order in $\mathrm{PSL}(2,q)$**
0	no fixed points	divides $q+1$	divides $\frac{1}{2}(q+1)$
1	fixes 1 point	p	p
2	fixes 2 points	divides $q-1$	divides $\frac{1}{2}(q-1)$

Theorem 5.6 (O. Schreier and B. L. van der Waerden [86], 1928)**.** *The homomorphism f defined above is onto. In particular when $q=p$, every automorphism of $\mathrm{PSL}(2,p)$ is induced via conjugation by an element of $\mathrm{PGL}(2,p)$.*

Let us now examine the case where $m=1$ and $q=p$. In this case,

$$\mathbb{P}^1(\mathbb{F}_p) = \{0,1,\ldots,p-1,\infty\},$$

$$\rho(\bar{T}) = (0\ 1\ \ldots\ p{-}1)(\infty) \quad \text{and} \quad \rho(\bar{U}) = (\infty\ \ \frac{1}{p-1}\ \ \ldots\ \ \frac{1}{2}\ \ \frac{1}{1})(0).$$

As easy to notice, the stabilizer of the point $\infty=[1:0]$ for the action of $\mathrm{PSL}(2,p)$ on $\mathbb{P}^1(\mathbb{F}_p)$ is the cyclic subgroup $H=\mathsf{gp}\left\{\bar{T}\right\}$ generated by $\bar{T}$. The square-tiled surface $O_p = O_{\mathrm{PSL}(2,p)/H,\bar{T},\bar{U}}$ will be called a *projective coset origami*. This is a $(p{+}1)$-square origami encoded by the permutations $\rho(\bar{T})$ and $\rho(\bar{U})$.

Proposition 5.7. *The Veech groups of the projective coset origami $O_p = O_{\mathrm{PSL}(2,p)/H,\bar{T},\bar{U}}$ and the regular origami $O_{\mathrm{reg}} = O_{\mathrm{PSL}(2,p),\bar{T},\bar{U}}$ coincide,*

$$\mathrm{GL}(O_p) = \mathrm{GL}(O_{\mathrm{reg}}).$$

Proof. Denote by ρ_1 the restriction of the faithful representation ρ in (5.2) to the normal subgroup $\mathrm{PSL}(2,p) \trianglelefteq \mathrm{PGL}(2,p)$,

$$\rho_1 : \mathrm{PSL}(2,p) \hookrightarrow S_{p+1}.$$

According to Theorem 5.6, any automorphism of the group $\mathrm{PSL}(2,p)$ is induced via conjugation $\bar{A} \mapsto \bar{B}\bar{A}\bar{B}^{-1}$ by an element $\bar{B} \in \mathrm{PGL}(2,q)$. Hence, any automorphism of the image $\rho_1(\mathrm{PSL}(2,p))$ comes from conjugation $\rho_1(\bar{A}) \mapsto \rho(\bar{B}) \cdot \rho_1(\bar{A}) \cdot \rho(\bar{B})^{-1}$ by a permutation $\rho(\bar{B}) \in S_{p+1}$. This means that the representation ρ_1 is structural, and by Theorem 4.7 we obtain $\mathrm{GL}(O_{\rho_1}) = \mathrm{GL}(O_{\mathrm{reg}})$, where $O_{\rho_1} = (\rho_1(\bar{T}), \rho_1(\bar{U}))^* = O_p$. □

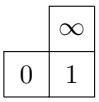
For the purpose of finding the genus and stratum of O_p, one should take a look at the commutator

$$C = [T,U] = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix},$$

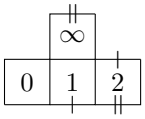
$$\bar{C} \cdot x = \frac{x+1}{x+2} \quad \text{for any } x \in \mathbb{P}^1(\mathbb{F}_p).$$

The eigenvalues of the matrix C are the roots of the polynomial $P(\lambda) = (\lambda{-}1)(\lambda{-}2){-}1 = \lambda^2{-}3\lambda{+}1$. Both of them belong either to $\mathbb{F}_p$ or to $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$.

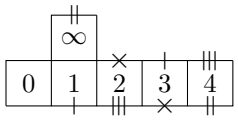
- When $p=2$, we have $\rho(\bar{T}) = (0\ 1)$, $\rho(\bar{U}) = (\infty\ 1)$ and $\rho(\bar{C}) = [(0\ 1),(1\ \infty)] = (\infty\ 1\ 0)$, so

the origami $O_2 =$  is in the stratum $\mathcal{H}(2)$ and has genus $g = 2$.

• When $p = 3$, we have $\rho(\bar{T}) = (0\ 1\ 2)$, $\rho(\bar{U}) = (\infty\ 2\ 1)$ and $\rho(\bar{C}) = (0\ 2)(1\ \infty)$, so

the origami $O_3 =$  is in the stratum $\mathcal{H}(1,1)$ and has genus $g = 2$.

• When $p = 5$, we have $\rho(\bar{T}) = (0\ 1\ 2\ 3\ 4)$, $\rho(\bar{U}) = (\infty\ 4\ 2\ 3\ 1)$ and $\rho(\bar{C}) = (0\ 3\ \infty\ 1\ 4)$, so

the origami $O_3 =$  is in the stratum $\mathcal{H}(4)$ and has genus $g = 3$.

• When $p \geq 7$, the characteristic polynomial $P(\lambda)$ has two distinct roots

$$\lambda_- = \frac{3-\sqrt{5}}{2} \quad \text{and} \quad \lambda_+ = \frac{3+\sqrt{5}}{2},$$

that are elements of the field $\mathbb{F}_p$ if and only if 5 is a quadratic residue modulo p. As easy to determine, 1 and 4 are quadratic residues modulo 5, while 2 and 3 are not. By quadratic reciprocity, we obtain

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)(-1)^{\frac{5-1}{2}\cdot\frac{p-1}{2}} = \left(\frac{p}{5}\right) = \begin{cases} +1 & \text{if } p \equiv 1, 4 \bmod 5, \\ -1 & \text{if } p \equiv 2, 3 \bmod 5, \end{cases}$$

where $\left(\frac{a}{p}\right)$ stands for the Legendre symbol[1].

We have the following decomposition

$$C = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = B \begin{pmatrix} \lambda_- & 0 \\ 0 & \lambda_+ \end{pmatrix} B^{-1}, \quad \text{where } B = \begin{pmatrix} 1 & (\sqrt{5})^{-1} \\ \frac{1-\sqrt{5}}{2} & \frac{1+(\sqrt{5})^{-1}}{2} \end{pmatrix}. \tag{5.4}$$

•• If $p \equiv 1$ or $4 \bmod 5$, then $\lambda_-, \lambda_+ \in \mathbb{F}_p$ and $B \in \mathrm{SL}(2, p)$. So, there is a one-to-one correspondence between the orbits for the action of $\bar{C} \in \mathrm{PSL}(2,\, p)$ on the projective line $\mathbb{P}^1(\mathbb{F}_p)$ and the orbits for the multiplication by

$$z = \frac{\lambda_-}{\lambda_+} = \frac{3-\sqrt{5}}{3+\sqrt{5}} = \frac{(3-\sqrt{5})^2}{4} = \frac{7-3\sqrt{5}}{2}, \quad \text{or else } z = \left(\frac{1-\sqrt{5}}{2}\right)^4,$$

$$\text{since } \begin{pmatrix} \lambda_- & 0 \\ 0 & \lambda_+ \end{pmatrix} \cdot x = \frac{\lambda_-}{\lambda_+} \cdot x.$$

Obviously $z \cdot 0 = 0$ and $z \cdot \infty = \infty$, and so the fixed points of $\bar{C}$ are

$$\bar{B} \cdot 0 = \frac{2(\sqrt{5})^{-1}}{1+(\sqrt{5})^{-1}} = -\frac{1-\sqrt{5}}{2} \quad \text{and} \quad \bar{B} \cdot \infty = \frac{2}{1-\sqrt{5}} = -\frac{1+\sqrt{5}}{2}.$$

[1]For a prime p and an integer a, the Legendre symbol is

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \text{ divides } a, \\ +1 & \text{if } x^2 \equiv a \bmod p \text{ has a nonzero solution in } \mathbb{F}_p, \\ -1 & \text{if } x^2 \equiv a \bmod p \text{ has no solution in } \mathbb{F}_p. \end{cases}$$

Let $k \in \mathbb{N}$ be the order of z in the group $\mathbb{F}_p^\times$. Then there are exactly

$$2 \text{ orbits of length } 1 \text{ and } \frac{p-1}{k} \text{ orbits of length } k,$$

when one multiplies the elements of the projective line $\mathbb{P}^1(\mathbb{F}_p)$ by z. The orbits of length k are the cosets in $\mathbb{F}_p^\times$ of the cyclic subgroup generated by z. We obtain that the cycle pattern of the permutation $\rho(\bar{C})$ is $1^2 k^{\frac{p-1}{k}}$, and so

$$\text{the origami } O_{\mathrm{PSL}(2,p)/H,\bar{T},\bar{U}} \text{ belongs to the stratum } \mathcal{H}\big((k-1)_{\frac{p-1}{k}}\big) \text{ and has genus } \frac{(k-1)(p-1)}{2k}+1.$$

•• If $p \equiv 2$ or $3 \bmod 5$, then $\lambda_-, \lambda_+ \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ and $B \in \mathrm{SL}(2, p^2)$. In this case, we have a one-to-one correspondence between the orbits in the projective line $\mathbb{P}^1(\mathbb{F}_{p^2})$ for the multiplication by $z = \frac{\lambda_-}{\lambda_+} \in \mathbb{F}_{p^2}$ and the orbits for the action of $\bar{C} \in \mathrm{PSL}(2,\, p)$ on $\mathbb{P}^1(\mathbb{F}_{p^2})$. Namely, for any $x \in \mathbb{P}^1(\mathbb{F}_{p^2}) = \mathbb{F}_{p^2} \cup \{\infty\}$, to the orbit

$$\mathrm{orb}_z(x) = \{x, zx, z^2x, \ldots, z^{k-1}x\}$$

corresponds the orbit

$$\mathrm{orb}_{\bar{C}}(x) = \{\bar{B}\cdot x, \bar{B}\cdot zx, \bar{B}\cdot z^2x, \ldots, \bar{B}\cdot z^{k-1}x\},$$

where k is the order of z in the cyclic group $\mathbb{F}_{p^2}^\times$ and the order of $\bar{C}$ in the projective group $\mathrm{PSL}(2,\, p)$ at the same time. Since $\lambda_-^0 = \frac{2-0\cdot\sqrt{5}}{2}$, $\lambda_-^1 = \frac{1-1\cdot\sqrt{5}}{2}$ and $\lambda_-^{r+1} = \lambda_-^r + \lambda_-^{r-1}$, for any $r \in \mathbb{N}$, it follows by induction on r that

$$\lambda_-^r = \left(\frac{1-\sqrt{5}}{2}\right)^r = \frac{(f_r + 2f_{r-1}) - f_r\cdot\sqrt{5}}{2},$$

where f_r is the r^{th} Fibonacci number[2]. Therefore, the order s of λ_- in the group $\mathbb{F}_{p^2}^\times$ is the smallest positive r such that $f_r \equiv 0 \bmod p$ and $f_{r-1} \equiv 1 \bmod p$. In other words, s is the period of the Fibonacci sequence modulo p (it is also called the p^{th} *Pisano period*). This period is always even ($p \geq 7$), because

$$f_{r+1}f_{r-1} = f_r^2 + (-1)^r \quad \text{for all } r \in \mathbb{N},$$

and in particular $f_{s+1} \equiv (-1)^s \bmod p$. We conclude that the order k of $z = \left(\frac{1-\sqrt{5}}{2}\right)^4$ in $\mathbb{F}_{p^2}^\times$ is the minimum integer amongst $\frac{s}{4}$ and $\frac{s}{2}$.

There are exactly $\frac{p+1}{k}$ orbits of length k for the action of $\bar{C}$ on the projective line $\mathbb{P}^1(\mathbb{F}_p)$. Thus, the cycle pattern of the permutation $\rho(\bar{C})$ is $k^{\frac{p+1}{k}}$, and so

$$\text{the origami } O_{\mathrm{PSL}(2,p)/H,\bar{T},\bar{U}} \text{ belongs to the stratum } \mathcal{H}\big((k-1)_{\frac{p+1}{k}}\big) \text{ and has genus } \frac{(k-1)(p+1)}{2k}+1.$$

In Table B.4 are given the strata and genera of the projective coset origamis $O_{\mathrm{PSL}(2,p)/H,\bar{T},\bar{U}}$ for the first 328 primes p. This table is obtained by a program written in Java (see Appendix A).

[2]The Fibonacci numbers are defined recurrently by $f_0 = 0$, $f_1 = 1$ and $f_{r+1} = f_r + f_{r-1}$ for all $r \in \mathbb{N}$.

5.2.2 Alternating coset origamis

Let n be a positive integer, and A_n the alternating group of degree n. Denote by H the stabilizer of the point 1 for the action of A_n on the set $\{1, 2, \ldots, n\}$. This subgroup consists of the even permutations fixing 1 and so $H \simeq A_{n-1}$.

Pick a generating pair (σ, τ) of A_n. The square-tiled surface $O_{A_n/H,\sigma,\tau}$ will be called an *alternating coset origami of degree n*. Evidently, we have $O_{A_n/H,\sigma,\tau} = (\sigma, \tau)^*$.

Proposition 5.8. *If $n \neq 6$, then the Veech groups of the alternating coset origami $O_{A_n/H,\sigma,\tau}$ and the regular origami $O_{A_n,\sigma,\tau}$ coincide,*

$$\mathrm{GL}(O_{A_n/H,\sigma,\tau}) = \mathrm{GL}(O_{A_n,\sigma,\tau}).$$

Moreover, the number of $\mathrm{GL}_2(\mathbb{Z})$-orbits of alternating coset origamis of degree n is equal to the number of $\mathrm{GL}_2(\mathbb{Z})$-orbits of regular alternating origamis of degree n.

Proof. Denote by $\rho : A_n \hookrightarrow S_n$ the natural inclusion $A_n \subseteq S_n$, and by $\rho_{\mathrm{reg}} : A_n \hookrightarrow S_n$ the regular representation of A_n.

According to Theorem 8.2A and Exercise 8.2.2 of the textbook [25] by John D. Dixon and Brian Mortimer, for each automorphism $f \in \mathrm{Aut}(A_n)$ there exists $\beta \in S_n$ such that $f(\alpha) = \beta\alpha\beta^{-1}$ for all $\alpha \in A_n$. This means that the representation ρ is structural, and so by Theorem 4.7 we obtain $\mathrm{GL}(O_{A_n/H,\sigma,\tau}) = \mathrm{GL}(O_{A_n,\sigma,\tau})$.

Moreover, the number of distinct alternating coset origamis of degree n is equal to the number $\mathrm{GL}_2(\mathbb{Z})$-orbits of regular alternating origamis of degree n (and so, since the Veech groups of $O_{A_n/H,\sigma,\tau}$ and $O_{A_n,\sigma,\tau}$ coincide for any generating pair (σ, τ), the respective numbers of $\mathrm{GL}_2(\mathbb{Z})$-orbits are equal as well). Indeed, the alternating coset origamis correspond to the conjugacy classes $(\sigma, \tau)^* = \left\{(\delta\sigma\delta^{-1}, \delta\tau\delta^{-1}) \mid \delta \in S_n\right\}$, where σ and τ generate A_n. The regular alternating origamis correspond, according to Lemma 4.2, to the $\mathrm{Aut}(A_n)$-orbits of the generating pairs. As we already noticed, $\mathrm{Aut}(A_d) = S_d$ and so the conjugacy class $(\sigma, \tau)^*$ coincides with the $\mathrm{Aut}(A_n)$-orbit of (σ, τ). This completes the proof of the proposition. □

Due to Proposition 5.8 and Theorem 4.4, the number of $\mathrm{GL}_2(\mathbb{Z})$-orbits of the coset origamis with monodromy group A_n is equal to the number of T_2-systems in A_n. Appropriate information for that matter is given in Table B.5. To fill in the table when $n \neq 6$, we used the following papers, in which the T_2-systems of the alternating group were calculated:

[73, 1951] by Bernhard H. Neumann and Hanna Neumann, and [38, 1936] by Philip Hall (for $d = 5$),

[42, 1998] by Osamu Higuchi and Izumi Miyamoto (for $d = 7, 8, 9$).

When $n = 6$ (the case that we cannot apply Proposition 5.8), we obtained the 5 orbits with the help of the mathematics system GAP.

Chapter 6
Subgroups of $\mathrm{PSL}_2(\mathbb{Z})$ and Veech groups

We will use the following notation:

$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $U = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$;

$\bar{A}$ is the image of a matrix $A \in \mathrm{SL}_2(\mathbb{Z})$ in the projective group $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$;

$\mathcal{T}$ **and** $\mathcal{U}$ denote the subgroups of $\mathrm{PSL}_2(\mathbb{Z})$ generated by $\bar{T}$ and $\bar{U}$ respectively;

$\mathcal{O}$ denotes the set of all square-tiled surfaces, including non-connected ones;

$\bar{\mathcal{O}}$ denotes the set of orbits of $\mathcal{O}$ for the action of the two-element group $\mathtt{gp}\{-I\}$;

$\bar{O}$ is the element of the set $\bar{\mathcal{O}}$ corresponding to an origami O, that is, $\bar{O} = \{O, -I \cdot O\}$;

$\mathbb{P}^1(\mathbb{Q})$ **or** $\hat{\mathbb{Q}} = \mathbb{Q} \cup \{\infty\}$ denotes the projective line over the field $\mathbb{Q}$ of rational numbers, where ∞ designates $[1 : 0] = \frac{1}{0}$;

$\mathrm{PSL}(\bar{O})$ denotes the integer Veech group of a modular origami $\bar{O}$ (see below);

$\left[\frac{p}{q}\right]_O$ denotes the $\mathrm{PSL}(\bar{O})$-orbit of an element $\frac{p}{q} \in \hat{\mathbb{Q}}$.

Definition 6.1. The elements of the set $\bar{\mathcal{O}}$ are called *modular square-tiled surfaces*, or else *modular origamis*. In terms of permutations, a modular n-square origamis corresponds to the union of two conjugacy classes $(\sigma, \tau)^* \cup (\sigma^{-1}, \tau^{-1})^*$, where $\sigma, \tau \in S_n$.

A modular origami $\bar{O}$ is said to be *connected* if the origami O is connected.

6.1 Action of $\mathrm{PSL}_2(\mathbb{Z})$ on $\mathbb{P}^1(\mathbb{Q})$

In the section 2.6, we described the natural action of the special linear group $\mathrm{SL}_2(\mathbb{Z})$ on the set $\mathcal{O}$ of origamis. Consider the action of the projective group $\mathrm{PSL}_2(\mathbb{Z})$ on the set $\bar{\mathcal{O}}$ of modular origamis such that the following diagram commutes:

$$\begin{array}{ccc} \mathrm{SL}_2(\mathbb{Z}) \times \mathcal{O} & \longrightarrow & \mathcal{O} \\ \downarrow & & \downarrow \\ \mathrm{PSL}_2(\mathbb{Z}) \times \bar{\mathcal{O}} & \longrightarrow & \bar{\mathcal{O}} \end{array} \qquad \begin{array}{ccc} (A, O) & \longmapsto & A \cdot O \\ \downarrow & & \downarrow \\ (\bar{A}, \bar{O}) & \longmapsto & \bar{A} \cdot \bar{O} \end{array} \tag{6.1}$$

In other words, we define $\bar{A} \cdot \bar{O}$ to be $\overline{A \cdot O} = \{A \cdot O, -A \cdot O\}$.

Definition 6.2. The *integer Veech group* of a modular origami $\bar{O}$ is its stabilizer for the action of the projective group $\mathrm{PSL}_2(\mathbb{Z})$. It will be denoted by $\mathrm{PSL}(\bar{O})$.

Recall that there is a transitive action of $\mathrm{PSL}_2(\mathbb{Z})$ on the projective line $\mathbb{P}^1(\mathbb{Q})$, namely,

$$\bar{A} \cdot [p : q] = [ap + bq : cp + dq], \qquad \text{where } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Without loss of correctness we will refer to $\mathbb{P}^1(\mathbb{Q})$ by means of the expanded set of rational numbers $\hat{\mathbb{Q}} = \mathbb{Q} \cup \{\infty\}$, where ∞ stands for $[1 : 0] = \frac{1}{0}$. In this context, the action of the modular group on $\hat{\mathbb{Q}}$ is given by

$$A \cdot \frac{p}{q} = \frac{ap + bq}{cp + dq}.$$

The stabilizer of ∞ is the group $\mathcal{T}$ generated by the matrix $\bar{T}$, and the stabilizer of 0 is the group $\mathcal{U}$ generated by $\bar{U}$. We are going to see how this action is related to Veech groups of modular origamis.

Let $\bar{O}$ be a connected modular origami. Consider the decomposition of its $\mathrm{PSL}_2(\mathbb{Z})$-orbit into $\mathcal{T}$-orbits

$$\mathrm{PSL}_2(\mathbb{Z}) \cdot \bar{O} = \bigsqcup_{1 \leqslant i \leqslant N} \mathcal{T} \cdot (\bar{A}_i \bar{O}), \tag{6.2}$$

where $\bar{A}_i \cdot \bar{O}$ are some representatives of the $\mathcal{T}$-orbits with $\bar{A}_i \in \mathrm{PSL}_2(\mathbb{Z})$ and $1 \leq i \leq N$. This gives rise to a partition of the set $\hat{\mathbb{Q}}$ into equivalence classes

$$\hat{\mathbb{Q}} = \bigsqcup_{1 \leqslant i \leqslant N} [\bar{A}_i^{-1} \infty]_O \tag{6.3}$$

via the following definition:

Definition 6.3. Consider two fractions

$$\frac{p}{q} = \bar{A}^{-1} \cdot \infty \quad \text{and} \quad \frac{r}{s} = \bar{B}^{-1} \cdot \infty, \quad \text{where } \bar{A}, \bar{B} \in \mathrm{PSL}_2(\mathbb{Z}),$$

We say that $\frac{p}{q}$ and $\frac{r}{s}$ are $\mathcal{T}$-*equivalent*, and write $\frac{p}{q} \underset{T}{\sim} \frac{r}{s}$, if the modular origamis $\bar{A} \cdot \bar{O}$ and $\bar{B} \cdot \bar{O}$ lie in the same $\mathcal{T}$-orbit, that is, if $\mathcal{T} \cdot \bar{A}\bar{O} = \mathcal{T} \cdot \bar{B}\bar{O}$.

The equivalence class of $\frac{p}{q} \in \hat{\mathbb{Q}}$ is denoted by $\left[\frac{p}{q}\right]_O$ or $[\bar{A}^{-1}\infty]_O$, and called a $\mathcal{T}$-*class*.

An explicit way of expressing $\mathcal{T}$-equivalence is

$$\bar{A}^{-1}\infty \underset{T}{\sim} \bar{B}^{-1}\infty \quad \Longleftrightarrow \quad \bar{A} = \bar{T}^k \bar{B} \bar{C} \ \text{ for some } k \in \mathbb{Z}, \ \ \bar{C} \in \mathrm{PSL}(\bar{O}), \tag{$*$}$$

and an integer k can actually be chosen in the interval $[0, \#(\mathcal{T} \cdot \bar{A}\bar{O}) - 1]$, where $\#(\mathcal{T} \cdot \bar{A}\bar{O})$ is the number of origamis in the $\mathcal{T}$-orbit of $\bar{A}\bar{O}$.

The geometric source of the above definition is the following: let ∞ correspond to the horizontal direction on the square-tiled surface O, then any rational direction $\frac{p}{q}$ on O (imagine a directional flow with the slope $\frac{p}{q}$) will, in its turn, correspond to the horizontal direction on another square-tiled surface $O(p/q)$. More exactly, if $\frac{p}{q} = A^{-1}\infty$ for some $A \in \mathrm{SL}(2, \mathbb{Z})$, then $O(p/q) = A \cdot O$. Now from this perspective, two rational numbers $\frac{p}{q}$ and $\frac{r}{s}$ are $\mathcal{T}$-equivalent if and only if the corresponding square-tiled surfaces $O(p/q)$ and $O(r/s)$ are in the same $\mathtt{gp}\{-I, T\}$-orbit, roughly meaning that they have similar decompositions into horizontal cylinders.

Replacing ∞ by 0, horizontal direction by vertical one and $\mathcal{T}$-orbits by $\mathcal{U}$-orbits we obtain the notions of *$\mathcal{U}$-equivalence* and *$\mathcal{U}$-classes*:

$$\bar{A}^{-1}\cdot 0 \underset{U}{\sim} \bar{B}^{-1}\cdot 0 \quad\Longleftrightarrow\quad \bar{A}=\bar{U}^k\bar{B}\bar{C} \ \text{ for some } k\in\mathbb{Z},\ \ \bar{C}\in \mathrm{PSL}(\bar{O}). \tag{$**$}$$

To the decomposition of the $\mathrm{PSL}_2(\mathbb{Z})$-orbit of $\bar{O}$ into $\mathcal{U}$-orbits

$$\mathrm{PSL}_2(\mathbb{Z})\cdot\bar{O}=\bigsqcup_{1\leqslant i\leqslant N}\mathcal{U}\cdot(\bar{B}_i\bar{O}) \tag{6.4}$$

corresponds a partition of the set $\hat{\mathbb{Q}}$ into $\mathcal{U}$-classes

$$\hat{\mathbb{Q}}=\bigsqcup_{1\leqslant i\leqslant N}[\bar{B}_i^{-1}0]_O\,. \tag{6.5}$$

Here are some immediate properties of the $\mathcal{T}$- and $\mathcal{U}$-equivalences:

A) *The partitions of $\hat{\mathbb{Q}}$ into $\mathcal{T}$-classes and $\mathcal{U}$-classes corresponding to a modular origami O coincide: for any $\bar{A}\in\mathrm{PSL}_2(\mathbb{Z})$ we have*

$$[\bar{A}^{-1}\cdot\infty]_O=[\bar{A}^{-1}\bar{S}\cdot 0]_O\,.$$

Indeed, since $U=STS^{-1}$, together with the decomposition (6.2) into $\mathcal{T}$-orbits we get the decomposition into $\mathcal{U}$-orbits:

$$\mathrm{PSL}_2(\mathbb{Z})\cdot\bar{O}=\bigsqcup_{1\leqslant i\leqslant N}\mathcal{U}\cdot(\bar{S}\bar{A}_i\bar{O}).$$

Furthermore, a fraction $\frac{p}{q}=\bar{A}^{-1}\infty$ is $\mathcal{T}$-equivalent to $\frac{r}{s}=\bar{B}^{-1}\infty$ if and only if $\bar{A}\cdot\bar{O}=\bar{T}^k\bar{B}\cdot\bar{O}$ for some $k\in\mathbb{Z}$, that is,

$$\bar{S}\bar{A}\cdot\bar{O}=(\bar{S}\bar{T}^k\bar{S}^{-1})\bar{S}\bar{B}\cdot O=\bar{U}^k\bar{S}\bar{B}\cdot\bar{O}.$$

Thus, the fractions $\bar{A}^{-1}\bar{S}\cdot 0=\frac{p}{q}$ and $\bar{B}^{-1}\bar{S}\cdot 0=\frac{r}{s}$ are $\mathcal{U}$-equivalent (recall that $\bar{S}=\bar{S}^{-1}$).

In fact, A) is also a direct consequence of the following property that allows us to speak of "classes" without reference[1] to $\mathcal{T}$ or $\mathcal{U}$.

B) (Lemma of Anton Zorich) *The $\mathcal{T}$-classes and the $\mathcal{U}$-classes are exactly the $\mathrm{PSL}(\bar{O})$-orbits of $\hat{\mathbb{Q}}$.*

If two fractions $\frac{p}{q}=A^{-1}\infty$ and $\frac{r}{s}=B^{-1}\infty$ drop in the same $\mathcal{T}$-class, then $\bar{A}^{-1}=\bar{C}\bar{B}^{-1}\bar{T}^k$ for some $k\in\mathbb{Z}$ and $\bar{C}\in\mathrm{PSL}(O)$, implying that $\frac{p}{q}=\bar{C}\bar{B}^{-1}\bar{T}^k\infty=\bar{C}\cdot\bar{B}^{-1}\infty=\bar{C}\cdot\frac{r}{s}$. Conversely, if $\frac{p}{q}=\bar{C}\cdot\frac{r}{s}$ with $\bar{C}\in\mathrm{PSL}(O)$, or else $\infty=\bar{A}\bar{C}\bar{B}^{-1}\cdot\infty$, then $\bar{A}\bar{C}\bar{B}^{-1}=\bar{T}^k$ for some $k\in\mathbb{Z}$, and so $\frac{p}{q}\underset{T}{\sim}\frac{r}{s}$ by $(*)$. Therefore, the $\mathcal{T}$-classes are the $\mathrm{PSL}(\bar{O})$-orbits of $\hat{\mathbb{Q}}$, and the same is true for the $\mathcal{U}$-classes.

[1] From now on, if $\frac{p}{q}$ and $\frac{r}{s}$ are in the same $\mathcal{T}$-class or $\mathcal{U}$-class for a modular origami $\bar{O}$, we will also write $\frac{p}{q}\underset{O}{\sim}\frac{r}{s}$ or implicitly $\frac{p}{q}\sim\frac{r}{s}$.

C) *Swapping initial modular origami $\bar{O}$ for a modular origami $\bar{C}\cdot\bar{O}$, where $\bar{C}\in\mathrm{PSL}_2(\mathbb{Z})$, means multiplying initial classes by $\bar{C}$.*

Indeed, by definition two fractions $\frac{p}{q}=\bar{C}^{-1}A^{-1}\infty$ and $\frac{r}{s}=\bar{C}^{-1}B^{-1}\infty$ are $\mathcal{T}$-equivalent (for $\bar{O}$) if the origamis $\bar{A}\cdot\bar{C}\bar{O}$ and $\bar{B}\cdot\bar{C}\bar{O}$ lie in the same $\mathcal{T}$-orbit, that is, if the fractions $\bar{A}^{-1}\infty=C\cdot\frac{p}{q}$ and $\bar{B}^{-1}\infty=\bar{C}\cdot\frac{r}{s}$ are $\mathcal{T}$-equivalent (for $\bar{C}\cdot\bar{O}$).

D) *Let*

$$\frac{p}{q}=a_1+\cfrac{1}{a_2+\cfrac{}{\ddots+\cfrac{1}{a_m}}}\qquad\text{and}\qquad\frac{p_k}{q_k}=a_1+\cfrac{1}{a_2+\cfrac{}{\ddots+\cfrac{1}{a_m+k}}}$$

be continued fractions with a_i, $k\in\mathbb{Z}$.

▷ *If <u>m is odd</u> introduce three matrices*

$$B_m=T^{a_1}U^{-a_2}\dots T^{a_{m-2}}U^{-a_{m-1}},\quad C_m=B_mT^{a_m-1}U^{-1}\quad\text{and}\quad D_m=B_mT^{a_m}.$$

Then the number $\frac{p}{q}$ lies in the class $[\bar{C}_m\cdot\infty]_O=[\bar{D}_m\cdot 0]_O$. Moreover, if k is divisible by the number of modular origamis in the $\mathcal{T}$-orbit of $\bar{B}_m^{-1}\bar{O}$, then $\frac{p}{q}\underset{O}{\sim}\frac{p_k}{q_k}$.

▷ *If <u><u>m is even</u></u> introduce three matrices*

$$B_m=T^{a_1}U^{-a_2}\dots U^{-a_{m-2}}T^{a_{m-1}},\quad C_m=B_mU^{-a_m}\quad\text{and}\quad D_m=B_mU^{-a_m+1}T.$$

Then the number $\frac{p}{q}$ lies in the class $[\bar{C}_m\cdot\infty]_O=[\bar{D}_m\cdot 0]_O$. Moreover if k is divisible by the number of origamis in the $\mathcal{U}$-orbit of $\bar{B}_m^{-1}\bar{O}$, then $\frac{p}{q}\underset{O}{\sim}\frac{p_k}{q_k}$.

Indeed, for any rational number x we have

$$\bar{T}\cdot x=x+1\quad\text{and}\quad\bar{U}^{-1}\cdot\frac{1}{x}=\frac{1}{1+x}.$$

Thus, it is easy to check by induction that in both case (m odd and even) we obtain the equalities

$$\frac{p}{q}=\bar{C}_m\cdot\infty\quad\text{and}\quad\frac{p}{q}=\bar{D}_m\cdot 0.$$

For instance,

$$\begin{aligned}\bar{T}^{a_1}\bar{U}^{-a_2}\dots\bar{T}^{a_{m-1}}\bar{U}^{-a_m}\cdot\frac{1}{0}&=\bar{T}^{a_1}\bar{U}^{-a_2}\dots\bar{T}^{a_{m-1}}\cdot\frac{1}{a_m}=\bar{T}^{a_1}\bar{U}^{-a_2}\dots\bar{U}^{-a_{m-2}}\cdot\left(a_{m-1}+\frac{1}{a_m}\right)\\&=\bar{T}^{a_1}\bar{U}^{-a_2}\dots\bar{U}^{-a_{m-2}}\cdot\cfrac{1}{\cfrac{1}{a_{m-1}+\cfrac{1}{a_m}}}\\&=\bar{T}^{a_1}\bar{U}^{-a_2}\dots\bar{T}^{a_{m-3}}\cdot\cfrac{1}{a_{m-2}+\cfrac{1}{a_{m-1}+\cfrac{1}{a_m}}}=\dots=\frac{p}{q}.\end{aligned}$$

So, we will always have $\frac{p}{q} \in [\bar{C}_m \cdot \infty]_O = [\bar{D}_m \cdot 0]_O$.

Now, let m be odd. The following equality holds (check by induction on m):

$$\frac{p_k}{q_k} = \bar{B}_m \bar{T}^k \bar{B}_m^{-1} \frac{p}{q}.$$

If we suppose that k is divisible by the number of origamis in the $\mathcal{T}$-orbit of $\bar{B}_m^{-1}\bar{O}$, then $\bar{T}^k \bar{B}_m^{-1}\bar{O} = \bar{B}_m^{-1}\bar{O}$, that is, the matrix $\bar{B}_m \bar{T}^k \bar{B}_m^{-1}$ is in the Veech group of $\bar{O}$. Therefore, we can conclude that $\frac{p_k}{q_k} \underset{O}{\sim} \frac{p}{q}$ using the property E) below.

If m is even and k is divisible by $\#(\mathcal{U} \cdot \bar{B}_m^{-1}\bar{O})$, then $\frac{p_k}{q_k} = \bar{B}_m \bar{U}^{-k} \bar{B}_m^{-1} \frac{p}{q}$ and $\frac{p_k}{q_k} \underset{O}{\sim} \frac{p}{q}$ by analogy.

E) *An element $\bar{C} \in \mathrm{PSL}_2(\mathbb{Z})$ preserves*[2] *the classes for $\bar{O}$ if and only if, for any $\bar{A} \in \mathrm{PSL}_2(\mathbb{Z})$, the modular origamis $\bar{A} \cdot \bar{O}$ and $\bar{A} \cdot \bar{C}\bar{O}$ belong to the same $\mathcal{T}$-orbit. The statement stays true when one replaces "$\mathcal{T}$-orbit" by "$\mathcal{U}$-orbit".*

In particular, if $\bar{C} \in \mathrm{PSL}(\bar{O})$, then $\bar{C}$ preserves the classes for $\bar{O}$.

Indeed, an element $\bar{C}$ preserves the classes whenever C^{-1} does. From the definition 6.3 follows that, for each $\bar{A} \in \mathrm{PSL}_2(\mathbb{Z})$, we have $\bar{C}^{-1}\bar{A}^{-1}\infty \underset{T}{\sim} \bar{A}^{-1}\infty$ if and only if the modular origamis $\bar{A} \cdot \bar{O}$ and $\bar{A}\bar{C} \cdot \bar{O}$ are in the same $\mathcal{T}$-orbit. By analogy one proves the $\mathcal{U}$-version of the statement.

6.2 Subgroups that are not $\hat{\mathbb{Q}}$-straining

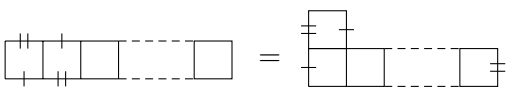
A natural question arises whether the inverse of the last statement of the property E) is satisfied.

Question 6.1. Describe the modular origamis $\bar{O}$ such that if an element $\bar{C} \in \mathrm{PSL}_2(\mathbb{Z})$ preserves the classes of $\hat{\mathbb{Q}}$ for $\bar{O}$, then $\bar{C}$ is in the Veech group $\mathrm{PSL}(\bar{O})$.

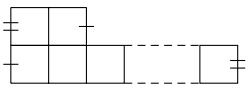
In the stratum $\mathcal{H}(2)$, all primitive origamis have this property:

Proposition 6.1. *Let O be a primitive origami from $\mathcal{H}(2)$. If $\bar{C} \in \mathrm{PSL}_2(\mathbb{Z})$ preserves the classes of $\hat{\mathbb{Q}}$ for the modular origami $\bar{O}$, then $\bar{C} \in \mathrm{PSL}(\bar{O})$.*

Proof. Due to the property C), once we fixed a $\mathrm{PSL}_2(\mathbb{Z})$-orbit, it is enough to verify the proposition for just one modular origami in the orbit. As we already know from the section 3.1, all primitive n-square origamis from the stratum $\mathcal{H}(2)$ get to at most two $\mathrm{SL}_2(\mathbb{Z})$-orbits: the first one contains the origami

$P_n =$  $=$

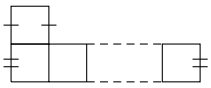
and in the second one, which exists for odd $n \geqslant 5$, there is

$R_n =$ 

[2] this means that $\bar{C} \cdot \frac{p}{q} \underset{O}{\sim} \frac{p}{q}$ for any $\frac{p}{q} \in \hat{\mathbb{Q}}$.

(the origami R_n is primitive and both permutations encoding R_n are even). Remark that the origamis P_n and R_n are stabilized by $-I$, and does any origami in their $\mathrm{SL}_2(\mathbb{Z})$-orbits. Therefore, for each primitive origami $O \in \mathcal{H}(2)$ we have $\bar{O} = \{O\}$. We are going to proceed in two different ways.

1st method. Consider an element $\bar{C} \in \mathrm{PSL}_2(\mathbb{Z})$ preserving the classes for $\bar{P}_n$. By the property E), the modular origamis $\bar{P}_n$ and $\bar{C} \cdot \bar{P}_n$ must be in same $\mathcal{T}$- and $\mathcal{U}$-orbits. However, in the $\mathcal{U}$-orbit of $\bar{P}_n$ there are exactly two modular origamis: $\bar{P}_n$ and the origami $\bar{U} \cdot \bar{P}_n$, where

$U \cdot P_n =$  .

The modular origamis $\bar{P}_n$ and $\bar{U} \cdot \bar{P}_n$ are not in the same $\mathcal{T}$-orbit, since the origami UP_n has two horizontal cylinders whilst P_n only one. We conclude that $\bar{C} \cdot \bar{P}_n = \bar{P}_n$, that is, $\bar{C} \in \mathrm{PSL}(\bar{O})$.

The case of the second $\mathrm{PSL}_2(\mathbb{Z})$-orbit is even easier, because there is a $\mathcal{U}$-orbit consisting of only one modular origami, due to the relation $R_n = U \cdot R_n$.

2nd method. Suppose there exists a matrix $\bar{C} \in \mathrm{PSL}_2(\mathbb{Z})$, that preserves the classes for $\bar{P}_n$ but doesn't preserve the modular origami $\bar{P}_n$. In order to get a contradiction, it suffices to look at two classes: $[\infty]_{P_n}$ and $[\bar{S} \cdot \infty]_{P_n}$.

Since $\bar{C}^{-1}\infty \underset{T}{\sim} \infty$ and $\bar{C}^{-1}\bar{S}^{-1}\infty \underset{T}{\sim} \bar{S}^{-1}\infty$, according to $(*)$ we obtain

$$\bar{C} = \bar{T}^k \bar{C}_1 \quad \text{and} \quad \bar{C} = \bar{S}^{-1}\bar{T}^l \bar{S}\bar{C}_2$$

for some $k, l \in \mathbb{Z}$ and $\bar{C}_1, \bar{C}_2 \in \mathrm{PSL}(\bar{P}_n)$. Moreover, such an integer l can be chosen in the set $\{0, 1, \ldots, \#(\mathcal{T}\cdot\bar{S}\bar{P}_n)-1\}$, where $\#(\mathcal{T} \cdot \bar{S}\bar{P}_n)$ is the number of modular origamis in the $\mathcal{T}$-orbit of $\bar{S} \cdot \bar{P}_n$, that is, $\#(\mathcal{T} \cdot \bar{S}\bar{P}_n) = 2$ and $0 \leqslant l < 2$. Since $\bar{C}$ is not in $\mathrm{PSL}(\bar{P}_n)$, it follows that $l = 1$. Therefore,

$$\bar{T}^{-k}\bar{S}^{-1}\bar{T}\bar{S} = \bar{C}_1\bar{C}_2^{-1} \in \mathrm{PSL}(\bar{P}_n).$$

In terms of permutations, we have

$$P_n = (\sigma, \tau)^* \quad \text{for} \quad \sigma = (1\ 2\ \ldots n),\ \tau = (1\ 2)$$

and

$$(\sigma, \tau)^* \overset{S}{\longmapsto} (\tau^{-1}, \sigma)^* \overset{T}{\longmapsto} (\tau^{-1}, \sigma\tau)^* \overset{S^{-1}}{\longmapsto} (\sigma\tau, \tau)^* \overset{T^{-k}}{\longmapsto} (\sigma\tau, \tau(\sigma\tau)^k)^*.$$

As the element $\bar{T}^{-k}\bar{S}^{-1}\bar{T}\bar{S}$ preserves the modular origami $\bar{P}_n = \{P_n\}$, the pairs (σ, τ) and $(\sigma\tau, \tau(\sigma\tau)^k)$ should be conjugate, which is impossible because the permutations σ and $\sigma\tau$ have unmatched parities. Contradiction.

Speaking of the modular origami $\bar{R}_n$, we notice that it is $\mathcal{U}$-invariant. So, $(**)$ shows that if $\bar{C}^{-1}0 \underset{U}{\sim} 0$ then $\bar{C} \in \mathrm{PSL}(\bar{R}_n)$. □

For any subgroup $\Gamma \subseteq \mathrm{PSL}_2(\mathbb{Z})$, we can consider the orbits for the action of Γ on the projective line $\hat{\mathbb{Q}}$ and determine which elements of $\mathrm{PSL}_2(\mathbb{Z})$ preserve those orbits.

Definition 6.4. A subgroup $\Gamma \subseteq \mathrm{PSL}_2(\mathbb{Z})$ will be called $\hat{\mathbb{Q}}$-*straining* if it is exactly the stabilizer of the Γ-orbits on $\hat{\mathbb{Q}}$.

In other words, Γ is $\hat{\mathbb{Q}}$-straining if from the fact that $\bar{C} \cdot \frac{p}{q} \in \Gamma \cdot \frac{p}{q}$ for any $\frac{p}{q} \in \hat{\mathbb{Q}}$, follows that $\bar{C} \in \Gamma$. We can now reformulate the question 6.1: *for which modular origamis the integer Veech group is* $\hat{\mathbb{Q}}$*-straining*?

As shown in Proposition 6.1, the Veech group $\mathrm{PSL}(\bar{O})$ for any primitive origami $O \in \mathcal{H}(2)$ is $\hat{\mathbb{Q}}$-straining.

Lemma 6.2. *Let Γ be a subgroup of $\mathrm{PSL}_2(\mathbb{Z})$. An element $\bar{C} \in \mathrm{PSL}_2(\mathbb{Z})$ preserves the Γ-orbits on $\hat{\mathbb{Q}}$ if and only if, for any $\bar{A} \in \mathrm{PSL}_2(\mathbb{Z})$, there exist $\bar{B} \in \Gamma$ and $k \in \mathbb{Z}$ such that*

$$\bar{A}\bar{C} = \bar{T}^k \bar{A}\bar{B}.$$

The same is true if we replace $\bar{T}$ by $\bar{U}$.

Proof. The element $\bar{C}^{-1}$ preserves the Γ-orbits if and only if, for any $\bar{A} \in \mathrm{PSL}_2(\mathbb{Z})$, we have

$$\bar{C}^{-1} \cdot \bar{A}^{-1}\infty = \bar{B}^{-1} \cdot \bar{A}^{-1}\infty \quad \text{for some } \ \bar{B} \in \Gamma,$$

that is, there exists $k \in \mathbb{Z}$ such that

$$\bar{A}\bar{C}\bar{B}^{-1}\bar{A}^{-1} = \bar{T}^k,$$

or else, $\bar{A}\bar{C} = \bar{T}^k\bar{A}\bar{B}$. The same is true if we replace ∞ by 0 and $\bar{T}$ by $\bar{U}$. □

The projective group $G = \mathrm{PSL}_2(\mathbb{Z})$ has the following presentation:

$$G = \left\langle \bar{T}, \bar{U} \;\middle|\; \bar{T}\bar{U}\bar{T} = \bar{U}\bar{T}\bar{U},\, (\bar{T}\bar{U}\bar{T})^2 = 1 \right\rangle. \tag{6.6}$$

To every subgroup $\Gamma \subseteq G$ of finite index corresponds a coset diagram $C(G/\Gamma)$, that is a 2-labeled digraph with labels $\bar{T}$ and $\bar{U}$. Moreover, a finite connected 2-labeled digraph Υ is isomorphic to a coset diagram $C(G/\Gamma)$ for some subgroup $\Gamma \subseteq G$ if and only if the paths $(\bar{T}\bar{U}\bar{T})^2[v]$ and $\bar{U}^{-1}\bar{T}^{-1}\bar{U}^{-1}\bar{T}\bar{U}\bar{T}[v]$ are closed for any vertex v of Υ. This is shown in Proposition 5.2.

We have the following theorem:

Theorem 6.3. *There are infinitely many finite index subgroups $\Gamma \subseteq G$ which are not $\hat{\mathbb{Q}}$-straining.*

Proof. Take $m \in \{2, 3, 6\}$. Let Γ_0 be a finite index subgroup of G such that the smallest positive integers x, y for which $\bar{T}^x, \bar{U}^y \in \Gamma_0$, are coprime with m. Moreover, we assume that the same is true for any conjugate of Γ_0: the smallest positive exponents of $\bar{T}$ and $\bar{U}$ in $\bar{A}\Gamma_0\bar{A}^{-1}$ are coprime with m. There are infinitely many such subgroups Γ_0 (for instance, principal congruence subgroups of level coprime with m). According to Proposition 5.2, the coset diagram $\Pi = C(G/\Gamma_0)$ has the following property:

(P) the paths $(\bar{T}\bar{U}\bar{T})^2[v]$ and $\bar{U}^{-1}\bar{T}^{-1}\bar{U}^{-1}\bar{T}\bar{U}\bar{T}[v]$ are closed for any vertex v.

We are going to construct another coset diagram with this property.

Let $\Upsilon = \Pi \times \mathbb{Z}_m$ be a 2-labeled digraph with vertices (v, k), where v is a vertex of Π and $k \in \mathbb{Z}_m$. We connect any two vertices (v, k) and $(\bar{T} \cdot v, k+1)$ by an edge with label $\bar{T}$, and any two vertices (v, k) and $(\bar{U} \cdot v, k+1)$ by an edge with label $\bar{U}$. See an example in Figure 6.1, where $v_k := (v, k)$. The digraph Υ is connected: if $v = W(\bar{T}, \bar{U}) \cdot \Gamma_0$ for a word W, then we have

$$W(\bar{T}, \bar{U}) \cdot (\Gamma_0, 0) = (v, l), \quad \text{where } l \text{ is the length of the word } W.$$

Since x is coprime to m, there exists an integer z such that $zx \equiv k - l \bmod m$, and so

$$W(\bar{T}, \bar{U})\, \bar{T}^{zx} \cdot (\Gamma_0, 0) = W(\bar{T}, \bar{U}) \cdot (\Gamma_0, k-l) = (v, k).$$

Thus, any vertex (v, k) is connected to $(\Gamma_0, 0)$. Also, the property (P) is verified for Υ:

$$(\bar{T}\bar{U}\bar{T})^2 \cdot (v, k) = ((\bar{T}\bar{U}\bar{T})^2 \cdot v, k+6) = (v, k),$$
$$\bar{U}^{-1}\bar{T}^{-1}\bar{U}^{-1}\bar{T}\bar{U}\bar{T} \cdot (v, k) = (\bar{U}^{-1}\bar{T}^{-1}\bar{U}^{-1}\bar{T}\bar{U}\bar{T} \cdot v, k) = (v, k).$$

Due to Proposition 5.2, the digraph Υ is the coset diagram $C(G/\Gamma)$ for a finite index subgroup $\Gamma \subseteq G$ that can be taken to be the stabilizer of the vertex $(\Gamma_0, 0)$.

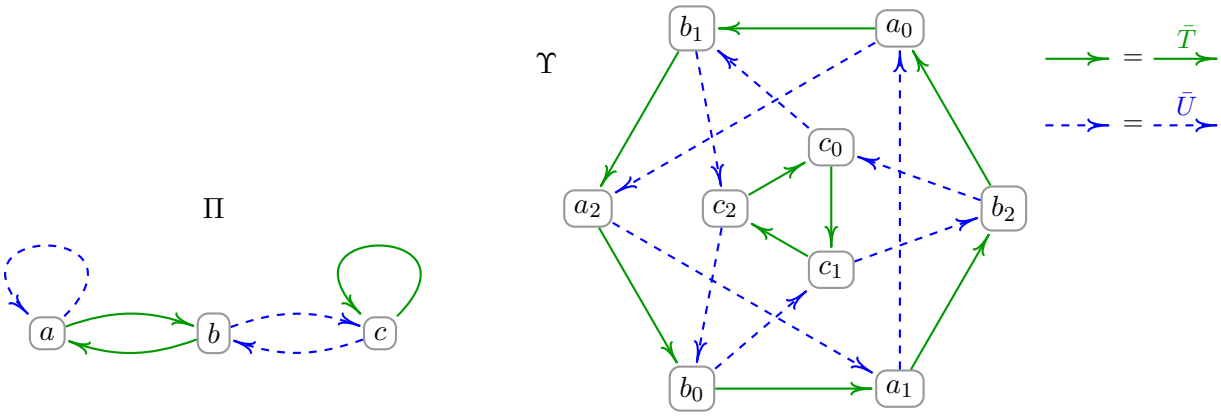


Figure 6.1: Two coset diagrams Π and $\Upsilon = \Pi \times \mathbb{Z}_3$.

According to Lemma 6.2, an element $\bar{C} \in G$ preserves the Γ-orbits on $\hat{\mathbb{Q}}$ if and only if, for any $\bar{A} \in G$, the vertices $\bar{A} \cdot \Gamma$ and $\bar{A}\bar{C} \cdot \Gamma$ of the coset diagram $C(G/\Gamma)$ are in the same $\mathcal{U}$-cycle[3] (that is, $\bar{A}\bar{C} \cdot \Gamma = \bar{U}^a \bar{A} \cdot \Gamma$ for some $a \in \mathbb{Z}$). Now, let us show that this is the case for $\bar{C} = \bar{T}^x$. Indeed, write $\bar{A}$ as a word on $\bar{T}$ and $\bar{U}$: $\bar{A} = W(\bar{T}, \bar{U})$. Then

$$\bar{A} \cdot \Gamma = W(\bar{T}, \bar{U}) \cdot (\Gamma_0, 0) = (v, l), \quad \text{where } v = W(\bar{T}, \bar{U}) \cdot \Gamma_0 \text{ and } l \text{ is the length of the word } W,$$
$$\bar{A}\bar{C} \cdot \Gamma = W(\bar{T}, \bar{U})\, \bar{T}^x \cdot (\Gamma_0, 0) = W(\bar{T}, \bar{U}) \cdot (\Gamma_0, x) = (v, x + l).$$

By what we assumed in the beginning, the vertex v gets into a $\mathcal{U}$-cycle of the digraph Π of length $b \in \mathbb{N}$ which is **coprime to** m. Thus there is an integer z such that $zb \equiv x \bmod m$, and so

$$\bar{U}^{zb} \bar{A} \cdot \Gamma = \bar{U}^{zb} \cdot (v, l) = (v, l + x) = \bar{A}\bar{C} \cdot \Gamma.$$

We conclude that the element $\bar{C}$ preserves the Γ-orbits on $\hat{\mathbb{Q}}$. It is left to notice that $\bar{C}$ doesn't belong to Γ, since $\bar{C} \cdot \Gamma = \bar{T}^x \cdot (\Gamma_0, 0) = (\Gamma_0, x) \neq (\Gamma_0, 0) = \Gamma$. This completes the proof that the subgroup Γ is not $\hat{\mathbb{Q}}$-straining. □

[3] We call a *$\mathcal{T}$-cycle* (a *$\mathcal{U}$-cycle*) a cycle with all edges labeled by $\bar{T}$ (respectively $\bar{U}$).

Appendix A
Projective coset origamis (Java)

```
// File FField.java
class FField{
        // Arithmetics in the projective line over a finite field modulo p.
        // All elements of the field are thought of as non-negative integers:
        //              0, 1, ..., p-1.
        // We take 2^{31}-1 for the infinity.
        int p;

        public static int infty = Integer.MAX_VALUE;

        FField(int p){
                this.p = p;
        }

        static int residue(int i, int p){
                if ((i == 0)||(i == infty))
                        return i;
                int res = i - p*(int)(i/p);
                if (res >= 0)
                        return res;
                return (p + res);  // if i=-5, p=3 then res=-2
        }

        public int inv(int i){  // gives i^{-1} modulo p
                int p = this.p;
                if (i == 0)
                        return infty;  // infinity
                if (i == infty)
                        return 0;
                for(int j=1; j<p; j++)
                        if (residue(i*j, p) == 1)
                                return j;
                return -2;
        }

        public int opp(int i){  // gives -i modulo p
                if ((i == 0)||(i == infty))
                        return i;
                return (p - residue(i, p));
        }

        public int sum(int a, int b){
```

```
        // for (a,b) in P1(Fp)\{(infty,infty)} gives a + b modulo p
                if ((a == infty)||(b == infty))
                        return infty;
                return residue(a + b, this.p);
        }

        public int difference(int a, int b){
        // for (a,b) in P1(Fp)\{(infty,infty)} gives a - b modulo p
                if ((a == infty)||(b == infty))
                        return infty;
                return residue(a - b, this.p);
        }

        public int product(int a, int b){
        // for (a,b) in P1(Fp)\{(0,infty),(infty,0)} gives a * b modulo p
                if ((a == infty)||(b == infty))
                        return infty;
                return residue(residue(a, p) * residue(b, p), this.p);
        }

        public int division(int a, int b){
        // for (a,b) in P1(Fp)\{(0,0),(infty,infty)} gives a / b modulo p
                if (a == infty)
                        return infty;
                return product(a, inv(b));
        }
}


// File ProjCosetOrigami.java
class ProjCosetOrigami{
   // Finds the stratum and genus of the projective coset origami
   // with monodromy group PSL(2,p) for p_{imin} <= p <= p_{imax}.
   static String folder = "/Users/Dave/PSL/output/";
   // The destination (output) folder

   public static void main(String[] args){

        StringBuffer buf = new StringBuffer();
        String       file = folder + "file.txt";

        final int imin = 1; // index of the first prime
        final int imax = 328;  // index of the last prime
        int[] prime = new int[imax+1]; // array of primes
        int i = 2, p = 3;

        prime[1] = 2;
        while (i <= imax){  //  find imax first primes
                boolean b = true;

                for(int d=2; d<(int)(Math.sqrt(p)) + 1; d++){
                        if (d*(int)(p/d) == p){
                                b = false;
                                break;
                        }
                }
```

```
        if (b){
                prime[i] = p;
                ++i;
        }

        ++p;
}

buf.append("$\\small" + (char)10 +
                "\\begin{array}{|lcl|}␣\\hline");
buf.append( (char)10 );
buf.append("\\textbf{Prime␣}(p)␣&␣\\textbf{Stratum␣}␣" +
                "&␣\\textbf{Genus␣}(g)\\\\␣\\hline");
buf.append( (char)10 );
for(i=imin; i<= imax; i++)
{
        p = prime[i];
        FField Fp = new FField(p);
        boolean[] bool = new boolean[p+1];
        int count = 0;
        int period = 0;

        for(int j=0; j<p; j++)
                bool[j] = false;

        int res = FField.residue(p, 5);
        if ((res == 1)||(res == 4))
                buf.append("\\centerdot\\;␣");
        else buf.append("\\;\\;");

        buf.append("p="); buf.append(p); buf.append("␣&␣");
        buf.append("\\mathcal{H}(");

        int a = 0, c = 0;
        int k = 1;              // degree of a zero
        int nzeros = 0;         // number of zeros
        int g = 0;              // genus

        while(count < p+1){
                while (bool[a]) ++a;

                bool[a] = true; period = 1;
                ++count;

                if (a == p)
                        a = FField.infty;
                c = Fp.difference(1, Fp.inv( Fp.sum(a, 2) ));
                while((c != a)&&(count < p+1)){
                        if (c == FField.infty)
                                bool[p] = true;
                        else bool[c] = true;
                        ++period;  ++count;
                        c = Fp.difference(1, Fp.inv( Fp.sum(c, 2) ));
                }
```

```
                        if (period > 1){
                                k = period;
                                ++nzeros;
                        }
                        g = g + period - 1;
                }

                buf.append(k-1);
                if (nzeros > 1){
                        buf.append("_{");
                        if ((res == 1)||(res == 4))
                                buf.append((int)((p-1)/k));
                        else buf.append((int)((p+1)/k));
                        buf.append("}");
                }
                buf.append(")␣&␣");
                g = (g + 2)/2;
                buf.append("g="); buf.append(g);
                buf.append("\\\\"); buf.append( (char)10 );
        }
        buf.append("\\hline"); buf.append( (char)10 );
        buf.append("\\end{array}$");
        FichierIO.ouvrir(file);
        FichierIO.ecrire(buf);
        FichierIO.fermer();
    }
}

// File FichierIO.java
import java.io.*;
class FichierIO{
    // Writes a StringBuffer to a file
    final static int N = 256;
    static BufferedWriter fichierSortie = null;

    static void ouvrir(String nom) {
        try{ fichierSortie = new BufferedWriter(new FileWriter(nom)); }
        catch (IOException e){ throw new Error(e.getMessage()); };
    }

    static void fermer() {
        try{ fichierSortie.close(); }
        catch (IOException e){ throw new Error(e.getMessage()); }
    }

    static void ecrire(StringBuffer buf) {
        try{
                String s = buf.toString();
                fichierSortie.write(s,0,s.length());
        }
        catch (IOException e){ throw new Error(e.getMessage()); }
    }
}
```

Appendix B
Tables

Table B.1: $\mathrm{SL}_2(\mathbb{Z})$-orbits of the 5- and 6-square origamis in the stratum $\mathcal{H}(4)$. Note that the monodromy groups of all such origamis are primitive.

Number of squares	**An orbit representative**	**Orbit length**	**Monodromy group (G)**	**Order of G**
$n = 5$	$\sigma = (1\ 2)(4\ 5)$ $\tau = (1\ 3)(2\ 4)$	3	$\mathbb{F}_5 \rtimes \{1, 4\} \simeq D_5$	10
	$\sigma = (1\ 2)(4\ 5)$ $\tau = (2\ 3\ 4\ 5)$	12	$\mathbb{F}_5 \rtimes \mathbb{F}_5^\times \simeq \mathrm{AGL}(1, 5)$	20
	$\sigma = (1\ 2)(4\ 5)$ $\tau = (2\ 3\ 4)$	10	A_5	60
	$\sigma = (1\ 2)(4\ 5)$ $\tau = (1\ 3)(2\ 4\ 5)$	15	S_5	120
$n = 6$	$\sigma = (1\ 2)(5\ 6)$ $\tau = (1\ 3\ 4)(2\ 5\ 6)$	10	$\mathrm{PSL}(2, 5) \simeq A_5$	60
	$\sigma = (1\ 2)(5\ 6)$ $\tau = (2\ 3\ 4\ 5)$	15	$\mathrm{PGL}(2, 5) \simeq S_5$	120
	$\sigma = (1\ 2\ 3)$ $\tau = (2\ 4\ 5\ 3\ 6)$	15	A_6	360
	$\sigma = (1\ 2\ 3)$ $\tau = (2\ 4\ 3\ 5\ 6)$	15		
	$\sigma = (1\ 2)(5\ 6)$ $\tau = (2\ 3\ 4\ 5\ 6)$	20		
	$\sigma = (1\ 2)(5\ 6)$ $\tau = (1\ 3\ 4)(2\ 5)$	30	S_6	720
	$\sigma = (1\ 2\ 3)$ $\tau = (2\ 4)(3\ 5\ 6)$	60		

Table B.2: $\mathrm{SL}_2(\mathbb{Z})$-orbits of all n-square-tiled surfaces in $\mathcal{H}(1,1)$ with $4 \leq n \leq 6$.

Number of squares	**An orbit representative**	**Orbit length**	**Monodromy group (G)**	**Order of G**	**Prim.**
$n = 4$	$\sigma = (1\ 2)$ $\tau = (1\ 3)(2\ 4)$	6	D_4	8	no
	$\sigma = (1\ 2)(3\ 4)$ $\tau = (2\ 3\ 4)$	4	A_4	12	yes
$n = 5$	$\sigma = (1\ 2)$ $\tau = (1\ 3)(2\ 4\ 5)$	24	S_5	120	yes
$n = 6$	$\sigma = (1\ 2)(3\ 4)$ $\tau = (1\ 3\ 5)(2\ 4\ 6)$	4	A_4	12	no
	$\sigma = (1\ 2)$ $\tau = (1\ 3\ 5)(2\ 4\ 6)$	12	$A_4 \times C_2$	24	no
	$\sigma = (1\ 2)$ $\tau = (1\ 3)(2\ 4\ 5\ 6)$	24	$(S_3)^2 \rtimes C_2$	72	no
	$\sigma = (1\ 2)(3\ 4)(5\ 6)$ $\tau = (2\ 3\ 5\ 4\ 6)$	24	S_5	120	yes
	$\sigma = (1\ 2\ 3)$ $\tau = (2\ 3\ 4\ 5\ 6)$	24	A_6	360	yes

Table B.3: $\mathrm{SL}_2(\mathbb{Z})$-orbits of the *primitive* n-square origamis in $\mathcal{H}(1,1)$ with $7 \leq n \leq 17$.

n	**An orbit representative**	**Orbit length**	$G = \mathrm{gp}\{\sigma, \tau\}$	**Order of** G
7	$\sigma = (1\,2)(3\,4)$ $\tau = (1\,3\,5\,2\,4\,6\,7)$	16	A_7	2520
	$\sigma = (1\,2)$ $\tau = (1\,3)(2\,4\,5\,6\,7)$	144	S_7	5040
8	$\sigma = (1\,2)(3\,4)$ $\tau = (1\,3\,5)(2\,4\,6\,7\,8)$	96	A_8	20160
	$\sigma = (1\,2)$ $\tau = (1\,3\,4)(2\,5\,6\,7\,8)$	144	S_8	40320
9	$\sigma = (1\,2)(3\,4)$ $\tau = (1\,3\,5\,6\,2\,4\,7\,8\,9)$	72	A_9	181440
	$\sigma = (1\,2)$ $\tau = (1\,3)(2\,4\,5\,6\,7\,8\,9)$	432	S_9	362880
10	$\sigma = (1\,2)(3\,4)$ $\tau = (1\,3\,5)(2\,4\,6\,7\,8\,9\,10)$	240	A_{10}	1814400
	$\sigma = (1\,2)$ $\tau = (1\,3\,4)(2\,5\,6\,7\,8\,9\,10)$	432	S_{10}	3628800
11	$\sigma = (1\,2)(3\,4)$ $\tau = (1\,3\,5\,2\,4\,6\,7\,8\,9\,10\,11)$	240	A_{11}	19958400
	$\sigma = (1\,2)$ $\tau = (1\,3)(2\,4\,5\,6\,7\,8\,9\,10\,11)$	1200	S_{11}	39916800
12	$\sigma = (1\,2)(3\,4)$ $\tau = (1\,3\,5\,6\,7)(2\,4\,8\,9\,10\,11\,12)$	480	A_{12}	$12!/2$
	$\sigma = (1\,2)$ $\tau = (1\,3\,4\,5\,6)(2\,7\,8\,9\,10\,11\,12)$	960	S_{12}	12!
13	$\sigma = (1\,2)(3\,4)$ $\tau = (1\,3\,5\,2\,4\,6\,7\,8\,9\,10\,11\,12\,13)$	560	A_{13}	$13!/2$
	$\sigma = (1\,2)$ $\tau = (1\,3)(2\,4\,5\,6\,7\,8\,9\,10\,11\,12\,13)$	2520	S_{13}	13!
14	$\sigma = (1\,2)(3\,4)$ $\tau = (1\,3\,5)(2\,4\,6\,7\,8\,9\,10\,11\,12\,13\,14)$	1008	A_{14}	$14!/2$
	$\sigma = (1\,2)$ $\tau = (1\,3\,4)(2\,5\,6\,7\,8\,9\,10\,11\,12\,13\,14)$	2160	S_{14}	14!
15	$\sigma = (1\,2)(3\,4)$ $\tau = (1\,3\,5\,6\,2\,4\,7\,8\,9\,10\,11\,12\,13\,14\,15)$	960	A_{15}	$15!/2$
	$\sigma = (1\,2)$ $\tau = (1\,3)(2\,4\,5\,6\,7\,8\,9\,10\,11\,12\,13\,14\,15)$	4032	S_{15}	15!
16	$\sigma = (1\,2)(3\,4)$ $\tau = (1\,3\,5)(2\,4\,6\,7\,8\,9\,10\,11\,12\,13\,14\,15\,16)$	1792	A_{16}	$16!/2$
	$\sigma = (1\,2)$ $\tau = (1\,3\,4)(2\,5\,6\,7\,8\,9\,10\,11\,12\,13\,14\,15\,16)$	4032	S_{16}	16!
17	$\sigma = (1\,2)(3\,4)$ $\tau = (1\,3\,5\,2\,4\,6\,7\,8\,9\,10\,11\,12\,13\,14\,15\,16\,17)$	2016	A_{17}	$17!/2$
	$\sigma = (1\,2)$ $\tau = (1\,3)(2\,4\,5\,6\,7\,8\,9\,10\,11\,12\,13\,14\,15\,16\,17)$	8064	S_{17}	17!

Table B.4: Projective coset origamis $O_{\mathrm{PSL}(2,p)/H,\bar{T},\bar{U}}$ with $2 \leq p \leq 2203$.

Prime (p)	**Stratum**	**Genus** (g)
$p = 2$	$\mathcal{H}(2)$	$g = 2$
$p = 3$	$\mathcal{H}(1_2)$	$g = 2$
$p = 5$	$\mathcal{H}(4)$	$g = 3$
$p = 7$	$\mathcal{H}(3_2)$	$g = 4$
$p = 11$	$\mathcal{H}(4_2)$	$g = 5$
$p = 13$	$\mathcal{H}(6_2)$	$g = 7$
$p = 17$	$\mathcal{H}(8_2)$	$g = 9$
$p = 19$	$\mathcal{H}(8_2)$	$g = 9$
$p = 23$	$\mathcal{H}(11_2)$	$g = 12$
$p = 29$	$\mathcal{H}(6_4)$	$g = 13$
$p = 31$	$\mathcal{H}(14_2)$	$g = 15$
$p = 37$	$\mathcal{H}(18_2)$	$g = 19$
$p = 41$	$\mathcal{H}(9_4)$	$g = 19$
$p = 43$	$\mathcal{H}(21_2)$	$g = 22$
$p = 47$	$\mathcal{H}(7_6)$	$g = 22$
$p = 53$	$\mathcal{H}(26_2)$	$g = 27$
$p = 59$	$\mathcal{H}(28_2)$	$g = 29$
$p = 61$	$\mathcal{H}(14_4)$	$g = 29$
$p = 67$	$\mathcal{H}(33_2)$	$g = 34$
$p = 71$	$\mathcal{H}(34_2)$	$g = 35$
$p = 73$	$\mathcal{H}(36_2)$	$g = 37$
$p = 79$	$\mathcal{H}(38_2)$	$g = 39$
$p = 83$	$\mathcal{H}(41_2)$	$g = 42$
$p = 89$	$\mathcal{H}(10_8)$	$g = 41$
$p = 97$	$\mathcal{H}(48_2)$	$g = 49$
$p = 101$	$\mathcal{H}(24_4)$	$g = 49$
$p = 103$	$\mathcal{H}(51_2)$	$g = 52$
$p = 107$	$\mathcal{H}(17_6)$	$g = 52$
$p = 109$	$\mathcal{H}(26_4)$	$g = 53$
$p = 113$	$\mathcal{H}(18_6)$	$g = 55$
$p = 127$	$\mathcal{H}(63_2)$	$g = 64$
$p = 131$	$\mathcal{H}(64_2)$	$g = 65$
$p = 137$	$\mathcal{H}(68_2)$	$g = 69$
$p = 139$	$\mathcal{H}(22_6)$	$g = 67$
$p = 149$	$\mathcal{H}(36_4)$	$g = 73$
$p = 151$	$\mathcal{H}(24_6)$	$g = 73$
$p = 157$	$\mathcal{H}(78_2)$	$g = 79$
$p = 163$	$\mathcal{H}(81_2)$	$g = 82$
$p = 167$	$\mathcal{H}(83_2)$	$g = 84$
$p = 173$	$\mathcal{H}(86_2)$	$g = 87$
$p = 179$	$\mathcal{H}(88_2)$	$g = 89$
$p = 181$	$\mathcal{H}(44_4)$	$g = 89$
$p = 191$	$\mathcal{H}(94_2)$	$g = 95$
$p = 193$	$\mathcal{H}(96_2)$	$g = 97$
$p = 197$	$\mathcal{H}(98_2)$	$g = 99$
$p = 199$	$\mathcal{H}(10_{18})$	$g = 91$
$p = 211$	$\mathcal{H}(20_{10})$	$g = 101$
$p = 223$	$\mathcal{H}(111_2)$	$g = 112$
$p = 227$	$\mathcal{H}(113_2)$	$g = 114$
$p = 229$	$\mathcal{H}(56_4)$	$g = 113$
$p = 233$	$\mathcal{H}(12_{18})$	$g = 109$
$p = 239$	$\mathcal{H}(118_2)$	$g = 119$

Prime (p)	**Stratum**	**Genus** (g)
$p = 241$	$\mathcal{H}(59_4)$	$g = 119$
$p = 251$	$\mathcal{H}(124_2)$	$g = 125$
$p = 257$	$\mathcal{H}(128_2)$	$g = 129$
$p = 263$	$\mathcal{H}(43_6)$	$g = 130$
$p = 269$	$\mathcal{H}(66_4)$	$g = 133$
$p = 271$	$\mathcal{H}(134_2)$	$g = 135$
$p = 277$	$\mathcal{H}(138_2)$	$g = 139$
$p = 281$	$\mathcal{H}(13_{20})$	$g = 131$
$p = 283$	$\mathcal{H}(141_2)$	$g = 142$
$p = 293$	$\mathcal{H}(146_2)$	$g = 147$
$p = 307$	$\mathcal{H}(21_{14})$	$g = 148$
$p = 311$	$\mathcal{H}(154_2)$	$g = 155$
$p = 313$	$\mathcal{H}(156_2)$	$g = 157$
$p = 317$	$\mathcal{H}(158_2)$	$g = 159$
$p = 331$	$\mathcal{H}(54_6)$	$g = 163$
$p = 337$	$\mathcal{H}(168_2)$	$g = 169$
$p = 347$	$\mathcal{H}(57_6)$	$g = 172$
$p = 349$	$\mathcal{H}(86_4)$	$g = 173$
$p = 353$	$\mathcal{H}(58_6)$	$g = 175$
$p = 359$	$\mathcal{H}(178_2)$	$g = 179$
$p = 367$	$\mathcal{H}(183_2)$	$g = 184$
$p = 373$	$\mathcal{H}(186_2)$	$g = 187$
$p = 379$	$\mathcal{H}(188_2)$	$g = 189$
$p = 383$	$\mathcal{H}(191_2)$	$g = 192$
$p = 389$	$\mathcal{H}(96_4)$	$g = 193$
$p = 397$	$\mathcal{H}(198_2)$	$g = 199$
$p = 401$	$\mathcal{H}(49_8)$	$g = 197$
$p = 409$	$\mathcal{H}(101_4)$	$g = 203$
$p = 419$	$\mathcal{H}(208_2)$	$g = 209$
$p = 421$	$\mathcal{H}(20_{20})$	$g = 201$
$p = 431$	$\mathcal{H}(214_2)$	$g = 215$
$p = 433$	$\mathcal{H}(216_2)$	$g = 217$
$p = 439$	$\mathcal{H}(218_2)$	$g = 219$
$p = 443$	$\mathcal{H}(221_2)$	$g = 222$
$p = 449$	$\mathcal{H}(111_4)$	$g = 223$
$p = 457$	$\mathcal{H}(228_2)$	$g = 229$
$p = 461$	$\mathcal{H}(22_{20})$	$g = 221$
$p = 463$	$\mathcal{H}(231_2)$	$g = 232$
$p = 467$	$\mathcal{H}(233_2)$	$g = 234$
$p = 479$	$\mathcal{H}(238_2)$	$g = 239$
$p = 487$	$\mathcal{H}(243_2)$	$g = 244$
$p = 491$	$\mathcal{H}(244_2)$	$g = 245$
$p = 499$	$\mathcal{H}(248_2)$	$g = 249$
$p = 503$	$\mathcal{H}(251_2)$	$g = 252$
$p = 509$	$\mathcal{H}(126_4)$	$g = 253$
$p = 521$	$\mathcal{H}(12_{40})$	$g = 241$
$p = 523$	$\mathcal{H}(261_2)$	$g = 262$
$p = 541$	$\mathcal{H}(44_{12})$	$g = 265$
$p = 547$	$\mathcal{H}(273_2)$	$g = 274$
$p = 557$	$\mathcal{H}(30_{18})$	$g = 271$
$p = 563$	$\mathcal{H}(93_6)$	$g = 280$
$p = 569$	$\mathcal{H}(141_4)$	$g = 283$

Prime (p)	**Stratum**	**Genus** (g)
. $p = 571$	$\mathcal{H}(284_2)$	$g = 285$
$p = 577$	$\mathcal{H}(288_2)$	$g = 289$
$p = 587$	$\mathcal{H}(293_2)$	$g = 294$
$p = 593$	$\mathcal{H}(296_2)$	$g = 297$
. $p = 599$	$\mathcal{H}(298_2)$	$g = 299$
. $p = 601$	$\mathcal{H}(149_4)$	$g = 299$
$p = 607$	$\mathcal{H}(303_2)$	$g = 304$
$p = 613$	$\mathcal{H}(306_2)$	$g = 307$
$p = 617$	$\mathcal{H}(308_2)$	$g = 309$
. $p = 619$	$\mathcal{H}(102_6)$	$g = 307$
. $p = 631$	$\mathcal{H}(314_2)$	$g = 315$
. $p = 641$	$\mathcal{H}(159_4)$	$g = 319$
$p = 643$	$\mathcal{H}(321_2)$	$g = 322$
$p = 647$	$\mathcal{H}(323_2)$	$g = 324$
$p = 653$	$\mathcal{H}(326_2)$	$g = 327$
. $p = 659$	$\mathcal{H}(328_2)$	$g = 329$
. $p = 661$	$\mathcal{H}(54_{12})$	$g = 325$
$p = 673$	$\mathcal{H}(336_2)$	$g = 337$
$p = 677$	$\mathcal{H}(112_6)$	$g = 337$
$p = 683$	$\mathcal{H}(341_2)$	$g = 342$
. $p = 691$	$\mathcal{H}(68_{10})$	$g = 341$
. $p = 701$	$\mathcal{H}(174_4)$	$g = 349$
. $p = 709$	$\mathcal{H}(58_{12})$	$g = 349$
. $p = 719$	$\mathcal{H}(358_2)$	$g = 359$
$p = 727$	$\mathcal{H}(363_2)$	$g = 364$
$p = 733$	$\mathcal{H}(366_2)$	$g = 367$
. $p = 739$	$\mathcal{H}(368_2)$	$g = 369$
$p = 743$	$\mathcal{H}(123_6)$	$g = 370$
. $p = 751$	$\mathcal{H}(374_2)$	$g = 375$
$p = 757$	$\mathcal{H}(378_2)$	$g = 379$
. $p = 761$	$\mathcal{H}(94_8)$	$g = 377$
. $p = 769$	$\mathcal{H}(47_{16})$	$g = 377$
$p = 773$	$\mathcal{H}(386_2)$	$g = 387$
$p = 787$	$\mathcal{H}(393_2)$	$g = 394$
$p = 797$	$\mathcal{H}(56_{14})$	$g = 393$
. $p = 809$	$\mathcal{H}(100_8)$	$g = 401$
. $p = 811$	$\mathcal{H}(134_6)$	$g = 403$
. $p = 821$	$\mathcal{H}(204_4)$	$g = 409$
$p = 823$	$\mathcal{H}(411_2)$	$g = 412$
$p = 827$	$\mathcal{H}(413_2)$	$g = 414$
. $p = 829$	$\mathcal{H}(68_{12})$	$g = 409$
. $p = 839$	$\mathcal{H}(418_2)$	$g = 419$
$p = 853$	$\mathcal{H}(426_2)$	$g = 427$
$p = 857$	$\mathcal{H}(428_2)$	$g = 429$
. $p = 859$	$\mathcal{H}(38_{22})$	$g = 419$
$p = 863$	$\mathcal{H}(431_2)$	$g = 432$
$p = 877$	$\mathcal{H}(438_2)$	$g = 439$
. $p = 881$	$\mathcal{H}(43_{20})$	$g = 431$
$p = 883$	$\mathcal{H}(441_2)$	$g = 442$
$p = 887$	$\mathcal{H}(443_2)$	$g = 444$
$p = 907$	$\mathcal{H}(453_2)$	$g = 454$
. $p = 911$	$\mathcal{H}(34_{26})$	$g = 443$
. $p = 919$	$\mathcal{H}(50_{18})$	$g = 451$
. $p = 929$	$\mathcal{H}(231_4)$	$g = 463$
$p = 937$	$\mathcal{H}(468_2)$	$g = 469$
. $p = 941$	$\mathcal{H}(234_4)$	$g = 469$

Prime (p)	**Stratum**	**Genus** (g)
$p = 947$	$\mathcal{H}(473_2)$	$g = 474$
$p = 953$	$\mathcal{H}(52_{18})$	$g = 469$
$p = 967$	$\mathcal{H}(43_{22})$	$g = 474$
. $p = 971$	$\mathcal{H}(484_2)$	$g = 485$
$p = 977$	$\mathcal{H}(162_6)$	$g = 487$
$p = 983$	$\mathcal{H}(491_2)$	$g = 492$
. $p = 991$	$\mathcal{H}(98_{10})$	$g = 491$
$p = 997$	$\mathcal{H}(498_2)$	$g = 499$
. $p = 1009$	$\mathcal{H}(62_{16})$	$g = 497$
$p = 1013$	$\mathcal{H}(506_2)$	$g = 507$
. $p = 1019$	$\mathcal{H}(508_2)$	$g = 509$
. $p = 1021$	$\mathcal{H}(254_4)$	$g = 509$
. $p = 1031$	$\mathcal{H}(102_{10})$	$g = 511$
$p = 1033$	$\mathcal{H}(516_2)$	$g = 517$
. $p = 1039$	$\mathcal{H}(518_2)$	$g = 519$
. $p = 1049$	$\mathcal{H}(130_8)$	$g = 521$
. $p = 1051$	$\mathcal{H}(524_2)$	$g = 525$
. $p = 1061$	$\mathcal{H}(264_4)$	$g = 529$
$p = 1063$	$\mathcal{H}(531_2)$	$g = 532$
. $p = 1069$	$\mathcal{H}(88_{12})$	$g = 529$
$p = 1087$	$\mathcal{H}(31_{34})$	$g = 528$
. $p = 1091$	$\mathcal{H}(544_2)$	$g = 545$
$p = 1093$	$\mathcal{H}(546_2)$	$g = 547$
$p = 1097$	$\mathcal{H}(182_6)$	$g = 547$
$p = 1103$	$\mathcal{H}(23_{46})$	$g = 530$
. $p = 1109$	$\mathcal{H}(276_4)$	$g = 553$
$p = 1117$	$\mathcal{H}(558_2)$	$g = 559$
$p = 1123$	$\mathcal{H}(561_2)$	$g = 562$
. $p = 1129$	$\mathcal{H}(281_4)$	$g = 563$
. $p = 1151$	$\mathcal{H}(114_{10})$	$g = 571$
$p = 1153$	$\mathcal{H}(576_2)$	$g = 577$
$p = 1163$	$\mathcal{H}(581_2)$	$g = 582$
. $p = 1171$	$\mathcal{H}(584_2)$	$g = 585$
. $p = 1181$	$\mathcal{H}(294_4)$	$g = 589$
$p = 1187$	$\mathcal{H}(593_2)$	$g = 594$
$p = 1193$	$\mathcal{H}(596_2)$	$g = 597$
. $p = 1201$	$\mathcal{H}(299_4)$	$g = 599$
$p = 1213$	$\mathcal{H}(606_2)$	$g = 607$
$p = 1217$	$\mathcal{H}(202_6)$	$g = 607$
$p = 1223$	$\mathcal{H}(203_6)$	$g = 610$
. $p = 1229$	$\mathcal{H}(306_4)$	$g = 613$
. $p = 1231$	$\mathcal{H}(204_6)$	$g = 613$
$p = 1237$	$\mathcal{H}(618_2)$	$g = 619$
. $p = 1249$	$\mathcal{H}(155_8)$	$g = 621$
. $p = 1259$	$\mathcal{H}(628_2)$	$g = 629$
$p = 1277$	$\mathcal{H}(212_6)$	$g = 637$
. $p = 1279$	$\mathcal{H}(212_6)$	$g = 637$
$p = 1283$	$\mathcal{H}(641_2)$	$g = 642$
. $p = 1289$	$\mathcal{H}(160_8)$	$g = 641$
. $p = 1291$	$\mathcal{H}(214_6)$	$g = 643$
$p = 1297$	$\mathcal{H}(648_2)$	$g = 649$
. $p = 1301$	$\mathcal{H}(324_4)$	$g = 649$
$p = 1303$	$\mathcal{H}(651_2)$	$g = 652$
$p = 1307$	$\mathcal{H}(217_6)$	$g = 652$
. $p = 1319$	$\mathcal{H}(658_2)$	$g = 659$
. $p = 1321$	$\mathcal{H}(329_4)$	$g = 659$

Prime (p)	**Stratum**	**Genus** (g)
$p = 1327$	$\mathcal{H}(663_2)$	$g = 664$
. $p = 1361$	$\mathcal{H}(169_8)$	$g = 677$
$p = 1367$	$\mathcal{H}(683_2)$	$g = 684$
$p = 1373$	$\mathcal{H}(686_2)$	$g = 687$
. $p = 1381$	$\mathcal{H}(114_{12})$	$g = 685$
. $p = 1399$	$\mathcal{H}(698_2)$	$g = 699$
. $p = 1409$	$\mathcal{H}(175_8)$	$g = 701$
$p = 1423$	$\mathcal{H}(711_2)$	$g = 712$
$p = 1427$	$\mathcal{H}(41_{34})$	$g = 698$
. $p = 1429$	$\mathcal{H}(356_4)$	$g = 713$
$p = 1433$	$\mathcal{H}(716_2)$	$g = 717$
. $p = 1439$	$\mathcal{H}(718_2)$	$g = 719$
$p = 1447$	$\mathcal{H}(723_2)$	$g = 724$
. $p = 1451$	$\mathcal{H}(724_2)$	$g = 725$
$p = 1453$	$\mathcal{H}(726_2)$	$g = 727$
. $p = 1459$	$\mathcal{H}(728_2)$	$g = 729$
. $p = 1471$	$\mathcal{H}(244_6)$	$g = 733$
. $p = 1481$	$\mathcal{H}(369_4)$	$g = 739$
$p = 1483$	$\mathcal{H}(105_{14})$	$g = 736$
$p = 1487$	$\mathcal{H}(743_2)$	$g = 744$
. $p = 1489$	$\mathcal{H}(371_4)$	$g = 743$
$p = 1493$	$\mathcal{H}(746_2)$	$g = 747$
. $p = 1499$	$\mathcal{H}(748_2)$	$g = 749$
. $p = 1511$	$\mathcal{H}(150_{10})$	$g = 751$
$p = 1523$	$\mathcal{H}(253_6)$	$g = 760$
. $p = 1531$	$\mathcal{H}(764_2)$	$g = 765$
$p = 1543$	$\mathcal{H}(771_2)$	$g = 772$
. $p = 1549$	$\mathcal{H}(386_4)$	$g = 773$
$p = 1553$	$\mathcal{H}(258_6)$	$g = 775$
. $p = 1559$	$\mathcal{H}(778_2)$	$g = 779$
$p = 1567$	$\mathcal{H}(783_2)$	$g = 784$
. $p = 1571$	$\mathcal{H}(784_2)$	$g = 785$
. $p = 1579$	$\mathcal{H}(262_6)$	$g = 787$
$p = 1583$	$\mathcal{H}(791_2)$	$g = 792$
$p = 1597$	$\mathcal{H}(16_{94})$	$g = 753$
. $p = 1601$	$\mathcal{H}(39_{40})$	$g = 781$
$p = 1607$	$\mathcal{H}(803_2)$	$g = 804$
. $p = 1609$	$\mathcal{H}(401_4)$	$g = 803$
$p = 1613$	$\mathcal{H}(806_2)$	$g = 807$
. $p = 1619$	$\mathcal{H}(808_2)$	$g = 809$
. $p = 1621$	$\mathcal{H}(404_4)$	$g = 809$
$p = 1627$	$\mathcal{H}(813_2)$	$g = 814$
$p = 1637$	$\mathcal{H}(818_2)$	$g = 819$
$p = 1657$	$\mathcal{H}(828_2)$	$g = 829$
$p = 1663$	$\mathcal{H}(831_2)$	$g = 832$
$p = 1667$	$\mathcal{H}(833_2)$	$g = 834$
. $p = 1669$	$\mathcal{H}(416_4)$	$g = 833$
$p = 1693$	$\mathcal{H}(846_2)$	$g = 847$
$p = 1697$	$\mathcal{H}(848_2)$	$g = 849$
. $p = 1699$	$\mathcal{H}(282_6)$	$g = 847$
. $p = 1709$	$\mathcal{H}(426_4)$	$g = 853$
. $p = 1721$	$\mathcal{H}(214_8)$	$g = 857$
$p = 1723$	$\mathcal{H}(861_2)$	$g = 862$
$p = 1733$	$\mathcal{H}(288_6)$	$g = 865$
. $p = 1741$	$\mathcal{H}(434_4)$	$g = 869$
$p = 1747$	$\mathcal{H}(873_2)$	$g = 874$

Prime (p)	**Stratum**	**Genus** (g)
$p = 1753$	$\mathcal{H}(876_2)$	$g = 877$
. $p = 1759$	$\mathcal{H}(878_2)$	$g = 879$
$p = 1777$	$\mathcal{H}(888_2)$	$g = 889$
$p = 1783$	$\mathcal{H}(891_2)$	$g = 892$
$p = 1787$	$\mathcal{H}(893_2)$	$g = 894$
. $p = 1789$	$\mathcal{H}(446_4)$	$g = 893$
. $p = 1801$	$\mathcal{H}(449_4)$	$g = 899$
. $p = 1811$	$\mathcal{H}(904_2)$	$g = 905$
$p = 1823$	$\mathcal{H}(303_6)$	$g = 910$
. $p = 1831$	$\mathcal{H}(914_2)$	$g = 915$
$p = 1847$	$\mathcal{H}(923_2)$	$g = 924$
. $p = 1861$	$\mathcal{H}(464_4)$	$g = 929$
$p = 1867$	$\mathcal{H}(933_2)$	$g = 934$
. $p = 1871$	$\mathcal{H}(186_{10})$	$g = 931$
$p = 1873$	$\mathcal{H}(936_2)$	$g = 937$
$p = 1877$	$\mathcal{H}(312_6)$	$g = 937$
. $p = 1879$	$\mathcal{H}(938_2)$	$g = 939$
. $p = 1889$	$\mathcal{H}(471_4)$	$g = 943$
. $p = 1901$	$\mathcal{H}(474_4)$	$g = 949$
$p = 1907$	$\mathcal{H}(953_2)$	$g = 954$
$p = 1913$	$\mathcal{H}(318_6)$	$g = 955$
. $p = 1931$	$\mathcal{H}(964_2)$	$g = 965$
$p = 1933$	$\mathcal{H}(966_2)$	$g = 967$
. $p = 1949$	$\mathcal{H}(486_4)$	$g = 973$
. $p = 1951$	$\mathcal{H}(194_{10})$	$g = 971$
$p = 1973$	$\mathcal{H}(328_6)$	$g = 985$
. $p = 1979$	$\mathcal{H}(988_2)$	$g = 989$
$p = 1987$	$\mathcal{H}(993_2)$	$g = 994$
$p = 1993$	$\mathcal{H}(996_2)$	$g = 997$
$p = 1997$	$\mathcal{H}(998_2)$	$g = 999$
. $p = 1999$	$\mathcal{H}(332_6)$	$g = 997$
$p = 2003$	$\mathcal{H}(1001_2)$	$g = 1002$
. $p = 2011$	$\mathcal{H}(1004_2)$	$g = 1005$
$p = 2017$	$\mathcal{H}(1008_2)$	$g = 1009$
$p = 2027$	$\mathcal{H}(337_6)$	$g = 1012$
. $p = 2029$	$\mathcal{H}(506_4)$	$g = 1013$
. $p = 2039$	$\mathcal{H}(1018_2)$	$g = 1019$
$p = 2053$	$\mathcal{H}(1026_2)$	$g = 1027$
$p = 2063$	$\mathcal{H}(1031_2)$	$g = 1032$
. $p = 2069$	$\mathcal{H}(516_4)$	$g = 1033$
. $p = 2081$	$\mathcal{H}(64_{32})$	$g = 1025$
$p = 2083$	$\mathcal{H}(1041_2)$	$g = 1042$
$p = 2087$	$\mathcal{H}(1043_2)$	$g = 1044$
. $p = 2089$	$\mathcal{H}(260_8)$	$g = 1041$
. $p = 2099$	$\mathcal{H}(1048_2)$	$g = 1049$
. $p = 2111$	$\mathcal{H}(1054_2)$	$g = 1055$
$p = 2113$	$\mathcal{H}(1056_2)$	$g = 1057$
. $p = 2129$	$\mathcal{H}(531_4)$	$g = 1063$
. $p = 2131$	$\mathcal{H}(1064_2)$	$g = 1065$
$p = 2137$	$\mathcal{H}(1068_2)$	$g = 1069$
. $p = 2141$	$\mathcal{H}(534_4)$	$g = 1069$
$p = 2143$	$\mathcal{H}(1071_2)$	$g = 1072$
$p = 2153$	$\mathcal{H}(1076_2)$	$g = 1077$
. $p = 2161$	$\mathcal{H}(19_{108})$	$g = 1027$
. $p = 2179$	$\mathcal{H}(98_{22})$	$g = 1079$
$p = 2203$	$\mathcal{H}(1101_2)$	$g = 1102$

Table B.5: $\mathrm{GL}_2(\mathbb{Z})$-orbits of n-square alternating coset origamis with $3 \leq n \leq 9$.

n	**Monodromy group** (A_n)	**Stratum**	**Number of orbits**	**Orbit length(s)**
3	$A_3 \simeq \mathbb{Z}_3$	$\mathcal{H}(0)$	1	4
4	A_4	$\mathcal{H}(1,1)$	1	4
5	A_5	$\mathcal{H}(2)$	1	9
		$\mathcal{H}(4)$	1	10
6	A_6	$\mathcal{H}(1,1)$	1	24
		$\mathcal{H}(3,1)$	1	32
		$\mathcal{H}(4)$	3	$15, 15, 20$
7	A_7	$\mathcal{H}(1,1)$	1	16
		$\mathcal{H}(2)$	1	36
		$\mathcal{H}(2,1,1)$	3	$24, 36, 48$
		$\mathcal{H}(2,2)$	2	$36, 72$
		$\mathcal{H}(3,1)$	1	192
		$\mathcal{H}(4)$	3	$30, 40, 120$
		$\mathcal{H}(6)$	5	$21, 21, 56, 84, 84$
8	A_8	$\mathcal{H}(1,1)$	1	96
		$\mathcal{H}(2,1,1)$	2	$252, 432$
		$\mathcal{H}(2,2)$	2	$90, 198$
		$\mathcal{H}(3,1)$	1	768
		$\mathcal{H}(3,3)$	2	$96, 384$
		$\mathcal{H}(4)$	2	$260, 270$
		$\mathcal{H}(4,2)$	4	$15, 45, 480, 540$
		$\mathcal{H}(5,1)$	1	1296
		$\mathcal{H}(6)$	3	$42, 1092, 1092$
9	A_9	$\mathcal{H}(1,1)$	1	72
		$\mathcal{H}(1,1,1,1)$	2	$114, 138$
		$\mathcal{H}(2)$	1	81
		$\mathcal{H}(2,1,1)$	3	$162, 222, 3144$
		$\mathcal{H}(2,2)$	4	$25, 324, 360, 828$
		$\mathcal{H}(2,2,2)$	2	$486, 612$
		$\mathcal{H}(3,1)$	1	2560
		$\mathcal{H}(3,2,1)$	1	5760
		$\mathcal{H}(3,3)$	2	$864, 4320$
		$\mathcal{H}(4)$	4	$25, 90, 135, 940$
		$\mathcal{H}(4,1,1)$	2	$460, 3980$
		$\mathcal{H}(4,2)$	4	$300, 315, 3120, 6300$
		$\mathcal{H}(5,1)$	1	12960
		$\mathcal{H}(6)$	5	$231, 252, 574, 3304, 5964$
		$\mathcal{H}(8)$	5	$243, 432, 567, 7452, 9288$

Bibliography

[1] Sergei I. Adian, *The Burnside problem and identities in groups*, Nauka, Moscow, 1975 (Translated by J. Lennox and J. Wiegold, Ergebnisse der Mathematik und ihrer Grenzgebiete 95, Springer-Verlag, Berlin, 1979.). 4.2.9

[2] Emil Artin, *Geometric algebra*, Wiley - Interscience Publishers Inc., New York, 1988. 3.2

[3] Artur Avila, Sébastien Gouëzel, and Jean-Christophe Yoccoz, *Exponential mixing for the Teichmüller flow*, Publications Mathématiques de L'IHÉS **104** (2006), no. 1, 143–211. 2.5

[4] László Babai, *On the order of uniprimitive permutation groups*, The Annals of Mathematics **113** (1981), no. 3, 553–568. 2.6

[5] ———, *On the order of doubly transitive permutation groups*, Inventiones Mathematicae **65** (1982), no. 3, 473–484. 2.6

[6] ———, *The probability of generating the symmetric group*, Journal of Combinatorial Theory (Series A) **52** (1989), 148–153. 2.3

[7] Homer Bechtell, *Theory of Groups*, Addison-Wesley Educational Publishers Inc, 1971. 4.2.10

[8] H. Behr and J. L. Mennicke, *A presentation of the groups* $\mathrm{PSL}(2,p)$, Canadian Journal of Mathematics **20** (1968), 1432–1438. 8

[9] Arthur T. Benjamin, Curtis T. Bennett, and Florence Newberger, *Recounting the odds of an even derangement*, Mathematics Magazine **78** (2005), no. 5, 387–390. 11

[10] Edward Bertram, *Even permutations as a product of two conjugate cycles*, Journal of Combinatorial Theory (Series A) **12** (1972), no. 3, 368–380. 3, 4.2.12

[11] Spencer Bloch and Andrei Okounkov, *The character of the infinite wedge representation*, Advances in Mathematics **149** (2000), no. 1, 1–60. 3.4

[12] J. N. Bray, M. D. E. Conder, C. R. Leedham-Green, and E. A. O'Brien, *Short presentations for alternating and symmetric groups*, Transactions of the American Mathematical Society **363** (2011), no. 6, 3277–3285. 4.2.12

[13] William Burnside, *On an unsettled question in the theory of discontinuous groups*, Quarterly Journal of Pure and Applied Mathematics (London) **33** (1902), 230– 238. 4.2.9

[14] ———, *Theory of groups of finite order*, 2nd ed., Dover Publications, 1955. 3.2, 3.2

[15] Peter J. Cameron, *Permutation groups*, London Mathematical Society Student Texts, vol. 45, Cambridge University Press, Cambridge, 1999. 3.3

[16] Colin M. Campbell, *Symmetric presentations and linear groups*, Finite Groups – Coming of Age: Proceedings of the Canadian Mathematical Society conference, Contemporary Mathematics, vol. 45, AMS, 1982, pp. 33–39. 8

[17] Colin M. Campbell and Peter P. Campbell, *On the minimal length of semigroup presentations*, Novi Sad Journal of Mathematics **34** (2004), no. 2, 17–26. 8

[18] Colin M. Campbell, George Havas, Colin Ramsay, and Edmund F. Robertson, *Nice efficient presentions for all small simple groups and their covers*, LMS Journal of Computation and Mathematics **7** (2004), 266–283. 4.2.12

[19] Robert D. Carmichael, *Abstract definitions of the symmetric and alternating groups and certain other permutation groups*, The Quarterly Journal of Mathematics **49** (1923), 226–270. 4.2.12

[20] D. J. Collins, R. I. Grigorchuk, P. F. Kurchanov, and H. Zieschang, *Combinatorial group theory and applications to geometry*, (2nd printing) 1st ed., Springer, Berlin - Heidelberg, 1998. 2.4

[21] Harold S. M. Coxeter and William O. J. Moser, *Generators and Relations for Discrete Groups*, 3rd ed., Springer-Verlag, Berlin - Heidelberg - New York, 1972. 4.2.12

[22] József Dénes, Paul Erdős, and Paul Turán, *On some statistical properties of the alternating group of degree n*, L'Enseignement mathématique **15** (1969), 88–99. 4.2.12

[23] Robbert Dijkgraaf, *Mirror symmetry and elliptic curves*, The Moduli Space of Curves (R. Dijkgraaf, C. Faber, and G. van der Geer, eds.), Progress in Mathematics, vol. 129, Birkhäuser, 1995. 3.4

[24] John D. Dixon, *The probability of generating the symmetric group*, Mathematische Zeitschrift **110** (1969), 199–205. 2.3

[25] John D. Dixon and Brian Mortimer, *Permutation groups*, Graduate Texts in Mathematics, vol. 163, Springer-Verlag, New York, 1996. 2.3, 2.8, 3.2, 3.2, 3.3, 3.4, 5.2.2

[26] Walther Dyck, *Gruppentheoretische Studien*, Mathematische Annalen **20** (1882), no. 1, 1–44. 2.4

[27] D. B. A. Epstein, *Finite presentations of groups and 3-manifolds*, The Quarterly Journal of Mathematics **12** (1961), no. 1, 205–212. 4.2.12

[28] Alex Eskin, Howard Masur, and Martin Schmoll, *Billiards in rectangles with barriers*, Duke Mathematical Journal **118** (2003), no. 3, 427–463. 3.1

[29] Martin J. Evans, *Problems concerning generating sets for groups*, Ph.D. thesis, University of Wales, Wales, 1985. 4.2.11

[30] Shelly Garion and Aner Shalev, *Commutator maps, measure preservation and T-systems*, Transactions of the American Mathematical Society **361** (2009), no. 9, 4631–4651. 2.4, 4.2.12

[31] Robert D. Girse, *The number of conjugacy classes of the alternating group*, BIT Numerical Mathematics **20** (1980), no. 4, 515–517. 4.2.12

[32] Henry Glover and Denis Sjerve, *The genus of* $\mathrm{PSL}_2(q)$, Journal für die reine und angewandte Mathematik (Crelle's Journal) **380** (1987), 59–86. 3.2

[33] R. M. Guralnick, W. M. Kantor, M. Kassabov, and A. Lubotzky, *Presentations of finite simple groups: a quantitative approach*, Journal of the American Mathematical Society **21** (2008), no. 3, 711–774. 4.2.12

[34] Robert Guralnick and Igor Pak, *On a question of B. H. Neumann*, Proceedings of the American Mathematical Society **131** (2003), no. 7, 2021–2025. 2.4, 4.2.11

[35] Eugene Gutkin and Chris Judge, *The geometry and arithmetic of translation surfaces with applications to polygonal billiards*, Mathematical Research Letters **3** (1996), 391–403. 2.5

[36] ———, *Affine mappings of translation surfaces: geometry and arithmetic*, Duke Mathematical Journal **103** (2000), no. 2, 191–213. 2.5

[37] Richard K. Guy, *Unsolved problems in number theory*, 3rd ed., Problem Books in Mathematics, Springer, New York, 2004. 10

[38] Philip Hall, *The Eulerian function of a group*, The Quarterly Journal of Mathematics (Oxford Ser.) **7** (1936), 134–151. 4.2.12, 5.2.2

[39] Godfrey H. Hardy and Srinivasa Ramanujan, *Asymptotic formulae in combinatory analysis*, Proceedings of the London Mathematical Society **s2-17** (1918), no. 1, 75–115. 4.2.12

[40] Frank Herrlich, *Teichmüller curves defined by characteristic origamis*, Contemporary Mathematics (2006), no. 397, 133–144. 4.2.3

[41] Frank Herrlich and Gabriela Schmithüsen, *An extraordinary origami curve*, Mathematische Nachrichten **281** (2008), no. 2, 219 – 237. 4.2.4

[42] Osamu Higuchi and Izumi Miyamoto, *The 2-generators for certain simple permutation groups of small degree*, SUT Journal of Mathematics **34** (1998), no. 1, 63–74. 4.2.12, 5.2.2

[43] Otto Hölder, *Bildung zusammengesetzter Gruppen*, Mathematische Annalen **46** (1895), no. 3, 321–422. 3.7, 3.2

[44] Pascal Hubert and Samuel Lelièvre, *Noncongruence subgroups in $\mathcal{H}(2)$*, International Mathematics Research Notices **2005** (2005), no. 1, 47–64. 3.1

[45] ———, *Prime arithmetic Teichmüller discs in $\mathcal{H}(2)$*, Israel Journal of Mathematics **151** (2006), 281–321. 1.1, 1.2, 2.5, 3.1

[46] Pascal Hubert and Thomas Schmidt, *An introduction to Veech surfaces*, Handbook of Dynamical Systems (B. Hasselblatt and A. Katok, eds.), vol. 1B, Elsevier Science Ltd, 2006, pp. 501–526. 2.5

[47] Bertram Huppert, *Endliche Gruppen*, vol. 1, Springer, Berlin, 1967. 4.2.12

[48] Bertram Huppert and Norman Blackburn, *Finite Groups III*, Springer-Verlag, Berlin - Heidelberg - New York, 1982. 2

[49] Dale H. Husemoller, *Ramified coverings of Riemann surfaces*, Duke Mathematical Journal **29** (1962), no. 1, 167–174. 3

[50] I. M. Isaacs and Thilo Zieschang, *Generating symmetric groups*, The American Mathematical Monthly **102** (1995), no. 8, 734–739. 2.2, 2.3

[51] D. L. Johnson, *Presentations of groups*, 2nd revised ed., London Mathematical Society Student Texts, no. 15, Cambridge University Press, 1997. 4.2.10, 4.2.10

[52] Camille Jordan, *Sur la limite de transitivité des groupes non alternés*, Bulletin de la Société Mathématique de France **1** (1873), 40–71. 2.5

[53] ———, *Sur la limite du degré des groupes primitifs qui contiennent une substitution donnée*, Journal für die reine und angewandte Mathematik (Crelle's Journal) **79** (1875), 248–258. 1.1, 1.2, 3.4

[54] Marshall Hall Jr., *Solution of the Burnside problem for exponent six*, Illinois Journal of Mathematics **2** (1958), no. 4B, 764–786. 4.2.9, 4.2.9

[55] ———, *Notes on groups of exponent four*, Conference on Group Theory, vol. 319, Springer, Berlin - Heidelberg, 319 1973, pp. 91–118. 4.2.9

[56] Karsten Kremer, *Invariants of complex and p-adic origami-curves*, Ph.D. thesis, Universität Karlsruhe (TH), Karlsruhe, 2009. 4.1

[57] Emmanuel Lecouturier and David Zmiaikou, *On a conjecture of H. Gupta*, Submitted to Discrete Mathematics in September 2010. (document)

[58] Samuel Lelièvre and Emmanuel Royer, *Orbitwise countings in $\mathcal{H}(2)$ and quasimodular forms*, International Mathematics Research Notices **2006** (2006), 30 pp., doi:10.1155/IMRN/2006/42151. 3.1

[59] Friedrich Levi and B. L. van der Waerden, *Über eine besondere Klasse von Gruppen*, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg **9** (1933), no. 1, 154–158. 4.2.9

[60] Pierre Lochak, *On arithmetic curves in the moduli spaces of curves*, Journal de l'Institut Mathematiques de Jussieu **4** (2005), no. 3, 443–508. 1.1, 1.2

[61] Roger C. Lyndon and Paul E. Schupp, *Combinatorial group theory*, Springer-Verlag, Berlin - Heidelberg - New York, 1977. 2.4

[62] Wilhelm Magnus, Abraham Karrass, and Donald Solitar, *Combinatorial group theory: Presentations of groups in terms of generators and relations*, Dover Publications, New York, 2004. 2.4, 2.4, 4.1

[63] Gunter Malle, Jan Saxl, and Thomas Weigel, *Generation of classical groups*, Geometriae Dedicata **49** (1994), no. 1, 85–116. 2.8

[64] Bernhard Marggraf, *Über primitive Gruppen mit transitiven Untergruppen geringeren Grades*, Inaugural-Dissertation, Giessen, 1892. 3.9

[65] Howard Masur, *Interval exchange transformations and measured foliations*, The Annals of Mathematics **115** (1982), no. 1, 169–200. 2.5

[66] Darryl J. McCullough and Marcus Wanderley, *Writing elements of* $\mathrm{PSL}(2,q)$ *as commutators*, to appear in *Communications in Algebra*, March 2008. 3.11, 4.2.11

[67] Curtis T. McMullen, *Teichmüller curves in genus two: discriminant and spin*, Mathematische Annalen **333** (2005), 87–130. 1.1, 1.2, 3.1

[68] ———, *Dynamics of $SL_2(\mathbb{R})$ over moduli space in genus two*, The Annals of Mathematics **165** (2007), no. 2, 397–456. 2.5

[69] Yair Minsky and Barak Weiss, *Nondivergence of horocyclic flows on moduli space*, Journal für die reine und angewandte Mathematik (Crelle's Journal) (2002), no. 552, 131–177. 2.5

[70] Martin Möller, *Affine groups of flat surfaces*, Preprint (https://titus.uni-frankfurt.de/fb/fb12/mathematik/ag/personen/moeller/summaries/styled_affine_groups.pdf). 2.5

[71] Jitsuro Nagura, *On the interval containing at least one prime number*, Proceedings of the Japan Academy **28** (1952), no. 4, 177–181. 4.2.12

[72] Eugen Netto, *The theory of substitutions and its applications to algebra*, Ann Arbor, Michigan, 1982. 2.3

[73] Bernhard H. Neumann and Hanna Neumann, *Zwei Klassen charakteristischer Untergruppen und ihre Faktorgruppen,*, Mathematische Nachrichten **4** (1951), 106–125. 2.4, 4.2.12, 5.2.2

[74] Bernhard Hermann Neumann, *Groups covered by finitely many cosets*, Publicationes Mathematicae Debrecen **3** (1954), 227–242. 3.3

[75] Jacob Nielsen, *Die Isomorphismen der allgemeinen, unendlichen Gruppe mit zwei Erzeugenden*, Mathematische Annalen **78** (1917), 385–397. 2.4

[76] ———, *Ober die isomorphismen unendlicher gruppen ohne relation*, Mathematische Annalen **79** (1918), 269–272. 2.4

[77] Petr S. Novikov and Sergei I. Adjan, *Infinite periodic groups i, ii, iii*, Mathematics of the USSR Izvestiya **2** (1968), 209–236, 241–479, 665–685. 4.2.9

[78] Øystein Ore, *Some remarks on commutators*, Proceedings of the American Mathematical Society **2** (1951), no. 2, 307–314. 3, 4.2.12

[79] Igor Pak, *What do we know about the product replacement algorithm?*, Groups and Computation, vol. III, de Gruyter, Berlin, 2001, pp. 301–347. 2.4

[80] László Pyber, *On the orders of doubly transitive permutation groups, elementary estimates*, Journal of Combinatorial Theory (Series A) **62** (1993), no. 2, 361–366. 2.6

[81] Joseph J. Rotman, *An introduction to the theory of groups*, 4th ed., Graduate Texts in Mathematics, vol. 148, Springer-Verlag, New York, 1999. 3.2

[82] Ivan N. Sanov, *Solution of Burnside's problem for $n = 4$*, Leningrad State University Annals (Uchenyi Zapiski) Math. Ser. **10** (1940), 166–170. 4.2.9

[83] Gabriela Schmithüsen, *An algorithm for finding the Veech group of an origami*, Experimental Mathematics **13** (2004), no. 4, 459–472. 4.1, 5.1

[84] ———, *Veech groups of origamis*, Ph.D. thesis, Universität Karlsruhe (TH), Karlsruhe, 2005. (document), 4.1

[85] ———, *Origamis with non congruence veech groups*, Proceedings of 34th Symposium on Transformation Groups (T. Kawakami, ed.), 2007, pp. 31 – 55. 4.2.7

[86] O. Schreier and B. L. van der Waerden, *Die automorphismon der projektiven gruppen*, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg **6** (1928), no. 1, 303–322. 5.6

[87] Issai Schur, *Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen*, Journal für die reine und angewandte Mathematik (Crelle's Journal) **132** (1907), 85–137. 4.2.12

[88] ———, *Über die Darstellung der symmetrischen und der alternierenden Gruppe durch gebrochene lineare Substitutionen*, Journal für die reine und angewandte Mathematik (Crelle's Journal) **139** (1911), 155–250. 4.2.12

[89] Daniel Stork, *The action of the automorphism group of F_2 upon the A_6- and* $\mathrm{PSL}(2,7)$*-defining subgroups of F_2*, Transactions of the American Mathematical Society **172** (1972), 111–117. 2.4, 4.2.12

[90] J. G. Sunday, *Presentations of the groups* $\mathrm{PSL}(2,m)$ *and* $\mathrm{SL}(2,m)$, Canadian Journal of Mathematics **24** (1972), no. 6, 1129–1131. 8

[91] Michio Suzuki, *Group Theory*, vol. 1, Springer-Verlag, 1982. 3

[92] William P. Thurston, *On the geometry and dynamics of diffeomorphisms of surfaces*, Bulletin of the American Mathematical Society **19** (1988), 417–431, (this paper was actually written around 1976). 1.1, 1.2

[93] Seán Tobin, *On groups with exponent 4*, Ph.D. thesis, University of Manchester, 1954. 4.2.9

[94] William A. Veech, *Gauss measures for transformations on the space of interval exchange maps*, The Annals of Mathematics **115** (1982), no. 2, 201–242. 2.5

[95] ———, *Teichmüller curves in moduli space, Eisenstein series and an application to triangular billiards*, Inventiones Mathematicae **97** (1989), no. 3, 553–583. 1.1, 1.2, 2.5

[96] Yaroslav Vorobets, *Planar structures and billiards in rational polygons: the Veech alternative*, Russian Mathematical Surveys **51** (1996), no. 5, 779–817. 2.5

[97] Donald D. Wall, *Fibonacci series modulo m*, The American Mathematical Monthly **67** (1960), no. 6, 525–532. 4.2.11

[98] Helmut Wielandt, *Finite permutation groups*, Academic Press, New York, 1964. 2.3, 3.2

[99] P. D. Williams, *Presentations of linear groups*, Ph.D. thesis, University of St Andrews, 1982. 8

[100] Heiner Zieschang, *Generators of the free product with amalgamation of two infinite cyclic groups*, Mathematische Annalen **227** (1977), no. 3, 195–221. 2.4

[101] Thilo E. Zieschang, *Primitive permutation groups containing a p-cycle*, Archiv der Mathematik **64** (1995), no. 6, 471–474. 3.10

[102] Anton Zorich, *Flat surfaces*, Frontiers in Number Theory, Physics, and Geometry I: On Random Matrices, Zeta Functions, and Dynamical Systems (P. Cartier, B. Julia, P. Moussa, and P. Vanhove, eds.), vol. I, Springer-Verlag, 2nd ed., 2006, pp. 437–583. 2.5

Index

U

V

W