



Combinatorial enumeration of cyclic covers of \mathbb{P}^1

Alberto BESANA¹ , Cristina MARTINEZ^{2,*} 

¹Dublin Business School, Dublin 2, Ireland

²Bank of America, Merrill Lynch, Dublin, Ireland

Received: 21.10.2016

Accepted/Published Online: 21.05.2018

Final Version: 24.07.2018

Abstract: We study plane algebraic curves defined over a field k of arbitrary characteristic that are ramified coverings of the projective line $\mathbb{P}^1(k)$ branched over a given configuration of distinct points by their ramification type specified by a partition of d the degree of the covering. We enumerate them by using the combinatorics of partitions and its connection to the representation theory of the symmetric group.

Key words: Algebraic curve, covering, symmetric group

1. Introduction

In the present paper we study the connection between plane curves and coverings of the projective line defined over a field k of arbitrary characteristic and their relations with the combinatorics of Hurwitz numbers. In particular, we study curves of the form

$$y^d = (x - a_1)^{m_1} \cdots (x - a_r)^{m_r}, \quad (1)$$

for given d, r and m_i , integer numbers. It is easy to see that these curves correspond to coverings of \mathbb{P}^1 with Galois group the cyclic group \mathbb{Z}_d of order d acting by multiplication with a d -root of unity on the coordinate y and with ramification at the points a_i . The data defining such a covering are encoded by a partition of length d . If d, r , and m_i are coprime numbers, the corresponding field extension $k(x) \hookrightarrow k(x, y)$ is a Kummer extension of the rational function field $k(x)$.

The Galois group of the plane curve C_f with the affine model defined by equation (1) is the Galois group of the polynomial

$$f(x) = (x - a_1)^{m_1} \cdots (x - a_r)^{m_r},$$

that is, the automorphism group $\text{Aut}(k(R_f)/k)$, where R_f denotes the set of branched points of the associated covering map $\pi : C_f \rightarrow \mathbb{P}^1$.

The Galois group of the curve C_f is a quotient of the automorphism group $\text{Aut}(C_f)$ of the curve and if it contains a cyclic subgroup \mathbb{Z}_p , where p is a prime number, such that the quotient curve C_f/\mathbb{Z}_p has genus 0, then the curve is called a cyclic p -gonal curve. If in addition \mathbb{Z}_p is normal in $\text{Aut}(C_f)$, then C_f is called

*Correspondence: cristinamartine@gmail.com

2010 AMS Mathematics Subject Classification: 05E15, 05A17

a normal cyclic p -gonal curve. In this case, the reduced automorphism group $\overline{\text{Aut}}(C_f) := \text{Aut}(C_f)/\mathbb{Z}_p$ is isomorphic to a finite subgroup of $\text{PGL}_2(k)$.

We study curves with Galois group S_n and their invariant fields under the action of finite subgroups of S_n . In particular, we consider the locus of curves X with reduced automorphism group isomorphic to one of the ternary groups $\mathbb{Z}_2 \times \mathbb{Z}_2, A_4, A_5, S_4$ or the dihedral group D_n .

In order to relate the moduli space of cyclic covers $\mathcal{R}_{g,n}$ [3], with the moduli of curves \mathcal{M}_g , we consider first the variety $\mathcal{C}_{d,m}$ parameterizing the curves $C_{f,d}$, that is, the parameter space of coefficients of the equations of the form (1). This is a Zariski open set in \mathbb{A}_k corresponding to the complement $V(D)$, where D is a suitable discriminant and itself an algebraic variety with coordinate ring $k[x_1, \dots, x_d]_D$. All the curves corresponding to points in $\mathcal{C}_{d,m}$ have the same genus g . The moduli space $H_{g,d}$ of pairs $(C_{f,d}, \pi : C \rightarrow \mathbb{P}^1)$ is a Hurwitz space.

The main contribution of the paper is Theorem 3.10, which realizes any cyclic covering of \mathbb{P}^1 over a field k of characteristic $p \geq 0$ as a plane curve of genus g and degree d defined by its ramification type above ∞ specified by the data of a partition of d .

In section 4, we study the enumerative problem of counting degree d coverings of \mathbb{P}^1 by distinguishing on the number of ramification points. The enumeration of coverings of the complex projective line with profile μ over ∞ and simple ramification over a fixed set of finite points is done by direct calculation in the Gromov–Witten theory of \mathbb{P}^1 . These numbers are known as Hurwitz numbers and arise as intersections in $\overline{\mathcal{M}}_{g,n}(\mathbb{P}^1)$. In Proposition 4.1 algebraic curves satisfying certain geometrical conditions are realized as cyclic coverings with profile over 0 and ∞ described by two partitions of d . The combinatorial enumeration of cyclic covers of \mathbb{P}^1 in Proposition 4.4 is done by counting conjugacy classes of permutations in the symmetric group. Finally, in proposition 4.6 the number of d -sheeted covers of \mathbb{P}^1 is expressed in terms of weighted cardinality of the moduli space of curves $\mathcal{M}_{g,n}$.

Conventions

For d a positive integer, let $\alpha = (\alpha_1, \dots, \alpha_m)$ be a partition of d into m parts with $\alpha_1 \geq \alpha_2 \geq \dots \geq \alpha_k$. We set $l(\alpha) = m$ for the length of α , that is the number of cycles in α , and l_i for the length of α_i . The notation (a_1, \dots, a_k) stands for a permutation in S_d that sends a_i to a_{i+1} . For us, scheme means separated scheme of finite type over an algebraically closed field k . A curve is an integral scheme of dimension 1, proper over k .

We write $\text{PGL}(2, k) = \text{GL}(2, k)/k^*$, and elements of $\text{PGL}(2, k)$ will be represented by equivalence classes of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

We will denote the greatest common divisor of two integers a and b as (a, b) .

2. Polynomial invariants under the action of a finite group

Let k be an algebraically closed field of characteristic $p \geq 0$. Let V be a finite dimensional k -vector space equipped with a linear action, that is, G acts via a representation $G \rightarrow \text{GL}(V)$. Fix a basis z_1, \dots, z_n for V ; in particular z_1, \dots, z_n can be thought as formal variables of degree one and the polynomial algebra over k on V is the polynomial ring $k[V] = k[z_1, \dots, z_n]$.

The action of G induces a natural action on the polynomial ring $k[V] \cong \text{Sym}(V^*)$. The coordinate ring of invariant polynomials $k[V]^G$ is finitely generated as an algebra, for some homogeneous polynomials called G -in-

variants. The locus $V(f_1, \dots, f_r)$ defined by the invariant polynomials is an algebraic variety X with coordinate ring $k[z_1, \dots, z_n]^G$. The affine scheme $\text{Spec}(k[V]^G)$ is an affine geometric invariant theory GIT quotient and is denoted by $X//G$. Moreover, as $k[V]^G$ is a graded ring, $(k[V]^G)$ one obtains a projective GIT quotient by taking the functor Proj . The function field of X is defined as the quotient field $k(z_1, \dots, z_n)/(f_1, \dots, f_r)$, where $k(z_1, \dots, z_n)$ is the function field of the projective space $\mathbb{P}^n(k)$, and (f_1, \dots, f_r) is the ideal generated by the polynomials f_1, \dots, f_r .

When G has a polynomial ring of invariants, we define the Jacobian determinant $J = J(f_1, \dots, f_n) = \det(\frac{\partial f_i}{\partial z_j})$. This polynomial is nonzero and well defined up to a nonzero element of \mathbb{C} depending on the choice of basic invariants of a basis $\{z_j\}$ of V^* .

When does G have a polynomial ring of invariants? Serre showed that in arbitrary characteristic every finite subgroup of $\text{GL}(V)$ with a polynomial ring of invariants must be generated by reflections (see [14]). The converse may fail when the characteristic of the field divides the order of G .

The ring of polynomials in n variables with complex coefficients admits a natural action of the orthogonal group $\text{SO}(n)$. We can also study the action of finite subgroups G of $\text{SO}(n)$ and give generators for the spaces $\mathbb{C}[x_0, \dots, x_n]_j^G$ of homogeneous G -invariant polynomials of degree j . We can even compute their dimension by considering the Poincaré series

$$p(t) := \sum_{j=0}^{\infty} \dim \mathbb{C}[x_0, \dots, x_n]_j^G \cdot t^j.$$

It can be written as

$$p(t) = \frac{1}{|G|} \sum \frac{n_g}{\det(g - 1 \cdot t)},$$

where the sum runs over all the conjugacy classes of G and n_g denotes the number of their elements.

We define the polynomials $f(x) = x^n + a_1x^{n-1} + \dots + a_n$, with $a_i \in \mathbb{Q}$, and $f(x, t) = f(x) - t$. Then, if f is a separable polynomial, the Galois group of $f(x, t)$ over $k(t)$ is a regular extension with Galois group S_n .

Example 1 Let $G = S_n$ acting on $\mathbb{Q}(x_1, \dots, x_n)$. Observe that $\mathbb{Q}(x_1, \dots, x_n)$ is the function field of an $(n-1)$ -dimensional projective space $\mathbb{P}^{n-1}(\mathbb{Q})$ over \mathbb{Q} . Suppose that z_1, \dots, z_n are the roots of f in a splitting field of f over \mathbb{Q} . Each coefficient a_i of x^i in f is symmetric in z_1, \dots, z_n ; thus by the theorem on symmetric functions, we can write a_i as a symmetric polynomial in z_1, \dots, z_n with rational coefficients. On the other side, for a permutation $\sigma \in S_n$, set $E_\sigma = x_1z_{(\sigma(1))} + \dots + x_nz_{(\sigma(n))}$ in $\mathbb{Q}(x_1, \dots, x_n)$ and $f(x) = \prod_{\sigma} (x - E_\sigma)$, where σ runs through all permutations in S_n .

Theorem 2.1 (Serre) *The field E of S_n -invariants is $\mathbb{Q}(t_1, \dots, t_n)$, where t_i is the i^{th} symmetric polynomial in x_1, \dots, x_n , and $\mathbb{Q}(x_1, \dots, x_n)$ has Galois group S_n over E : it is the splitting field of the polynomial*

$$f(x) = x^n - t_1x^{n-1} + t_2x^{n-2} + \dots + (-1)^n t_n.$$

In particular, if we consider $f(x, y)$ as a polynomial in $\mathbb{F}_q[x, y]$ and we apply Theorem 2.1 to the i^{th} elementary symmetric polynomial in the n symbols $x, x^q, x^{2q}, \dots, x^{q^{n-1}}$, we get that the field of S_n -invariants

is an extension \mathbb{F}_{q^n} of \mathbb{F}_q . Moreover, due to a result given by Ling et al. [10], if $f \in \mathbb{F}_q[x]$ and $\beta \in \mathbb{F}_q^s$, then $f(\beta) = 0$ if and only if $f(\beta^{q^i}) = 0$ of all $0 \leq i \leq s - 1$. In particular, this result is very useful when we consider cyclic coverings of the projective line defined over finite fields.

Example 2 *Dihedral invariants.* A dihedral group is the group of symmetries of a regular polygon, including both rotations and reflections. The Dihedral group D_s is generated by a rotation τ of order s , and a reflection σ of order 2, such that $\sigma\tau\sigma = \tau^{-1}$. In geometric terms, in the mirror a rotation looks like an inverse rotation. The action of the Dihedral group D_s on $\mathbb{C}(x_1, \dots, x_s)$ is given by

$$\begin{aligned} \tau : x_j &\mapsto \epsilon^i x_j, \quad \text{for } i = 1, \dots, \lfloor \frac{s}{2} \rfloor, \\ \sigma : x_i &\mapsto x_{s-i}, \quad \text{for } i = 0, \dots, \lfloor \frac{s}{2} \rfloor, \end{aligned}$$

where ϵ is an s primitive root of unity.

If $s = 1$, then the above actions are trivial. If $s = 2$, then $\tau(x_1) = -x_1, \tau_1(x_2) = x_2, \tau_2 = Id$, and the action is not dihedral but cyclic on the first factor.

We need to find the invariant polynomials in the coordinates (x_1, \dots, x_s) by the action of the Dihedral group. Let $s > 2$ and then the elements

$$\begin{aligned} u_i(x_1, \dots, x_s) &:= x_1^{s-i} x_i + x_{s-1}^{s-i} x_{s-i}, \\ u_{s-i}(x_1, \dots, x_s) &:= x_1^i x_{s-i} + x_{s-1}^i x_i, \end{aligned}$$

for $1 \leq i \leq s$, are invariant polynomials under the action of the group D_s defined above. The elements u_i are called the dihedral invariants of D_s .

3. Cyclic coverings of \mathbb{P}^1 with prescribed ramification

Let $k(x)$ be the function field of the projective line and consider a finite Galois extension E of $k(x)$ with group G which is regular, i.e. $\bar{k} \cap E = k$. Moreover, given a set $S = \{a_1, \dots, a_n\} \subseteq \mathbb{A}^1(k) \subseteq \mathbb{P}^1(k)$, there is a correspondence between isomorphism classes of Galois extensions of $k(x)$ with Galois group G and branch points contained in S .

Lemma 3.1 *Let $G = \text{Gal}(E/k(x))$ be the Galois group of the extension. The inclusion $k(x) \hookrightarrow E$ corresponds to a (branched) Galois covering $C \rightarrow \mathbb{P}^1$ defined over k with Galois group G .*

Proof Geometrically, E can be viewed as the function field $k(C)$ of a smooth projective curve C that is absolutely irreducible over k , i.e. y satisfies an algebraic equation over $k[x, t]$

$$\{(x, t) \in k^2 \mid f(x, t) = 0\},$$

where $f(x, t) = \sum_{i=1}^m \sum_{j=1}^n x^i y^j = \sum_{j=1}^n a_j(x) y^j = 0$ is an irreducible polynomial in x and y . We assume that not all a_{ij} vanish and that $a_n(x) = 1$ (which can be arranged by a change of variables). Thus n is the

degree of the polynomial in y . Since k is algebraically closed, at a generic point x there are n roots $y^{(k)}$, $k = 1, \dots, n$ which implies that the algebraic curve defines an n -sheeted ramified covering of the x -plane given by projecting over the x -axis. If the number of distinct roots $y^{(k)}$ is lower than the degree n , this means there are roots that occur with multiplicity greater than or equal to 2. \square

Conjecture 3.2 *Every finite group G occurs as the Galois group of such a covering.*

Let X be a smooth curve and $f : X \rightarrow \mathbf{P}^1$ a branched cover, and the ramification index at the branch point $y \in \mathbf{P}^1$ is the absolute value of the local degree of the map f at the point y . Analytically, the map looks locally like $y \rightarrow y^m$, $m > 1$.

The total ramification above a point of \mathbb{P}^1 is the sum of the ramification numbers of the branch loci mapping to that point. For any map f from a nodal curve to a nonsingular curve, the ramification number defines a divisor on the target:

$$\sum_L r_L f(L),$$

where L runs through the branch loci and r_L is the ramification index. The monodromy m_i of the branch point b_i is the permutation of L obtained by applying analytic continuation on L following a path from x_0 to b_i going around b_i counter-clockwise and returning to x_0 . The order of the branch points is chosen in such a way that the complex numbers b_i have increasing arguments. The monodromy group G is the permutation group generated by the m_i .

Definition 3.3 *Given a covering $\pi : C \rightarrow \mathbb{P}^1$ of degree d , the profile of π over a point $q \in \mathbb{P}^1$ is the partition η of d obtained by the multiplicities of $\pi^{-1}(q)$. If one of the multiplicities is different from 1, we say that q is a branched point. If η is the partition (1^d) with all its parts equal to the integer 1, we say that the covering simply ramifies at the point q . The data of the partition determines the ramification type of the covering at this point.*

Definition 3.4 *Two ramified coverings $(C_f; \pi_f)$ and $(C_g; \pi_g)$ are called topologically equivalent in the Zariski topology if there exists a homeomorphism $h : C_f \rightarrow C_g$ making the following diagram commutative:*

$$\begin{array}{ccc} C_f & \xrightarrow{h} & C_g \\ & \searrow \pi_f & \swarrow \pi_g \\ & \mathbb{P}^1 & \end{array}$$

In particular, the ramification points of the coverings coincide, as do the genera of the covering curves.

In the present paper we will concentrate in the case of *cyclic Galois coverings*. Namely, given a polynomial f in $k[x]$ of degree n with roots β_1, \dots, β_r repeated according to the multiplicity in the splitting field L of the extension of $f(x)$ over k , and a positive integer d , let $C_{f,d}$ be the smooth projective curve over k with affine model

$$y^d = f(x). \tag{2}$$

If the characteristic p of the field k is positive, in order to get a Galois extension, we will assume that p is relative prime to d . We denote by ξ_d a primitive d^{th} root in \bar{k} . Consider the natural action $(x, y) \rightarrow (x, \xi_d y)$

of the d^{th} roots of unity on $C_{f,d}$ over $k(\xi_q)$. In particular, we have that the Galois group of the extension $\text{Gal}(k(C_{f,d}/k(x)) \cong \mathbb{Z}_d$ is cyclic. It is a cyclic Galois covering of the projective line that ramifies exactly at the places $x = \beta_i$, and the corresponding ramification indices are defined by

$$e_i = \frac{d}{(d, d_i)},$$

with $d_i \in \mathbb{Z}$ the corresponding multiplicity of β_i in f . There are ramification points with different ramification behavior. The monodromy above ∞ defines the ramification type of the covering: it is determined by the Galois group of the extension and it is specified by a partition α of d .

As all the cyclic groups of order d are isomorphic, we will refer to the additive cyclic group \mathbb{Z}_d generated by the class of 1 modulo d or to the multiplicative group μ_d of roots of unity if we are interested in the multiplicative structure.

By the Riemann–Hurwitz formula, it follows that the function field \mathbb{F} has genus

$$g(\mathbb{F}) = 1 - d + \frac{1}{2} \sum_{i=1}^r (d - (d_i, d)). \tag{3}$$

We denote by R_f the set of roots of f in \bar{k} . The function field of the curve is $\mathbb{F} = k(x, y)$ where y satisfies the algebraic equation (2) over the algebra $k[x]$, that is, $k(C_f) = k(x, y)$. Observe that $\text{Gal}(\mathbb{F}/k(x)) \subseteq \text{Aut}(\mathbb{F})$.

We can consider the quotient surface C/G for any finite subgroup G of the automorphism group $\text{Aut}(\mathbb{F})$ of the curve $C_{f,d}$. As we have seen, C admits an automorphism τ of order d such that $C/\langle \tau \rangle$ is isomorphic to \mathbb{P}^1 . The quotient surface is obtained via uniformizing a neighborhood of 0 by $y \rightarrow y^d$; this means the surface has at least an orbifold point of order d . The uniformization induces naturally an orbifold structure on the hyperplane class bundle, such that the cyclic group \mathbb{Z}_d acts trivially on the corresponding bundle. The resulting orbifold bundle is denoted by $\mathcal{O}^{\text{unif}}(1)$.

Definition 3.5 *The Galois group of the curve $C_{f,d}$ is defined as the Galois group $\text{Gal}(f(x))$ of the polynomial $f(x)$, that is, the automorphism group $\text{Aut}(k(R_f/k))$.*

Definition 3.6 *The discriminant of the polynomial f is $\Delta = \delta^2$, where*

$$\delta = \prod_{1 \leq i < j \leq n} (\beta_j - \beta_i).$$

If f has a repeated root, then $\delta = 0$, and f is a separable polynomial if and only if $\delta \neq 0$.

Remark 3.1 In general the problem is reduced to study configurations $M_{0,n}$ of points in the affine line as the set of branch points for a ramified cover and in this way moduli of points lead naturally to moduli of positive genus algebraic curves M_g . In particular any cover that is simply ramified corresponds to an unordered tuple of n points in \mathbb{P}^1 . Thus, there is an isomorphism

$$\text{Sym}^n \mathbb{P}^1 \cong (\mathbb{P}^1)^n / S_n \cong k^n \setminus V_{D_n},$$

where V_{D_n} is the zero set of the discriminant of the polynomial. Since the symmetric group S_n is generated by 3 elements, a reflection of order 2, a symmetry of order 3, and a rotation of order n , the variety parameterizing S_n -covers is of dimension $n - 3$.

Remark 3.2 Alternatively $C_{f,d}$ may be seen as an unramified Galois covering of a Riemann surface. To describe the associated Riemann surface, one has to be able to identify the branching structure of the curve at the branch points, that is, one has to specify which sheets of the covering are connected in which way at a given branch point. This is equivalent to identifying the monodromy of the surface. Moreover, every Riemann surface arises as a quotient of one of the simply connected domains \mathbb{H}, \mathbb{C} , and \mathbb{P}^1 by a discrete subgroup of the group of its automorphisms. These discrete subgroups are the fundamental groups of the corresponding underlying Riemann surface (see [1]). The cyclic coverings studied here have genus greater or equal to 2 and are uniformized by the hyperbolic plane. Only rational curves have universal covering the projective line and only elliptic curves have universal covering the complex plane.

Let \mathbb{F}_0 be the fixed field \mathbb{F}^{μ_d} by the action of the cyclic group ξ_d . It is the rational function field $\mathbb{F}_0 = \mathbb{F}^{\mu_d}$ and $\text{Gal}(\mathbb{F}/\mathbb{F}_0)$ is the Galois group $\text{Gal}(C_f/\mathbb{P}_k^1)$ of the curve C_f that is the Galois group of the polynomial $f(x)$.

Let $\text{Gal}(\mathbb{F}/k(x)) = \langle \sigma \rangle$ with σ a generator of the Galois group, if $\tau \notin \text{Gal}(\mathbb{F}/k(x))$, τ is said to be an extra automorphism. There is an exact sequence:

$$1 \rightarrow \mu_d \rightarrow G \xrightarrow{\pi} G_0 \rightarrow 1,$$

where $G_0 = \text{Aut}(\mathbb{F})/\mu_d$ and $G = \text{Aut}(\mathbb{F})$. Moreover, if the extension splits then $G_0 \cong \text{Gal}(\mathbb{F}/\mathbb{F}_0)$ and $\text{Aut}(\mathbb{F}) \cong \mu_d \times G_0$. If $\langle \sigma \rangle$ is a normal subgroup of the whole automorphism group $\text{Aut}(\mathbb{F})/\langle \sigma \rangle$ we can consider the reduced group $\overline{G} = \text{Aut}(\mathbb{F})/\langle \sigma \rangle$, which is a finite subgroup of $\text{Aut}(\mathbb{P}_k^1) = \text{PGL}(2, k)$. In [9], some configuration spaces of Galois cyclic covers $X \rightarrow \mathbb{P}_k^1$ with cyclic Galois group $\text{Gal}(X/\mathbb{P}_k^1)$ are constructed generalizing the theory of hyperelliptic curves.

Let $b = \text{div}(f(x))_0$ be the root divisor of the polynomial $y^d = f(x)$ in $k(x)$. The ramifications are determined by the profile of the covering over the branch points. Any branch point is induced by a permutation in S_d . In particular, if a point is simply ramified its monodromy is determined by a simple transposition. If we vary a branch point of the curve C in \mathbb{P}^1 , we obtain a one-dimensional Hurwitz space parameterizing such coverings. Each conjugacy class in S_d determines a divisor class in the Hurwitz space of all degree d and fixed genus g connected coverings of \mathbb{P}^1 .

Definition 3.7 A ramification type is realizable if the Galois group $\text{Gal}(\mathbb{F}/\mathbb{F}_0)$ is a normal subgroup in the whole automorphism group $G = \text{Aut}(\mathbb{F})$.

Observe that any normal finite subgroup G_0 of $\text{Gal}(\mathbb{F}/\mathbb{F}_0)$ determines a ramification type.

Lemma 3.8 Any partition $\lambda = (\lambda_1, \dots, \lambda_m)$ of d into m parts corresponds to a degree d branched covering of \mathbb{P}^1 with monodromy above ∞ given by λ , and $r = d + m + 2(g - 1)$ other simple branch points and no other branching.

Proof For each partition $\lambda = (\lambda_1 \geq \dots \geq \lambda_m)$ in $\mathcal{P}(d)$, consider a configuration of points $\{p_1, \dots, p_m\}$ on the x -axis with coordinates

$$\{(x_1, 0), \dots, (x_m, 0)\} \subseteq k^* \times \{0\} \subset k^* \times k.$$

To this configuration of points there corresponds a unique polynomial

$$f(x) = (x - x_1)^{\lambda_1} \dots (x - x_m)^{\lambda_m} \in k[x]$$

that defines a covering of $\mathbb{P}^1(k)$. The divisor $D_\lambda = \sum_{i=1}^m \lambda_i p_i$ corresponds to a ramification type defining the profile of the covering at ∞ . Every permutation $\sigma \in S_d$ defines an automorphism of the covering acting by permuting the places corresponding to the points $p_i, i = 1, \dots, m$.

In particular, permutations in the same conjugacy class have the same cycle structure and thus give the same ramification type. □

Remark 3.3 Observe that if the base field k is of characteristic different from 0, then no configuration of points in the affine line $\mathbb{A}^1(k)$ as in Lemma 3.8 gives rise to a polynomial in $k[x]$.

Definition 3.9 A set of integers $R \bmod n$ is said to be a set of roots if it is the set of roots of some polynomial, that is, if it corresponds to R_f for some polynomial $f \in \mathbb{Z}[x]$.

Let $q = p^n$ and consider the Galois extension $\mathbb{F}_q/\mathbb{F}_p$ with Galois group the cyclic group of order n . According to the Chinese remainder theorem, finding and counting sets of roots $\bmod n$ reduces to compute roots modulo a prime power (see [12]). Indeed there is a functorial correspondence between polynomials in $\mathbb{Z}[x]$ modulo a prime and root sets.

On the other hand, the set of roots of a polynomial over \mathbb{Z} coincides with the set of roots of a polynomial over \mathbb{Q} , that is, every rational root of a polynomial in \mathbb{Z} is an integer.

Example 3 Consider the curve $C_{n,m}$ with affine equation $y^m + x^n = 1$ defined over a finite field \mathbb{F}_q of q elements, where q is a power of a prime and n, m are integer numbers greater than or equal to 2.

We denote by $F_{n,m}$ the function field $k(x, y)$ of $C(n, m)$, where $y^m + x^n = 1$. If $m|q^2 - 1$ then the points $P_0 = (\alpha, 0)$ and $P_1 = (\beta, 0)$ with $\alpha^m = 1$ and $\beta^n = 1$ are \mathbb{F}_{q^2} -rational points of the curve $C_{n,m}$ and the root divisors of the elements $x, y \in k(x, y)$ are expressed as $div(y)_0 = mP_0$ and $div(x)_0 = nP_1$. It is a cyclic covering of $\mathbb{P}^1(\mathbb{F}_{q^2})$ of degree d , the greatest common divisor of n and m . The Galois group is generated by two elements $g_1, g_2 \in \text{PSL}(2, q^2)$ of orders n and m respectively.

Theorem 3.10 Fix a genus g , a degree d , and a partition $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_m)$ of d . There is a branched covering $C_{\alpha,d}$ of \mathbb{P}^1 with $r = d + m + 2(g - 1)$, monodromy above ∞ defined by α , and no other specified simple branched points. Moreover, any such covering is induced by the conjugacy class of a subgroup S of $\text{PGL}(2, k)$. We recover any possible degree d , branched coverings of \mathbb{P}^1 by a genus g connected Riemann surface by realizing any normal subgroup of the Galois group $\text{Gal}(C_{\alpha,d}/\mathbb{P}^1)$.

Proof Any degree d irreducible cyclic covering C_d of the projective line, after a birational transformation, corresponds to a cyclic extension $k(x, z)$ of the rational function field $k(x)$ of degree d , where z satisfies an algebraic equation:

$$z^d := \prod_{i=1}^m (x - \rho_i)^{\alpha_i}, \quad 0 < \alpha_i < d. \tag{4}$$

If $n \equiv 0 \pmod{d}$, where $n := \sum_{i=1}^r d_i$, then the place at ∞ does not ramify at the above extension. The only places of $k(x)$ that are ramified are the places P_i that correspond to the points $x = \rho_i$. If the curve ramifies at ∞ , then $\alpha_i \geq 2$. If the multiplicity $d_j = 1$, then the point simply ramifies and the monodromy above the point is induced by a simple transposition.

If the covering ramifies only at 0 and there is no other branching, then $\text{Gal}(k(C_d/k(x)) \cong \mathbb{Z}_d$. In this case there is no ramification over ∞ (i.e. $\alpha = (1^m)$).

If C_d ramifies at ∞ , we recover all possible cases by projecting G/\mathbb{Z}_d into the known finite subgroups of $\text{PGL}(2, k)$, which constitutes the automorphism group of the rational function field. If k is algebraically closed, as we are only interested in enumerating all possible conjugacy classes that can appear and as the base field k contains all roots of unity, it is enough to determine all finite subgroups of $\text{PSO}(2)$, the special projective orthogonal group. By the classification theorem of finite simple groups of $\text{SO}(3)$, these are the ternary groups, which are known to be $\mathbb{Z}_2 \times \mathbb{Z}_2$, D_m , A_4 , A_5 , and S_4 . In addition we have all the finite cyclic subgroups of order p prime, corresponding to elements in $\text{PGL}(2, k)$ fixing just one point that we may assume is ∞ , and all the p regular cyclic subgroups of $\text{PGL}(2, k)$ corresponding to elements in $\text{PGL}(2, k)$ fixing two points, say 0 and ∞ . If k is arbitrary of positive characteristic $p > 0$, $\text{PGL}(2, k)$ is contained in $\text{PGL}(2, \bar{k})$, where \bar{k} denotes the algebraic closure of k . In this case, we must include all the finite groups isomorphic to $\text{PSL}(2, \mathbb{F}_q)$ or $\text{PGL}(2, \mathbb{F}_q)$ with q a prime power of p whenever the field k contains the finite group \mathbb{F}_q , as well as the conjugacy classes of elementary subgroups of order $p^m n$ with $n \in \mathbb{N}/p\mathbb{N}$ or a semidirect product of an elementary abelian group by a cyclic one. If $\chi + \chi^{-1} \in k$ for some primitive n -root of unity χ , then $\text{PGL}(2, k)$ contains all dihedral groups D_{2n} of order $2n$. If $q = q_1^l$ ($l \in \mathbb{N}$) we consider the subfield subgroup $\text{PGL}(2, \mathbb{F}_{q_1})$. \square

Example 4 We consider the roots of the polynomial $x^8 - 1 \in \mathbb{F}_5[x]$ in the splitting field \mathbb{F}_{5^2} . The decomposition into irreducible polynomials over $\mathbb{F}_5[x]$ is $(x-1)(x+1)(x-2)(x+2)(x^2+1)(x^2-2)(x^2+2)$. Now we consider the field extensions $F_1 := \mathbb{F}_5[x]/(x^2-2)$ and $F_2 := \mathbb{F}_5[x]/(x^2+2)$ of \mathbb{F}_5 that are isomorphic to the field extension \mathbb{F}_{25} of \mathbb{F}_5 . Call α the root of x^2-2 in the field extension F_1 ; then $4 \cdot \alpha$ is the other root of x^2-2 , and $2 \cdot \alpha$, $3 \cdot \alpha$ the roots of x^2+2 in F_1 . If we consider the factorization of the polynomial $x^8 - 1 = (x^2 - 1)(x^2 + 1)(x^4 + 1)$ over $\mathbb{F}_5[x]$, we see that the point $(\alpha, 0) \in \mathbb{P}(\mathbb{F}_q^2)$ with $\alpha^4 = 4$ is an \mathbb{F}_{25} -rational point of the affine curve $C : y^2 = (x^4 + 1)$. The other rational places are $(2, 0), (-2, 0)$ and the place $(0, \alpha)$ at ∞ . The Galois group $\text{Gal}(C/\mathbb{P}^1(\mathbb{F}_{25})) \cong \mathbb{Z}_2$.

Corollary 3.11 All the coverings of \mathbb{P}^1 that ramify over 3 points are encoded by the partitions of 3 parts: $(2, 2, n)$, for some $n \geq 2$, $(2, 3, 3)$, $(2, 3, 4)$, and $(2, 3, 5)$ induced by the groups generated by 2 of the 3 transpositions of S_3 . There are $\binom{3}{2}$ coverings of \mathbb{P}^1 that ramify over 3 fixed points.

Proof All the coverings of \mathbb{P}^1 that ramify over 3 points are induced by the two groups generated by 2 of the 3 transpositions of S_3 , that is $H_1 = \langle (12), (23) \rangle$ and the group $H_2 = \langle (23), (13) \rangle$. Thus the covering whose ramification is given by the 3 permutations (12) , (23) , and $(12)(23)$ in $H_1 = \langle (23), (13) \rangle$ has two simple branch points corresponding to the two transpositions and a branch point with multiplicity at least 3 corresponding to the permutation of order 3, (132) and all its powers. These coverings have ramification type above ∞ defined by the partition $(2, 2, n)$ corresponding to the orders of the three orbifold points and the Galois group is the dihedral group D_n . If we consider the group $H_2 = \langle (23), (13) \rangle$, we recover the other possible triangle groups A_4 , S_4 , and A_5 corresponding to the partitions $(2, 3, 3)$, $(2, 3, 4)$, and $(2, 3, 5)$. \square

Definition 3.12 A complex algebraic curve C will be termed triangle curve if it admits a finite group of

automorphisms $G < \text{Aut}(C)$ so that $C/G \cong \mathbb{P}^1$ and the natural projection

$$C \rightarrow C/G,$$

ramifies over 3 values, say $0, 1,$ and ∞ . In particular, if the group is the dihedral group D_n then the curve is called *dihedral covering*.

If the branching orders at these points are $p, q,$ and r we will say that C/G is an orbifold of type (p, q, r) . Due to a celebrated theorem by Belji [2], triangle curves are known to be defined over a number field. If the number of orbifold points is at least 3, we have the following possibilities for the orders of the orbifold points: $(2, 2, n)$, for some $n \geq 2$, $(2, 3, 3)$, $(2, 3, 4)$, and $(2, 3, 5)$.

The corresponding fundamental group is the dihedral, tetrahedral, or icosahedral group, respectively, and the universal covering is \mathbb{P}^1 . Any finitely generated discrete subgroup G of $\text{PSL}(2, \mathbb{R})$ is the fundamental group of an orbifold and hence it has a presentation of the form:

$$G = \langle a_1, b_1, \dots, a_g, b_g, c_1, \dots, c_k \mid c_1^{n_1} = c_2^{n_2} = \dots \\ \dots = c_k^{n_k} = 1, [a_1, b_1][a_2, b_2] \cdots [a_g, b_g]c_1c_2 \dots c_k = 1 \rangle.$$

4. Enumerative geometry of coverings of \mathbb{P}^1

4.1. Coverings of \mathbb{P}^1 with specified ramification above 0 and ∞

In this section, we will assume that the ground field k is the field of complex numbers \mathbb{C} . The problem of enumerating branched coverings of \mathbb{P}^1 is reduced to the combinatorial problem of studying factorizations $\sigma = \tau_1 \dots \tau_r$ into r transpositions for any $d, \sigma,$ and r [13]. The case in which there is no ramification at ∞ corresponds to the partition $\alpha = (1^d)$. Hurwitz numbers enumerate nonsingular, genus g curves expressible as d -sheeted coverings of \mathbb{P}^1 , with specified branching above one point, simple branching over other specified points, and no other branching.

Let d and $g \geq 0$ be integer numbers representing the degree and the genus of a covering of \mathbb{P}^1 , and let λ and ρ be partitions of d prescribing the profiles of the covering over 0 and ∞ . Each covering corresponds to a combinatorial object: a labeled graph with d vertices, $d + g - 1$ edges, and without loops.

A connected labeled floor diagram \mathcal{D} of degree d and genus g is a connected oriented graph $G = (V, E)$ on linearly ordered d -element vertex V , together with a weight function $w : \mathbb{E} \rightarrow \mathbb{Z}_{>0}$ such that the edge set E consists of $d + g - 1$ edges, and each edge in E is directed from a vertex u to a vertex $v > u$, expressing compatibility with linear ordering on V . The multiplicity $\mu(\mathcal{D})$ is the product of the squares of $w(e)$ for every edge $e \in E$, that is,

$$\mu(\mathcal{D}) = \prod_{e \in E} (w(e))^2.$$

Proposition 4.1 *Given λ and ρ two partitions of d , the set of irreducible complex algebraic curves*

- *of degree d and genus g passing through a generic configuration of $2d - 1 + g + l(\rho)$ points in \mathbb{C}^2*
- *having tangency to the x -axis for a given collection \mathcal{P}_λ of $l(\lambda)$ points in $\mathbb{C} \times \{0\}$ and other $l(\rho)$ points*

coincides with the set of irreducible plane curves γ of given degree and genus realizable as d -sheeted coverings of $\mathbb{P}^1(\mathbb{C})$ with ramification type at 0 and ∞ described by the partitions λ and ρ and simple ramification over the specified collection of points \mathcal{P}_λ .

Proof As we showed in Lemma 3, given an irreducible plane algebraic curve, if we impose the curve to pass through a generic point in the plane, we get a d -sheeted branched covering of $\mathbb{P}^1(\mathbb{C})$, by projecting onto the x -axis. Furthermore, we can recover the y -coordinates by taking d -roots of the x -coordinate. If the curve has a tangency to the x -axis at a generic point of affine coordinates $(x_i, 0)$, the corresponding sheeted covering is branched at this point with the same multiplicity. \square

Remark 4.2 The authors proved in [6] that the Gromov–Witten invariant $N_{d,g}$ representing the number of irreducible curves of degree d and genus g passing through a fixed generic configuration of $3d + g - 1$ points on \mathbb{P}^2 can be obtained by summing the product of corresponding multiplicities $\mu(\mathcal{D}) \cdot \nu(\mathcal{D})$ over all labeled floor diagrams \mathcal{D} of degree d and genus g . The numbers $N_{d,g}(\lambda, \rho)$ count irreducible plane curves γ of given degree and genus realizable as d -sheeted coverings of \mathbb{P}^1 with ramification type at 0 and ∞ described by the partitions μ and ν and simple ramification over other specified points. If λ and ρ are two partitions with $|\lambda| + |\rho| = d$, the number $N_{d,g}(\lambda, \rho)$ can be obtained by summing the multiplicities $\mu(\mathcal{D})\nu_{\lambda,\rho}(\mathcal{D})$, where $\nu_{\lambda,\rho}(\mathcal{D})$ is the multiplicity of a certain combinatorial decoration of a labelled floor diagram \mathcal{D} .

4.2. Coverings of \mathbb{P}^1 with 4 or more branch points

Let p_1, \dots, p_r be points in \mathbb{P}^1 and (s_1, \dots, s_r) a set of r permutations defined up to conjugation in S_d such that $s_1 s_2 \dots s_r = 1$. The cycle type defining each permutation s_i is encoded in a partition $\lambda^i = (\lambda_1^i, \dots, \lambda_m^i)$ of d , defining the ramification profile over p_i .

There are only finitely many coverings $H_d^{\mathbb{P}^1}(\lambda^1, \dots, \lambda^r)$ of the projective line up to isomorphism by smooth connected curves of specified degree and genus, and monodromy λ^i at p_i . Each covering π has a finite group of automorphisms $\text{Aut}(\pi)$. This number can be computed by operating in the group algebra $\mathbb{Q}S_d = \{\sum_{\sigma \in S_d} \lambda_\sigma \sigma, \lambda_\sigma \in \mathbb{Q}\}$ of S_d . Let $\mathcal{P}(d)$ denote the set of partitions of d indexing the irreducible representations of S_d . The class algebra $\mathcal{Z}_d \subset \mathbb{Q}S_d$ is the center of the group algebra. Let $c_\lambda \in \mathcal{Z}_d$ be the conjugacy class corresponding to the partition λ ; then

$$H_d^{\mathbb{P}^1}(\lambda^1, \dots, \lambda^r) = \frac{1}{d!} [C_{(1^d)}] \prod C_{\lambda^i}, \tag{5}$$

where $C_{(1^d)}$ stands for the coefficient of the identity class.

A labeled partition of d is a partition in which the terms are considered distinguished. For example, there are $\binom{7}{3}$ ways of splitting the labeled partition $\alpha = [1^7]$ into two labeled partitions $\beta = [1^3]$ and $[\gamma] = [1^4]$ ($\gamma = \alpha \setminus \beta$).

The \mathbb{Q} -algebra structure of $\mathbb{Q}S_d$ is given by the unit u and the multiplication $m : \mathbb{Q}S_d \otimes \mathbb{Q}S_d \rightarrow \mathbb{Q}S_d$ defined by the formula: $[\lambda] \otimes [\mu] = \bigoplus_\rho k_{\lambda\mu}^\rho [\rho]$, where $[\lambda]$ is the representation associated to a partition λ and $k_{\lambda\mu}^\rho \in \mathbb{N}$ are the structure constants of the product, which are known as Kronecker coefficients. If we look at the group algebra $\mathbb{Q}S_d$ from a Hopf algebra perspective, an additive basis of $\mathbb{Q}S_d$ is indexed by partitions $\{[\lambda]\}_{\lambda \in \mathcal{P}(d)}$. In particular there is an isomorphism with the Hopf algebra of Schur functions and with the Hopf

algebra of irreducible representations of the general linear group $GL(d, \mathbb{C})$. Let us call by $c_{\lambda\mu}^\eta$ the structure constants for the coproduct $\Delta[\eta] = \sum c_{\lambda,\mu}^\eta [\lambda] \otimes [\mu]$ and S the antipode, that is, $S(\sigma) = \sigma^{-1}$, $\forall \sigma \in S_d$. We see in the next lemma that the coefficients $c_{\lambda\mu}^\eta$ for the coproduct $\Delta[\eta]$ correspond to the structure constants of the dual Hopf algebra $(\mathbb{Q}S_d)^*$, which are known as Littlewood–Richardson coefficients.

Proposition 4.3 *There is an isomorphism between the Hopf algebra of the symmetric group with the Hopf algebra of Schur functions and with the Hopf algebra of representations of the linear group $GL(d, \mathbb{C})$.*

Proof First, we need to see there is an isomorphism at the level of \mathbb{C} –vector spaces. As the underlying complex vector spaces of the respective \mathbb{C} –algebras are finite dimensional and are indexed by partitions $\mathcal{P}(d)$ of d , they are isomorphic as vector spaces. Secondly, we need to see there is an isomorphism at the level of Hopf algebra structures. The matrix encoding the coproduct for the Hopf algebra of the symmetric group admits a base change of invertible transformations to the coding for the coproduct of the commutative Hopf algebra of symmetric functions, which is graded and self-dual under the Hall inner product $\langle \cdot, \cdot \rangle$; see [15]. \square

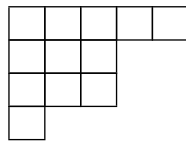
Lemma 4.1 1. *The structure constants $c_{\lambda,\mu}^\eta$ for the coproduct Δ of the Hopf algebra $\mathbb{Q}S_d$ are the Littlewood–Richardson coefficients.*

2. *The coefficients $k_{\lambda\mu}^\rho$ of the product m of the group algebra $\mathbb{Q}S_d$ are the structure constants for the coproduct of the dual Hopf algebra.*

Proof In terms of irreducible representations of $GL(d, \mathbb{C})$, a partition η corresponds to a finite irreducible representation that we denote as $V(\eta)$. Since $GL(d, \mathbb{C})$ is reductive, any finite dimensional representation decomposes into a direct sum of irreducible representations, and the structure constant $c_{\lambda,\mu}^\eta$ is the number of times that a given irreducible representation $V(\eta)$ appears in an irreducible decomposition of $V(\lambda) \otimes V(\mu)$. This is known as the Littlewood–Richardson coefficient, since they were the first to give a combinatorial formula encoding these numbers (see [7]).

(2) In terms of the Hopf algebra Λ of Schur functions, let s_λ be the Schur function indexed by the partition λ , we have $s_\lambda \cdot s_\mu = \sum_\nu k_{\lambda\mu}^\nu s_\nu$ for the product, and we get the coefficients $k_{\lambda\mu}^\eta$ as the structure constants of the dual Hopf algebra Λ^* . These are known as Kronecker coefficients (see [11, 15]). \square

To each partition $\lambda = (\lambda_1, \dots, \lambda_k)$ we associate a Young diagram consisting of a collection of boxes ordered in consecutive rows, where the i^{th} row has exactly λ_i boxes. The columns are indexed by another partition μ , where $\mu_k = \#\{\mu_i = k\}$ is the number of times the multiplicity corresponding to the integer k is realized. For example, if we consider the partition $\lambda = (5, 3, 3, 1)$, its Young diagram is



The hook-length H_b at any box b is the number of boxes directly below it vertically or the number of boxes directly to the right of it horizontally of b counting b once. If we represent the partitions λ, μ, η by the

corresponding Young diagrams, the coefficient $c_{\lambda, \mu}^{\eta}$ represents the number of ways to fill the boxes $\eta \setminus \lambda$, with one integer in each box, so that the following conditions are satisfied:

- The entries in any row are weakly increasing from left to right.
- The entries in each column are strictly increasing from top to bottom.
- The integer i occurs exactly μ_i times.
- For any p with $1 \leq p < \sum \mu_i$, and any i with $1 \leq i < n$, the number of times i occurs in the first p boxes of the ordering is at least as large as the number of times that $i + 1$ occurs in these first p boxes.

4.3. Connection with the moduli space of curves

Let k be an algebraically closed field of characteristic 0 and consider the action of the symmetric group S_n on the ring of polynomials $k[x_1, \dots, x_n]$ by

$$(s \cdot f)(x_1, \dots, x_n) = f(x_{s(1)}, \dots, x_{s(n)}), \quad \text{for } s \in S_n, \quad f \in k[x_1, \dots, x_n].$$

We can view this as the action of S_n on $\mathcal{P}(k^n)$ arising from the representation of S_n on k^n as permutation matrices, with $x = (x_1, \dots, x_n) \in k^n$.

If V_{S_n} is the variety parametrizing curves with Galois group S_n then the subvariety of invariants by the action of finite subgroups of S_n defines an stratification of the ambient variety V_{S_n} .

Fix m points q_1, \dots, q_m in \mathbb{P}^1 , where $q_i = (x_i, 1)$ and a conjugacy class $\sigma = (l_1) \dots (l_m)$ in S_n . Consider the corresponding covering $p : C \rightarrow \mathbb{P}^1$ with ramification type prescribed by the partition $\mu = (l_1, \dots, l_m) \in \mathcal{P}(d)$ with the integers l_i for $i = 1, \dots, m$ ordered by nondecreasing order. The preimage $p^{-1}(\infty) = \sum_{i=1}^m l_i q_i$ defines a divisor on C . Let $k(C_{\mu, d})$ be the function field of the curve C , and we have that $k(C_{\mu, d}) \cong k(a_1, \dots, a_n)$, where

$$y^d = \prod_{i=1}^m (x - x_i)^{l_i} \dots (x - x_m)^{l_m} = \sum_{i=0}^n a_i x^i, \tag{6}$$

and the coefficients a_0, \dots, a_n are symmetric polynomials of q_i multiplied by $(-1)^{s-i}$. The partition μ gives information on the cycle structure of the permutation σ .

Proposition 4.4 *Fix q_1, \dots, q_m points in \mathbb{P}^1 , and a divisor $\sum_{i=1}^m l_i q_i$. Let $\gamma_k = \#\{l_i = k\}$ be the number of times the multiplicity corresponding to the integer k is realized, and then for each degree d dividing $n = \sum_{i=1}^m l_i$, the number of branched coverings with the same monodromy type above ∞ defined by the partition μ , that is the number of coverings defined by equation (6), coincides with the number*

$$\frac{r!}{\prod_{b \in [\lambda]} H_b} = \frac{r!}{\prod_{i=1}^m i^{\gamma_i} \gamma_i}.$$

Proof To each configuration of points $(\mathbb{P}^1, q_1, \dots, q_m)$ and ramification divisor $\sum_{i=1}^m l_i q_i$ corresponds a cyclic covering of type λ a partition of n that ramifies over $\sum_{i=1}^m l_i q_i$ and whose function field extension of the rational

function field $k(x)$ is given by equation $y^d = \prod_{i=1}^m (x - x_i)^{l_i}$. Consider the hypersurface of equation

$$f(x, x_1, \dots, x_m) = x^n + a_1 x^{n-1} + \dots + a_{n-1} x - (x - x_1)^{l_1} \dots (x - x_m)^{l_m},$$

where $a_j = (-1)^j \sigma_j(x_1, \dots, x_m)$, and σ_j is the j^{th} elementary symmetric function. Since $\sigma_j(x_1, \dots, x_m)$ is invariant under permutation of the roots (x_1, \dots, x_m) , any permutation of the set root gives the same coefficient a_j and leads to the same covering branched over the points (q_1, \dots, q_m) . In particular we may assume that the integer partition λ is unordered. Thus the number of these branched coverings is the product of hook-lengths over all boxes in the Young diagram of the partition λ , which is the number of permutations $\Gamma(r; \gamma_1, \dots, \gamma_m) = \frac{r!}{1^{\gamma_1} \gamma_1! 2^{\gamma_2} \gamma_2! \dots m^{\gamma_m} \gamma_m!}$ of λ with exactly γ_i cycles of length i for each $1 \leq i \leq m$. Here r is the rank of the permutation λ , which is the largest part in the partition minus the number of parts and it is the number uniquely representing the partition. □

Remark 4.5 If we vary one of the branch points q_i of the curve defined by (6), we obtain a one-dimensional Hurwitz space parameterizing such coverings.

Lemma 4.2 *The variety $V_{d,g,\sigma}$ parameterizing coverings with ramification type corresponding to a conjugacy class in $\sigma \in S_d$ is a one-dimensional subvariety of the variety parameterizing degree d and genus g coverings $V_{d,g}$ of the projective line $\mathbb{P}^1(k)$.*

Proof Consider the natural identification of σ_d with an element A_σ in $GL(d, k)$ (respectively $SL(d, k)$), via a linear representation. This element determines an automorphism of the function field given by multiplication of the corresponding matrix representation A_σ in $GL(d, k)$ with the vector field of coordinates (a_1, \dots, a_m) . The invariant field $k(a_1, \dots, a_m)^{\sigma_d}$ is the quotient surface $C_{\mu,d}/G$ by the group G generated by the corresponding element A_σ in $GL(d, k)$, and thus a one-dimensional scheme in $V_{d,g}$. □

Corollary 4.3 *The variety parameterizing degree d coverings of \mathbb{P}^1 with a unique branched point is a one-dimensional subvariety of the variety $V_{d,g}$.*

Proof The ramification type of such coverings is defined by a partition $(l_1, 1, \overbrace{\dots}^{m-1}, 1) \in \mathcal{P}(m)$, where m is the number of ramification points that can be computed with the Riemann–Hurwitz formula (3), and $l_1 \in \mathbb{Z}$ is the multiplicity corresponding to the branched point. Since a branch point is induced by a permutation in the symmetric group S_d , the result follows. □

Corollary 4.4 *The variety parameterizing degree d dihedral coverings is a 2-dimensional subvariety of the variety parametrizing degree d and genus g coverings and the function field of the parameter space is the invariant field $k(c_1, \dots, c_m)^{D_m} \cong k(u_1, \dots, u_m)$.*

Proof Just observe that the dihedral group D_m is generated by two elements, a rotation τ and a reflection σ . Via the identification of the triangle groups with the permutation cycles, we write the m dihedral group as $D_m = \langle (13)(24), ((12)(34)(13)(24))^m \rangle$. Thus the fixed field

$$k(c_1, \dots, c_m)^{D_m} \cong k(u_1, \dots, u_m),$$

where $u_1 \dots, u_m$ are the dihedral invariants defined in section 2, is the function field of the variety parameterizing dihedral coverings. □

Let $H_{g,\mu}$ be the Hurwitz number, that is, the number of genus g degree d coverings of \mathbb{P}^1 with profile μ over ∞ and simple ramification over a fixed set of finite points. The Hurwitz numbers are naturally expressed in terms of tautological intersections in the moduli space $M_{g,n}$ of projective nonsingular curves of genus g and n marked points, and its compactification $\overline{M}_{g,n}$, whose points correspond to projective, connected, nodal curves of arithmetic genus g , satisfying a stability condition (due to Deligne and Mumford), and with orbifold singularities if regarded as ordinary coarse moduli spaces.

The intersection theory of $\overline{M}_{g,n}$ must be studied in the orbifold category or the category of Deligne–Mumford stacks to correctly handle the automorphisms group of the pointed curves. For each marking i , there exists a canonical line bundle \mathbb{L}_i . The fiber at the stable pointed curve (C, x_1, \dots, x_n) is the cotangent space $T_C^*(x_i)$ of C at x_i . \mathbb{L}_i determines a \mathbb{Q} –divisor on the coarse moduli space. Let ψ_i denote the first Chern class of \mathbb{L}_i . Witten’s conjecture concerns the complete set of evaluations of intersections of the ψ classes:

$$\int_{\overline{M}_{g,n}} \psi_1^{k_1} \dots \psi_n^{k_n}. \tag{7}$$

The symmetric group S_n acts naturally on $\overline{M}_{g,n}$ by permuting the markings. Since the ψ classes are permuted by this S_n action, the integral is unchanged by a permutation of the exponents k_i . A notation for these intersections that exploits the S_n symmetry is given by

$$\langle \tau_{k_1} \dots, \tau_{k_n} \rangle_g = \int_{\overline{M}_{g,n}} \psi_1^{k_1} \dots \psi_n^{k_n}. \tag{8}$$

Let the Hodge bundle

$$\mathbb{E} \rightarrow \overline{M}_{g,n}$$

be the rank g vector bundle with fiber $H^0(C, w_C)$ over the moduli point $(C, p_1 \dots, p_n)$. The λ classes are the Chern classes of the Hodge bundle:

$$\lambda_i = c_i(E) \in H^{2i}(\overline{M}_{g,n}, \mathbb{Q}).$$

The ψ and λ classes are *tautological* classes on the moduli space of curves.

Let H_d^g be the number of such branched coverings that are connected; then the following formula due to Ekedahl et al. [4] expresses Hurwitz numbers in terms of Hodge integrals (see [8]):

$$H_\alpha^g = \frac{r!}{\#\text{Aut}(\alpha)} \prod_{i=1}^m \frac{\alpha_i^{\alpha_i}}{\alpha_i} \int_{\overline{M}_{g,m}} \frac{1 - \lambda_1 + \dots, \pm \lambda_g}{\prod(1 - \alpha_i \psi_i)}$$

In the case where there is no ramification over ∞ (i.e. $\alpha = (1^n)$), Hurwitz numbers enumerate coverings of the projective line by smooth connected curves of specified degree and genus, with specified branching above one point, simple branching over other specified points, and no other branching.

Example 5 *In the case of genus 0, the formula reads*

$$H_d^0 = \frac{(2d - 2)!}{d!} d^{d-3}.$$

4.3.1. Connection with the moduli space of curves: counting coverings of \mathbb{P}^1 over finite fields

Let $\overline{M}_{g,n}(\mathbb{F}_p)$ be the moduli space of stable curves of genus g with n marked points defined over the finite field \mathbb{F}_p of p elements. The moduli space of Hurwitz covers $H_g(\mu^1, \dots, \mu^m)$ parameterizes morphisms, $f : C \rightarrow \mathbb{P}^1$, where C is a complete, connected, nonsingular curve with marked profiles μ^1, \dots, μ^m over m ordered points of the target (and no ramifications elsewhere), [5]. The moduli space $M_{1,1}$ of elliptic curves can be realized over \mathbb{C} as the analytic space $\mathbb{H}/\text{SL}(2, \mathbb{Z})$. The cardinality $\sharp M_{1,1}(\mathbb{F}_p)$ of the moduli space is the count of elliptic curves over \mathbb{F}_p up to \mathbb{F}_p -isomorphism with weight factor $\frac{1}{\sharp \text{Aut}_{\mathbb{F}_p}(E)}$, and so $\sharp M_{1,1}(\mathbb{F}_p) = p$. The next proposition shows that the count of curves expressible as d -sheeted coverings of $\mathbb{P}^1(\mathbb{F}_p)$ coincides with the cardinality of $M_{g,m}(\mathbb{F}_p)$.

Proposition 4.6 *The number of genus g curves expressible as d -sheeted coverings of \mathbb{P}^1 coincides with the cardinality of $M_{g,m}$ over \mathbb{F}_p (up to \mathbb{F}_p isomorphism), where $g = \frac{(d-1)(m-2)}{2}$, weighted by the factor $\frac{1}{\sharp \text{Aut}_{\mathbb{F}_p}(C)}$.*

Proof Let C be a complete, connected nonsingular curve with m marked points p_1, \dots, p_m . We obtain a morphism $f : C \rightarrow \mathbb{P}^1$ from the linear series attached to the divisor $p_1 + \dots + p_m$. The branched covering f expresses C in the form $y^d = \prod_{i=1}^m (x - p_i)^{l_i}$, with profile defined by the partition (l_1, \dots, l_m) of d , expressing the monodromy above ∞ . By the Riemann–Hurwitz formula we can compute m , the number of different branch points. Now the number of polynomials of degree $n = d + m + 2(g - 1)$ with m different roots is the falling factorial polynomial $(p)_{m+1} := p(p-1)(p-2) \dots (p-m)$, divided by the order of the affine transformation group of $\mathbb{A}^1 = \mathbb{P}^1 \setminus \infty$, that is, $p^2 - p$. □

Remark 4.7 *Observe that $(q)_n = \sum_{k=0}^n s(n, q) q^k$, where $s(n, q)$ is the Stirling number of the first kind and it counts the number of ways to partition a set of cardinality n into exactly k nonempty subsets. The Stirling number of the second kind $\begin{bmatrix} n \\ m \end{bmatrix}$ counts the number of permutations of n elements with m disjoint cycles and it satisfies the relation:*

If $q \rightarrow 1$, $\sum_{k=0}^n \begin{bmatrix} n \\ k \end{bmatrix} = p(n) = \text{number of partitions of } n$.

There is a formula for the generating series of $p(n)$:

$$\sum_{n=0}^{\infty} p(n) x^n = \prod_{k=1}^{\infty} \left(\frac{1}{1 - x^k} \right)$$

Acknowledgments

We would like to thank Fei Xu and Vivek Mallick for interesting discussions during the preparation of the work and Joachim Kock for reading the paper and some useful comments. This work has been partially supported by the project MTM2009-10359 “Métodos combinatorios en Geometría Aritmética y Geometría Algebraica”.

References

[1] Behrend K, Noohi B. Uniformization of Deligne-Mumford curves. J Reine Angew Math 2016; 599: 111-153.

- [2] Belyi GV. On galois extensions of a maximal cyclotomic field. Math USSR R Izvestija 1980; 14: 247-256.
- [3] Chiodo A, Eisenbud D, Farkas G, Schreyer FO. Syzygies of torsion bundles and the geometry of the level l modular variety over \overline{M}_g . Invent Math 2013; 194: 73-118.
- [4] Ekedahl T, Lando S, Shapiro M, Wainshtein A. Hurwitz numbers and intersections on moduli spaces of curves. Invent Math 2001; 146: 297-327.
- [5] Faber C, Pandharipande R. Relative maps and tautological classes. J Eur Math Soc 2005; 7: 13-49.
- [6] Fomin S, Mikhalkin G. Label floor diagrams for plane curves. J Eur Math Soc 2010; 12: 1453-1496.
- [7] Fulton W. Eigenvalues, invariant factors, highest weights and Schubert calculus. Bull Amer Math Soc 2000; 37: 209-249.
- [8] Goulden IP, Jackson DM, Vakil R. The Gromov-Witten potential of a point, Hurwitz numbers, and Hodge integrals. In Proc London Math Soc 83 2001, pp. 563-581.
- [9] Kontogeorgis A. On cyclic covers of the projective line. Manuscripta Mathematica 2006; 1: 121.
- [10] Ling S, Niederreiter H, Xing C. Symmetric polynomials and some good codes. Finite Fields and Their Applications 2001; 7: 142-148.
- [11] Manivel L. On rectangular Kronecker coefficients. J Algebr Comb 2011; 33: 153-162.
- [12] Maulik D. Root sets of polynomials modulo prime powers. J Comb Theory A 2001; 93: 125-140.
- [13] Okounkov A, Pandharipande R. Gromov-Witten theory, Hurwitz theory and completed cycles. Ann Math 2006; 163: 517-560.
- [14] Serre JP. Topics in Galois Theory, course at Harvard University, Fall 1988.
- [15] Sottile F, Lam T, Lauve A. A skew Littlewood-Richardson rule from Hopf algebras. IMRN 2011; 2011: 205-219.
- [16] Vakil R. Twelve points on the projective line, branched covers, and rational elliptic fibrations. Math Ann 2001; 320: 33-54.