Galois Theory, Monodromy Groups and Flexes of Plane Cubic Curves

Baran Can Öner

Geboren am 8. September 1988 in Düsseldorf

21. Juli 2012

Bachelorarbeit Mathematik

Betreuer: Prof. Dr. Daniel Huybrechts

MATHEMATISCHES INSTITUT

MATHEMATISCH-NATURWISSENSCHAFTLICHE FAKULTÄT DER

RHEINISCHEN FRIEDRICH-WILHELMS-UNIVERSITÄT BONN

Contents

1 Abstract

In 1979, J. Harris' paper *Galois Groups of Enumerative Problems* was published, which "[...] is concerned with the solvability of certain enumerative problems in algebraic geometry". The emphasis of my thesis will be the first problem Harris introduces, which consists of two questions: Given a complex plane curve C of degree d, how many flexes exist on this curve? Secondly, can we find them?

We will at first introduce the Galois and the monodromy group of a dominant morphism between varieties, which turn out to be identical. The first group will be defined in terms of the induced extension of function fields - and in fact reflect the second question above - whereas the monodromy group allows for an effective computation by considering loops in the base space (which will be the parameter space of the curves we consider) and their corresponding lift to the total space.

We will then turn our attention to the first question and use the classical Plücker formulas to outline the fact that a smooth plane curve C of degree d has precisely $3d(d-2)$ flexes counted with multiplicities. The relevant special case that any elliptic curve has nine distinct flexes is proven directly. These formulas will tell us a bit more about the geometry of mildly singular plane curves as they relate various numerical invariants to each other: Namely, the degree, the number of flexes, the number of bitangents, the number of cusps, the number of double points and the corresponding values for the *dual curve* of C. This is an algebraic curve in the dual projective plane that is defined as the set of all tangent lines to C.

In the next section, we describe elliptic curves as complex tori, which will be needed when we compute the Galois group of the nine flexes. Hence, we will introduce elliptic functions and period lattices to construct a group isomorphism from a suitable one-dimensional complex torus to any given elliptic curve in Weierstrass form.

We will observe that the nine flexes of a general plane cubic C have the structure of a two-dimensional vector space over $\mathbb{F}_3$, and the monodromy group introduced in the first chapter turns out to preserve much of this structure: In fact, it is the solvable group of affine-linear transformations with determinant one on $\mathbb{F}_3^2$. Finally, we will see that the flexes of an elliptic curve in Weierstrass form may be explicitly calculated.

German Summary. Diese Bachelorarbeit befasst sich mit dem ersten Problem, das J. Harris' in seinem 1979 veröffentlichten Werk *Galois Groups of Enumerative Problems* vorstellt und welches aus zwei Fragen besteht: Wie viele Wendepunkte existieren auf einer komplexen, ebenen algebraischen Kurve C vom Grad d und können wir diese finden?

Hierzu führt Harris die Galois- und Monodromiegruppe eines dominanten Morphismus zwischen komplexen Varietäten ein, welche sich als identisch herausstellen. Die erste Gruppe wird mithilfe der induzierten Erweiterung der Funktionenkörper definiert und reflektiert die zweite obige Frage, wobei die Monodromiegruppe in der späteren Anwendung für die Berechnung verwendet wird.

Die erste Frage wird mithilfe der Plückerformeln beantwortet, die verschiedene numerische Invarianten von ebenen Kurven miteinander in Verbindung setzen. Der für uns relevante Spezialfall, dass eine elliptische Kurve genau neun verschiedene Wendepunkte besitzt, wird gesondert bewiesen.

Zur Berechnung der Monodromiegruppe der neun Wendepunkte einer elliptischen Kurve stellen wir diese als komplexen Torus dar. Hierzu werden wir elliptische Funktionen und Gitter einführen, um einen Gruppenisomorphismus von einem geeigneten eindimensionalen komplexen Torus auf eine gegebene elliptische Kurve in Weierstrassform zu konstruieren.

In dem letzten Teil stellen wir fest, dass die Monodromiegruppe viel von der Untergruppenstruktur der neun Wendepunkte bewahrt und wir berechnen sie als die auflösbare Gruppe $\mathrm{ASL}_2(\mathbb{F}_3^2)$. Zuletzt werden wir die Wendepunkte einer elliptischen Kurve in Weierstrassform explizit anhand der Koeffizienten ihrer Gleichung ermitteln.

Acknowledgements. I would like to thank my advisor, Prof. Dr. Daniel Huybrechts, for his thorough support as well as for his highly instructive lectures which made this thesis possible. I am also thankful to Michael Kemeny for readily answering my questions and for giving great general advice.

Some remarks on notation. The ground field is always assumed to be $\mathbb{C}$ unless stated otherwise. Affine n-space (over the complex numbers) is denoted $\mathbb{A}^n$, and projective n-space will referred to as $\mathbb{P}^n := (\mathbb{C}^{n+1}\setminus\{0\})/\mathbb{C}^\times$. The coordinate ring and the function field of a variety X are called $K[X]$ and $K(X)$, respectively.

2 Galois and Monodromy Groups

Let X and Y be irreducible projective or affine varieties over the complex numbers of the same dimension. Throughout the first part, $\pi : Y \longrightarrow X$ is assumed to be a *rational map of degree* $d > 0$, that is, a dominant rational map such that the induced inclusion $\pi^* : K(X) \to K(Y)$ is a field extension of degree d. Note that $\dim(X) = \dim(Y)$ is a necessary condition for such a morphism to exist since $\dim(X) = \mathrm{trdeg}_{\mathbb{C}} K(X)$ and $\dim(Y) = \mathrm{trdeg}_{\mathbb{C}} K(Y)$.

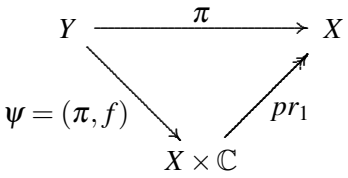
2.1. General Fibres of a Degree *d* Rational Map The morphism π is also called *generically finite*, a terminology that is justified by the next lemma which gives a geometrical meaning to the degree of a map.

Lemma 2.1. *[7, Proposition 7.16.] The number of points in a general fibre of π is equal to the degree of the extension $K(Y)/K(X)$.*

Proof. If X or Y are projective varieties, we may cover them by affine open sets X_i and Y_j respectively and consider each intersection $Y_{i,j} = \pi^{-1}(X_i) \cap Y_j$. The restriction $\pi_{|Y_{i,j}} : Y_{i,j} \longrightarrow X_i$ to affine subsets still induces an extension of degree d since there are isomorphisms of function fields

$$K(Y_{i,j}) \cong K(Y),\ K(X_i) \cong K(X).$$

We may thus replace X and Y by affine varieties, so suppose in particular that $X \subset \mathbb{A}^n$. Since the function fields have characteristic zero, we may apply the primitive element theorem and conclude that $K(Y)$ is generated over $K(X)$ by a single algebraic element f. We factorize π as follows:



Define $W = \overline{\psi(Y)}$ and restrict the target space of ψ accordingly. For $\tilde{f}(y,z) = z$, we have $\psi^*(\tilde{f}) = f$ and hence $\psi^* : K(W) \xrightarrow{\simeq} K(Y)$. Since ψ is dominant by definition and induces an isomorphism of function fields, it is birational, or equivalently, it is an isomorphism restricted to nonempty Zariski open sets. We thus conclude that $|\psi^{-1}(w)| = 1$ on a dense open subset W' of W, so it remains to investigate the fibres under the projection map pr_1. Let $d = [K(W) : K(X)] = [K(Y) : K(X)]$ and let

$$G(t) = \sum_{i=0}^{d} a_i T^i$$

be the minimal polynomial in $K(X)[T]$ of the last coordinate on W. After clearing denominators, we may assume that the $a_i(x_1, \ldots, x_n)$ are regular functions on X, i.e. they are elements of the coordinate ring $K[X]$. Let $\Delta_G(x_1, \ldots, x_n)$ be the discriminant of G. Since $\mathrm{char}(K(X)) = 0$, the algebraic extension $K(W)/K(X)$ is separable. Irreducibility

of $G \in K[X][T]$ then implies that Δ_G is a nonzero element of $K[X]$. This means that Δ_G cannot vanish identically on X, and the same holds for the leading coefficient a_n of G. To summarize, the loci $V(\Delta_G)$ and $V(a_n)$ are proper subvarieties of X, and on the complement of their union, the fibres of

$$pr_1 : W' \longrightarrow X$$

consist of exactly d distinct points: Just observe that if $x \notin (V(\Delta_G) \cup V(a_n))$, the polynomial $G(x,T) \in \mathbb{C}[T]$ is of degree d and separable since its discriminant $\Delta_G(x)$ is nonzero. □

Therefore, we define $\Gamma = \pi^{-1}(p) = \{q_1, q_2, \ldots, q_d\}$ for a general point p of X and let Σ_d be the permutation group of Γ. We will now construct two subgroups of Σ_d, the *Galois group* and the *monodromy group* of π.

2.2. The Galois Group As in the proof of the previous lemma, the function field of Y is generated over $K(X)$ by a single rational function $f \in K(Y)$ with minimal polynomial

$$P(T) = T^d + \pi^*(g_1)T^{d-1} + \ldots + \pi^*(g_d)$$

where $g_1, \ldots, g_d \in K(X)$. We will now construct the Galois closure L of $K(Y)/K(X)$, i.e. the splitting field of P. Identifying the roots of P with the fibre of a generic point, the Galois group will then simply be $\mathrm{Gal}(L/K(X))$ embedded into Σ_d via the usual action on the roots.

Lemma 2.2. *An algebraic variety Z over the complex numbers is a complex manifold in a small analytic open neighbourhood of any non-singular point p. Furthermore, the algebraic and complex dimension coincide.*

Proof. Taking an affine open covering, we may assume that Z is an algebraic subset of $\mathbb{A}^n$ given as the zero locus of finitely many polynomials $\{f_1, \ldots, f_m\}$. For any point $p \in Z$, the tangent space of Z at p is given by

$$T_pZ = \bigcap_{i=1}^{m} V\Big(J_{\mathbb{C}}(f_i)(p) \cdot (x-p)\Big) \subset \mathbb{A}^n,$$

where $J_{\mathbb{C}}(f_i)(p)$ denotes the complex Jacobian of f_i evaluated at the point p. Define $f = (f_1, \ldots, f_m) : \mathbb{C}^n \to \mathbb{C}^m$. Since T_pZ is the intersection of m hyperplanes, i.e. the space of solutions to a system of m linear equations, we have that

$$\dim_{\mathbb{C}} T_pZ = n - \mathrm{rk}(J_{\mathbb{C}}(f)(p)). \tag{1}$$

Now assume that p is a non-singular point of Z. By definition, $\dim(Z) = \dim_{\mathbb{C}} T_pZ$, therefore equation (1) translates to $r := \mathrm{codim}(Z) = \mathrm{rk}(J_{\mathbb{C}}(f)(p)) \leq n, m$. Consider the map

$$\begin{aligned} \Phi : \mathbb{A}^n &\longrightarrow \mathbb{A}^m \\ (x_1, \ldots, x_n) &\longmapsto (f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)). \end{aligned}$$

The preceding discussion allows us to choose the f_i such that

$$\left(\frac{\partial \Phi_j}{\partial x_i}(p)\right)_{i,j=1,\dots,r} = \left(\frac{\partial f_j}{\partial x_i}(p)\right)_{i,j=1,\dots,r}$$

is an invertible matrix. By the complex implicit function theorem, there exists a holomorphic map $\zeta : U \longrightarrow V$ where $U \subset \mathbb{C}^{n-r}$, $V \subset \mathbb{C}^r$ are open and $p \in V \times U$ such that

$$\{(\zeta(y), y) : y \in U\} = \{(x,y) \in V \times U : \Phi(x,y) = 0\} = \{(x,y) \in (V \times U) \cap Z\}.$$

Hence, the graph $y \longmapsto (\zeta(y), y)$ is a chart of Z around p and the open neighbourhood $(V \times U) \cap Z$ is therefore a complex manifold of dimension $n - r = \dim(Z)$. □

We may therefore consider the open and dense sets Y_{ns} and X_{ns} of non-singular points as complex manifolds. In the next step, we turn them into locally ringed spaces which allows us to introduce the *field of germs of meromorphic functions* around a smooth point.

Definition 2.3. *Let Z be a complex manifold. The* sheaf of holomorphic functions *on Z is defined as*

$$\mathscr{O}_Z(U) = \{f : U \to \mathbb{C} : \ f \text{ is holomorphic}\},$$

where $U \subset Z$ is open. A function $f : U \to \mathbb{C}$ is called holomorphic *if, for any chart (U_i, ϕ_i) of a holomorphic atlas of U, the map $f \circ \phi_i^{-1} : \phi_i(U_i) \to \mathbb{C}$ is holomorphic. For $p \in Z$, the stalk $\mathscr{O}_{Z,p}$ is a local UFD (cf. [10, Prop. 1.1.15]), hence an integral domain and we may thus define the* field of germs of meromorphic functions *around p as the quotient field $\mathscr{K}_{Z,p} = Q(\mathscr{O}_{Z,p})$.*

Let $\mathscr{K}_\alpha = \mathscr{K}_{Y_{ns},q_\alpha}$ and $\mathscr{K} = \mathscr{K}_{X_{ns},p}$ be the fields of germs of meromorphic functions around q_α and p respectively. We need the following lemma, which will also be helpful later on when we define the monodromy group.

Lemma 2.4. *A suitable restriction of the map π to an open and dense subset is a local biholomorphism between the complex manifolds Y_{ns} and X_{ns}.*

Proof. We first of all restrict the map π to the open subset $\pi^{-1}(X_{ns}) \cap Y_{ns} \subset Y$ and thus obtain a map between complex manifolds by the previous lemma. Now, let π be given by an m-tuple of rational functions $f = (f_1, \dots, f_m),\ f_i \in \mathbb{C}(X_0, \dots, X_n)$ and consider the set

$$J_s = \{p \in Y : \mathrm{rk}(J_{\mathbb{C}}(f)(p)) = s\}.$$

The rank of the Jacobian at a point is equal to s if and only if one of the $s \times s$-minors has nonzero determinant, hence J_s is a Zariski-open subset of Y. If we assume without loss of generality that $m \leq n$, we may set $s := m$ and thus J_s is the set of points such that $J_{\mathbb{C}}(f)(p)$ has full rank. It is furthermore nonempty because π is dominant. Now, if we let $d = \dim(X) = \dim(Y)$ and take holomorphic charts ϕ around p and ψ around $\pi(p)$, we see that the Jacobian of

$$\psi^{-1} \circ \pi \circ \phi : \mathbb{C}^d \to \mathbb{C}^d$$

is invertible for each $p \in J_s$ and hence it is biholomorphic in a small neighbourhood of p by the complex inverse function theorem. □

Thus, the map π induces an isomorphism $\pi_\alpha : \mathscr{K}_\alpha \xrightarrow{\simeq} \mathscr{K}$ by the composition $f \mapsto f \circ \pi^{-1}$, where we note that the inverse of π is only locally defined. Furthermore, we may embed the function field of X into $\mathscr{K}$ by restriction:

$$\phi : K(X) \longrightarrow \mathscr{K}.$$

Similarly, by embedding rational functions on Y into $\mathscr{K}_\alpha$ and then applying π_α, we obtain an injection

$$\phi_\alpha : K(Y) \longrightarrow \mathscr{K}.$$

Define $K_\alpha = \phi_\alpha(K(Y)) \subset \mathscr{K}$ and let L be the subfield of $\mathscr{K}$ generated by the subfields K_α. If we let

$$\begin{aligned} \tilde{g}_i &= \phi(g_i) \\ \tilde{f}_\alpha &= \phi_\alpha(f) \\ \tilde{P}(T) &= T^d + \tilde{g}_1 T^{d-1} + \ldots + \tilde{g}_d \end{aligned}$$

then each function $\tilde{f}_\alpha$ satisfies

$$\tilde{P}(\tilde{f}_\alpha) = \tilde{f}_\alpha^d + \tilde{g}_1 \tilde{f}_\alpha^{d-1} + \ldots + \tilde{g}_d = 0.$$

Simply note that $\phi_\alpha(P(f)) = 0$ by definition of P, and so - expanding the left-hand side - the claim follows since $\phi_\alpha(\pi^*(g_i)) = \tilde{g}_i$.

To see that L is indeed the splitting field of P, it suffices to show that all the $\tilde{f}_\alpha$ are distinct since P has degree d and L is by definition the smallest field containing all the $\tilde{f}_\alpha$. But if $\tilde{f}_{\alpha_1} = \tilde{f}_{\alpha_2}$, then in particular $f(q_{\alpha_1}) = \tilde{f}_{\alpha_1}(p) = \tilde{f}_{\alpha_2}(p) = f(q_{\alpha_2})$, which is impossible because otherwise *all* the rational functions in $K(Y)$ would coincide at q_{α_1} and q_{α_2}, which is false (simply note that for any two distinct points on a variety, there exists a polynomial function vanishing on precisely one of them. Furthermore, none of the q_{α_i} will be poles of f for a general p).

We may thus define $G = \mathrm{Gal}(L/K(X))$, and every automorphism in G induces a permutation of the d roots $\{\tilde{f}_\alpha\}$ of P. Consequently, we have an inclusion $G \hookrightarrow \Sigma_d$.

2.3. The Monodromy Group The monodromy group is constructed merely in terms of a covering map between topological spaces and an action of the fundamental group of the base space on the fibre of p. The next result shows that we may regard a certain restriction of π as a d-sheeted covering.

Theorem 2.5. *There exists a sufficiently small Zariski open subset $U \subset X$ with preimage $V = \pi^{-1}(U) \subset Y$ so that $\pi : V \to U$ is an unbranched covering map with respect to the analytic topology.*

Proof. Using Lemma 2.1, we readily obtain an unramified restriction of π. Further restriction of π via Lemma 2.4 yields a local biholomorphism $\pi : V \to U$, i.e. for each point $q \in \pi^{-1}(p)$, there exists a neighbourhood V_q which is mapped biholomorphically onto some open neighbourhood U_p of p. It remains to show that we may shrink U_p such that all d preimages V_q are mapped to the same open neighbourhood, which follows from the fact that preimages under π of compact sets remain compact. The latter statement is true by properness of π and can be found in [1, A.14.6]. □

Thus, we discard the algebraic properties of π for now and define the monodromy group using some basic topological methods. The first step is the following lemma, also known as the *path lifting property*, which assures that loops may be uniquely lifted to the total space. Figure 1 illustrates the proof of this lemma and the effect on the fibre of a point.

Lemma 2.6. *[2, Theorem 3.3] For any loop $\gamma : [0,1] \to U$ with base point p and any $q_\alpha \in \pi^{-1}(p)$, there exists a unique lifting $\tilde{\gamma}_\alpha$ of γ to a path in V with $\tilde{\gamma}_\alpha(0) = q_\alpha$.*

Proof. Each point $x \in U$ has an open neighbourhood U' that is an elementary set, i.e. $\pi^{-1}(U')$ is a disjoint union of open sets, each of which is homeomorphic to U' via π. Since this property yields an open cover of the compact set $\gamma([0,1])$, we may take a finite subcover $(U_i)_{i\in I}$.
Applying Lebesgue's number lemma (cf. [2, p. 28]) to the collection of preimages $(\gamma^{-1}(U_i))_{i\in I}$, we obtain a natural number n such that each interval $[\frac{j}{n}, \frac{j+1}{n}]$ is contained in one $\gamma^{-1}(U_i)$. Let $O_j := U_i$ and note that this is an elementary set . We may now inductively define $\tilde{\gamma}_\alpha$.

The base point p lies in O_0 since $\gamma(0) = p$. Select the sheet C of $\pi^{-1}(O_0) = \bigsqcup C_k$ which contains q_α. Since the restriction $\pi_| : C \to O_0$ is a homeomorphism, the composition $\pi_|^{-1} \circ \gamma : [0, \frac{1}{n}] \to C$ is a path starting at q_α. This lifting uniquely determines $\tilde{\gamma}_\alpha$ on the first interval.

Assume that $\tilde{\gamma}_\alpha$ is defined on $[0, \frac{j}{n}]$ and recall that $\gamma([\frac{j}{n}, \frac{j+1}{n}])$ is contained in the elementary set O_j. There is exactly one sheet in $\pi^{-1}(O_j)$ which contains $\tilde{\gamma}_\alpha(\frac{j}{n})$, so we can extend $\tilde{\gamma}_\alpha$ to $[\frac{j}{n}, \frac{j+1}{n}]$ just like we did in the first step using the local homeomorphism property of π. We may conclude that the lifting is uniquely defined on the whole unit interval.

Continuity of $\tilde{\gamma}_\alpha$ is clear since the path is well-defined on the endpoints $\frac{j}{n}$ and continuous on each of the intervals. □

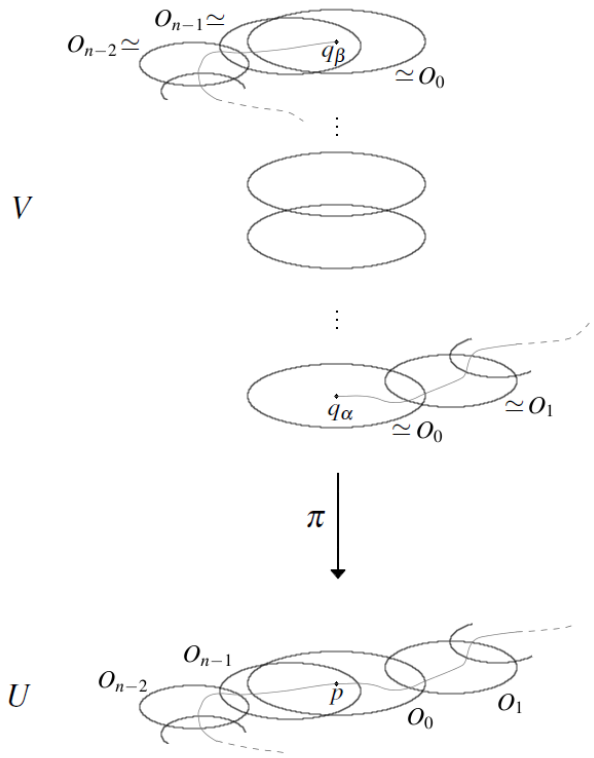


Fig. 1 - Lifting a loop to the total space and the monodromy action

While it is obvious that $\tilde{\gamma}_\alpha(1)$ must lie in Γ, the crucial point is that it may not coincide with q_α, so each lifting defines a permutation of the fibre:

$$\begin{aligned} \phi_\gamma : \Gamma &\longrightarrow \Gamma \\ q_\alpha &\longmapsto \tilde{\gamma}_\alpha(1). \end{aligned}$$

Let I denote the unit interval [0,1]. The covering homotopy theorem (cf. [2, Theorem 3.4.]) states that, for any locally connected space W and homotopy $F : W \times I \longrightarrow X$ with prescribed lifting $f : W \times \{0\} \longrightarrow Y$, there exists a unique homotopy $G : W \times I \longrightarrow Y$ making the following diagram commute:

$$\begin{array}{ccc} W \times \{0\} & \xrightarrow{f} & V \\ \downarrow & \overset{G}{\nearrow} & \downarrow \pi \\ W \times I & \xrightarrow{F} & U \end{array}$$

If F is a homotopy relative to W' for an arbitrary $W' \subset W$, then so is G. In particular, letting the map F be a homotopy of two paths γ_1 and γ_2 rel. ∂I (i.e. $W = I$), any two liftings $\tilde{\gamma}_1$ and $\tilde{\gamma}_2$ with $\tilde{\gamma}_1(0) = \tilde{\gamma}_2(0)$ will satisfy $\tilde{\gamma}_1(1) = \tilde{\gamma}_2(1)$. Therefore, ϕ_γ only depends on the homotopy class of γ, so we have a group homomorphism

$$\begin{aligned} \pi_1(U,p) &\longrightarrow \Sigma_d \\ [\gamma] &\longmapsto \phi_\gamma \end{aligned}$$

The image M of this map is called the *monodromy group* of π. To conclude this chapter, we have the following result.

Theorem 2.7. *The monodromy and Galois group are identical.*

We refer to [8, p. 689] for details. The idea is that analytic continuation of a germ $h \in K_\alpha$ along a loop defines an automorphism of L leaving the embedded function field $\phi(K(X))$ fixed, and hence any loop in U which gives rise to an element of the monodromy group also permutes the roots of $\tilde{P}$. Conversely, one has to show that every automorphism in G is obtained by analytic continuation. Harris does this by proving that the fixed field of $M \subset G$ is $\phi(K(X))$, from which $G = M$ already follows by definition of the Galois group.

3 Flexes of Plane Curves

This chapter is dedicated to the monodromy group of the nine flexes of a plane cubic curve, a problem that has yet to be made precise. In the first part, the issue of defining the varieties I_d and W_d - the latter one being the space of plane curves of degree d - as well as the morphism $I_d \xrightarrow{\pi} W_d$ is addressed.

The first objective will be to compute the degree of this map, or equivalently, the cardinality of a general fibre. Since the fibre of a curve will biject onto the set of its inflection points, the problem of determining the degree is reduced to the computation of the number of flexes on a general plane curve, which we will deal with in Section 3.2.

Before we finally can compute the monodromy group of π as $\mathrm{ASL}_2(\mathbb{Z}/3)$, we will describe elliptic curves as complex tori by means of the Weierstrass $\wp$-function.

3.1. Linear Systems of Plane Curves Before setting up the main problem, we recall some basic results and definitions. A *plane curve* C over the complex numbers is the zero locus of a homogeneous polynomial $F \in \mathbb{C}[X_0, X_1, X_2]_d$, i.e.

$$C = V(F) \subset \mathbb{P}^2.$$

More precisely then, C is called a plane curve of degree d. For an irreducible polynomial G, the loci $V(G)$ and $V(G^n)$ coincide for a positive power n, so we may assume that the powers of the irreducible factors in the decomposition of a polynomial F are one. We will always assume this in Section 3.2 about the Plücker formulas. Now, let C and C' be two plane curves with no common component defined by homogeneous

polynomials F and G, respectively. We define the *intersection multiplicity* of C and C' at a point $p \in \mathbb{P}^2$ as

$$I_p(C,C') = \dim_{\mathbb{C}} \mathscr{O}_{\mathbb{P}^2,p}/(F,G)$$

where, for an algebraic variety X and $p \in X$, $\mathscr{O}_{X,p}$ is the stalk at p of the structure sheaf of X, i.e. the local ring of regular functions at p with maximal ideal $\mathfrak{m}_p = \{f \in \mathscr{O}_{X,p} : f(p) = 0\}$. Note that $I_p(C,C') \geq 1$ if and only if $p \in C \cap C'$ by the very definition. It is also worthwhile to note that intersection multiplicities may be computed in terms of affine coordinates: If $p = [p_0 : p_1 : p_2]$ and $p_0 \neq 0$ - i.e. p lies in the affine open set $\{[x : y : z] : x \neq 0\}$ - then

$$\dim_{\mathbb{C}} \mathscr{O}_{\mathbb{P}^2,p}/(F,G) = \dim_{\mathbb{C}} \mathscr{O}_{\mathbb{A}^2,(p_1,p_2)}/(F(1,X_1,X_2), G(1,X_1,X_2)).$$

Here, we made use of the fact that affine and projective function fields are isomorphic, cf. [9, p. 75]. The following classical statement about the intersection theory of plane algebraic curves is indispensable for us and can be found as Theorem 4.8 in [9].

Theorem 3.1. *(Bézout) Let C and C' be two plane algebraic curves of degree d and d' respectively, which have no common components. Then C and C' intersect in dd' points counted with multiplicities, i.e.*

$$\sum_{p \in \mathbb{P}^2} I_p(C,C') = dd'.$$

The curves C and C' are said to intersect *transversely* at $p \in C \cap C'$ if both curves are smooth at p and $T_pC \cap T_pC' = \{p\}$, where T_pC and T_pC' denote the respective tangent spaces at p. By Nakayama's Lemma (cf. [9, p. 119]), this is the case if and only if $I_p(C,C') = 1$. Finally, a smooth point $p \in C$ is called a *flex* or *inflection point* of C if $I_p(C,T_pC) \geq 3$, and p is a *simple* flex if equality holds.

We denote by W_d the set of all projective plane curves of degree d, i.e. $W_d = \mathbb{P}(\mathbb{C}[X_0,X_1,X_2]_d)$. Note that two homogeneous polynomials which differ by a nonzero scalar define the same curve by this definition, but we - contrary to the next section - still distinguish two curves from one another if the prime powers occurring in both factorizations do not coincide.

Lemma 3.2. *The parameter space W_d is the complex-projective space of dimension $\binom{2+d}{2} - 1$.*

Proof. For any k-vector space of dimension n, we have that

$$\dim_k S^d(V) = \binom{n+d-1}{d},$$

where $S^d(V)$ denotes the d-th symmetric algebra of V. Since $\mathbb{C}[X_0,X_1,X_2]_d \cong S^d(\mathbb{C}^3)$, we may conclude that $\dim_{\mathbb{C}} \mathbb{C}[X_0,X_1,X_2]_d = \binom{2+d}{d}$ by the above equation and therefore identify W_d with $\mathbb{P}^{\binom{2+d}{2}-1} = \mathbb{P}^{\frac{d(3+d)}{2}}$. □

Let $N = \binom{2+d}{2}$.

Definition 3.3. *An algebraic subset $L \subset W_d = \mathbb{P}^{N-1}$ is called an* algebraic system of plane curves *of degree d. We refer to L as a* linear system of plane curves *of degree d if L is defined by linear equations.*

In particular, W_d itself is a linear system of plane curves. To prove smoothness of a general plane curve, we need the result that $\mathbb{P}^2$ is a complete variety, which is a special case of Theorem 3.12. in [7].

Lemma 3.4. *Let Y be any variety and $\pi : Y \times \mathbb{P}^2 \to Y$ be the projection to the first factor. Then π is a closed morphism.*

Theorem 3.5. *The subset of smooth curves is open and dense in W_d. In other words, a general plane curve of degree d is smooth.*

Proof. We have precisely N distinct monomials $X_0^i X_1^j X_2^k$ with $i+j+k=d$. An arbitrary homogeneous polynomial of degree d is of the form

$$f = \sum_{i+j+k=d} c_{i,j,k} X_0^i X_1^j X_2^k \in \mathbb{C}[X_0, X_1, X_2]_d$$

where we interpret the coefficients $c_{i,j,k}$ as indeterminates, i.e.

$$f \in \mathbb{C}[X_0, X_1, X_2, \{c_{i,j,k}\}].$$

Hence, the locus $Y := V(f)$ is a subset of $\mathbb{P}^2 \times \mathbb{A}^N$. Consider the projection map

$$pr_2 : \mathbb{P}^2 \times \mathbb{A}^N \longrightarrow \mathbb{A}^N$$

and the restriction

$$pr_{2|Y} : Y \longrightarrow \mathbb{A}^N.$$

For any $c = (c_{i,j,k}) \in \mathbb{A}^N$, we have that

$$pr_{2|Y}^{-1}(c) = \{([x_0 : x_1 : x_2], \{c_{i,j,k}\}) : \sum c_{i,j,k} x_0^i x_1^j x_2^k = 0\},$$

i.e. the first three homogeneous coordinates comprise the zero locus of the curve obtained by the coefficients c. Let

$$X = V\left(\frac{\partial f}{\partial X_0}, \frac{\partial f}{\partial X_1}, \frac{\partial f}{\partial X_2}\right) \subset V(f) \subset \mathbb{P}^2 \times \mathbb{A}^N$$

and note that the fibre $pr_{2|Y}^{-1}(c)$ in Y corresponds to a smooth curve if and only if it has empty intersection with X, since a curve is non-singular if its partial derivatives vanish nowhere simultaneously. By Lemma 3.4 we may conclude that $pr_{2|Y}(X)$ is a closed subset of $\mathbb{A}^N$, which is not the whole affine space since smooth curves exist. Take the complement of this set and recall that the map

$$p : \mathbb{A}^N_{\mathbb{C}} \longrightarrow \mathbb{P}^{N-1}_{\mathbb{C}}$$

is open, so the statement follows. □

Corollary 3.6. *A general plane curve of degree d is irreducible.*

Proof. This follows from the fact that any reducible plane curve is singular, which is obvious by Bézout's theorem: If $C = V(F_1) \cup V(F_2)$ is a decomposition into irreducible components, then there exists some $p \in \mathbb{P}^2$ such that $F_1(p) = F_2(p) = 0$. Now, $\frac{\partial(F_1F_2)}{\partial X_i} = \frac{(\partial F_1)F_2}{\partial X_i} + \frac{(\partial F_2)F_1}{\partial X_i}$ and so p is a singular point of C. □

We will now set up the morphism π. Recall that the *dual projective space* $\mathbb{P}^{n*}$ is the space of lines in $\mathbb{P}^n$. Now, let $I_0 \subset \mathbb{P}^2 \times \mathbb{P}^{2*}$ be the subset $I_0 = \{(p,l) : p \in l\}$.

Lemma 3.7. *The set I_0 is an irreducible threefold.*

Proof. This is an application of a much more general theorem. We let $\mathbb{G}(r+1,n+1)$ be the Grassmanian variety, i.e. the set of linear $r+1$-dimensional subspaces of the affine $n+1$-space considered as a projective variety via the Plücker embedding. We then define

$$I(r,d,n) = \{(X,e) \in \mathbb{P}^{\binom{n+d}{d}-1} \times \mathbb{G}(r+1,n+1) : e \subset X\},$$

that is, the set of tuples (X,e) where X is a projective hypersurface of degree d in $\mathbb{P}^n$ containing the linear subspace e. Note that $\mathbb{G}(1,n+1)$ is isomorphic to $\mathbb{P}^n$ (cf. [4, p. 107]), so we have $I_0 = I(0,1,2)$. Lemma 12.6 in [4] says that $I(r,d,n)$ is an irreducible subvariety of $\mathbb{P}^{\binom{n+d}{d}-1} \times \mathbb{G}(r+1,n+1)$ of dimension

$$(r+1)(n-r) + \binom{n+d}{d} - \binom{r+d}{d} - 1,$$

so we obtain the desired result. □

Define $I_d \subset W_d \times I_0$ as $I_d = \{(C,p,l) : I_p(C,l) \geq 3\}$, that is, the set of triples (C,P,l) such that P is a flex of C with tangent line l. If we let $\eta : I_d \to I_0$ be the projection on the second factor, we see that I_d is irreducible by Lemma 12.7 in [4] and Lemma 3.7.

Let $\pi : I_d \to W_d$ be the projection on the first factor. The fibre of a curve is in one-to-one correspondence with the set of its inflection points, hence we see that the cardinality of the general fibre - and thus, the degree of π - is given as the number of flexes on a general plane curve of degree d. By the previous theorem, we may assume such a curve to be smooth, which turns out to be helpful for plane cubic curves. In this case, every smooth cubic curve - that is, every elliptic curve - has precisely nine distinct flexes, so the problem of determining the degree of π is reduced to proving this statement.

3.2. The Classical Plücker Formulas One may ask oneself how many points exhibiting a certain property can be found on a plane algebraic curve. In our case, we would like to count the flexes, but one may similarly ask how many bitangents or certain singularities a given plane curve C has.

For a general cubic curve C, the answer to these questions is particularly easy: Such a curve will be smooth by the previous section and possess no bitangents by Bézout's theorem. Furthermore, every flex must obviously be simple - also by Bézout - which implies that there are exactly nine distinct flexes on C as we shall prove soon.

This result is in fact sufficient for our purposes, but we will nonetheless roughly investigate the more general case. If we pass on to higher degrees and allow the curve to be singular, the problem becomes vastly more complicated: Even if we restrict the types of singularities, the numerical invariants of a plane curve turn out to be intertwined. The *class formula* essentially says that the degree of the dual curve is reduced by the amount of simple double points and cusps, whereas the *inflection point formula* states that those singularities also reduce the number of flexes. We will outline the proofs of both formulas, which together make up the *classical Plücker relations*. We will mostly follow chapters 3, 4 and 5 in [5].

First of all, we have to introduce some elementary results on tangent lines and singularities, where the following basic proposition will come in handy.

Theorem 3.8. *(The "homogeneous" fundamental theorem of algebra.) Let k be an algebraically closed field and $F \in k[X_1, X_2]_d$ with $d > 0$. Then there exists a factorization*

$$F = (a_1X_2 - b_1X_1)^{n_1}(a_2X_2 - b_2X_1)^{n_2} \dots (a_lX_2 - b_lX_1)^{n_l},$$

with $[a_i : b_i] \in \mathbb{P}^1_k$ pairwise distinct and $\sum_{i=1}^{l} n_i = d$. In particular, $V(F)$ is finite as a subset of the projective line.

Proof. We may dehomogenize F with respect to, say, X_2. By assumption, the polynomial $F(X_1, 1)$ splits into linear factors, so the statement follows after homogenizing again. □

By definition, a singular point on a hypersurface is a point in which every partial derivative simultaneously vanishes. To introduce a more refined measure of how singular a point is, we start by defining the *order* of a curve at a point. We solely work with polynomials in two variables for now as these are all local statements.

Definition 3.9. *For $f \in \mathbb{C}[X_1, X_2]$ and $p = (p_1, p_2)$, consider the Taylor expansion of f around p*

$$f(X_1, X_2) = \sum_{k \geq 0} f_{(k)}, \quad f_{(k)} = \sum_{\mu+\nu=k} a_{\mu\nu}(X_1 - p_1)^{\mu}(X_2 - p_2)^{\nu},$$

where the coefficients $a_{\mu\nu}$ are given by

$$a_{\mu\nu} = \frac{1}{\mu!\nu!} \frac{\partial^{\mu+\nu}}{\partial X_1^{\mu} \partial X_2^{\nu}} f(p).$$

We define the order *of f at p as*

$$\operatorname{ord}_p(f) = \min\{k : f_{(k)} \neq 0\}.$$

For $C = V(f)$, we define $\operatorname{ord}_p(C) = \operatorname{ord}_p(f)$.

The following result is immediate from the definition.

Lemma 3.10. *Let f and p be as before. The order of f in p is bounded via*

$$0 \leq \mathrm{ord}_p(C) \leq \deg(C),$$

with $\mathrm{ord}_p(C) > 0$ *if and only if* $p \in C$. *Furthermore, smoothness in p is equivalent to* $\mathrm{ord}_p(C) = 1$. *In other words, C is singular in p if and only if* $\mathrm{ord}_p(C) > 1$.

Lemma 3.11. *Let $C = V(f) \subset \mathbb{A}^2$ be an algebraic curve and l a line through $p \in C$. Then* $\mathrm{ord}_p(C) \leq I_p(C,l)$, *and there are at most* $\mathrm{ord}_p(C)$ *lines through p for which this inequality is strict.*

Proof. After a linear transformation, we may assume that p is the origin. Let $f = \sum_{k=r}^{n} f_{(k)}$ be the Taylor expansion of f around p with $r = \mathrm{ord}_p(f)$ and $d = \deg(f)$, and let l be parametrized by $\gamma(T) = (\lambda_1 T, \lambda_2 T)$. Consider

$$g(T) := f(\gamma(T)) = \sum_{k=r}^{d} f_{(k)}(\lambda_1, \lambda_2) T^k.$$

Thus $I_p(C,l) = \mathrm{ord}_p(g) \geq \mathrm{ord}_p(f)$. Note that this inequality is strict if and only if $f_{(r)}(\lambda_1, \lambda_2) = 0$, and $f_{(r)}$ has at most r distinct zeroes in $\mathbb{P}^1$ by Lemma 3.8. □

We may now generalize our definition of tangent lines and obtain a description of a certain type of singularity in the process.

Definition 3.12. *Let C and l be as before, $p \in C \cap l$ and $r = \mathrm{ord}_p(C)$. The line l is* tangent *to C at p if $r < I_p(C,l)$. By the above proposition, there are at most r such lines. The point p is an* ordinary r-fold point *if this maximum is attained, i.e. there are r distinct tangent lines at p.*

Lemma 3.13. *Let $C = V(f) \subset \mathbb{A}^2$ be an algebraic curve which is smooth at the origin with tangent line $l = V(X_2)$. Suppose that $s = I_P(C,l) < \infty$ (i.e. l is not contained in C). Then*

$$f(X_1, X_2) = X_1^s g(X_1) + X_2 h(X_1, X_2)$$

with $g(0) \neq 0$ and $h(0,0) \neq 0$.

Proof. Let $r = \mathrm{ord}_{(0,0)}(f)$, $d = \deg(f)$ and consider the Taylor expansion around the origin

$$f(X_1, X_2) = \sum_{k \geq r} f_{(k)} = \sum_{k \geq r} \sum_{\mu+\nu=k} a_{\mu\nu} X_1^\mu X_2^\nu.$$

Let l be parametrized by $\gamma(X) = (X, 0)$ and define

$$g(X) := f(\gamma(X)) = \sum_{k \geq r} f_{(k)}(1,0) X^k.$$

Then $s = \mathrm{ord}_{(0,0)}(g)$, and so $f_{(k)}(1,0) = 0$ for all $k < s$. This implies $\frac{\partial}{\partial X_1^k} f(0,0) = 0$ for all such k, so we conclude

$$\begin{aligned} f(X_1,X_2) &= \sum_{k\geq r} f_{(k)} \\ &= \sum_{k\geq s} \sum_{\substack{\mu=k \\ \nu=0}} a_{\mu\nu} X_1^\mu X_2^\nu + \sum_{k\geq r} \sum_{\substack{\mu+\nu=k \\ \nu>0}} a_{\mu\nu} X_1^\mu X_2^\nu \\ &= X_1^s g(X_1) + X_2 h(X_1,X_2). \end{aligned}$$

□

The following property of the intersection number will be important (cf. [6, p.37]).

Remark 3.14. *Let $C_1, C_2 \subset \mathbb{A}^2$ be algebraic curves that have no common component. Then*

$$I_p(C_1,C_2) \geq \mathrm{ord}_p(C_1) \cdot \mathrm{ord}_p(C_2)$$

for $p \in C_1 \cap C_2$, and equality holds if and only if C_1 and C_2 do not have a common tangent at p.

Our next objective is to prove a special case of the inflection point formula: The existence of nine flexes on an elliptic curve. This will be done using fairly elementary methods, requiring only the notion of the *Hessian of a curve*. Corollary 3.6 allows us to restrict to irreducible plane curves, which we will do in order to simplify the computations, but note that all statements about the Hessian hold under the assumption that the curves we deal with contain no lines.

Definition 3.15. *Let $C = V(F) \subset \mathbb{P}^2$ be an irreducible curve of degree $d \geq 2$. Then*

$$H_F := \left(\frac{\partial^2 F}{\partial X_i \partial X_j} \right)_{0\leq i,j\leq 2}$$

is called the Hessian matrix *of F, and if $\deg(\det H_F) \geq 1$, we call $H(C) := V(\det(H_F))$ the* Hessian curve *of C.*

Obviously, H_F is a symmetric matrix and $H(C)$ is a plane curve of degree $3(d-2)$ if $\det(H_F)$ does not vanish entirely.

Lemma 3.16. *Let $F \in \mathbb{C}[X_0,X_1,X_2]_d$ and let $F_i := \frac{\partial F}{\partial X_i}$, $F_{ij} := \frac{\partial^2 F}{\partial X_j \partial X_i}$. Then*

$$\det(H_F) = \frac{d-1}{X_0^2} \det \begin{pmatrix} dF & F_1 & F_2 \\ (d-1)F_1 & F_{11} & F_{21} \\ (d-1)F_2 & F_{12} & F_{22} \end{pmatrix}$$

Proof. Clearly,

$$\det \begin{pmatrix} F_{00} & F_{10} & F_{20} \\ F_{01} & F_{11} & F_{21} \\ F_{02} & F_{12} & F_{22} \end{pmatrix} = \frac{1}{X_0X_1X_2} \det \begin{pmatrix} X_0F_{00} & X_0F_{10} & X_0F_{20} \\ X_1F_{01} & X_1F_{11} & X_1F_{21} \\ X_2F_{02} & X_2F_{12} & X_2F_{22} \end{pmatrix}$$

$$= \frac{1}{X_0} \det \begin{pmatrix} X_0F_{00}+X_1F_{01}+X_2F_{02} & X_0F_{10}+X_1F_{11}+X_2F_{22} & X_0F_{20}+X_1F_{21}+X_2F_{22} \\ F_{01} & F_{11} & F_{21} \\ F_{02} & F_{12} & F_{22} \end{pmatrix}.$$

Euler's formula states that, for any homogeneous polynomial $G \in k[X_0, X_1, \ldots, X_n]_d$, we have

$$\sum_{i=0}^{n} \frac{\partial G}{\partial X_i} = d \cdot G.$$

Applying this to each F_i, we may replace the first row of the latter matrix and obtain

$$\frac{d-1}{X_0} \det \begin{pmatrix} F_0 & F_1 & F_2 \\ F_{01} & F_{11} & F_{21} \\ F_{02} & F_{12} & F_{22} \end{pmatrix} = \frac{d-1}{X_0^2 X_1 X_2} \det \begin{pmatrix} X_0F_0 & X_1F_1 & X_2F_2 \\ X_0F_{01} & X_1F_{11} & X_2F_{21} \\ X_0F_{02} & X_1F_{12} & X_2F_{22} \end{pmatrix}$$
$$= \frac{d-1}{X_0^2} \det \begin{pmatrix} X_0F_0 + X_1F_1 + X_2F_2 & F_1 & F_2 \\ X_0F_{01} + X_1F_{11} + X_2F_{21} & F_{11} & F_{21} \\ X_0F_{02} + X_1F_{12} + X_2F_{22} & F_{12} & F_{22} \end{pmatrix}.$$

Using Euler's formula again to replace the first column, we get the desired equality. □

Corollary 3.17. *The Hessian $H(C)$ contains all the singular points of C.*

Proof. Let $p \in C$ be singular, where we may assume that $p_0 \neq 0$ since the Hessian is independent of the coordinates. Then the statement is immediate by Lemma 3.16, since the first row $\begin{pmatrix} dF & F_1 & F_2 \end{pmatrix}(p)$ vanishes. □

Theorem 3.18. *[5, Section 4.5] Let $C = V(F) \subset \mathbb{P}^2$ be an irreducible curve of degree $d \geq 2$. Then a smooth point $p \in C$ is a flex if and only if $p \in H(C)$. In particular, for a smooth curve C, the intersection $C \cap H(C)$ consists of all flexes on C. Finally, C and $H(C)$ intersect transversely in every simple flex.*

Proof. Let $p = [1:0:0] \in C$ be a smooth point with tangent line $t = V(X_2)$. Lemma 3.13 allows us to write $F(1, X_1, X_2)$ as

$$f(X_1, X_2) = X_1^k g(X_1) + X_2 h(X_1, X_2)$$

with $g(0) \neq 0$, $h(0,0) \neq 0$ and $k = I_p(C,t) \geq 2$. Hence, we write $X_1^k g = a_2 X_1^2 + a_3 X_1^3 + \ldots$ and $h = b + b_1 X_1 + b_2 X_2 + \ldots$, $b \neq 0$, where the dots stand for terms of higher order. Computing derivatives and using Lemma 3.16, we obtain

$$\det H_F(p) = (d-1)^2 \begin{pmatrix} 0 & 0 & b \\ 0 & 2a_2 & b_1 \\ b & b_1 & 2b_2 \end{pmatrix} = -2(d-1)^2 b^2 a_2.$$

Now, recall that p is a flex if and only if $k \geq 3$, which is equivalent to $a_2 = 0$. This concludes the first and second statement. It remains to prove that if $I_p(C,t) = 3$, then $I_p(C, H(C)) = 1$. First of all, we expand the determinant of $H_F(1, X_1, X_2)$ and obtain

$$(d-1)(f f_{11} f_{22} + f_1 f_{21} (d-1) f_2 + f_2 (d-1) f_1 f_{12}$$
$$- (d-1) f_2 f_{11} f_2 - (d-1) f_1^2 f_{22} - f f_{12} f_{21}),$$

where the lower case f denotes the dehomogenized polynomial. We define

$$\tilde{f} = f_2^2 f_{11} + f_1^2 f_{22} - 2 f_{12} f_2 f_1$$

and note that $I_p(C,H(C)) = I_0(V(f),V(\tilde{f}))$ (in the definition of $\tilde{f}$, we omit those terms containing f). A short calculation reveals that in $\tilde{f}$, the monomial X_1 has the coefficient $6a_3b$, which does not vanish if p is a simple flex. In particular, $V(\tilde{f})$ is smooth at p and the tangent lines of both curves are distinct, which proves the statement by Remark 3.14: Simply recall that smoothness at a point p is equivalent to having order one in p. □

Corollary 3.19. *A general plane cubic curve C has nine distinct flexes.*

Proof. Consider the polynomial $\det(H_F)$. Similarly to Theorem 3.5, one proves that $\det(H_F)$ is not identically zero for an open and dense subset of the parameter space W_d, or in other words, $H(C)$ is a cubic curve for a general C. The cubic C only has simple flexes by Bézout, so C and $H(C)$ intersect transversely in each point $C \cap H(C)$ by Theorem 3.18. Hence, applying Bézout again, we see that C has nine distinct flexes. □

One may prove the previous result for *all* smooth cubic curves, not just a general one. To ensure that $\det(H_F)$ is nonvanishing, we need the existence of at least one point that is not a flex, whilst the rest of the proof remains unchanged. This observation immediately yields a slight generalization.

Remark 3.20. *A smooth plane curve C of degree d such that every flex is simple has precisely $3d(d-2)$ distinct flexes.*

We now make several preparations for the formulation and proof of the Plücker relations. Unless stated otherwise, the curves are allowed to be reducible again.

Definition 3.21. *Let $C = V(F) \subset \mathbb{P}^2$ be an algebraic curve with $\deg(F) \geq 2$. For a point $q = [q_0 : q_1 : q_2] \in \mathbb{P}^2$, define*

$$F_q = q_0 \frac{\partial F}{\partial X_0} + q_1 \frac{\partial F}{\partial X_1} + q_2 \frac{\partial F}{\partial X_2}$$

and $C_q = V(F_q)$, the first polar *of C with respect to q.*

Theorem 3.22. *Let C and q be as before with the additional assumption that C contains no lines through q. Then C_q is an algebraic curve of degree $\deg(C) - 1$ that has no common component with C. The intersection $C \cap C_q$ consists of all the singularities of C as well as the points on C whose tangents pass through q.*

Proof. Let $d = \deg(C)$ and $q = [1 : 0 : 0]$ after a suitable coordinate transformation. Suppose $\deg(F_q) < d-1$, which immediately implies $F_q = 0$. Hence, $F(X_0,X_1,X_2) = F(1,X_1,X_2) \in \mathbb{C}[X_1,X_2]$ is homogeneous of degree d, so Lemma 3.8 tells us that C contains a line through q (in fact, C degenerates into a union of lines).
Now, suppose F and F_q share a common prime factor G. Then

$$F = GH \text{ and } GH' = F_q = \frac{\partial F}{\partial X_0} = H\frac{\partial G}{\partial X_0} + G\frac{\partial H}{\partial X_0},$$

hence G also divides $H\frac{\partial G}{\partial X_0}$. If $\frac{\partial G}{\partial X_0}$ is nonzero, then G divides H because it is prime by assumption and $\frac{\partial G}{\partial X_0}$ is of strictly smaller degree. Thus, G^2 is a divisor of F, but

this is not possible: We may always choose F to be minimal, in the sense that it is not divisible by the square of any prime (cf. Section 3.1). On the other hand, if $\frac{\partial G}{\partial X_0}$ vanishes, then $G \in \mathbb{C}[X_1, X_2]$ is a linear factor, which implies that C contains a line through q, contradicting our assumption. The statement about the intersection $C \cap C_q$ is obvious from the definitions. □

Theorem 3.23. *[5, Proposition 4.3] Let $q \notin C$ and $p \in C$ be a point with simple tangent line l (i.e. $I_p(C,l) = 2$) passing through q. Then the curve C and its polar C_q intersect transversely in p.*

Definition 3.24. *We define the* dual curve *of C as*

$$C^* = \{l \in \mathbb{P}^{2*} : l \text{ is tangent to } C\}.$$

We define the class *of C as the maximal number of tangents to smooth points of C that pass through a fixed point in $\mathbb{P}^2$, and denote this value d^* if C is a curve of degree d.*

We will need three results on the dual curve: That it is algebraic, that it is irreducible if C itself was irreducible and that dualizing C^* yields C. We expect the class of a curve to be related to the dual curve, which will be formalized by the class formula. First of all, the algebraicity of C^* relies on the following lemma, which is proven in Chapter 8 of [5].

Lemma 3.25. *Let $C \subset \mathbb{P}^2$ be an algebraic curve and let p be some point contained in C. A line $l \subset \mathbb{P}^2$ is tangent to C at p is and only if there is a sequence of smooth points $\{p_\nu\}_{\nu \in \mathbb{N}} \subset C$ converging to p such that*

$$l = \lim_{\nu \to \infty} T_{p_\nu} C.$$

Theorem 3.26. *(Duality) (1) The dual curve is algebraic.*
(2) If C is irreducible, then so is C^*. Furthermore, $C^{**} = C$.

Proof. (1) Let $C = V(F)$, $\deg F = d$. We consider the intersection of C with an arbitrary line $l = V(y_0X_0 + y_1X_1 + y_2X_2)$, where we may assume that $y_2 \neq 0$. Hence, we can solve the equation of l for X_2 and thus obtain a polynomial

$$G(X_0, X_1) := y_2^d F(X_0, X_1, -\frac{1}{y_2}(y_0X_0 + y_1X_1)) = b_0X_1^d + b_1X_1^{d-1}X_0 + \ldots + b_dX_0^d$$

the zero locus of which coincides with $C \cap l$. Note that each b_i is homogeneous of degree d in y_0, y_1 and y_2 - which we now interpret as variables - and so the resultant of $g(X_1) := G(1, X_1)$ and g' is an element of $\mathbb{C}[Y_0, Y_1, Y_2]_{2d^2-d}$. Define

$$C' := V(b_0\Delta_g) = V((-1)^{\frac{d(d-1)}{2}} \operatorname{res}(g, g')) \subset \mathbb{P}^{2*},$$

which is an algebraic curve of degree $2d^2 - d$. This is not yet the dual curve, but contains it: If $l \in C^*$, that is, l is tangent to C in some point p, then $I_p(C,l) > 1$ and thus G has a multiple zero. If this point is $[0:1]$, then $G(0,1) = b_0(y) = 0$, otherwise g has a multiple zero and so its discriminant Δ_g vanishes. In both cases, $l \in C'$ follows. As we will now see, C' contains two sorts of lines which we must eliminate.

Consider a point $x = [x_0 : x_1 : x_2] \in C \cap V(X_0)$, where we may assume that $[0:0:1] \notin C$ and so $x_1 \neq 0$. Any point $y \in \mathbb{P}^{2*}$ that corresponds to a line through x must then be of the form $[y_0 : -x_2 : x_1]$ for some y_0. By assumption, $G(0,x_1)$ vanishes, so $b_0(y)x_1^n = G(0,x_1) = 0$ and thus $b_0(y) = 0$. Hence $-x_2Y_1 + x_1Y_2$ divides b_0 and consequently,

$$l'_x := V(-x_2Y_1 + x_1Y_2) \subset C'.$$

Recall Lemma 3.11, which said that for any curve C and line $l = V(y_0X_0 + y_1X_1 + y_2X_2)$ through $x = [x_0 : x_1 : x_2] \in C$, we have $\mathrm{ord}_x(C) \leq I_x(C,l)$. Hence, if x is singular - that is, $\mathrm{ord}_x(C) > 1$ - then we must have $I_x(C,l) > 1$ and thus g has a multiple zero. Equivalently, $\Delta_g(y) = 0$, so the set of lines through x is contained in C':

$$l''_x := V(x_0Y_0 + x_1Y_1 + x_2Y_2) \subset C'.$$

We now claim that

$$C'' := C' \setminus \left(\bigcup_{x \in C \cap V(X_0)} l'_x \cup \bigcup_{x \in Csing} l''_x \right) \subset C^*.$$

If $y = [y_0 : y_1 : y_2]$ is contained in the left-hand side, then $y \in V(b_0\Delta_g)$, but y neither intersects a point in $C \cap V(X_0)$ nor a singularity. This implies $y \notin V(b_0)$, because otherwise G would vanish in $[0:1]$, contradicting the first condition. Hence $y \in V(\Delta_g)$, so g has a multiple zero and thus $I_x(C \cap l) > 1$ for some x. But x must be smooth by the second condition, and so the line l defined by y is tangent to C, which we had to show.

It remains to prove that the Zariski closure of C'' is C^*. First of all, note that the amount of lines we have taken out of C' is finite, so the analytic and Zariski closure of C'' coincide. Hence the statement follows from Remark 3.25.
(2) A full proof of this statement is beyond the scope of this section, but can be found in Chapters 5 and 9 of [5]. The crucial point is the existence of a compact connected Riemann surface S and a holomorphic map $\phi : S \to C$ whose restriction to $\phi^{-1}(C_{ns})$ is biholomorphic. This gives rise to a holomorphic parametrization $\phi^* : S \to C^*$ of the dual curve, which one uses to prove both assertions: These are Sections 5.3, 5.4 and 5.5 in [5]. □

In the course of this proof, one obtains the local numerical invariants of a holomorphic parametrization. More specifically, if $0 \in U \subset \mathbb{C}$ is open and $\phi : U \to \mathbb{P}^2$ holomorphic such that $\phi(U)$ is not contained in a line, then there exist unique integers α_1, α_2 and a suitable coordinate transformation such that

$$\phi(t) = [1 : t^{1+\alpha_1} + \ldots : t^{2+\alpha_1+\alpha_2} + \ldots].$$

When we parametrize a curve C with $\phi(0) = p$, then $1 + \alpha_1 = \mathrm{ord}_p(C)$ and $2 + \alpha_1 + \alpha_2 = I_p(C, T_pC)$ (Section 5.4). In particular, we see that p is a singular point of C if and only if $\alpha_1 \neq 0$, whereas p is a flex of C if and only if $\alpha_1 = 0$ and $\alpha_2 \neq 0$. Moreover, the local numerical invariants of the parametrization ϕ^* are related to ϕ via $\alpha_1^* = \alpha_2$ and $\alpha_2^* = \alpha_1$ (Section 5.5). We will now characterize two types of singularities of plane curves.

Definition 3.27. *Let $p \in C$ be singular and* $\mathrm{ord}_p(C) = 2$. *We call p a* simple double point *if C has two tangents at p such that $I_p(C,T) = 3$ for each tangent T. We call p a* simple cusp *if C has just one tangent at p with $I_p(C,T) = 3$.*

Remark 3.28. *[5, Section 5.6] Each branch of a simple double point p has a local (affine) parametrization $(t^2 + \ldots, t)$, and a simple cusp is parametrized via $(t^2, t^3 + \ldots)$.*

In particular, the local numerical invariants of a simple cusp are given as $\alpha_1 = 1$ and $\alpha_2 = 0$, hence, a simple cusp of C corresponds to a simple flex of C^* and conversely. The following is a special case of the class formula.

Theorem 3.29. *If C is irreducible and* $\deg(C) \geq 2$, *then $d^* = \deg(C^*)$.*

Proof. Let $q \in \mathbb{P}^2$. The set of all lines in $\mathbb{P}^2$ through q is itself a line $q^* \subset \mathbb{P}^{2*}$, and each point in $q^* \cap C^*$ corresponds to a tangent to C through q. By Bézout's theorem, both curves intersect in $\deg(C^*)$ points, counted with multiplicities. Now we choose the point q such that these points of intersection are transversal.

Consider a point $r \in \mathbb{P}^{2*}$ which does not lie on C^*. The polar C_r^* and C^* intersect in finitely many points, so a general line q^* through r will not meet $C^* \cap C_r^*$, and thus q^* is nowhere tangent to C^* (cf. Theorem 3.22). This concludes the statement, as there are now $\deg(C^*)$ distinct points of intersection, each of which corresponds to a tangent line to some fixed point $q \in \mathbb{P}^2$ (which is the point associated to the line q^* we constructed). □

Lemma 3.30. *If C is smooth, then $d^* = d(d-1)$.*

Proof. Let $q \in \mathbb{P}^2$. By Theorem 3.22, the number of tangents to C through q is precisely the number of distinct points in $C \cap C_q$. This in turn is maximized if each point of intersection is transversal. Now, Theorem 3.23 tells us how to do this: Each tangent to C through q must be simple, but this condition is satisfied by a general point q in the projective plane, simply because the number of inflection points - and hence, the number of inflectional tangents - is finite. Finally, Bézout's theorem implies that there are $d(d-1)$ points in the intersection of C and C_q, and q was constructed such that all points are distinct from one another. □

We may now generalize Corollary 3.19 and Lemma 3.30.

Theorem 3.31. *Let C be an irreducible curve of degree $d \geq 2$ such that C and C^* only have simple cusps and simple double points. Denote the amount of those singularities by s, s^* and b, b^*, respectively. We then have*
(1) $d^* = d(d-1) - 2b - 3s$ (class formula)
(2) $s^* = 3d(d-2) - 6b - 8s$ (inflection point formula).

Proof. Similar to the proof of Lemma 3.30, we note that a general point $q \in \mathbb{P}^2$ does not lie on an inflectional tangent or bitangent, and intersect C with C_q. By definition of d^*, there are $\{p_1, \ldots, p_{d^*}\}$ smooth points whose tangents pass through q. Now, by the choice of q and Theorem 3.23, the polar P_qC and C intersect transversely in each p_i. Hence, Bézout's Theorem yields

$$d(d-1) = \sum_{p \in C_{ns}} I_p(C, P_qC) + \sum_{p \in C_{sing}} I_p(C, P_qC) = d^* + \sum_{p \in C_{sing}} I_p(C, P_qC).$$

The class formula then follows from the fact that C and I_pC intersect with multiplicities 2 and 3 in a simple double point or simple cusp, respectively. This calculation can be found in [5, p. 91]. For the inflection point formula, we note that C only has simple flexes by assumption on the dual curve and consider $C \cap H(C)$. Recall that both curves intersect transversely in a simple flex, hence we get

$$3d(d-2) = \sum_{p \in C_{ns}} I_p(C, H(C)) + \sum_{p \in C_{sing}} I_p(C, H(C)) = s^* + \sum_{p \in C_{sing}} I_p(C, H(C)).$$

It thus remains to compute the intersection numbers, namely that C and $H(C)$ intersect with multiplicity 6 and 8 in a simple double point or simple cusp, respectively (cf. [5, p. 92]). □

A generalization of those formulas to encompass arbitrary singular curves can be found as Theorem 2 in [3, Chapter 9.1]. In any case, the flexes of higher order have to be counted with multiplicities: That is, a smooth point p with $I_p(C, T_pC) > 3$ counts as $I_p(C, T_pC) - 2$ flexes. Hence, to prove that all $3d(d-2)$ flexes of a general plane curve C are distinct, one would necessarily have to show that C just has simple flexes.

3.3. Elliptic Curves and Complex Tori This section follows chapters II, III and VI of [11]. Recall that an elliptic curve - that is, a smooth plane cubic - carries the structure of an abelian group (cf. [11, Paragraph 2]).

We define a *lattice* $\Lambda \subset \mathbb{C}$ to be the $\mathbb{Z}$-module generated by two $\mathbb{R}$-linearly independent complex numbers. Our aim in this section will be to show that an elliptic curve can be expressed as a torus $\mathbb{C}/\Lambda$ for some suitable lattice, in the sense that there exists an isomorphism between both groups. More precisely then, we focus on those theorems and definitions in [11] necessary to prove this assertion.

We first of all introduce the Weierstass $\wp$-function, and then we derive some of its elementary properties.

Definition 3.32. *An* elliptic function *relative to the lattice Λ is a meromorphic function $f : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ such that $f(z+w) = f(z)$ for all $z \in \mathbb{C}$ and $w \in \Lambda$.*

The field of all elliptic functions relative to Λ, denoted $\mathbb{C}(\Lambda)$, may therefore be seen as meromorphic functions on the torus $\mathbb{C}/\Lambda$.

Definition 3.33. *A* fundamental parallelogram *for Λ is a set*

$$D = \{a + t_1\omega_1 + t_2\omega_2 : t_1, t_2 \in [0,1)\}$$

where $a \in \mathbb{C}$ and $\{\omega_1, \omega_2\}$ is a $\mathbb{Z}$-basis of Λ.

Elementary complex analysis shows that for any holomorphic function $f(z)$ on an open domain and any isolated singularity $w \in \mathbb{C}$ that is not essential, there exists a smallest number $k \in \mathbb{Z}$ such that $(z-w)^k f(z)$ has a liftable singularity in w. We then define $\mathrm{ord}_w(f) = -k$ as the order of f in w, which is easily seen to be a discrete valuation. Hence, poles of f are precisely those points in which f has negative order.

Definition 3.34. *The* order *of an elliptic function $f(z)$ is the number of poles in a fundamental parallelogram D counted with negative multiplicity, i.e.*

$$\operatorname{ord}(f) = \sum_{\substack{w \in D \\ pole}} -\operatorname{ord}_w(f)$$

This is a finite sum because D is compact and poles are required to be discrete, and furthermore, the definition is independent of the choice of D by periodicity.

An elliptic function $f(z)$ of order zero is holomorphic. In particular, it is continuous on the closure of every fundamental parallelogram $\overline{D}$ which is of course compact, hence $|f(z)|$ must be bounded on D. Periodicity of f then implies boundedness on $\mathbb{C}$ and f must therefore be constant by Liouville's theorem.

Furthermore, for an arbitrary elliptic function $f(z)$, we may choose D such that ∂D contains no poles of f. We have that

$$2\pi i \sum_{w \in D} \operatorname{res}_w(f) = \int_{\partial D} f(z)dz$$

by the residue theorem. The latter expression vanishes because f is periodic with respect to Λ, from which it immediately follows that there exist no elliptic functions of order one.

The following definition is not only important as a mean to describe elliptic curves, but also turns out to be an example of an elliptic function of order two. Additionally, we briefly introduce Eisenstein series which will be needed later on.

Definition 3.35. *The* Weierstrass $\wp$-function *relative to the lattice Λ is defined as*

$$\wp(z;\Lambda) = \wp(z) = \frac{1}{z^2} + \sum_{\substack{w \in \Lambda \\ w \neq 0}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right).$$

The Eisenstein series *of weight $2k$ (relative to Λ) is given by*

$$G_{2k}(\Lambda) = G_{2k} = \sum_{\substack{w \in \Lambda \\ w \neq 0}} \frac{1}{w^{2k}}.$$

Lemma 3.36. *G_{2k} converges absolutely for all $k > 0$.*

Proof. Let $\{\omega_1, \omega_2\}$ be a $\mathbb{Z}$-basis of Λ. We have that

$$\sum_{\substack{w \in \Lambda \\ w \neq 0}} \frac{1}{|w|^{2k}} = \sum_{\substack{(m,n) \in \mathbb{Z}^2 \\ (m,n) \neq (0,0)}} \frac{1}{|(m\omega_1)^2 + (m\omega_2)^2|^{2k}} \leq \sum_{\substack{w \in \Lambda \\ 0 < |w| \leq 1}} \frac{1}{|w|^{2k}} + \int_{\mathbb{R}^2 \setminus B_1(0)} \frac{dxdy}{(x^2+y^2)^{2k}}.$$

The sum over all non-zero lattice points within the unit disk is finite. Substituting $x = r\cos\theta$ and $y = r\sin\theta$, we can estimate the integral as follows:

$$\int_0^{2\pi} \int_1^{\infty} \frac{r}{(r^2\cos^2\theta + r^2\sin^2\theta)^{2k}} dr d\theta = 2\pi \int_1^{\infty} \frac{dr}{r^{4k-1}} < \infty.$$

□

Theorem 3.37. *The Weierstrass $\wp$-function is holomorphic on $\mathbb{C}\backslash\Lambda$ with double poles in each lattice point. It is an even elliptic function of order two, and its derivative $\wp'$ is an uneven elliptic function of order three.*

Proof. We show that the series defining the $\wp$-function converges absolutely and uniformly on every compact subset of $\mathbb{C}\backslash\Lambda$. By the inverse and the usual triangle inequality, we have that

$$\left|\frac{1}{(z-w)^2}-\frac{1}{w^2}\right| = \left|\frac{z(2w-z)}{w(z-w)^2}\right| = \frac{|z||2-\frac{z}{w}|}{|w|^3|1-\frac{z}{w}|^2} \leq \frac{|z|(2+|\frac{z}{w}|)}{|w|^3(1-|\frac{z}{w}|)^2}.$$

Since the underlying set is compact, we may assume that $|z| \leq r$ for some positive r. Furthermore, assuming that $|w| \geq 2r$ (which implies $\frac{|z|}{|w|} \leq \frac{1}{2}$), we can estimate all but a finite number of terms:

$$\frac{|z|(2+|\frac{z}{w}|)}{|w|^3(1-|\frac{z}{w}|)^2} \leq \frac{r\frac{5}{2}}{|w|^3\frac{1}{4}} \leq \frac{10r}{|w|^3}.$$

As in the proof of the previous lemma, $\sum_{\substack{w\in\Lambda\\ w\neq 0}} \frac{1}{|w|^3}$ converges, which establishes the claim. Thus, by a theorem of Weierstrass, $\wp$ is a holomorphic function on $\mathbb{C}\backslash\Lambda$ and we may differentiate term-wise to obtain $\wp'$:

$$\wp'(z) = -2\sum_{w\in\Lambda}\frac{1}{(z-w)^3}.$$

It suffices to show periodicity with respect to a basis of Λ, so we fix a basis vector ω and consider

$$\wp'(z+\omega) = -2\sum_{w\in\Lambda}\frac{1}{(z+\omega-w)^3} = \wp'(z),$$

which proves ellipticity of $\wp'$. Consequently, $g(z) := \wp(z+\omega)-\wp(z)$ is a constant function because its derivative vanishes. Observing that $\frac{1}{2}\omega \notin \Lambda$ and that $\wp$ is an even function, we have

$$g(-\frac{1}{2}\omega) = \wp(\frac{1}{2}\omega)-\wp(-\frac{1}{2}\omega) = 0,$$

so $g(z) = 0$ everywhere: This proves that $\wp$ is also elliptic. The remaining statements are obvious. □

Remark 3.38. *The field of elliptic functions relative to a lattice Λ is given by $\mathbb{C}(\wp,\wp')$, i.e. every elliptic function is expressible as a rational function in the Weierstrass $\wp$-function and its derivative.*

In the next step, the Laurent expansion of the $\wp$-function around the origin will be computed and expressed in terms of the Eisenstein series. This makes it possible to deduce a differential equation that is satisfied by $\wp$ and its derivative, which is closely related to elliptic curves in their Weierstrass normal form.

Lemma 3.39. *The Laurent series of the Weierstrass $\wp$-function in a neighbourhood of zero is given by*

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{n=1}^{\infty} (2n+1) G_{2(n+1)}(\Lambda) z^{2n}.$$

Proof. The function $g(z) := \wp(z) - \frac{1}{z^2}$ is even and holomorphic around the origin. All its Taylor coefficients with an odd index must therefore vanish, so it has a series expansion of the form

$$g(z) = \sum_{n=0}^{\infty} a_{2n} z^{2n}, \;\; a_{2n} = \frac{g^{(2n)}(0)}{(2n)!}. \tag{2}$$

We have $a_0 = 0$ since $g(0) = 0$, and for $n > 0$, we inductively obtain

$$g^{(n)}(z) = \frac{d^n}{dz^n} \sum_{\substack{w \in \Lambda \\ w \neq 0}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right) = (-1)^n (n+1)! \sum_{\substack{w \in \Lambda \\ w \neq 0}} \frac{1}{(z-w)^{n+2}}.$$

In particular, the coefficients are given as

$$a_{2n} = (-1)^{2n} \frac{(2n+1)!}{(2n)!} \sum_{\substack{w \in \Lambda \\ w \neq 0}} \frac{1}{w^{2(n+1)}} = (2n+1) G_{2(n+1)}(\Lambda),$$

and so - substituting these terms in equation (2) - the proof is complete. □

Lemma 3.40. *The Weierstrass $\wp$-function relative to Λ and its derivative satisfy the relation*

$$\wp'(z)^2 = \wp(z)^3 - g_2 \wp(z) - g_3, \tag{3}$$

where $g_2 = 60 G_4(\Lambda)$ and $g_3 = 140 G_6(\Lambda)$.

Proof. Consider the Laurent expansion $\wp(z) = z^{-2} + 3G_4 z^2 + 5G_6 z^4 + \ldots$. One can derive this expression and square it to obtain the series for $\wp'^2$:

$$\wp'(z) = -2z^{-3} + 6G_4 z + 20 G_6 z^3 + \ldots,$$
$$\wp'(z)^2 = 4z^{-6} - 24 G_4 z^{-2} - 80 G_6 + \ldots.$$

Similarly, we have that

$$\wp(z)^2 = z^{-4} + 6G_4 + 10 G_6 z^2 + \ldots,$$
$$\wp(z)^3 = z^{-6} + 9G_4 z^{-2} + 15 G_6 + \ldots.$$

It is sufficient to expand $\wp^3$ and $\wp'^2$ only up to the third nonzero term since those of higher order are holomorphic in z and will become irrelevant in the following argument. Let $a, b, c \in \mathbb{C}$ and consider

$$\wp'(z) + a\wp(z)^3 + b\wp(z) + c = \frac{4+a}{z^6} + \frac{-24G_4 + b + 9aG_4}{z^2} - 80G_6 + 15aG_6 + c + \ldots$$

For this expression to vanish, we in particular need $a = -4$ which then implies $b = 60G_4$ and $c = 140G_6$. The left hand side is now a holomorphic elliptic function which is zero for $z = 0$, and therefore it globally vanishes which proves the assertion. □

Definition 3.41. *An affine cubic C in* Weierstrass form *is given by an equation*

$$X_2^2 = 4X_1^3 - g_2X_1 - g_3,$$

where $g_2, g_3 \in \mathbb{C}$. The corresponding projective curve is denoted

$$C_{g_2,g_3} : X_0X_2^2 = 4X_1^3 - g_2X_0^2X_1 - g_3X_0^3.$$

Remark 3.42. *The curve C_{g_2,g_3} is smooth - that is, an elliptic curve - if and only if $\Delta := g_2^3 - 27g_3^2 \neq 0$. Any smooth cubic is projectively equivalent to some C_{g_2,g_3} (Propositions 4.22. and 4.23. in [9]).*

We now formulate the main theorem of this chapter.

Theorem 3.43. *[11, Corollary 5.1.1.] Let C_{g_2,g_3} be an elliptic curve over the complex numbers in Weierstrass form. Then there exists a lattice Λ with $g_2 = 60G_4(\Lambda)$ and $g_3 = 140G_6(\Lambda)$ such that*

$$\begin{aligned}\Phi : \mathbb{C}/\Lambda &\longrightarrow C_{g_2,g_3}\\ \Phi(z) &= [1 : \wp(z;\Lambda) : \wp'(z;\Lambda)] \text{ if } z \notin \Lambda,\\ \Phi(z) &= [0:0:1] \text{ if } z \in \Lambda\end{aligned}$$

is a group isomorphism.

One may even show that Φ is an isomorphism of complex Lie groups, but this does not concern us here.

The proof will be done in three parts. We first of all assume that if a lattice is given and C is the elliptic curve in Weierstrass form associated to the quantities g_1 and g_2, then Φ is well-defined and bijective. In the next step, we prove that it is a group homomorphism using the language of divisors, and finally, we address the existence of a lattice Λ having prescribed quantities g_1, g_2.

Lemma 3.44. *The map Φ is well-defined and bijective.*

Proof. Let $C' \subset \mathbb{A}^2$ be the dehomogenization of C, that is, the locus of the equation $X_2^2 = 4X_1^3 - g_2X_1 - g_3$. The map

$$\begin{aligned}\Phi' : \big(\mathbb{C}/\Lambda\big)\backslash\{0\} &\longrightarrow C'\\ z &\longmapsto (\wp(z), \wp'(z))\end{aligned}$$

is well-defined by periodicity of $\wp$ and $\wp'$ as well as the differential equation that is satisfied by both functions.

Let $(p_1, p_2) \in C'$. Since a nonconstant elliptic function f attains each value $\mathrm{ord}(f)$ times and since every pole of $\wp$ is a lattice point, there exists a $z \in \big(\mathbb{C}/\Lambda\big)\backslash\{0\}$ such that $\wp(z) = p_1$. Hence, $\wp'(z)^2 = p_2^2$ by equation (3) and therefore - recalling that $\wp$ is even and $\wp'$ uneven - we either have $(\wp(z), \wp'(z)) = (p_1, p_2)$ or $(\wp(-z), \wp'(-z)) = (p_1, p_2)$, which proves surjectivity of Φ'.

Suppose that $(\wp(z), \wp'(z)) = (\wp(w), \wp'(w))$ for $z, w \in \big(\mathbb{C}/\Lambda\big)\backslash\{0\}$. In particular, $g(x) = \wp(x) - \wp(w)$ is an elliptic function of order two, and its zeroes are given as

$x = w$ and $x = -w$. Hence, we either have $z \equiv w \mod \Lambda$, in which case there is nothing to show, or $z \equiv -w \mod \Lambda$. The latter case implies

$$\wp'(z) = \wp'(-w) = -\wp'(w) = -\wp'(z),$$

so $\wp'(z) = 0$. Now, let $\{\omega_1, \omega_2\}$ be a basis of Λ and $\omega \in \{\frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}\}$. Then $2\omega \in \Lambda$ and

$$\wp'(\omega) = \wp'(\omega - 2\omega) = \wp'(-\omega) = -\wp'(\omega),$$

so $\wp'$ vanishes at those three distinct points. Since $\wp'$ is an elliptic function of order three, it cannot have any other root, so $2z$ must be one of them. In particular, $2z$ is contained in Λ, which gives $z \equiv w \mod \Lambda$ and hence proves injectivity of Φ'.
Finally, the map

$$\begin{aligned} C' &\xrightarrow{\iota} C \\ (p_1, p_2) &\longmapsto [1 : p_1 : p_2] \end{aligned}$$

is onto except for those points in the codomain with vanishing first coordinate p_0. If $[0 : p_1 : p_2] \in C$, then necessarily $p_1 = 0$ and $p_2 \neq 0$ by the homogeneous equation of C, so only $[0 : 0 : 1]$ does not lie in the image of $\iota \circ \Phi'$. Hence, Φ is bijective. □

To prove that Φ is a group homomorphism, we will introduce a second group structure $\mathrm{Pic}^0(C)$, one that we may define for any smooth curve. In our case - when C is elliptic - the curve C endowed with the geometric group structure and $\mathrm{Pic}^0(C)$ will be isomorphic, which is a key step in proving our main theorem.

Definition 3.45. *Let C be an algebraic curve. The* divisor group *of C is the free abelian group generated by the points of C, that is*

$$\mathrm{Div}(C) = \bigoplus_{p \in C} \mathbb{Z}.$$

An element of $\mathrm{Div}(C)$ *will be denoted by*

$$D = \sum_{p \in C} n_p(p),$$

where all but finitely many coefficients vanish. The degree *of a divisor D is the sum* $\deg D = \sum_{p \in C} n_p$. *The divisors of degree 0 form a subgroup of* $\mathrm{Div}(C)$ *which we call* $\mathrm{Div}^0(C)$.

We now assume C to be smooth and consider the local ring $\mathcal{O}_{C,p}$ with maximal ideal $\mathfrak{m}_P = \{f \in \mathcal{O}_{C,p} : f(p) = 0\}$. Recall that there is a natural isomorphism of vector spaces (cf. [9, Theorem 3.14])

$$T_pC \cong (\mathfrak{m}_p/\mathfrak{m}_p^2)^*,$$

so in particular, $\dim_{\mathbb{C}} \mathfrak{m}_p/\mathfrak{m}_p^2 = 1$ for a smooth point p. By Nakayamas lemma, $\mathfrak{m}_p$ is a principal ideal generated by some $t \in \mathfrak{m}_p$. We employ two results from commutative algebra:

Remark 3.46. *(1) For any noetherian integral domain A and any non-unit $t \in A$, we have that $\bigcap_{k=1}^{\infty}(t^k) = (0)$.*
(2) Let $(A, \mathfrak{m})$ be a local integral domain with quotient field $K = \mathrm{Quot}(A)$ and $\mathfrak{m} = (t) \neq 0$. If $\bigcap_{k=1}^{\infty}(t^k) = (0)$, then the following two statements hold:

1. *For each non-zero $a \in A$, there exists a unique $k > 0$ and a unit α such that $a = \alpha t^k$ (t is called a* uniformizing parameter*).*
2. *The map $v : K^\times \to \mathbb{Z}$ which sends each a to $k > 0$ (as in 1.) and each a/a' to $k - k' \in \mathbb{Z}$ is a discrete valuation with valuation ring A.*

We may thus conclude that, for each non-singular point $p \in C$, the map

$$\begin{aligned} \mathrm{ord}_p : K(C)^\times &\longrightarrow \mathbb{Z} \\ g/h &\longmapsto \mathrm{ord}_p(g) - \mathrm{ord}_p(h), \end{aligned}$$

where $\mathrm{ord}_p(f) = \max\{k : f \in \mathfrak{m}_p^k\}$ for $f \in \mathscr{O}_{C,p}$, is a discrete valuation on the function field $K(C) = \mathrm{Quot}(\mathscr{O}_{C,p})$ with valuation ring $\mathscr{O}_{C,p}$.

Definition 3.47. *For a nonzero rational function $f \in K(C)$, we define the* divisor associated to f *by*

$$\mathrm{div}(f) = \sum_{p \in C} \mathrm{ord}_p(f)(p) \in \mathrm{Div}(C).$$

We call a divisor D principal *if $D = \mathrm{div}(f)$ for some $f \in K(C)^\times$.*

Note that since ord_p is a discrete valuation, the map

$$\begin{aligned} \mathrm{div} : K(C)^\times &\longrightarrow \mathrm{Div}(C) \\ f &\longmapsto \mathrm{div}(f) \end{aligned}$$

is a group homomorphism. In particular, the set of principal divisors form a subgroup of $\mathrm{Div}(C)$.

Definition 3.48. *Two divisors D and D' are called* linearly equivalent *if $D - D' = \mathrm{div}(f)$ for some $f \in K(C)^\times$, i.e. if their difference is principal. The* Picard group *of C, called* $\mathrm{Pic}(C)$*, is the quotient of* $\mathrm{Div}(C)$ *by the subgroup of principal divisors, i.e.*

$$\mathrm{Pic}(C) = \mathrm{Div}(C)/\mathrm{div}(K(C)^\times).$$

The principal divisors form a subgroup of $\mathrm{Div}^0(C)$*, so we may define*

$$\mathrm{Pic}^0(C) = \mathrm{Div}^0/\mathrm{div}(K(C)^\times),$$

the degree zero part of the Picard group of C.

Definition 3.49. *We call a divisor $D \in \mathrm{Div}(C)$* effective*, denoted by $D \geq 0$, if $n_p \geq 0$ for all $p \in C$. Hence, the group $\mathrm{Div}(C)$ is partially ordered via $D_1 \geq D_2$ if $D_1 - D_2$ is effective. For each divisor $D \in \mathrm{Div}(C)$, we define the $\mathbb{C}$-vector space*

$$\mathscr{L}(D) = \{f \in K(C)^\times : \mathrm{div}(f) \geq -D\} \cup \{0\}$$

and denote its dimension by $l(D) = \dim_{\mathbb{C}} \mathscr{L}(D)$.

The space $\mathscr{L}(D)$ is finite-dimensional by [9, Proposition 5.2]. We now state a central result and refer to [11, p. 32] for the definition of a canonical divisor.

Theorem 3.50. *(Riemann-Roch) Let C be a smooth curve and let K_C be a canonical divisor on C. Then there exists an integer $g \geq 0$ such that for every divisor $D \in \mathrm{Div}(C)$,*

$$l(D) - l(K_C - D) = \deg(D) - g + 1.$$

The number g is called the *genus* of C. To connect this theorem to our preceding discussion of plane cubics, we note the nontrivial fact that elliptic curves as in our definition are precisely the smooth curves of genus one. This is Proposition 3.1 in [11]. Our next aim is to introduce the already mentioned second group structure on an elliptic curve, for which we need the following two results.

Lemma 3.51. *If C is an elliptic curve, then $l(D) = \deg(D)$ for any divisor $D \in \mathrm{Div}(C)$ of strictly positive degree.*

Proof. It follows from the Riemann-Roch theorem that $l(K_C) = g$ for any curve of genus g and canonical divisor K_C on C (cf. [9, Corollary 5.5 (a)]). Hence, applying the Riemann-Roch theorem to $D = K_C$, we have

$$\deg(K_C) - g + 1 = l(K_C) - l(0)$$

and so $\deg(K_C) = 2g - 2$. Here we used the fact that any regular function on an irreducible projective variety is constant, eg. $l(0) = 1$. Now, if we substitute $g = 1$, we obtain that any canonical divisor on an elliptic curve has degree 0, hence a divisor D with $\deg(D) > 0$ will satisfy $\deg(K_C - D) < 0$. By Proposition 5.2 in [11], this implies $l(K_C - D) = 0$ and hence the formula in question is a special case of the Riemann-Roch theorem. □

Corollary 3.52. *Let C be an elliptic curve and $p, q \in C$. Then the points p and q as divisors are linearly equivalent if and only if $p = q$.*

Proof. If $(p) \sim (q)$, then by definition there is some $f \in K(C)$ such that $\mathrm{div}(f) = (p) - (q)$, so $f \in \mathscr{L}((q))$. By Lemma 3.51, we have $l((q)) = 1$ and hence f is a constant function, which concludes the proof. □

Theorem 3.53. *[11, Proposition 3.4.] Let C be an elliptic curve with identity element O. Then for every $D \in \mathrm{Div}^0(C)$ there exists a unique point $p \in C$ such that $D \sim (p) - (O)$. The map $\sigma : \mathrm{Div}^0(C) \to C$ which assigns to any degree-0 divisor its associated point is surjective and descends to a group isomorphism (also denoted σ)*

$$\sigma : \mathrm{Pic}^0(C) \to C$$

with inverse $\kappa : C \to \mathrm{Pic}^0(C)$ which sends p to the divisor class of $(p) - (O)$.

Proof. We have $l(D+(O)) = 1$ by Lemma 3.51. Let $f \in K(C)$ be a generator of $\mathscr{L}(D+(O))$. Now, $\operatorname{div}(f) \geq -D-(O)$ and $\deg(\operatorname{div}(f)) = 0$ since (f) is principal, which implies $\operatorname{div}(f) = -D-(O)+(p)$ for some $p \in C$. Hence, D is linearly equivalent to $(p)-(O)$, which concludes the first claim.

Uniqueness of p follows from Corollary 3.52, and surjectivity holds because $\sigma((p)-(O)) = p$ for any $p \in C$. Furthermore, if $D_1, D_2 \in \operatorname{Div}^0(C)$, then $\sigma(D_1)-\sigma(D_2) \sim D_1 - D_2$. Hence if $\sigma(D_1) = \sigma(D_2)$, then $D_1 \sim D_2$. Conversely, if $D_1 \sim D_2$, then $\sigma(D_1) = \sigma(D_2)$ which is equivalent to $\sigma(D_1) = \sigma(D_2)$ by Corollary 3.52. Thus, we have a bijection $\sigma : \operatorname{Pic}^0(C) \to C$, which clearly is inverse to κ. It remains to show that the latter map is a homomorphism.

Suppose $p, q \in C$ and let $l = V(F) \subset \mathbb{P}^2$ be the line through p and q. Let r be the third point of intersection of l and C, and let $l' = V(F') \subset \mathbb{P}^2$ be the line through r and q. By definition of the group structure on elliptic curves and since $V(X_0)$ is the inflectional tangent at O (see Lemma 3.58 in the next section), we have

$$\operatorname{div}\left(\frac{F}{X_0}\right) = (p)+(q)+(r)-3(O),$$
$$\operatorname{div}\left(\frac{F'}{X_0}\right) = (r)+(p+q)-2(O).$$

This gives us $(p+q)-(p)-(q)+(O) = \operatorname{div}(\frac{F}{F'})$ which is linearly equivalent to 0 since $\frac{F}{F'}$ is principal, and so $\kappa(p+q)-\kappa(p)-\kappa(q) = 0$ in $\operatorname{Pic}^0(C)$. □

Corollary 3.54. *Let C be an elliptic curve and $D = \sum n_p(p)$ a divisor on C. Then D is principal if and only if $\sum n_p = 0$ and $\sum n_p p = 0$, where the second sum is addition of C via the geometric group law.*

Proof. Every principal divisor has degree 0. Now, D is principal if and only if $\sigma(D) = 0$ by Theorem 3.53, and since this map is an isomorphism, we have that $\sigma(D) = 0$ is equivalent to $\sum_{P \in C} n_p \sigma((p)-(O)) = 0$. Note that $\sigma((p)-(O)) = p$ by definition of σ, so the statement follows. □

Using the theory of infinite products on $\mathbb{C}$, and more specifically the Weierstrass σ-function

$$\sigma(z;\Lambda) = \sigma(z) = z \prod_{\substack{w \in \Lambda \\ w \neq 0}} (1 - \frac{z}{w}) e^{\frac{z}{w} + \frac{1}{2}(\frac{z}{w})^2},$$

one proves the following lemma, which is Proposition 3.4 in [11].

Lemma 3.55. *Let Λ be a lattice and let $n_1, \ldots, n_r \in \mathbb{Z}$, $z_1, \ldots, z_r \in \mathbb{C}$ such that $\sum n_i = 0$ and $\sum n_i z_i \in \Lambda$. Then there exists an elliptic function f relative to Λ such that* $\operatorname{div}(f) = \sum n_i(z_i)$.

Lemma 3.56. *The map Φ in Theorem 3.43 is a group homomorphism.*

Proof. Let $z_1, z_2 \in \mathbb{C}$. By the previous lemma, there exists an elliptic function f such that $\operatorname{div}(f) = (z_1+z_2)-(z_1)-(z_2)+(0)$. Remark 3.38 says that $f(z) = F(\wp(z), \wp'(z))$

for some rational function $F \in \mathbb{C}(X,Y)$. We may interpret F as an element of $K(C)$ and thus obtain

$$\operatorname{div}(F) = (\Phi(z_1+z_2)) + (\Phi(z_1)) + (\Phi(z_2)) + (\Phi(0)).$$

Hence, $\Phi(z_1+z_2) = \Phi(z_1)+\Phi(z_2)$ follows from Corollary 3.54. □

Our last concern in this section is the existence of a lattice whose Eisenstein series $60G_4$ and $140G_6$ have prescribed values. This is done via the modular function j and will only be cited here for brevity.

Theorem 3.57. *Let g_2 and g_3 be complex numbers such that $\Delta = 4g_2^3 - 27g_3^2 \neq 0$. Then there exists a lattice $\Lambda \subset \mathbb{C}$ such that $g_2 = 60G_4(\Lambda)$ and $g_3 = 140G_6(\Lambda)$.*

This result can be found as Theorem 5.1 in [11]. Recall that $\Delta \neq 0$ is always fulfilled by an elliptic curve C_{g_2,g_3}, so the proof of Theorem 3.43 is complete.

3.4. The Monodromy Group of the Nine Flexes By Section 3.2, we have that the monodromy group of the map $I_3 \xrightarrow{\pi} W_3$ is a subgroup of Σ_9. We investigate the subset of flexes of an elliptic curve C, which we shall denote by Γ, more closely before we explicitly compute the monodromy group.

Let $C = V(F = -X_0X_2^2 + 4X_1^3 - g_2X_0^2X_1 - g_3X_0^3) \subset \mathbb{P}^2$ be an elliptic curve in Weierstrass form. The composition law (cf. [11]) endows C with the structure of an abelian group, where we may let $O = [0:0:1]$ - the point at infinity - act as the neutral element. This turns Γ into a subgroup of C, as the following three results show.

Lemma 3.58. *The point O is a flex of C. More precisely, $I_O(C, T_OC) = 3$.*

Proof. Consider the partial derivatives

$$\frac{\partial f}{\partial X_0} = -2g_2X_0X_1 - 3g_3X_0^2 - X_2^2, \quad \frac{\partial f}{\partial X_1} = 12X_1^2 - g_2X_0^2, \quad \frac{\partial f}{\partial X_2} = -2X_0X_2.$$

The tangent line of C at a point P is given by

$$T_PC = V\left(\frac{\partial f}{\partial X_0}(P)X_0 + \frac{\partial f}{\partial X_1}(P)X_1 + \frac{\partial f}{\partial X_2}(P)X_2\right),$$

so in particular, T_OC is the zero locus of $-X_0$. Now,

$$T_OC \cap C = \{[0:p_1:p_2]\} \cap C = \{[0:0:1]\},$$

hence O is a flex of C by Bézout's theorem. □

Lemma 3.59. *A point $P \in C$ is a flex if and only if $3P = O$. In other words, the inflection points of an elliptic curve are precisely its 3-torsion points.*

Proof. Let $P \in C$. Then the third point of intersection of T_PC and C is given as $-2P$, hence $3P = O$ is equivalent to $C \cap T_PC = \{P\}$. Via Bézout, the latter condition translates to $I_P(C, T_PC) = 3$, which concludes the statement. □

Corollary 3.60. *The flexes on C form a subgroup* $\Gamma \cong \mathbb{Z}/3 \times \mathbb{Z}/3$.

Proof. By Lemma 3.58, the origin O is contained in Γ. Let P, Q be two flexes. Equivalently, the points P and Q satisfy $3P = 3Q = O$ by the previous result, hence $3(P+Q) = O$. Applying Lemma 3.59 again, we see that $P+Q$ is a flex. Obviously $-3P = O$ holds, so every additive inverse is an inflection point.

As mentioned before, we have nine flexes on C and thus Γ must be either the cyclic group of order nine, or a two-dimensional vector space over $\mathbb{F}_3$. Since every flex is a 3-torsion point, the latter case is true. □

The previous section allows us to view C as a complex torus $\mathbb{C}/\Lambda$ for some suitable lattice Λ and a group isomorphism $\Phi : \mathbb{C}/\Lambda \to C$. The following lemma describes the subgroup of flexes on the torus, i.e. the group $\Phi^{-1}(\Gamma)$.

Lemma 3.61. *There is precisely one subgroup of* $\mathbb{C}/\Lambda$ *isomorphic to* $\mathbb{Z}/3 \times \mathbb{Z}/3$*, namely* $\frac{\frac{1}{3}\Lambda}{\Lambda}$.

Proof. Let $\mathbb{Z}/3 \times \mathbb{Z}/3 \cong G$ be a subgroup of $\mathbb{C}/\Lambda$. Then G is generated by two elements of order three, which must be contained in $\frac{\frac{1}{3}\Lambda}{\Lambda}$ since this is the 3-torsion subgroup of $\mathbb{C}/\Lambda$. Hence, $G \subset \frac{\frac{1}{3}\Lambda}{\Lambda}$ and thus equality holds because the latter group itself is isomorphic to $\mathbb{Z}/3 \times \mathbb{Z}/3$. □

With all this in mind, we may finally compute the monodromy group of $I_3 \xrightarrow{\pi} W_3$. Recall that the codomain is restricted to a suitably small open subset U consisting of smooth curves such that π becomes a covering map. The previous results in this section show that Γ has the structure of a two-dimensional vector space over $\mathbb{F}_3$, and each element of the monodromy group M acts as a bijection on Γ by definition. This group turns out to respect the vector space structure of Γ: In fact, it is a certain *affine group*, namely, the affine special linear group

$$\mathrm{ASL}_2(\mathbb{Z}/3) = (\mathbb{Z}/3)^2 \rtimes \mathrm{SL}_2(\mathbb{Z}/3)$$

with the natural homomorphism $\mathrm{SL}_2(\mathbb{Z}/3) \hookrightarrow \mathrm{Aut}((\mathbb{Z}/3)^2)$. This is the group of maps generated by linear transformations with determinant one and translations. We recall that three flexes $\{P, Q, R\}$ are collinear in $\mathbb{P}^2$ if and only if their sum vanishes, which of course can be checked in the subgroup $\mathbb{F}_3^2$ - hence, collinearity of flexes in $\mathbb{P}^2$ is equivalent to collinearity as points within the vector space $\mathbb{F}_3^2$, where $P = -Q - R$ says that those points lie on a single line.

Lemma 3.62. *Three collinear points in* Γ *remain collinear under the monodromy action.*

Proof. Let $C \in U$ be an elliptic curve and $P_1, P_2, P_3 \in C$ three collinear flexes. Moreover, let $\gamma(t) = C(t)$ be a loop in U with base point C, e.g. $\gamma(0) = \gamma(1) = C$. We have to show that the three images Q_i of P_i under the monodromy action are collinear. More precisely, there are three liftings

$$\tilde{\gamma}_i = (C(t), P_i(t), l_i(t))$$

of γ to I_3 with $\tilde{\gamma}_i(1) = (C, Q_i, t_i)$. Now, if we let $P(t)$ be the third point of intersection of the line $\overline{P_1(t)P_2(t)}$ with C and $l(t) = T_{P(t)}C(t)$, we may explicitly define a lifting via

$$\alpha(t) = (C(t), P(t), l(t)).$$

Clearly, $\alpha(0) = (C, P_3, l_3)$, so by uniqueness of the lifted path (cf. Lemma 2.6), $\alpha = \tilde{\gamma}_3$ and so Q_3 is the third point of intersection of $\overline{Q_1Q_2}$ with C. □

Corollary 3.63. *The monodromy group is a subgroup of* $\mathrm{ASL}_2(\mathbb{Z}/3)$.

Proof. We have $M \subset \mathrm{AGL}_2(\mathbb{F}_3)$ by the previous lemma, so it remains to assert that no matrices of determinant two are contained in M (cf. [8, p. 693]). □

As further preparation for the main theorem, we have the following elementary results.

Lemma 3.64. *Let X be a Zariski-open subset of $\mathbb{P}^n$ or $\mathbb{A}^n$. Then X is path connected with respect to the analytic topology.*

Proof. The projective case follows from the affine case via the standard open covering. Thus, suppose that x and y are elements of $X \subset \mathbb{A}^n$. Let l be the unique line through both points and note that it is sufficient to find a path within $l \cap X$, which is an open subset of l. Hence, the complement $l \backslash (l \cap X)$ is closed in l and thus finite. Any line in affine space is homeomorphic to $\mathbb{R}^2$, so we conclude that there exists a finite set of points S such that $l \cap X \cong \mathbb{R}^2 \backslash S$. The latter set is obviously path connected, so the proof is complete. □

Lemma 3.65. *Let Y be a path connected space and let $p : Y \to X$ be a covering map. Then the monodromy of p acts transitively on the fibre of any point $x \in X$.*

Proof. Let γ be a path between two points $y_1, y_2 \in p^{-1}(x)$. Then $[p \circ \gamma] \in \pi_1(X, x)$ is a loop which tautologically lifts to γ, and so the induced permutation of the fibre sends y_1 to y_2. □

As an immediate conclusion, we have:

Corollary 3.66. *The monodromy of the nine flexes acts transitively.* □

Theorem 3.67. $M = \mathrm{ASL}_2(\mathbb{Z}/3)$.

Proof. Let $C \in U$ be a smooth plane cubic. After a linear transformation, we may assume that the neutral element is $O = [0 : 0 : 1]$ with tangent line $V(X_0)$. The preceding section guarantees the existence of a lattice $\Lambda =< \omega_1, \omega_2 >_{\mathbb{Z}}$ such that

$$\Phi : \mathbb{C}/\Lambda \xrightarrow{\sim} C.$$

Moreover, the subgroup of flexes is $V := \frac{\frac{1}{3}\Lambda}{\Lambda} = \Phi^{-1}(\Gamma)$. We first of all claim that $\mathrm{SL}_2(\mathbb{Z}/3)$ is contained in M and that this is precisely the stabilizer of O in M, i.e.

$$\mathrm{Stab}(O) := \{g \in M : g.O = O\} = \mathrm{SL}_2(\mathbb{Z}/3).$$

Let $\overline{A} \in \mathrm{SL}_2(\mathbb{Z}/3)$ and choose some representative $A \in \mathrm{SL}_2(\mathbb{Z})$ reducing to $\overline{A}$. Since $\mathrm{SL}_2(\mathbb{R})$ is path connected, there exists an arc $A(t) \in \mathrm{SL}_2(\mathbb{R})$ with $A(0) = \mathrm{Id}_2$ and $A(1) = A$. For every matrix $A(t)$, we define an $\mathbb{R}$-basis of $\mathbb{C}$ via

$$(\omega_1(t), \omega_2(t)) := A(t) \cdot \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$$

and a corresponding lattice

$$\Lambda_t := < \omega_1(t), \omega_2(t) >_{\mathbb{Z}} .$$

If we let $\wp_t(z) := \wp(z; \Lambda_t)$ be the Weierstrass function relative to Λ_t, we obtain an elliptic curve C_t as the image of

$$\Phi_t : \mathbb{C}/\Lambda_t \hookrightarrow \mathbb{P}^2.$$

Then $C_0 = C$ by construction, and $C_1 = C$ since Λ and Λ_1 - which differ by an element of $\mathrm{SL}_2(\mathbb{Z})$ - are homothetic (cf. [11, Corollary 4.1.1.]). Thus, $\gamma : t \mapsto C_t$ is a loop in U (note that Weierstrass curves whose coefficients are given as quantities associated to a lattice are smooth, see for instance [11, Proposition 3.6 (a)]). To see that γ is continuous, we formalize the above construction by expressing γ as the composition of the following continuous maps:

$$\begin{array}{ccccccccc} [0,1] & \longrightarrow & \mathrm{SL}_2(\mathbb{R}) & \longrightarrow & \mathbb{C}^2 & \longrightarrow & \mathbb{C}^2 & \longrightarrow & U \\ t & \longmapsto & A(t) & \longmapsto & (\omega_1(t), \omega_2(t)) & \longmapsto & (g_2, g_3) & \longmapsto & C_{g_2,g_3} \end{array}$$

where $g_2 = 60G_4(\Lambda_t)$ and $g_3 = 140G_6(\Lambda_t)$. If a flex $Q = \Phi(v), v = m\frac{\omega_1}{3} + n\frac{\omega_2}{3}$ with inflectional tangent l is given, we obtain a flex Q_t of C_t with tangent l_t by setting

$$Q_t = \Phi_t(m\frac{\omega_1(t)}{3} + n\frac{\omega_2(t)}{3})$$

and $T_t = T_{Q_t}C_t$. Both expressions are continuous in t since Φ_t is, so we may lift γ to a path in I_3 with $\tilde{\gamma}(0) = (C, Q, l)$ via

$$\tilde{\gamma}(t) = (C_t, Q_t, l_t).$$

By construction, $Q_1 = \Phi_1(A \cdot \begin{pmatrix} \frac{m}{3} \\ \frac{n}{3} \end{pmatrix})$, so the linear transformation $\overline{A}$ permutes the inflection points precisely like the lifting $\tilde{\gamma}$, which is unique by Lemma 2.6. Hence, $\mathrm{SL}_2(\mathbb{Z}/3)$ embeds into M, and the statement about the stabilizer is clear.

To conclude the proof, let $\psi \in \mathrm{ASL}_2(\mathbb{Z}/3)$ and consider $\psi(O) \in \Gamma$. By Corollary 3.66, there exists $\phi \in M$ such that $\phi(O) = \psi(O)$. This implies that $\phi^{-1}\psi$ is contained in $\mathrm{Stab}(O) = \mathrm{SL}_2(\mathbb{Z}) \subset M$, hence $\psi \in M$. □

3.5. Locating the Flexes The proof that $\mathrm{ASL}_2(\mathbb{F}_3)$ is solvable will be omitted here (cf. [8, p. 695]), but we quickly note an immediate consequence: Solvability of the Galois group implies that the minimal polynomial we dealt with in Section 2 is itself solvable by radicals, since G was defined as the Galois group associated to its splitting field over

$K(W_3)$. Now, the roots of this minimal polynomial correspond to the points in a general fibre $\pi^{-1}(C)$, which biject onto the flexes of C. Hence, we see that each flex may be expressed in terms of the function field $K(W_3)$.
We now calculate the coordinates of an elliptic curve in Weierstrass form in terms of its coefficients by elementary means. Let

$$F(X_0,X_1,X_2) = -X_0X_2^2 + 4X_1^3 - g_2X_0^2X_1 - g_3X_0^3$$

and consider the partial derivatives $F_{00} = -2g_2X_1 - 6g_3X_0$, $F_{11} = 24X_1$, $F_{22} = -2X_0$, $F_{10} = -2g_2X_0$, $F_{12} = 0$ and $F_{20} = -2X_2$. Hence, the determinant of the Hessian has the form

$$\begin{aligned}\det(H(F)) &= F_{00}F_{11}F_{22} - F_{02}F_{11}F_{20} - F_{01}F_{10}F_{22}\\ &= 96g_2X_0X_1^2 + 288g_3X_0^2X_1 - 96X_1X_2^2 + 8g_2^2X_0^3.\end{aligned}$$

We have already shown that the point at infinity $[0:0:1]$ is a flex, so it suffices to consider the affine plane $X_0 = 1$. Hence, we seek the common zeroes of the polynomials

$$\begin{aligned}f(X_1,X_2) &:= F(1,X_1,X_2),\\ h(X_1,X_2) &:= \frac{1}{8}H(F)(1,X_1,X_2) = 12g_2X_1^2 + 36g_3X_1 - 12X_1X_2^2g_2^2.\end{aligned}$$

We substitute $X_2^2 = 4X_1^3 - g_2X_1 - g_3$ in h and obtain

$$0 = 12g_2X_1^2 + 36g_3X_1 - 12X_1(4X_1^3 - g_2X_1 - g_3) + g_2^2 \Leftrightarrow 0 = X_1^4 - \frac{g_2}{2}X_1^2 - g_3X_1 - \frac{g_2^2}{48},$$

which is an equation of degree four and hence solvable. It follows that all eight remaining flexes lie on four vertical lines in the affine plane $\{[1:X_1:X_2]\}$.

4 References

[1] E. Bombieri, W. Gubler: *Heights in Diophantine Geometry*, Cambridge University Press, 2006.

[2] G. E. Bredon: *Geometry and Topology*, Springer, 1993.

[3] E. Brieskorn, H. Knörrer: *Plane Algebraic Curves*, Birkhäuser, 1986.

[4] I. Dolgachev: *Introduction to Algebraic Geometry*, http://www.math.lsa.umich.edu/∼idolga/lecturenotes.html, 2010.

[5] G. Fischer: *Plane Algebraic Curves*, AMS Student Mathematical Library, 2001.

[6] W. Fulton: *Algebraic Curves - An Introduction to Algebraic Geometry*, Addison Wesley Longman, 1969.

[7] J. Harris: *Algebraic Geometry - A First Course*, Springer, 2010.

[8] J. Harris: *Galois Groups of Enumerative Problems*, Duke Mathematical Journal Vol. 46 No.4 p. 685-724, 1979.

[9] K. Hulek: *Elementary Algebraic Geometry*, AMS Student Mathematical Library, 2003.

[10] D. Huybrechts: *Complex Geometry*, Springer, 2004.

[11] J. H. Silverman: *The Arithmetic of Elliptic Curves*, Springer, 2nd Edition.