ON ALGEBRAS OF LOW RANK AND ON BELYI MAPS

A Thesis

Submitted to the Faculty

in partial fulfillment of the requirements for the

degree of

Doctor of Philosophy

in

Mathematics

by Samuel Schiavone

Guarini School of Graduate and Advanced Studies

DARTMOUTH COLLEGE

Hanover, New Hampshire

July 10, 2019

Examining Committee:

John Voight, Chair

Thomas Shemanske

Asher Auel

David P. Roberts

F. Jon Kull, Ph.D.
Dean of the Guarini School of Graduate and Advanced Studies

Abstract

This thesis comes in two parts. The first concerns the classification of algebras of low rank. The main goal of this part is to study the moduli space of rank 3 algebras. Our investigations lead to a generalization of a theorem of Levin that shows that rank 3 algebras over an integral domain occur in essentially two types. We extend this result to rank 3 algebras over a commutative ring, and then to sheaves of rank 3 algebras over a scheme.

In the second part we describe a method for computing Belyi maps. In 1984, Grothendieck described an action of the absolute Galois group of the rational numbers on the set of isomorphism classes of Belyi maps. Thus Belyi maps provide a tantalizing possibility of better understanding this important group. We explain in detail the steps used to compute Belyi maps defined on elliptic and hyperelliptic curves. We conclude with our progress in computing an exhaustive catalogue of Belyi maps, and make some basic observations about the Galois action on these maps.

Preface

I would like to thank everyone who helped me along my way to this point. Thanks to the Dartmouth faculty, graduate students, and staff who made the department a warm, friendly, and intellectually stimulating environment.

Thanks to my friend, office mate, and math buddy Mike Musty for all his kindness, generosity, and reliability both inside and outside of the office. And for putting up with my at times, shall we say, irascible nature! Thanks to Jeroen Sijsling and Edgar José Martins Dias Costa for being wonderful mathematical older brothers and answering all the questions I was too embarrassed to ask John about. Thanks to my advisor John Voight, whose enthusiasm, dedication, and expertise have helped me become a better mathematician over the course of the seven years that I've known him.

Finally, thanks to my parents, family, and friends, whose love, affection, and encouragement have supported me throughout the years.

Contents

Chapter 1

Introduction

This thesis comes in two parts. The first deals with the classification of algebras of low rank, and the second with the computation of Belyi maps.

Section 1.1

On algebras of low rank

The goal of this part is to study the moduli space of rank 3 algebras. In [Levin, 2013], the author shows that a rank 3 algebra over an integral domain is either commutative or possesses a standard involution. The main results of the first part of the thesis are generalizations of this result to the case of rank 3 algebras over a commutative ring, and then to the case of sheaves of rank 3 algebras over a scheme.

We begin by studying framed algebras, that is, algebras equipped with a choice of basis. To do this, we first form the "universal" framed rank n algebra A_{univ} whose structure constants satisfy the minimal conditions to ensure that A_{univ} is associative and unital. We then show in Proposition 3.2.1 that the base ring R_{univ} of A_{univ} (the "universal base") represents framed rank n algebras, in the sense that $X_{\text{univ}} :=$

$\mathrm{Spec}(R_{\mathrm{univ}})$ is the fine moduli space for the functor classifying isomorphism classes of framed algebras over a commutative ring.

We then turn to the particular case of rank 3 algebras over a commutative ring. We show in Theorem 3.2.5 and Corollary 3.2.6 that the moduli space of such algebras has two irreducible components $X_{\mathrm{univ},C}$ and $X_{\mathrm{univ},E}$, the first corresponding to commutative algebras, and the second to exceptional algebras. We use this universal result and representability to show in Theorem 3.4.1 that the same decomposition holds over an arbitrary base ring.

Theorem (Theorem 3.4.1)**.** *Let R be a commutative ring, and let A be a free R-algebra of rank* 3*.*

(a) *There exist ideals I_C and I_E of R such that*

(i) *$A_C := A \otimes_R (R/I_C)$ is commutative; and*

(ii) *$A_E := A \otimes_R (R/I_E)$ is exceptional,*

and I_C and I_E are minimal in the following sense. If J is an ideal of R such that $A \otimes_R (R/J)$ is commutative (resp., exceptional), then $I_C \subseteq J$ (resp., $I_E \subseteq J$).

(b) *For any choice of modest basis (e_1, e_2, e_3) for A with associated structure constants $c_{ij}^{(k)}$, we have $I_C = (c_{23}^{(3)}, c_{32}^{(2)})$ and*

$$I_E = (c_{22}^{(1)}, c_{22}^{(2)} - c_{23}^{(3)}, c_{22}^{(3)}, c_{23}^{(1)}, c_{32}^{(1)}, c_{32}^{(2)} - c_{33}^{(3)}, c_{33}^{(1)}, c_{33}^{(2)})\,.$$

(c) *We have*

$$A_{CE} := A \otimes_R (R/I_C) \otimes_R (R/I_E)$$

is isomorphic to the nilproduct algebra $R[x,y]/(x,y)^2$.

We show in Proposition 3.4.3 that the formation of the ideals I_C and I_E is functorial, in the following sense. Given a commutative ring R, the ideals $I_{R,C}$ and $I_{R,E}$ corresponding to commutative and exceptional rank 3 algebras, respectively, are simply the extensions of the corresponding ideals of the universal base R_{univ} along the unique ring homomorphism $\varphi : R_{\text{univ}} \to R$. We also show that these ideals are independent of the choice of basis.

These last two results allow us to extend our result to the case of a sheaf of rank 3 algebras over an arbitrary base scheme X. For each affine open subscheme $\operatorname{Spec}(R)$ of X, our result for algebras over a commutative ring produces ideals $I_{R,C}$ and $I_{R,E}$. Our functoriality result allows us to glue these ideals and form corresponding quasicoherent $\mathscr{O}_X$-ideal sheaves $\mathscr{I}_C$ and $\mathscr{I}_E$ in Theorem 3.5.12 and their corresponding closed subschemes X_C and X_E in Corollary 3.5.14.

Theorem (Theorem 3.5.12)**.** *Let X be a scheme, and let $\mathscr{A}$ be sheaf of algebras on X that is locally free of rank 3. Then there exist quasicoherent ideal sheaves $\mathscr{I}_C$ and $\mathscr{I}_E$ on X such that*

(a) $\mathscr{A}_C := \mathscr{A} \otimes_{\mathscr{O}_X} \dfrac{\mathscr{O}_X}{\mathscr{I}_C}$ *is commutative; and*

(b) $\mathscr{A}_E := \mathscr{A} \otimes_{\mathscr{O}_X} \dfrac{\mathscr{O}_X}{\mathscr{I}_E}$ *is exceptional;*

and $\mathscr{I}_C$ and $\mathscr{I}_E$ are the minimal ideal sheaves with these properties in the following sense. If $\mathscr{J}$ is an ideal sheaf on $\mathscr{O}_X$ such that $\mathscr{A} \otimes_{\mathscr{O}_X} \dfrac{\mathscr{O}_X}{\mathscr{J}}$ is commutative (resp., exceptional), then $\mathscr{I}_C(U) \subseteq \mathscr{J}(U)$ (resp., $\mathscr{I}_E(U) \subseteq \mathscr{J}(U)$) for every affine open subset U of X.

Furthermore,

$$\mathscr{A} \otimes_{\mathscr{O}_X} \frac{\mathscr{O}_X}{\mathscr{I}_C} \otimes_{\mathscr{O}_X} \frac{\mathscr{O}_X}{\mathscr{I}_E}$$

is nilproduct.

Corollary (Corollary 3.5.14)**.** *Let X be a scheme, and let $\mathscr{A}$ be sheaf of algebras on X that is locally free of rank 3. Then there exist closed subschemes $\iota_C : X_C \hookrightarrow X$ and $\iota_E : X_E \hookrightarrow X$ of X such that*

(a) *$\iota_C^*(\mathscr{A})$ is commutative;*

(b) *$\iota_E^*(\mathscr{A})$ is exceptional*

and X_C and X_E are the largest closed subschemes with these properties.

Let $X_{CE} = X_C \cap X_E = X_C \times_X X_E$ with closed embedding $\iota_{CE} : X_{CE} \hookrightarrow X$. Then $\iota_{CE}^*(\mathscr{A})$ is the nilproduct algebra.

In the last section we study the action on the structure constants induced by change of basis of a rank 3 algebra. The orbits of this action are naturally in bijective correspondence with isomorphism classes of rank 3 algebras (*without* a choice of basis). This points toward a direction of future research: classify algebras without a choice of basis. We would like to obtain an explicit description of the moduli space of rank 3 algebras (without a choice of basis). We hope to achieve this by forming the GIT quotient of the moduli space of framed algebras by the action given by change of basis.

We also study "degenerations" of rank 3 algebras. We realize the moduli space of framed rank 3 algebras as a subset of the affine space $\mathbb{A}^{27}$ by means of the structure constants. It is then natural to wonder what the closure of the moduli space in $\mathbb{P}^{27}$ looks like, and if we can give some algebraic meaning to the points on the hyperplane at infinity. We make some initial steps toward understanding the class of objects this compactified moduli functor represents.

Section 1.2

On computing Belyi maps

The second part of the thesis discusses a method for computing Belyi maps, i.e., three-point branched covers of the projective line. This is based on joint work with Michael Klug, Michael Musty, Jeroen Sijsling, and John Voight in [Klug et al., 2014] and [Musty et al., 2019].

Belyi maps have many applications, but our interest in them arises from their connection to the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Belyi showed that an algebraic curve X over $\mathbb{C}$ has a model over $\overline{\mathbb{Q}}$ if and only if X admits a Belyi map. This result enthralled Grothendieck and led him to define an action of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the set of isomorphism classes of Belyi maps. He then recast this action in terms of a certain graphs called *dessins d'enfants*, providing the tantalizing possibility of understanding this important and mysterious group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in a combinatorial way.

Our goal is to compute explicit equations for Belyi maps in hopes of understanding the Galois action. The method we employ relies on a web of bijections between several different classes of objects. We traverse this web, beginning in a combinatorial setting with permutations, passing to a group theoretic setting with subgroups of triangle groups, and finally arriving at an algebro-geometric setting with Belyi maps. We outline this strategy and then discuss in detail the steps necessary to obtain explicit equations for Belyi maps defined on elliptic and hyperelliptic curves.

We have used this method to compute an exhaustive database of Belyi maps of low degree. This data is available in the beta version of the L-functions and

Modular Forms Database (LMFDB) at `https://beta.lmfdb.org/Belyi/`, and the raw text files of which the database is comprised are available on GitHub at `https://github.com/michaelmusty/BelyiDB`. We make some basic observations about the arithmetic features of the data, namely counting the number of orbits of the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in each degree and genus, which are described in the following theorems.

Theorem (Theorem 4.4.8)**.** *There are* 118 *Galois orbits of elliptic Belyi maps with degree* $d \leq 7$*. They are distributed with respect to degree as shown in the table below.*

d	Number of orbits
3	1
4	2
5	7
6	35
7	73

Theorem (Theorem 4.5.8)**.** *There are* 12 *Galois orbits of hyperelliptic Belyi maps with degree* $d \leq 6$*. There are* 4 *orbits of Belyi maps in degree* 5 *and 8 orbits in degree* 6.

Chapter 2

Background on algebras

Section 2.1

Introduction

The endeavor to classify (associative) algebras dates back to at least the late 1800s, when Benjamin Peirce [Peirce, 1881] sought to classify all algebras of dimension at most 5. Peirce approached the problem by considering multiplication tables for the basis elements. However, the scope of his results are somewhat difficult to determine: Peirce used his own peculiar notation and terminology, and did not explicity state the base ring or field over which the algebras are defined, though from his presentation it seems that he considered $\mathbb{C}$-algebras. (See [Fialowski and Penkava, 2009, §2] for more on the validity and shortcomings of Peirce's work.)

Since Peirce's work, many different techniques have been used in an effort to classify algebras. In the 1960s, Gerstenhaber [Gerstenhaber, 1964] presented a deformation theoretic approach using Hochschild cohomology, which has been further pursued in many other works, such as [Fialowski and Penkava, 2009]. Deformation theory has also been used in classifying other algebraic structures, such as Lie algebras, Jordan algebras, Weyl algebras, and infinity algebras.

Later in the 1960s, Flanigan [Flanigan, 1968] coined the phrase “algebraic geography” for his study of the moduli space of associative, but not necessarily unital, algebras, the action of GL_n given by change of basis, and the orbits of this action. Flanigan considered this moduli space concretely, as we will, in terms of the structure constants of an algebra. Flanigan also connected his study of the GL_n-orbits to the deformation theoretic approach of Gerstenhaber.

In the 1970s Gabriel [Gabriel, 1974] and Mazzola [Mazzola, 1979] classified algebras of dimensions 4 and 5, respectively, using the representation theory of quivers. (See also [Assem et al., 2006] and [Benson, 1998] for more recent presentations of this approach.) The basic idea is to associate to an algebra A a quiver Q (called the Ext-quiver of A in [Benson, 1998]), and then realize A as a quotient of the path algebra of Q. This allows one to classify algebras just by creating an exhaustive list of the possible quivers, as done in [Gabriel, 1974, §5] and [Mazzola, 1979, §1].

Benson extends the definition of the Ext-quiver of an algebra to an arbitrary base field (not assumed algebraically closed), but it is no longer clear that one can realize the algebra as a quotient of its path algebra. At the end of [Benson, 1998, §4.1], the author remarks, “There should be a way of modifying the definition of the Ext-quiver of A to contain sufficient cocycle information so that a suitable ‘path algebra’ will always map onto A. To the best of my knowledge no-one has attempted to do this.”

All the above mentioned efforts concentrated on the case of algebras defined over a field, often assumed algebraically closed, or even just the particular case of algebras over $\mathbb{C}$. In this work we are interested in a more arithmetic setting—we seek to classify algebras over an arbitrary commutative base ring, and even sheaves of algebras over an arbitrary base scheme.

Some results have already been obtained in this direction. In [Poonen, 2008], Poonen studies the moduli space of commutative algebras that are locally free of rank n over a commutative ring, equipped with a choice of basis. He investigates its geometric properties, and explicitly determines the isomorphism type of the moduli space for $n \leq 3$, discovering that in each of these cases it is isomorphic to an affine space.

In [Gross and Lucianovic, 2009], the authors fix a base ring R that is either a local ring or a principal ideal domain, and consider two types of algebras over R: commutative algebras that are free of rank 3, which they call cubic rings, and quaternion rings, which are generalizations of quaternion algebras. They study the action of GL_n given by change of basis and in each case identify this representation as a symmetric power twisted by the determinant. This allows them to find bijections between isomorphism classes of cubic rings (resp., quaternion rings) and the orbits of these actions.

In [Voight, 2011a], Voight extends the results of Gross and Lucianovic by classifying quaternion rings over an arbitrary commutative ring. He first gives several different characterizations of quaternion rings, one in terms of Clifford algebras. He then gives an enhanced version of the bijection presented in [Gross and Lucianovic, 2009, Proposition 4.1] that preserves extra structure. (Similar results are shown in [Venkata Balaji, 2007], but in slightly different language.)

In [Voight, 2011c], Voight proves two main results on algebras of low rank. He first shows that under some mild assumptions, an algebra B has degree 2 if and only if it possesses a standard involution. He then proceeds to show that in the case of a rank 3 algebra B has a standard involution if and only if it is exceptional. (These terms will be defined in the following section.)

The central goal of this chapter is to generalize the main result of [Levin, 2013]. Levin shows that for R an integral domain, every free R-algebra of rank 3 is either commutative or possess a standard involution. We aim to extend this result in various directions, first to the case of arbitrary commutative base rings, then to locally free rank 3 algebras over a commutative ring, and finally to sheaves of locally free rank 3 algebras over an arbitrary base scheme.

Section 2.2

Definitions and conventions

Throughout we insist that all rings are unital, and that all ring homomorphisms map 1 to 1. Let R be a commutative ring.

Definition 2.2.1. An *algebra over R* (or *R-algebra*) is a ring A together with a ring homomorphism $\varphi : R \to A$ such that $\varphi(R)$ is contained in the center of A. We call φ the *structure map* of A.

Given an R-algebra A with structure map $\varphi : R \to A$, let $I = \ker(\varphi)$. Then there is a natural (R/I)-module structure on A induced by the canonical quotient map $R \to R/I$. Moreover, the induced structure map $\overline{\varphi} : R/I \to A$ is injective. Thus by replacing R by R/I, we may assume that the structure map is an embedding. Henceforth, we insist that the structure map is injective. Thus an R-algebra is a ring A equipped with an embedding $\varphi : R \hookrightarrow A$ such that $\varphi(R)$ is contained in the center of A. Furthermore, we identify R with its image under the embedding $R \hookrightarrow A$.

Definition 2.2.2. An R-algebra A is *free* if it is free as an R-module, and its *rank* is its rank as an R-module.

2.2.1. An example: quaternion algebras

The moduli space of algebras is vast. In order to try to navigate it, we stratify it using different sorts of discrete invariants. Many of these occur in "nature" and can be seen in particular in quaternion algebras.

Let F be a field of characteristic $\neq 2$.

Definition 2.2.3. An algebra A over F is a *quaternion algebra* if there exists a basis $1, i, j, k$ for A as an F-vector space such that

$$i^2 = a, \quad j^2 = b, \quad k = ij = -ji$$

for some $a, b \in F^\times$. We denote the algebra defined in this way by $\left(\dfrac{a,b}{F}\right)$. We begin by examining some of the properties of a quaternion algebra A—we will abstract and generalize these properties as we investigate algebras of low rank.

Rank. Since $1, i, j, k$ is a basis, then A has dimension 4 as an F-vector space. Nearly all the algebras we will consider will be free, or at least locally free.

Involution. A quaternion algebra A has a notion of conjugation: for $\alpha \in A$ with $\alpha = t + xi + yj + zk$, let

$$\overline{\alpha} = t - xi - yj - zk\,.$$

The map $\overline{\cdot} : A \to A$ is F-linear and satisfies the following properties:

(i) $\overline{1} = 1$;

(ii) $\overline{\cdot}$ is an anti-homomorphism: $\overline{\alpha\beta} = \overline{\beta}\,\overline{\alpha}$ for all $\alpha, \beta \in A$;

(iii) $\overline{\cdot}$ is an involution, i.e., $\overline{\overline{\alpha}} = \alpha$ for all $\alpha \in A$; and

(iv) $\alpha\overline{\alpha} \in F$ for all $\alpha \in A$.

A map with these properties is called a standard involution.

Degree. For $\alpha \in A$ define the *reduced trace* and *norm* of α by

$$\operatorname{trd}(\alpha) = \alpha + \overline{\alpha} \qquad \operatorname{nrd}(\alpha) = \alpha\overline{\alpha}\,.$$

Then every $\alpha \in A$ satisfies a polynomial of degree 2, namely

$$\mu_\alpha(T) := T^2 - \operatorname{trd}(\alpha)T + \operatorname{nrd}(a) \in F[T]\,.$$

Characteristic polynomial. Let A act on itself by left multiplication. This gives a ring homomorphism $\lambda : A \to \mathrm{M}_4(F)$. With μ_α as above, then we have

$$\chi_\alpha(T) = \mu_\alpha(T)^2$$

for all $\alpha \in A$, where χ_α is the characteristic polynomial of $\lambda(\alpha)$.

2.2.2. Properties of algebras

We remind the reader of our running assumption that R is a commutative ring and A is an R-algebra, as stated in section 2.2.

Definition 2.2.4. An *involution* $\overline{\cdot} : A \to A$ is an R-linear map that is self-inverse (i.e., $\overline{\overline{x}} = x$ for all $x \in A$), and a ring anti-homomorphism, meaning $\overline{xy} = \overline{y}\,\overline{x}$ for all $x, y \in A$. An involution $\overline{\cdot}$ is *standard* if $x\overline{x} \in R$ for all $x \in A$.

Remark 2.2.5. Note that if $\overline{\cdot}$ is a standard involution, then

$$R \ni (x+1)(\overline{x+1}) = (x+1)(\overline{x}+1) = x\overline{x} + x + \overline{x} + 1$$

and hence $x+\overline{x} = x\overline{x} - 1 \in F$ for all $x \in A$ as well. Consequently, $(x+\overline{x})x = x(x+\overline{x})$ so $x\overline{x} = \overline{x}x$ for all $x \in A$.

Remark 2.2.6. An algebra equipped with a standard involution is sometimes called a *Cayley algebra*; cf., [Bourbaki, 1998, Ch. III, §2.4].

Definition 2.2.7. The *degree* of an R-algebra A, written $\deg_R(A)$, is the smallest positive integer n such that every $\alpha \in A$ satisfies a monic polynomial of degree n with coefficients in R. If no such n exists, then A has degree ∞.

Remark 2.2.8. We have seen that quaternion algebras, and indeed all algebras with a standard involution, have degree at most 2.

Proposition 2.2.9. *Let A be a free R-algebra of rank n. Then A has degree $\leq n$.*

This proposition follows from a generalized version of the classical Cayley-Hamilton theorem from linear algebra.

Proposition 2.2.10 (Theorem 4.3, [Eisenbud, 2013])**.** *Let $I \subseteq R$ be an ideal and M an R-module that can be generated by n elements. Let φ be an endomorphism of M. If*

$$\varphi(M) \subseteq IM,$$

then there is a monic polynomial

$$p(x) = T^n + p_1 T^{n-1} + \cdots + p_n$$

with $p_j \in I^j$ for each j, such that $p(\varphi) = 0$ as an endomorphism of M.

Proof of 2.2.9. Given $a \in A$, let $\lambda_a : A \to A, x \mapsto ax$ be the R-algebra endomorphism given by left multiplication by a. Taking $\varphi = \lambda_a$ in Proposition 2.2.10, we obtain a polynomial p with the properties above. In particular, $p(T) \in R[T]$ is monic and $p(\lambda_a) = 0 \in \operatorname{End}(M)$. Then

$$0 = p(\lambda_a)(1) = a^n + p_1 a^{n-1} + \cdots + p_n \,,$$

so a has degree $\leq n$. □

It turns out that the naïve notion of degree introduced above is not invariant under base change. In [Voight, 2011c, Example 1.20], Voight presents an example of an algebra whose degree increases under base change. The author then proposes the following variant of degree, which is manifestly invariant under base change.

Definition 2.2.11. The *geometric degree* of A, denoted $\operatorname{gdeg}_R(A)$, is the maximum of $\deg_S(A \otimes_R S)$ taken over all homomorphisms $R \to S$ with S a commutative ring.

Remark 2.2.12. [Voight, 2011c, Lemma 1.23] shows that the above definition of geometric degree can be interpreted in terms of a “universal” or “generic” element, and consequently agrees with the definition of degree given in [Jacobson, 1963].

One more related property that will be useful is the notion of an *exceptional algebra*.

Definition 2.2.13. An R-algebra A is *exceptional* if there exists a left ideal M of A such that $A = R \oplus M$ (as R-modules) and an R-linear map $t : M \to R$ such that the map $M \to \mathrm{Hom}_R(M, A)$ given by left multiplication factors through t, i.e., the following diagram commutes.

$$\begin{tikzcd}
M \arrow[rr] \arrow[dr, "t"'] & & \mathrm{Hom}_R(M, A) \\
& R \arrow[ur] &
\end{tikzcd}$$

In other words, $\alpha\beta = t(\alpha)\beta$ for all $\alpha, \beta \in M$.

Remark 2.2.14. For an exceptional algebra A, the map $\overline{\alpha} := t(\alpha) - \alpha$ defines a standard involution on A. Thus exceptional algebras have degree at most 2.

Section 2.3

Moduli spaces and representability

In the following we state the definitions for contravariant functors, but they are also valid for covariant functors with the necessary reversing of arrows.

Definition 2.3.1. Let $\mathscr{C}$ and $\mathscr{D}$ be categories and $\mathscr{F}, \mathscr{G} : \mathscr{C} \to \mathscr{D}$ be contravariant functors. A *morphism* or *natural transformation* of functors $\tau : \mathscr{F} \to \mathscr{G}$ is a collection of morphisms $\{\tau_X\}_{X \in \mathrm{Ob}(\mathscr{C})}$ in $\mathscr{D}$ such that for each morphism $\varphi : X \to Y$ in $\mathscr{C}$ (i.e., $X, Y \in \mathrm{Ob}(\mathscr{C})$ and $\varphi \in \mathrm{Hom}_{\mathscr{C}}(X, Y)$), the following diagram commutes.

$$\begin{tikzcd}
\mathscr{F}(Y) \arrow[r, "\mathscr{F}(\varphi)"] \arrow[d, "\tau_Y"'] & \mathscr{F}(X) \arrow[d, "\tau_X"] \\
\mathscr{G}(Y) \arrow[r, "\mathscr{G}(\varphi)"'] & \mathscr{G}(X)
\end{tikzcd}$$

A *natural isomorphism* or *isomorphism of functors* is a natural transformation with a two-sided inverse.

Remark 2.3.2. Equivalently, a natural transformation τ is an isomorphism if and only if τ_X is an isomorphism for each object X.

Definition 2.3.3. Let $\mathscr{C}$ be a locally small category and C be an object in $\mathscr{C}$. The *covariant* and *contravariant hom-functors* h^C and h_C are defined as

$$\begin{aligned} h^C = \mathrm{Hom}_{\mathscr{C}}(C, \_\,) : \mathscr{C} &\to (\text{sets}) \\ X &\mapsto \mathrm{Hom}_{\mathscr{C}}(C, X) \\ h_C = \mathrm{Hom}_{\mathscr{C}}(\_\,, C) : \mathscr{C} &\to (\text{sets}) \\ X &\mapsto \mathrm{Hom}_{\mathscr{C}}(X, C) \end{aligned}$$

and acting on morphisms by post- and pre-composition, respectively.

Definition 2.3.4. The *functor of points* of a scheme X is the contravariant hom-functor

$$\begin{aligned} h_X = \mathrm{Hom}(\_\,, X) : (\text{schemes}) &\to (\text{sets}) \\ Y &\mapsto \mathrm{Hom}(Y, X) \end{aligned}$$

which acts on morphisms by pre-composition. That is, given a morphism $f : Y \to Y'$ of schemes, define

$$f^{\#} := h_X(f) : h_X(Y') = \mathrm{Hom}(Y', X) \to \mathrm{Hom}(Y, X) = h_X(Y)$$

by $f^{\#}(g) = g \circ f$.

$$\begin{tikzcd}
Y \arrow[r, "f"] \arrow[dr, dashed, "g\circ f"'] & Y' \arrow[d, "g"] \\
 & X
\end{tikzcd}$$

A contravariant functor $\mathscr{F}$: (schemes) → (sets) is *representable* if there exists a scheme X such that $\mathscr{F}$ and h_X are isomorphic as functors. In this case we say that *X represents $\mathscr{F}$.*

Remark 2.3.5. Given a commutative ring R, we define the functor of points of R to be that of $\mathrm{Spec}(R)$.

Definition 2.3.6. If a contravariant functor $\mathfrak{M}$: (schemes) → (sets) is represented by a scheme X, we say that X is a *fine moduli space* for $\mathfrak{M}$.

Lemma 2.3.7 (Yoneda)**.** *Let $\mathscr{C}$ be a category, X an object in $\mathscr{C}$ and $\mathscr{F} : \mathscr{C} \to$ (sets) a contravariant functor. There exists a natural bijection*

$$\mathrm{Hom}(h_X, \mathscr{F}) \xrightarrow{\sim} \mathscr{F}(X)\,.$$

Proof. Given a natural transformation $\tau : h_X \to \mathscr{F}$, the key idea is to consider the identity element $\mathrm{id}_X \in \mathrm{Hom}(X,X) = h_X(X)$. We get a map

$$\begin{aligned} \alpha : \mathrm{Hom}(h_X, \mathscr{F}) &\to \mathscr{F}(X) \\ \tau &\mapsto \tau_X(\mathrm{id}_X)\,. \end{aligned}$$

Conversely, suppose $\xi \in \mathscr{F}(X)$. We seek to construct a natural transformation $\tau^\xi : h_X \to \mathscr{F}$ such that $\tau^\xi_X(\mathrm{id}_X) = \xi$. If we had such a transformation, then for each morphism $f : Y \to X$ we would have the following commutative diagram.

$$\begin{tikzcd}
\mathrm{id}_X \arrow[rrr, mapsto] \arrow[ddd] & & & f^{\#}(\mathrm{id}_X) = f \arrow[ddd, mapsto] \\
& h_X(X) \arrow[r, "f^{\#}"] \arrow[d, "\tau^{\xi}_X"'] & h_X(Y) \arrow[d, "\tau^{\xi}_Y"] & \\
& \mathscr{F}(X) \arrow[r, "\mathscr{F}(f)"'] & \mathscr{F}(Y) & \\
\tau^{\xi}_X(\mathrm{id}_X) = \xi \arrow[rrr, mapsto] & & & \mathscr{F}(f)(\xi) = \tau^{\xi}_Y(f)
\end{tikzcd}$$

Thus we are forced to define τ^{ξ} by $\tau^{\xi}_Y(f) = \mathscr{F}(f)(\xi)$ for each morphism $f : Y \to X$ in $\mathscr{C}$. We show that with this definition $\tau^{\xi} = \{\tau^{\xi}_Y\}_{Y\in\mathrm{Ob}(\mathscr{C})}$ is indeed a natural transformation. Given a morphism $f : Y \to Z$, we must show that the following diagram is commutative.

$$\begin{tikzcd}
h_X(Z) \arrow[r, "f^{\#}"] \arrow[d, "\tau^{\xi}_Z"'] & h_X(Y) \arrow[d, "\tau^{\xi}_Y"] \\
\mathscr{F}(Z) \arrow[r, "\mathscr{F}(f)"'] & \mathscr{F}(Y)
\end{tikzcd}$$

Given $g \in h_X(Z) = \mathrm{Hom}(Z, X)$, then

$$\mathscr{F}(f)(\tau^{\xi}_Z(g)) = \mathscr{F}(f)(\mathscr{F}(g)(\xi)) = \mathscr{F}(g \circ f)(\xi) = \tau^{\xi}_Y(g \circ f) = \tau^{\xi}_Y(f^{\#}(g))$$

so the diagram commutes and τ^{ξ} is natural. Thus the above definition yields a map

$$\beta : \mathscr{F}(X) \to \mathrm{Hom}(h_X, \mathscr{F})$$
$$\xi \mapsto \tau^{\xi}\,.$$

We claim that α and β are mutually inverse. Given $\xi \in \mathscr{F}(X)$, then

$$\alpha(\beta(\xi)) = \alpha(\tau^{\xi}) = \tau^{\xi}_X(\mathrm{id}_X) = \mathscr{F}(\mathrm{id}_X)(\xi) = \mathrm{id}_{\mathscr{F}(X)}(\xi) = \xi\,.$$

Given $\tau \in \mathrm{Hom}(h_X, \mathscr{F})$, then $\beta(\alpha(\tau)) = \beta(\tau_X(\mathrm{id}_X)) = \tau^{\tau_X(\mathrm{id}_X)}$. Thus it suffices to show that $\tau^{\tau_X(\mathrm{id}_X)} = \tau$. Given a morphism $f : Y \to X$ in $\mathscr{C}$, then

$$\tau_Y^{\tau_X(\mathrm{id}_X)}(f) = \mathscr{F}(f)(\tau_X(\mathrm{id}_X)) = \tau_Y(f^{\#}(\mathrm{id}_X)) = \tau_Y(f)$$

by the commutativity of the above diagram. Thus $\tau^{\tau_X(\mathrm{id}_X)} = \tau$. □

Remark 2.3.8. The quantity $\mathscr{F}(f)(\xi) \in \mathscr{F}(X)$ considered in the above proof plays an important role. It is sometimes denoted $f^*\xi$.

Definition 2.3.9. Let $\mathscr{C}$ be a category and $\mathscr{F} : \mathscr{C} \to$ (sets) be a contravariant functor. A pair (U, ξ) consisting of an object U in $\mathscr{C}$ and $\xi \in \mathscr{F}(U)$ is called a *universal pair* and U a *universal object* if for each pair (C, x) consisting of an object C in $\mathscr{C}$ and $x \in \mathscr{F}(C)$ there is a unique morphism $\varphi : U \to C$ with $\mathscr{F}(f)(\xi) = x$.

Proposition 2.3.10. *Let $\mathscr{C}$ be a category, $\mathscr{F} : \mathscr{C} \to$ (sets) a contravariant functor, U be an object of $\mathscr{C}$, and $\tau : h_U \to \mathscr{F}$ a natural transformation. Then τ is an isomorphism (i.e., U represents $\mathscr{F}$) iff $(U, \tau_X(\mathrm{id}_X))$ is a universal pair of $\mathscr{F}$.*

Section 2.4

Framed algebras

The presence of automorphisms makes it difficult or impossible to construct moduli spaces as schemes. To eliminate these unwanted automorphisms, we equip our algebras with a choice of basis.

A *framed R-algebra* is an (associative, unital) R-algebra A that is free of rank n over R, along with a choice of basis $e_1, \ldots, e_n$. A *morphism* of framed R-algebras $(A, (e_1, \ldots, e_n))$ and $(A', (e'_1, \ldots, e'_n))$ is an R-algebra homomorphism $\Phi : A \to A'$ such that $\Phi(e_i) = e'_i$ for each $i = 1, \ldots, n$.

Since A is free of rank n, then each product $e_i e_j$ can be written as an R-linear combination of the e_k:

$$e_i e_j = \sum_{k=1}^{n} c_{ij}^{(k)} e_k \tag{2.4.1}$$

for some constants $c_{ij}^{(k)} \in R$, with $i, j, k \in \{1, \ldots, n\}$, called the *structure constants* of the framed algebra $(A, (e_1, \ldots, e_n))$. As every $a \in A$ can be written as a linear combination of $e_1, \ldots, e_n$, these structure constants determine the multiplication table for A.

The associativity of A imposes polynomial relations on the structure constants $c_{ij}^{(k)}$. Note that

$$\begin{aligned} (e_i e_j) e_k &= \sum_{\ell} c_{ij}^{(\ell)} e_\ell e_k = \sum_{\ell} c_{ij}^{(\ell)} \sum_{m} c_{\ell k}^{(m)} e_m = \sum_{\ell} \sum_{m} c_{ij}^{(\ell)} c_{\ell k}^{(m)} e_m \\ e_i (e_j e_k) &= e_i \sum_{\ell} c_{jk}^{(\ell)} e_\ell = \sum_{\ell} c_{jk}^{(\ell)} e_i e_\ell = \sum_{\ell} c_{jk}^{(\ell)} \sum_{m} c_{i\ell}^{(m)} e_m = \sum_{\ell} \sum_{m} c_{jk}^{(\ell)} c_{i\ell}^{(m)} e_m \,. \end{aligned}$$

Since $(e_i e_j) e_k = e_i (e_j e_k)$, equating the coefficient of e_m in the above equations yields

$$\sum_{\ell=1}^{n} c_{ij}^{(\ell)} c_{\ell k}^{(m)} = \sum_{\ell=1}^{n} c_{jk}^{(\ell)} c_{i\ell}^{(m)} \tag{2.4.2}$$

for all choices of $i, j, k, m \in \{1, \ldots, n\}$. Conversely, given any constants $c_{ij}^{(k)} \in R$

satisfying (2.4.2), we can define a framed R-algebra by defining multiplication of basis elements as in (2.4.1) and extending linearly. This allows us to associate to each framed R-algebra $(A, (e_i)_i)$ with associated structure constants $c_{ij}^{(k)}$ the point $(c_{ij}^{(k)})_{i,j,k}$ in the affine subvariety of $\mathbb{A}^{n^3}$ cut out by (2.4.2).

An important example of a framed R-algebra is the algebra

$$\frac{R[x_1, \ldots, x_{n-1}]}{(x_1, \ldots, x_{n-1})^2}$$

with basis $(1, x_1, \ldots, x_{n-1})$.

Definition 2.4.1. A framed R-algebra A with basis $(e_1, \ldots, e_{n-1})$ is *nilproduct* if it is isomorphic as framed R-algebras to

$$\frac{R[x_1, \ldots, x_{n-1}]}{(x_1, \ldots, x_{n-1})^2}$$

with basis $(1, x_1, \ldots, x_{n-1})$.

Section 2.5

Modest bases

Given a framed R-algebra A, we can equip it with a particular kind of basis that further rigidifies the situation and makes our classification easier. In [Voight, 2011c], Voight shows that R is a direct summand of A (as an R-module).

Lemma 2.5.1 ([Voight, 2011c, Lemma 1.3]). *Let A be an R-algebra that is finitely generated and projective as an R-module. Assume further that A has constant rank, meaning that there is some constant $c \in \mathbb{Z}_{\geq 0}$ such that $\operatorname{rank}_{R_\mathfrak{p}}(A_\mathfrak{p}) = c$ for all $\mathfrak{p} \in$*

Spec(R). *Then R is a direct summand of A.*

In the course of the proof of this lemma, Voight shows that A/R is locally free. Thus there exist $f_1, \ldots, f_m \in R$ with $(f_1, \ldots, f_m) = R$ such that $(A/R)_{f_i} = (A/R) \otimes_R R_{f_i}$ is free for each i. Since

$$A_{f_i} \cong (R \oplus A/R)_{f_i} \cong R_{f_i} \oplus (A/R)_{f_i}\,,$$

and 1 is a basis for R_{f_i}, then for each i there is a basis of A_{f_i} containing 1.

Definition 2.5.2. Let A be a free R algebra. A basis $(e_i)_i$ of A is *unital* if $e_1 = 1$.

For the moment, suppose we are in the case where A itself has a unital basis. Since $e_1 = 1$, this imposes further restrictions on the structure constants. Since

$$\begin{aligned} e_i &= e_i e_1 = \sum_k c_{i1}^{(k)} e_k \\ e_j &= e_1 e_j = \sum_k c_{1j}^{(k)} e_k \end{aligned}$$

we see that

$$c_{i1}^{(k)} = \delta_{ik} = \begin{cases} 1\,, & \text{if } i = k\,; \\ 0\,, & \text{otherwise}\,; \end{cases} \qquad \text{and} \qquad c_{1j}^{(k)} = \delta_{jk} = \begin{cases} 1\,, & \text{if } j = k\,; \\ 0\,, & \text{otherwise}\,; \end{cases} \tag{2.5.1}$$

for all $i, j, k \in \{1, \ldots, n\}$. (Here δ_{ik} denotes the Kronecker delta.)

There are still two degrees of freedom left in the choice of basis, so we can impose even further conditions.

Definition 2.5.3. A unital basis $(e_i)_i$ for A with associated structure constants

$\{c_{ij}^{(k)}\}_{i,j,k}$ is *modest* if

$$c_{i,i+1}^{(i)} = 0 \text{ for } i = 2, \ldots, n-1 \quad \text{and} \quad c_{n,2}^{(n)} = 0. \tag{2.5.2}$$

(Note that $c_{i,i+1}^{(i)}$ is the coefficient of e_i in the product e_ie_{i+1}.)

Remark 2.5.4. For a free R-algebra A of rank $n = 2$, the criterion (2.5.2) is vacuous. For $n = 3$, (2.5.2) implies $c_{23}^{(2)} = c_{32}^{(3)} = 0$, meaning that

$$e_2e_3 = r + se_3 \qquad \text{and} \qquad e_3e_2 = t + ue_2$$

for some $r, s, t, u \in R$.

Remark 2.5.5. Our definition of modest basis is similar, but slightly different from, the notion of a *normal basis* introduced in [Delone and Faddeev, 1940, §15] and that of a *good basis* given in [Gross and Lucianovic, 2009].

We now show that any unital basis can be transformed into a modest basis.

Lemma 2.5.6. *Let A be a framed R-algebra of rank n with unital basis $(e_i)_i$. Then A has a modest basis.*

Proof. Define the basis $(e'_i)_i$ by $e'_1 = 1$, $e'_2 = e_2 - c_{n,2}^{(n)}$, and $e'_{i+1} = e_{i+1} - c_{i,i+1}^{(i)}$ for $i = 2, \ldots n-1$. Then for $i \neq n$ we have

$$e'_ie'_{i+1} = (e_i - c_{i-1,i}^{(i-1)})(e_{i+1} - c_{i,i+1}^{(i)}) = c_{i-1,i}^{(i-1)}c_{i,i+1}^{(i)} - c_{i-1,i}^{(i-1)}e_{i+1} - c_{i,i+1}^{(i)}e_i + \sum_{k=1}^{n} c_{i,i+1}^{(k)}e_k\,.$$

Thus the e_i term in the last sum cancels out, yielding

$$e'_i e'_{i+1} = c^{(i-1)}_{i-1,i} c^{(i)}_{i,i+1} + (c^{(i+1)}_{i,i+1} - c^{(i-1)}_{i-1,i}) e_{i+1} + \sum_{\substack{k=1 \\ k\neq i,i+1}}^{n} c^{(k)}_{i,i+1} e_k \,.$$

Using the identity $e_k = e'_k + c^{(k-1)}_{k-1,k}$ to rewrite this expression in terms of $(e'_i)_i$, we find

$$\begin{aligned} e'_i e'_{i+1} &= c^{(i-1)}_{i-1,i} c^{(i)}_{i,i+1} + (c^{(i+1)}_{i,i+1} - c^{(i-1)}_{i-1,i})(e'_{i+1} + c^{(i)}_{i,i+1}) + \sum_{\substack{k=1 \\ k\neq i,i+1}}^{n} c^{(k)}_{i,i+1}(e'_k + c^{(k-1)}_{k-1,k}) \\ &= c^{(i-1)}_{i-1,i} c^{(i)}_{i,i+1} - c^{(i-1)}_{i-1,i} c^{(i)}_{i,i+1} + \left(\sum_{\substack{k=1 \\ k\neq i}}^{n} c^{(k)}_{i,i+1} c^{(k-1)}_{k-1,k} \right) \\ &\qquad + (c^{(i+1)}_{i,i+1} - c^{(i-1)}_{i-1,i}) e'_{i+1} + \sum_{\substack{k=1 \\ k\neq i,i+1}}^{n} c^{(k)}_{i,i+1} e'_k \,. \end{aligned}$$

Thus there is no e'_i appearing in this expression, as desired. A similar computation for $i = n$ shows that the coefficient of e'_n in $e'_n e_2$ is also 0. Thus $(e'_i)_i$ is a modest basis. □

Section 2.6

Sheaves and gluing

Our strategy for proving classification results for sheaves of algebras over a scheme is to first prove the corresponding results for algebras over a ring, and then show that we can glue these algebras together in order to get a sheaf. Thus we will need the following definitions and results on extending sheaves on a base. We refer the reader to [Stacks Project Authors, 2019, §6.30] for further details.

Definition 2.6.1. Let X be a topological space and let $\mathcal{B}$ be a basis for the topology on X.

(1) A *presheaf* $\mathscr{F}$ *of sets on* $\mathcal{B}$ is a rule which assigns to each $U \in \mathcal{B}$ a set $\mathscr{F}(U)$ and to each inclusion $V \subseteq U$ of elements of $\mathcal{B}$ a map $\mathrm{res}_V^U : \mathscr{F}(U) \to \mathscr{F}(V)$ such that $\mathrm{res}_U^U = \mathrm{id}_{\mathscr{F}(U)}$ for all $U \in \mathcal{B}$ and whenever $W \subseteq V \subseteq U$ in $\mathcal{B}$ we have $\mathrm{res}_W^U = \mathrm{res}_W^V \circ \mathrm{res}_V^U$.

(2) A *morphism* $\varphi : \mathscr{F} \to \mathscr{G}$ *of presheaves of sets on* $\mathcal{B}$ is a rule which assigns to each element $U \in \mathcal{B}$ a map of sets $\varphi : \mathscr{F}(U) \to \mathscr{G}(U)$ compatible with restriction maps.

(3) A *sheaf* $\mathscr{F}$ *of sets on* $\mathcal{B}$ is a presheaf of sets on $\mathcal{B}$ which satisfies the following additional property: given any $U \in \mathcal{B}$, and any covering $\{U_i\}_i$ of U with $U_i \in \mathcal{B}$ for all i, and any coverings $\{U_{ijk}\}_{k \in I_{ij}}$ of $U_i \cap U_j$ with $U_{ijk} \in \mathcal{B}$ for all i, j, k, the following condition holds. Given a collection of sections $\{s_i\}_i$ with $s_i \in \mathscr{F}(U_i)$ for all i such that for all $i, j \in I$ and all $k \in I_{jk}$

$$s_i|_{U_{ijk}} = s_j|_{U_{ijk}}$$

there exists a unique section $s \in \mathscr{F}(U)$ such that $s_i = s|_{U_i}$ for all $i \in I$.

We can make a similar definition for sheaves on a base taking values in other categories. We first give a general definition of an algebraic structure following [Stacks Project Authors, 2019, §6.15].

Definition 2.6.2. A *type of algebraic structure* is given by a category $\mathscr{C}$ and functor $\mathscr{F} : \mathscr{C} \to$ (sets) with the following properties:

(1) $\mathscr{F}$ is faithful;

(2) $\mathscr{C}$ has limits and $\mathscr{F}$ commutes with limits;

(3) $\mathscr{C}$ has filtered colimits and $\mathscr{F}$ commutes with them; and

(4) $\mathscr{F}$ reflects isomorphisms.

The main algebraic structures we consider are the categories of abelian groups, rings, and R-modules for a fixed ring R, each equipped with the appropriate forgetful functor.

Definition 2.6.3. Let X be a topological space and let $\mathcal{B}$ be a basis for the topology on X. Let $(\mathscr{C}, F)$ be a type of algebraic structure.

(1) A *presheaf* $\mathscr{F}$ *with values in* $\mathscr{C}$ *on* $\mathcal{B}$ is a rule which assigns to each $U \in \mathcal{B}$ an object $\mathscr{F}(U)$ of $\mathscr{C}$ and to each inclusion $V \subseteq U$ of elements of $\mathcal{B}$ a morphism res_V^U such that $\operatorname{res}_U^U = \operatorname{id}_{\mathscr{F}(U)}$ for all $U \in \mathcal{B}$ and whenever $W \subseteq V \subseteq U$ in $\mathcal{B}$ we have $\operatorname{res}_W^U = \operatorname{res}_W^V \circ \operatorname{res}_V^U$.

(2) A *morphism* $\varphi : \mathscr{F} \to \mathscr{G}$ *of presheaves with values in* $\mathscr{C}$ *on* $\mathcal{B}$ is a rule which assigns to each element $U \in \mathcal{B}$ a map of sets $\varphi : \mathscr{F}(U) \to \mathscr{G}(U)$ compatible with restriction maps.

(3) A *sheaf* $\mathscr{F}$ *with values in* $\mathscr{C}$ *on* $\mathcal{B}$ is a presheaf with values in $\mathscr{C}$ on $\mathcal{B}$ whose underlying presheaf of sets is a sheaf.

The next result shows that a sheaf on a basis uniquely extends to a sheaf.

Lemma 2.6.4 ([Stacks Project Authors, 2019, Lemma 6.30.9])**.** *Let X be a topological space. Let $(\mathscr{C}, F)$ be a type of algebraic structure. Let $\mathcal{B}$ be a basis for the topology* *on X. Let $\mathscr{F}$ be a sheaf on $\mathcal{B}$ with values in $\mathscr{C}$. Then there exists a unique sheaf $\widetilde{\mathscr{F}}$ on X with values in $\mathscr{C}$ such that $\widetilde{\mathscr{F}}(U) = \mathscr{F}(U)$ for all $U \in \mathcal{B}$ compatibly with the restriction maps.*

Section 2.7

Results from algebraic geometry

We collect here some results from algebraic geometry which we will use to study the moduli of the framed cubic algebras in the next chapter.

We use the following results to characterize when a property is affine local.

Proposition 2.7.1 (Nike's Trick, [Vakil, 2015, Proposition 5.3.1])**.** *Suppose* $\operatorname{Spec}(A)$ *and* $\operatorname{Spec}(B)$ *are affine open subschemes of a scheme X. Then* $\operatorname{Spec}(A) \cap \operatorname{Spec}(B)$ *is the union of open sets that are simultaneously distinguished open subschemes of* $\operatorname{Spec}(A)$ *and* $\operatorname{Spec}(B)$.

Lemma 2.7.2 (Affine Communication Lemma, [Vakil, 2015, Lemma 5.3.2])**.** *Let P be some property enjoyed by some affine open subsets of a scheme X, such that*

(i) *if an affine open subset* $\operatorname{Spec}(R) \hookrightarrow X$ *has property P then for any $f \in R$,* $\operatorname{Spec}(R_f) \hookrightarrow X$ *does, too; and*

(ii) *if $(f_1, \dots, f_m) = R$, and* $\operatorname{Spec}(R_{f_i}) \hookrightarrow X$ *has P for all i, then so does* $\operatorname{Spec}(R) \hookrightarrow X$.

Suppose that $X = \bigcup_{i \in I} \operatorname{Spec}(R_i)$*, where* $\operatorname{Spec}(R_i)$ *has property P. Then every affine open subset of X has P, too.*

Definition 2.7.3. A property P satisfying (i) and (ii) above is called *affine-local.*

We will also need the following result on sheaves of modules on an affine scheme.

Proposition 2.7.4 (Corollary II.5.5, [Hartshorne, 2013])**.** *Let R be a commutative ring and let $X = \operatorname{Spec}(R)$. The functor $M \mapsto \widetilde{M}$ gives an equivalence of categories between the category of R-modules and the category of quasicoherent $\mathscr{O}_X$-modules. Its inverse is the functor $\mathscr{F} \mapsto \Gamma(X, \mathscr{F})$. If R is noetherian, the same functor also gives an equivalence of categories between the category of finitely generated R-modules and the category of coherent $\mathscr{O}_X$-modules.*

The following definition and result show that quasicoherent sheaves of ideals and closed subschemes are in bijective correspondence.

Definition 2.7.5. Let X be a scheme, Y a closed subscheme of X, and $i : Y \hookrightarrow X$ the inclusion morphism. The *ideal sheaf* of Y, denoted $\mathscr{I}_Y$, is the kernel of the morphism of sheaves $i^\# : \mathscr{O}_X \to i_*\mathscr{O}_Y$.

Proposition 2.7.6 ([Hartshorne, 2013, Proposition II.5.9], [Liu, 2002, Ch. 5, Proposition 1.15])**.** *Let X be a scheme. For any closed subscheme Y of X, the corresponding ideal sheaf $\mathscr{I}_Y$ is a quasicoherent sheaf of ideals on X. If X is noetherian it is coherent. Conversely, any quasicoherent sheaf of ideals on X is the ideal sheaf of a uniquely determined closed subscheme of X.*

We collect below some useful results on quasicoherent sheaves.

Proposition 2.7.7 ([Liu, 2002, Ch. 5, Proposition 1.8])**.** *Let X be an affine scheme. Let $0 \to \mathscr{F} \to \mathscr{G} \to \mathscr{H} \to 0$ be an exact sequence of $\mathscr{O}_X$-modules with $\mathscr{F}$ quasicoherent. Then the sequence of global sections*

$$0 \to \mathscr{F}(X) \to \mathscr{G}(X) \to \mathscr{H}(X) \to 0$$

is exact.

Proposition 2.7.8 ([Liu, 2002, Ch. 5, Proposition 1.12])**.** *Let X be a scheme.*

(a) *If $\mathscr{F}, \mathscr{G}$ are quasicoerent (resp., finitely generated quasicoherent) $\mathscr{O}_X$-modules, then so is $\mathscr{F} \otimes_{\mathscr{O}_X} \mathscr{G}$. Moreover, for any affine open subset U of X, we have $(\mathscr{F} \otimes_{\mathscr{O}_X} \mathscr{G})(U) \cong \mathscr{F}(U) \otimes_{\mathscr{O}_X(U)} \mathscr{G}(U)$.*

(b) *Let $u : \mathscr{F} \to \mathscr{G}$ be a morphism of quasicoherent sheaves. Then* $\ker(u)$, $\operatorname{img}(u)$, *and* $\operatorname{coker}(u)$ *are quasicoherent.*

Proposition 2.7.9 ([Liu, 2002, Ch. 5, Proposition 1.14])**.** *Let $f : X \to Y$ be a morphism of schemes and let $\mathscr{G}$ be an $\mathscr{O}_Y$-module.*

(a) *For any $x \in X$, we have a canonical isomorphism*

$$(f^*\mathscr{G})_x \cong \mathscr{G}_{f(x)} \otimes_{\mathscr{O}_{Y,f(x)}} \mathscr{O}_{X,x}\,.$$

(b) *Suppose $\mathscr{G}$ is quasicoherent. Let U be an affine open subset of X such that $f(U)$ is contained in an affine open subset V of Y. Then*

$$f^*\mathscr{G}|_U \cong (\mathscr{G}(V) \otimes_{\mathscr{O}_Y(V)} \mathscr{O}_X(U))\tilde{}$$

In particular, $f^*\mathscr{G}$ is quasicoherent.

Finally, we will use the projection formula (also known as the push-pull formula) below, which describes the result of first pulling back and then pushing forward a sheaf by a morphism.

Proposition 2.7.10 ([Hartshorne, 2013, Exercise II.5.1])**.** *Let $f : X \to Y$ be a morphism of ringed spaces, $\mathscr{F}$ be an $\mathscr{O}_X$-module and $\mathscr{E}$ be a locally free $\mathscr{O}_Y$-module of finite rank. Then there is a natural isomorphism $f_*(\mathscr{F} \otimes_{\mathscr{O}_X} f^*\mathscr{E}) \cong f_*(\mathscr{F}) \otimes_{\mathscr{O}_Y} \mathscr{E}$.*

Chapter 3

Moduli of cubic algebras

Section 3.1

Results in the literature

The main results of this part are generalizations of the following theorem.

Theorem 3.1.1 (Theorem 5.1, [Levin, 2013]). *Let R be a domain. A free R-algebra of rank 3 is either commutative or possesses a standard involution.*

In [Voight, 2011c], Voight shows that having a standard involution and being exceptional are equivalent properties for rank 3 algebras.

Theorem 3.1.2 (Theorem B, [Voight, 2011c]). *An R-algebra A of rank 3 has a standard involution if and only if it is exceptional.*

We will generalize Theorem 3.1.1, first to the case of arbitrary commutative base rings, then to sheaves of locally free rank 3 algebras over an arbitrary base scheme. We approach the problem from an algebro-geometric and moduli theoretic perspective. Our results bear similarities to the following proposition.

Proposition 3.1.3 (Proposition 4.4, [Voight, 2011b]). *Let A be an R-algebra of rank 4 with a standard involution. The set of primes $\mathfrak{p}$ such that $A \otimes_R R/\mathfrak{p} \cong A/\mathfrak{p}A$ is a quaternion (resp. exceptional) ring is Zariski-closed in* $\operatorname{Spec}(R)$*. Given an algebra of rank 4 over R with standard involution, there exists a decomposition* $\operatorname{Spec}(R_Q) \cup \operatorname{Spec}(R_E) \hookrightarrow \operatorname{Spec}(R)$ *such that $A_{R_Q} := A \otimes_R R_Q$ is a quaternion ring, A_{R_E} is an exceptional ring, and* $\operatorname{Spec}(R_Q)$ *and* $\operatorname{Spec}(R_E)$ *are the largest (closed) subschemes with these properties.*

Section 3.2

The universal case

Define the functor $\mathfrak{M}_n^\square$: (commutative rings) → (sets) by

$$\mathfrak{M}_n^\square(R) = \{\text{isomorphism classes of modestly framed rank } n \text{ } R\text{-algebras}\} .$$

We complete the definition by specifying the action on morphisms: given a ring homomorphism $\varphi : R \to R'$, define

$$\begin{aligned} \mathfrak{M}_n^\square(\varphi) : \mathfrak{M}_n^\square(R) &\to \mathfrak{M}_n^\square(R') \\ (A, (e_i)_i) &\mapsto (A \otimes_R R', (e_i \otimes 1)_i) \end{aligned}$$

where we consider R' as an R-module via the homomorphism φ.

Proposition 3.2.1. *The functor $\mathfrak{M}_n^\square$ is representable by an affine scheme of finite type over $\mathbb{Z}$.*

Proof. Define $R_{\text{univ}} = \mathbb{Z}[\gamma_{ij}^{(k)}]/I$ where I is the ideal of all the relations listed in (2.4.2), (2.5.1), and (2.5.2):

$$\begin{aligned} I = &\left(\sum_{\ell}\gamma_{ij}^{(\ell)}\gamma_{\ell k}^{(m)} - \sum_{\ell}\gamma_{jk}^{(\ell)}\gamma_{i\ell}^{(m)} : i,j,k,m \in \{1,\dots,n\}\right) \\ &+ \left(\gamma_{i1}^{(k)} - \delta_{ik} : i,k \in \{1,\dots,n\}\right) + \left(\gamma_{1j}^{(k)} - \delta_{jk} : j,k \in \{1,\dots,n\}\right) \\ &+ (\gamma_{ii+1}^{(i)} : i \in \{2,\dots,n-1\}) + (\gamma_{n2}^{(n)}) \end{aligned} \tag{3.2.1}$$

where δ_{ik} and δ_{jk} are Kronecker deltas. Define the A_{univ} to be the free R_{univ}-algebra of rank n with basis $1 = \varepsilon_1, \varepsilon_2, \dots, \varepsilon_n$, and with multiplication defined by (2.4.1), i.e.,

$$\varepsilon_i\varepsilon_j = \sum_{k=1}^{n}\gamma_{ij}^{(k)}\varepsilon_k \tag{3.2.2}$$

for $i,j \in \{1,\dots,n\}$.

Suppose R is a commutative ring and $(A,(e_i)_i)$ is a modestly framed R-algebra with associated structure constants $c_{ij}^{(k)}$. Define the ring homomorphism

$$\begin{aligned} \varphi : \mathbb{Z}[\gamma_{ij}^{(k)}] &\to R \\ \gamma_{ij}^{(k)} &\mapsto c_{ij}^{(k)} . \end{aligned}$$

Since the structure constants $\{c_{ij}^{(k)}\}_{i,j,k}$ satisfy the relations given in (2.4.2), (2.5.1), and (2.5.2), then φ descends to a homomorphism $\overline{\varphi} : R_{\text{univ}} = \mathbb{Z}[\gamma_{ij}^{(k)}]/I \to R$. Giving R the structure of an R_{univ}-module via $\overline{\varphi}$, then $A \cong A_{\text{univ}} \otimes_{R_{\text{univ}}} R$ as R-algebras.

It remains to show that $\overline{\varphi}$ is unique. Suppose $\psi : R_{\text{univ}} \to R$ is a homomorphism such that $A \cong A_{\text{univ}} \otimes_{R_{\text{univ}}} R$ where R is given the R_{univ}-module structure induced by ψ. Denote the isomorphism $A \xrightarrow{\sim} A_{\text{univ}} \otimes_{R_{\text{univ}}}$ by Ψ. Given $i,j \in \{1,\dots,n\}$, on one hand we have

$$(\varepsilon_i \otimes 1)(\varepsilon_j \otimes 1) = \varepsilon_i\varepsilon_j \otimes 1 = \sum_k \gamma_{ij}^{(k)}\varepsilon_k \otimes 1 = \sum_k \varepsilon_k \otimes \psi(\gamma_{ij}^{(k)}) = \sum_k \psi(\gamma_{ij}^{(k)})(\varepsilon_k \otimes 1)\,.$$

On the other, since Ψ is a framed R-algebra homomorphism, then

$$\begin{aligned}(\varepsilon_i \otimes 1)(\varepsilon_j \otimes 1) = \Psi(e_i)\Psi(e_j) = \Psi(e_ie_j) = \Psi\left(\sum_k c_{ij}^{(k)}e_k\right) &= \sum_k c_{ij}^{(k)}\Psi(e_k)\\ = \sum_k c_{ij}^{(k)}(\varepsilon_k \otimes 1)\,.\end{aligned}$$

Since $\{\varepsilon_k \otimes 1\}_k$ is a basis for $A_{\text{univ}} \otimes_{R_{\text{univ}}}$, then $\psi(\gamma_{ij}^{(k)}) = c_{ij}^{(k)} = \overline{\varphi}(\gamma_{ij}^{(k)})$ for all k. Since R_{univ} is generated by $\{\gamma_{ij}^{(k)}\}_{i,j,k}$ as a ring (i.e., as a $\mathbb{Z}$-algebra), then $\psi = \overline{\varphi}$. Thus R_{univ} represents $\mathfrak{M}_n^{\square}$ with universal object A_{univ}. □

Remark 3.2.2. Let R be a commutative ring and $(A, (e_i)_i)$ a framed R-algebra of rank n with associated structure constants $c_{ij}^{(k)}$. Applying the proof of Yoneda's lemma to the representability proved in Proposition 3.2.1, this means that there exists a unique ring homomorphism $\varphi : R_{\text{univ}} \to R$, $\gamma_{ij}^{(k)} \mapsto c_{ij}^{(k)}$ such that $A_{\text{univ}} \otimes_{R_{\text{univ}}} R \cong A$ as R-modules via the map $\varepsilon_i \otimes 1 \mapsto e_i$. This is shown in the diagram below.

$$\begin{tikzcd}
\mathrm{id}_{R_{\mathrm{univ}}} \arrow[rrr, mapsto] \arrow[ddd] & & & \varphi_{\#}(\mathrm{id}_{R_{\mathrm{univ}}}) = \varphi \circ \mathrm{id}_{R_{\mathrm{univ}}} = \varphi \arrow[ddd, mapsto] \\
& h_{R_{\mathrm{univ}}}(R_{\mathrm{univ}}) \arrow[r, "\varphi_{\#}"] \arrow[d, "\tau_{R_{\mathrm{univ}}}"'] & h_{R_{\mathrm{univ}}}(R) \arrow[d, "\tau_R"] & \\
& \mathfrak{M}_n^{\square}(R_{\mathrm{univ}}) \arrow[r, "\mathfrak{M}_n^{\square}(\varphi)"'] & \mathfrak{M}_n^{\square}(R) & \\
\tau_{R_{\mathrm{univ}}}(\mathrm{id}_{R_{\mathrm{univ}}}) = A_{\mathrm{univ}} \arrow[rrr, mapsto] & & & \tau_R(\varphi) = A \\
& & & = \mathfrak{M}_n^{\square}(\varphi)(A_{\mathrm{univ}}) \\
& & & = A_{\mathrm{univ}} \otimes_{R_{\mathrm{univ}}} R
\end{tikzcd}$$

The relations found above—those stemming from $e_1 = 1$, associativity, and modest basis—give explicit equations for the moduli space of rank n framed algebras. Let $n = 3$. Computing with Magma [Cannon et al., 2006], we form the ideal I in $\mathbb{Z}[c_{ij}^{(k)}]$, a polynomial ring with $3^3 = 27$ variables, generated by these relations.

Lemma 3.2.3. *Let I be the ideal of relations in $\mathbb{Z}[\gamma_{ij}^{(k)}]$ as in (3.2.1). Then I has the following set of generators.*

$$\begin{aligned}
&\{\gamma_{11}^{(1)} - 1, \gamma_{11}^{(2)}, \gamma_{11}^{(3)}, \gamma_{12}^{(1)}, \gamma_{12}^{(2)} - 1, \gamma_{12}^{(3)}, \gamma_{13}^{(1)}, \gamma_{13}^{(2)}, \gamma_{13}^{(3)} - 1,\\
&\gamma_{21}^{(1)}, \gamma_{21}^{(2)} - 1, \gamma_{21}^{(3)}, \gamma_{22}^{(1)} + \gamma_{22}^{(3)}\gamma_{33}^{(3)}, \gamma_{22}^{(2)}\gamma_{23}^{(3)} - {\gamma_{23}^{(3)}}^2, \gamma_{22}^{(2)}\gamma_{32}^{(1)} + \gamma_{22}^{(3)}\gamma_{33}^{(1)},\\
&\gamma_{22}^{(2)}\gamma_{32}^{(2)} - \gamma_{23}^{(3)}\gamma_{33}^{(3)}, \gamma_{22}^{(2)}\gamma_{33}^{(2)} + \gamma_{33}^{(1)}, \gamma_{22}^{(3)}\gamma_{23}^{(3)}, \gamma_{22}^{(3)}\gamma_{32}^{(2)}, \gamma_{22}^{(3)}\gamma_{33}^{(2)} - \gamma_{32}^{(1)},\\
&\gamma_{23}^{(1)} - \gamma_{32}^{(1)}, \gamma_{23}^{(2)}, \gamma_{23}^{(3)}\gamma_{32}^{(1)}, \gamma_{23}^{(3)}\gamma_{32}^{(2)} - \gamma_{23}^{(3)}\gamma_{33}^{(3)}, \gamma_{23}^{(3)}\gamma_{33}^{(1)}, \gamma_{23}^{(3)}\gamma_{33}^{(2)},\\
&\gamma_{31}^{(1)}, \gamma_{31}^{(2)}, \gamma_{31}^{(3)} - 1, \gamma_{32}^{(1)}\gamma_{32}^{(2)}, {\gamma_{32}^{(2)}}^2 - \gamma_{32}^{(2)}\gamma_{33}^{(3)}, \gamma_{32}^{(2)}\gamma_{33}^{(1)}, \gamma_{32}^{(2)}\gamma_{33}^{(2)}, \gamma_{32}^{(3)}\}
\end{aligned}$$

Proof. This is a straightforward computation in Magma. (Indeed the above set is a

Gröbner basis for I with respect to the lexicographic monomial ordering.) □

Lemma 3.2.4. *Let R be a commutative ring and A be a framed R-algebra of rank 3 with modest basis $1 = e_1, e_2, e_3$ and associated structure constants $c_{ij}^{(k)}$. Then $c_{23}^{(1)} = c_{32}^{(1)}$.*

Proof. By 3.2.1 there exists a unique ring homomorphism $\varphi : R_{\text{univ}} \to R$ such that $\varphi(\gamma_{ij}^{(k)}) = c_{ij}^{(k)}$ for all i, j, k. Since $\gamma_{23}^{(1)} - \gamma_{32}^{(1)} = 0$ in R_{univ} by Lemma 3.2.3, then $c_{23}^{(1)} = \varphi(\gamma_{23}^{(1)}) = \varphi(\gamma_{32}^{(1)}) = c_{32}^{(1)}$. □

Theorem 3.2.5. *Let $R_{\text{univ}} = \mathbb{Z}[\gamma_{ij}^{(k)}]/I$ be defined as in (3.2.1) and let $(A_{\text{univ}}, (\varepsilon_1, \varepsilon_2, \varepsilon_3))$ be the framed rank 3 R_{univ}-algebra defined as in (3.2.2). Let $I_{\text{univ},C} = (\gamma_{23}^{(3)}, \gamma_{32}^{(2)})$ and*

$$I_{\text{univ},E} = (\gamma_{22}^{(1)}, \gamma_{22}^{(2)} - \gamma_{23}^{(3)}, \gamma_{22}^{(3)}, \gamma_{23}^{(1)}, \gamma_{32}^{(1)}, \gamma_{32}^{(2)} - \gamma_{33}^{(3)}, \gamma_{33}^{(1)}, \gamma_{33}^{(2)})$$

and let $R_{\text{univ},C} = R_{\text{univ}}/I_{\text{univ},C}$ and $R_{\text{univ},E} = R_{\text{univ}}/I_{\text{univ},E}$. Then

(a) *The zero ideal (0) in R_{univ} has primary decomposition $(0) = I_{\text{univ},C} \cap I_{\text{univ},E}$.*

(b) *$I_{\text{univ},C}$ and $I_{\text{univ},E}$ are prime.*

(c) *$R_{\text{univ}}/I_{\text{univ},C} \cong \mathbb{Z}[\gamma_{22}^{(2)}, \gamma_{22}^{(3)}, \gamma_{33}^{(2)}, \gamma_{33}^{(3)}]$ and $R_{\text{univ}}/I_{\text{univ},E} \cong \mathbb{Z}[\gamma_{23}^{(3)}, \gamma_{32}^{(2)}]$, polynomial rings in 4 and 2 variables, respectively.*

Proof. Using the built-in Gröbner basis capabilities of Magma [Cannon et al., 2006], we compute the primary decomposition of (0) in R_{univ}. In 0.240 seconds, we find that $(0) = I_{C,\text{univ}} \cap I_{E,\text{univ}}$ and that $I_{C,\text{univ}}$ and $I_{E,\text{univ}}$ are prime.

Observe that

$$\frac{R_{\text{univ}}}{I_{\text{univ},C}} \cong \frac{\mathbb{Z}[\gamma_{ij}^{(k)}]}{I + I_{\text{univ},C}}$$

and similarly for $I_{\mathrm{univ},E}$. Again using Magma, we find that $I + I_{\mathrm{univ},C}$ has generators

$$\begin{aligned}
&\{\gamma_{11}^{(1)} - 1, \gamma_{11}^{(2)}, \gamma_{11}^{(3)}, \gamma_{12}^{(1)}, \gamma_{12}^{(2)} - 1, \gamma_{12}^{(3)}, \gamma_{13}^{(1)}, \gamma_{13}^{(2)}, \gamma_{13}^{(3)} - 1,\\
&\gamma_{21}^{(1)}, \gamma_{21}^{(2)} - 1, \gamma_{21}^{(3)}, \gamma_{22}^{(1)} + \gamma_{22}^{(3)}\gamma_{33}^{(3)}, \gamma_{22}^{(2)}\gamma_{32}^{(1)} + \gamma_{22}^{(3)}\gamma_{33}^{(1)}, \gamma_{22}^{(2)}\gamma_{33}^{(2)} + \gamma_{33}^{(1)}, \gamma_{22}^{(3)}\gamma_{33}^{(2)} - \gamma_{32}^{(1)},\\
&\gamma_{23}^{(1)} - \gamma_{32}^{(1)}, \gamma_{23}^{(2)}, \gamma_{23}^{(3)},\\
&\gamma_{31}^{(1)}, \gamma_{31}^{(2)}, \gamma_{31}^{(3)} - 1, \gamma_{32}^{(2)}, \gamma_{32}^{(3)}\}
\end{aligned}$$

Eliminating superfluous variables, we find

$$\frac{R_{\mathrm{univ}}}{I_{\mathrm{univ},C}} \cong \frac{\mathbb{Z}[\gamma_{ij}^{(k)}]}{I + I_{\mathrm{univ},C}} \cong \frac{\mathbb{Z}[\gamma_{22}^{(1)}, \gamma_{22}^{(2)}, \gamma_{22}^{(3)}, \gamma_{23}^{(1)}, \gamma_{32}^{(2)}, \gamma_{33}^{(1)}, \gamma_{33}^{(2)}, \gamma_{33}^{(3)}]}{(f_1, f_2, f_3, f_4, f_5)}$$

where

$$\begin{aligned}
f_1 &= \gamma_{22}^{(1)} + \gamma_{22}^{(3)}\gamma_{33}^{(3)}\\
f_2 &= \gamma_{22}^{(2)}\gamma_{32}^{(1)} + \gamma_{22}^{(3)}\gamma_{33}^{(1)}\\
f_3 &= \gamma_{22}^{(2)}\gamma_{33}^{(2)} + \gamma_{33}^{(1)}\\
f_4 &= \gamma_{22}^{(3)}\gamma_{33}^{(2)} - \gamma_{32}^{(1)}\\
f_5 &= \gamma_{23}^{(1)} - \gamma_{32}^{(1)}
\end{aligned}$$

The relations given by f_1, f_3, f_4, and f_5 allow us to rewrite $\gamma_{22}^{(1)}, \gamma_{23}^{(1)}, \gamma_{32}^{(2)}, \gamma_{33}^{(1)}$ in terms of $\gamma_{22}^{(2)}, \gamma_{22}^{(3)}, \gamma_{33}^{(2)}$, and $\gamma_{33}^{(3)}$, and thus eliminate them in the quotient. Substituting the relations $\gamma_{32}^{(1)} = \gamma_{22}^{(3)}\gamma_{33}^{(2)}$ and $\gamma_{33}^{(1)} = -\gamma_{22}^{(2)}\gamma_{33}^{(2)}$ given by f_4 and f_3 into f_2, we find

$$\gamma_{22}^{(2)}\gamma_{32}^{(1)} + \gamma_{22}^{(3)}\gamma_{33}^{(1)} = \gamma_{22}^{(2)}(\gamma_{22}^{(3)}\gamma_{33}^{(2)}) + \gamma_{22}^{(3)}(-\gamma_{22}^{(2)}\gamma_{33}^{(2)}) = 0\,.$$

Thus

$$\begin{aligned}\frac{R_{\mathrm{univ}}}{I_{\mathrm{univ},C}} &\cong \frac{\mathbb{Z}[\gamma_{22}^{(1)}, \gamma_{22}^{(2)}, \gamma_{22}^{(3)}, \gamma_{23}^{(1)}, \gamma_{32}^{(2)}, \gamma_{33}^{(1)}, \gamma_{33}^{(2)}, \gamma_{33}^{(3)}]}{(f_1, f_2, f_3, f_4, f_5)} \cong \frac{\mathbb{Z}[\gamma_{22}^{(2)}, \gamma_{22}^{(3)}, \gamma_{33}^{(2)}, \gamma_{33}^{(3)}]}{(0)} \\ &\cong \mathbb{Z}[\gamma_{22}^{(2)}, \gamma_{22}^{(3)}, \gamma_{33}^{(2)}, \gamma_{33}^{(3)}]\,.\end{aligned}$$

Similarly, we find that $I + I_{\mathrm{univ},E}$ has generators

$$\begin{aligned}\{&\gamma_{11}^{(1)} - 1, \gamma_{11}^{(2)}, \gamma_{11}^{(3)}, \gamma_{12}^{(1)}, \gamma_{12}^{(2)} - 1, \gamma_{12}^{(3)}, \gamma_{13}^{(1)}, \gamma_{13}^{(2)}, \gamma_{13}^{(3)} - 1, \\ &\gamma_{21}^{(1)}, \gamma_{21}^{(2)} - 1, \gamma_{21}^{(3)}, \gamma_{22}^{(1)}, \gamma_{22}^{(2)} - \gamma_{23}^{(3)}, \gamma_{22}^{(3)}, \gamma_{23}^{(1)}, \gamma_{23}^{(2)}, \\ &\gamma_{31}^{(1)}, \gamma_{31}^{(2)}, \gamma_{31}^{(3)} - 1, \gamma_{32}^{(1)}, \gamma_{32}^{(2)} - \gamma_{33}^{(3)}, \gamma_{32}^{(3)}, \gamma_{33}^{(1)}, \gamma_{33}^{(2)}\}\,.\end{aligned}$$

Eliminating superfluous variables as before yields

$$\frac{R_{\mathrm{univ}}}{I_{\mathrm{univ},E}} \cong \frac{\mathbb{Z}[\gamma_{ij}^{(k)}]}{I + I_{\mathrm{univ},C}} \cong \mathbb{Z}[\gamma_{23}^{(3)}, \gamma_{32}^{(2)}]\,,$$

as desired. □

Corollary 3.2.6. *Let* $X_{\mathrm{univ}} = \mathrm{Spec}(R_{\mathrm{univ}})$. *Then*

(a) *The irreducible components of* X_{univ} *are*

$$X_{\mathrm{univ},C} = \mathrm{Spec}(R_{\mathrm{univ}}/I_{\mathrm{univ},C}) \qquad \textit{and} \qquad X_{\mathrm{univ},E} = \mathrm{Spec}(R_{\mathrm{univ}}/I_{\mathrm{univ},E})\,.$$

Moreover, $X_{\mathrm{univ},C} \cong \mathbb{A}^4_{R_{\mathrm{univ}}}$ *and* $X_{\mathrm{univ},E} \cong \mathbb{A}^2_{R_{\mathrm{univ}}}$

(b) $X_{\mathrm{univ},C}$ *and* $X_{\mathrm{univ},E}$ *intersect in the point (i.e., subscheme of relative dimension* 0 *over* $\mathbb{Z}$*)* $\mathrm{Spec}(R_{\mathrm{univ}}/(I_{\mathrm{univ},C} + I_{\mathrm{univ},E}))$.

Proof. The primary decomposition given in Theorem 3.2.5 shows that $I_{\text{univ},C}$ and $I_{\text{univ},E}$ are the minimal primes of R_{univ}, and thus correspond to maximal irreducible closed subschemes of $\operatorname{Spec}(R_{\text{univ}})$. Moreover,

$$\begin{aligned} X_{\text{univ}C} \cap X_{\text{univ}E} &= \operatorname{Spec}(R_{\text{univ}}/I_{\text{univ},C}) \times_{\operatorname{Spec}(R_{\text{univ}})} \operatorname{Spec}(R_{\text{univ}}/I_{\text{univ},E}) \\ &\cong \operatorname{Spec}(R_{\text{univ}}/I_{\text{univ},C} \otimes_{R_{\text{univ}}} R_{\text{univ}}/I_{\text{univ},E}) \\ &\cong \operatorname{Spec}(R_{\text{univ}}/(I_{\text{univ},C} + I_{\text{univ},E})) \cong \operatorname{Spec}(\mathbb{Z}) \end{aligned}$$

by the calculation of $I_{\text{univ},C} + I_{\text{univ},E}$ given in the proof of Theorem 3.2.5. □

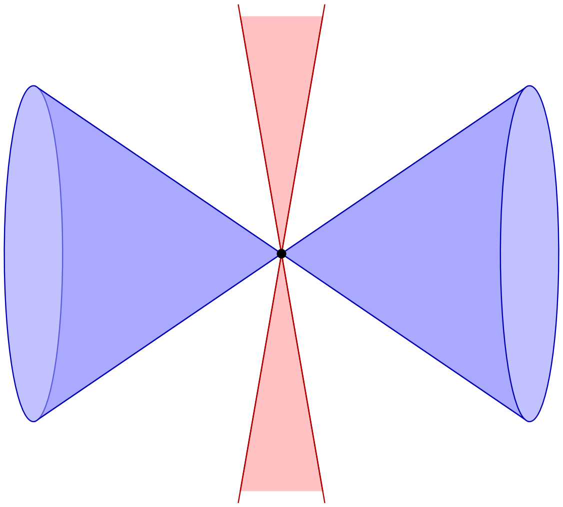


Figure 3.2.1: An illustration of the moduli space X_{univ}. The blue component represents the 4-dimensional component corresponding to commutative algebras, the red component represents the 2-dimensional component corresponding to exceptional algebras, and these two components intersect in a point, corresponding to the nil-product algebra. (It should be noted that, despite appearances in the illustration, this point is not singular.)

The ideals $I_{\text{univ},C}$ and $I_{\text{univ},E}$ correspond to commutative and exceptional algebras—just as R_{univ} represents $\mathfrak{M}_n^{\square}$, $R_{\text{univ},C}$ and $R_{\text{univ},E}$ represent the closed subfunctors of

$\mathfrak{M}_n^{\square}$ classifying commutative and exceptional algebras, respectively. Define the functors

$$\mathfrak{M}_{n,C}^{\square}, \mathfrak{M}_{n,E}^{\square} : (\text{commutative rings}) \to (\text{sets})$$

by

$$\begin{aligned} \mathfrak{M}_{n,C}^{\square}(R) = \{&\text{isomorphism classes of commutative modestly framed} \\ &\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{rank } n \text{ } R\text{-algebras}\} \\ \mathfrak{M}_{n,E}^{\square}(R) = \{&\text{isomorphism classes of exceptional modestly framed} \\ &\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{rank } n \text{ } R\text{-algebras}\}\,. \end{aligned}$$

Proposition 3.2.7. *The functors* $\mathfrak{M}_{3,C}^{\square}, \mathfrak{M}_{3,E}^{\square}$ *are represented by* $\operatorname{Spec}(R_{\text{univ},C}) = \operatorname{Spec}(R_{\text{univ}}/I_{C,\text{univ}})$ *and* $\operatorname{Spec}(R_{\text{univ},E}) = \operatorname{Spec}(R_{\text{univ}}/I_{E,\text{univ}})$, *respectively.*

Proof. Let R be a commutative ring. Given a modestly framed commutative R-algebra A of rank 3, then by Proposition 3.2.1 there is a unique ring homomorphism $\varphi : R_{\text{univ}} \to R$ such that $A \cong A_{\text{univ}} \otimes R$ as framed R-algebras. Since A is commutative then $e_2e_3 - e_3e_2 = 0$. Expanding this commutator in terms of structure constants, we find

$$0 = e_2e_3 - e_3e_2 = \cancel{c_{23}^{(1)}} + c_{23}^{(3)}e_3 - \cancel{c_{32}^{(1)}} - c_{32}^{(2)}e_2 = -c_{32}^{(2)}e_2 + c_{23}^{(3)}e_3\,.$$

Since e_1, e_2, e_3 is a basis, this implies that $c_{23}^{(3)} = c_{32}^{(2)} = 0$. Thus $I_{\text{univ},C} \subseteq \ker(\varphi)$ so $\varphi : R_{\text{univ}} \to R$ descends to a homomorphism $\overline{\varphi} : R_{\text{univ},C} = R_{\text{univ}}/I_{\text{univ},C} \to R$. It remains to show that $\overline{\varphi}$ is unique. Let $\pi : R_{\text{univ}} \to R_{\text{univ}}/I_{\text{univ},C}$ be the canonical quotient map. Given another homomorphism $\overline{\varphi}' : R_{\text{univ}}/I_{\text{univ},C} \to R$, then $\overline{\varphi}' \circ \pi : R_{\text{univ}} \to R$

gives R the structure of a R_{univ}-module such that $A \cong A_{\text{univ}} \otimes R$. By the uniqueness of φ, then $\overline{\varphi}' \circ \pi = \varphi$. Given $y \in R_{\text{univ}}/I_{\text{univ},C}$ with $\pi(x) = y$, then

$$\overline{\varphi}'(y) = \overline{\varphi}'(\pi(x)) = \varphi(x) = \overline{\varphi}(\pi(x)) = \overline{\varphi}(y)\,.$$

Thus $\overline{\varphi}' = \overline{\varphi}$.

It remains to show that $A_{\text{univ},C} := A_{\text{univ}} \otimes_{R_{\text{univ}}} R_{\text{univ},C}$ is commutative. It suffices to show that $\varepsilon_2 \otimes 1$ and $\varepsilon_3 \otimes 1$ commute. Recall that $\gamma_{23}^{(1)} = \gamma_{32}^{(1)}$ and $\gamma_{23}^{(2)} = \gamma_{32}^{(3)} = 0$ in R_{univ} (the latter following from the modest basis condition). Moreover, since $\gamma_{23}^{(3)}, \gamma_{32}^{(2)} \in I_{\text{univ},C}$, then $\gamma_{23}^{(3)} = \gamma_{32}^{(2)} = 0$ in $R_{\text{univ},C}$. Then

$$(\varepsilon_2 \otimes 1)(\varepsilon_3 \otimes 1) = \gamma_{23}^{(1)} = \gamma_{32}^{(1)} = (\varepsilon_3 \otimes 1)(\varepsilon_2 \otimes 1)$$

so $A_{\text{univ},C}$ is commutative.

Suppose A is a modestly framed exceptional R-algebra of rank 3. Then there exists an R-linear map $t : M \to R$ such that $\alpha\beta = t(\alpha)\beta$ for all $\alpha, \beta \in M$. Let $r = t(e_2)$ and $s = t(e_3)$. Then

$$\begin{aligned} e_2^2 &= t(e_2)e_2 = re_2 \\ e_3^2 &= t(e_3)e_3 = se_3 \\ e_2e_3 &= t(e_2)e_3 = re_3 \\ e_3e_2 &= t(e_3)e_2 = se_2\,. \end{aligned}$$

In terms of structure constants, this means that

$$\begin{aligned}
c_{22}^{(1)} &= c_{22}^{(3)} = 0\\
c_{22}^{(2)} &= r = c_{23}^{(3)}\\
c_{23}^{(1)} &= c_{23}^{(2)} = 0\\
c_{33}^{(1)} &= c_{33}^{(2)} = 0\\
c_{33}^{(3)} &= s = c_{32}^{(2)}\\
c_{32}^{(1)} &= c_{32}^{(3)} = 0
\end{aligned}$$

Again by Proposition 3.2.1 there is a unique ring homomorphism $\varphi : R_{\text{univ}} \to R$ such that $A \cong A_{\text{univ}} \otimes R$ as framed R-algebras. By the computations above, we see that $I_{\text{univ},E} \subseteq \ker(\varphi)$ so φ descends to a homomorphism $\overline{\varphi} : R_{\text{univ},E} = R_{\text{univ}}/I_{\text{univ},E} \to R$. Uniqueness of $\overline{\varphi}$ follows analogously to the commutative case.

It remains to show that $A_{\text{univ},E} := A_{\text{univ}} \otimes_{R_{\text{univ}}} R_{\text{univ},E}$ is exceptional. Let M be the submodule of $A_{\text{univ},E}$ generated by $\varepsilon_2 \otimes 1$ and $\varepsilon_3 \otimes 1$. Since $\gamma_{22}^{(2)} - \gamma_{23}^{(3)}, \gamma_{32}^{(2)} - \gamma_{33}^{(3)} \in I_{\text{univ},E}$, then $\gamma_{22}^{(2)} = \gamma_{23}^{(3)}$ and $\gamma_{32}^{(2)} = \gamma_{33}^{(3)}$ in $R_{\text{univ},E}$. Let

$$\begin{aligned}
r &= \gamma_{22}^{(2)} = \gamma_{23}^{(3)}\\
s &= \gamma_{32}^{(2)} = \gamma_{33}^{(3)}
\end{aligned}$$

and define $t : M \to R_{\text{univ},E}$ by

$$t(\varepsilon_2 \otimes 1) = r \qquad \text{and} \qquad t(\varepsilon_3 \otimes 1) = s$$

and extending linearly. Then

$$\begin{aligned}(\varepsilon_2 \otimes 1)^2 &= r\varepsilon_2 \otimes 1 = t(\varepsilon_2 \otimes 1)\ \varepsilon_2 \otimes 1\\ (\varepsilon_3 \otimes 1)^2 &= s\varepsilon_3 \otimes 1 = t(\varepsilon_3 \otimes 1)\ \varepsilon_3 \otimes 1\\ (\varepsilon_2 \otimes 1)(\varepsilon_3 \otimes 1) &= r\varepsilon_3 \otimes 1 = t(\varepsilon_2 \otimes 1)\ \varepsilon_3 \otimes\\ (\varepsilon_3 \otimes 1)(\varepsilon_2 \otimes 1) &= s\varepsilon_2 \otimes 1 = t(\varepsilon_3 \otimes 1)\ \varepsilon_2 \otimes 1\,.\end{aligned}$$

Thus left multiplication factors through t, so $A_{\mathrm{univ},E}$ is exceptional. □

Corollary 3.2.8. *Let $R_{\mathrm{univ},C}, R_{\mathrm{univ},E}, I_{\mathrm{univ},C}, I_{\mathrm{univ},E}$ be as in Theorem 3.2.5. Then*

$$A_{\mathrm{univ}} \otimes_{R_{\mathrm{univ}}} R_{\mathrm{univ},C} \otimes_{R_{\mathrm{univ}}} R_{\mathrm{univ},E}$$

is the nilproduct algebra.

Proof. We have the following commutative diagram of ring homomorphisms.

$$\begin{tikzcd} R_{\mathrm{univ}} \arrow[r] \arrow[d] & R_{\mathrm{univ},C} \arrow[d] \\ R_{\mathrm{univ},E} \arrow[r] & R_{\mathrm{univ},C} \otimes_{R_{\mathrm{univ}}} R_{\mathrm{univ},E} \end{tikzcd}$$

Applying Proposition 3.2.7 to each of these morphisms shows that $A_{\mathrm{univ}} \otimes_{R_{\mathrm{univ}}} R_{\mathrm{univ},C} \otimes_{R_{\mathrm{univ}}} R_{\mathrm{univ},E}$ is both commutative and exceptional, hence is nilproduct.

Alternatively, note that

$$R_{\mathrm{univ},C} \otimes_{R_{\mathrm{univ}}} R_{\mathrm{univ},E} \cong (R_{\mathrm{univ}}/I_{\mathrm{univ},C}) \otimes_{R_{\mathrm{univ}}} (R_{\mathrm{univ}}/I_{\mathrm{univ},E}) \cong \frac{R_{\mathrm{univ}}}{I_{\mathrm{univ},C} + I_{\mathrm{univ},E}}\,.$$

Computing a Gröbner basis for $I_{\mathrm{univ},C} + I_{\mathrm{univ},E}$, we find that $\gamma_{ij}^{(k)} \in I_{\mathrm{univ},C} + I_{\mathrm{univ},E}$

for all $i, j \in \{2, 3\}$ and all $k \in \{1, 2, 3\}$. This implies that $(e_i \otimes 1)(e_j \otimes 1) = 0$ for all $i, j \in \{2, 3\}$, i.e., $A \otimes_R R_C \otimes_R R_E$ is the nilproduct algebra. □

Section 3.3

The framed case

We begin by showing that commutativity and exceptionality are preserved under base change.

Lemma 3.3.1. *Let $(A, (e_i)_i)$ be a framed R-algebra, let S be a commutative ring, and let $\varphi : R \to S$ be a ring homomorphism.*

(a) *If A is commutative, then $A \otimes_R S$ is a commutative S-algebra.*

(b) *If A is exceptional, then $A \otimes_R S$ is an exceptional S-algebra.*

Proof. (a) Since A and S are both commutative rings, then $A \otimes_R S$ is commutative as well.

(b) Since A is exceptional, then there exists a left ideal M of A such that $A = R \oplus M$, and an R-linear map $t : M \to \mathrm{Hom}_R(M, A)$ as in Definition 2.2.13. Then

$$A \otimes_R S = (R \oplus M) \otimes_R S \cong (R \otimes_R S) \oplus (M \otimes_R S) \cong S \oplus (M \otimes_R S)$$

and $M \otimes_R S$ is a left ideal of $A \otimes_R S$. Moreover, the map $t \otimes \mathrm{id}_S : M \otimes_R S \to R \otimes_R S \cong S$ satisfies the necessary property described in Definition 2.2.13, so $A \otimes_R S$ is exceptional.

□

Theorem 3.3.2. *Let R be a commutative ring and $(A, (e_1, e_2, e_3))$ be a modestly framed R-algebra of rank 3 and associated structure constants $c_{ij}^{(k)}$, and let $\varphi : R_{\text{univ}} \to R$ be the unique homomorphism such that $A \cong A_{\text{univ}} \otimes_{R_{\text{univ}}} R$. Let*

$$I_C := \varphi(I_{\text{univ},C})R = (c_{23}^{(3)}, c_{32}^{(2)})$$

and

$$I_E := \varphi(I_{\text{univ},E})R = (c_{22}^{(1)}, c_{22}^{(2)} - c_{23}^{(3)}, c_{22}^{(3)}, c_{23}^{(1)}, c_{32}^{(1)}, c_{32}^{(2)} - c_{33}^{(3)}, c_{33}^{(1)}, c_{33}^{(2)})\,.$$

Then

(a) *I_C is the minimal ideal of R (with respect to inclusion) such that $A \otimes_R (R/I_C) \cong A/I_C A$ is commutative.*

(b) *I_E is the minimal ideal of R (with respect to inclusion) such that $A \otimes_R (R/I_E) \cong A/I_E A$ is exceptional.*

Proof. We prove the statement for I_C; the proof for I_E is analogous. Since φ induces the R_{univ}-module structure on R, then

$$\frac{R}{I_C} = \frac{R}{\varphi(I_{\text{univ},C})R} \cong \frac{R_{\text{univ}}}{I_{\text{univ},C}} \otimes_{R_{\text{univ}}} R$$

Since $A \cong A_{\text{univ}} \otimes_{R_{\text{univ}}} R$, then

$$A \otimes_R \frac{R}{I_C} \cong (A_{\text{univ}} \otimes_{R_{\text{univ}}} R) \otimes_R \left(\frac{R_{\text{univ}}}{I_{\text{univ},C}} \otimes_{R_{\text{univ}}} R \right) \cong A_{\text{univ}} \otimes_{R_{\text{univ}}} \frac{R_{\text{univ}}}{I_{\text{univ},C}} \otimes_{R_{\text{univ}}} R\,.$$

Since $A_{\text{univ}} \otimes_{R_{\text{univ}}} \dfrac{R_{\text{univ}}}{I_{\text{univ},C}}$ is commutative, then $A_{\text{univ}} \otimes_{R_{\text{univ}}} \dfrac{R_{\text{univ}}}{I_{\text{univ},C}} \otimes_{R_{\text{univ}}} R$ is commutative by Lemma 3.3.1. Thus $A \otimes_R \dfrac{R}{I_C}$ is commutative, so it remains to show that I_C is minimal.

Given an ideal J of R such that $A \otimes_R R/J$ is commutative, then by Proposition 3.2.7 there is a unique homomorphism

$$\varphi : R_{\text{univ},C} = \frac{R_{\text{univ}}}{I_{\text{univ},C}} \to \frac{R}{J}$$

such that $A \otimes_R R/J \cong (A_{\text{univ}} \otimes_{R_{\text{univ}}} R_{\text{univ}}/I_{\text{univ},C}) \otimes_{R_{\text{univ}}} (R/J)$. The fact that φ is well-defined means that $\varphi(I_{\text{univ},C}) \subseteq J$. Thus $I_C = \varphi(I_{\text{univ},C})R \subseteq J$, hence I_C is minimal. □

Corollary 3.3.3. *With notation as above, the ideals I_C and I_E are independent of choice of modest basis.*

Proof. We prove the corollary for I_C; the proof for I_E is analogous. Given modest bases $(e_i)_i$ and $(e'_i)_i$ for A, let I_C and I'_C be the ideals as in Theorem 3.3.2. Then $A/I_C A$ and $A/I'_C A$ are both commutative, so by minimality we have $I_C \subseteq I'_C$ and $I'_C \subseteq I_C$. □

Remark 3.3.4. One can also prove that I_C and I_E are independent of choice of modest basis by considering the effect a change of modest basis has on the associated structure constants. We will examine this action of GL_2 on the structure constants in section 3.6.

Corollary 3.3.5. *Let R be a commutative ring and A be a framed R-algebra of rank 3 with modest basis $1 = e_1, e_2, e_3$ and associated structure constants $c_{ij}^{(k)}$. Then*

(a) *A is commutative if and only if $c_{23}^{(3)} = c_{32}^{(2)} = 0$.*

(b) *A is exceptional if and only if the following equations hold.*

$$\begin{aligned} &c_{22}^{(1)} = c_{22}^{(3)} = c_{23}^{(1)} = c_{32}^{(1)} = c_{33}^{(1)} = c_{33}^{(2)} = 0 \\ &c_{22}^{(2)} = c_{23}^{(3)}\,, \qquad c_{32}^{(2)} = c_{33}^{(3)}\,. \end{aligned} \tag{3.3.1}$$

Section 3.4

The free case

The preceding corollary allows us to remove the dependence on a choice of modest basis from Theorem 3.3.2.

Theorem 3.4.1. *Let R be a commutative ring, and let A be a free R-algebra of rank 3 thats admits a unital basis. There exist minimal ideals I_C and I_E of R such that*

(a) *$A_C := A/I_CA \cong A \otimes_R (R/I_C)$ is commutative;*

(b) *$A_E := A/I_EA \cong A \otimes_R (R/I_E)$ is exceptional;*

Moreover, for any choice of modest basis (e_1, e_2, e_3) with associated structure constants $c_{ij}^{(k)}$, we have $I_C = (c_{23}^{(3)}, c_{32}^{(2)})$ and

$$I_E = (c_{22}^{(1)}, c_{22}^{(2)} - c_{23}^{(3)}, c_{22}^{(3)}, c_{23}^{(1)}, c_{32}^{(1)}, c_{32}^{(2)} - c_{33}^{(3)}, c_{33}^{(1)}, c_{33}^{(2)})\,.$$

Finally, we also have that

$$A_{CE} := A/(I_C + I_E)A \cong A \otimes_R (R/I_C) \otimes_R (R/I_E)$$

is the nilproduct algebra.

Proof. The follows immediately from Theorem 3.3.2 and Corollary 3.3.3. □

Lemma 3.4.2. *Let R and S be commutative rings, let A be a framed R-algebra of rank 3 with modest basis e_1, e_2, e_3 and let $\psi : R \to S$ be a ring homomorphism. Then $A_S := A \otimes_R S$ is free of rank 3 with modest basis $e_1 \otimes 1, e_2 \otimes 1, e_3 \otimes 1$. Considering A_S as an R-algebra via ψ, then the map $A \to A_S$ given by $e_i \mapsto e_i \otimes 1$ is a morphism of framed R-algebras. Let $\varphi_R : R_{\text{univ}} \to R$ and $\varphi_S : R_{\text{univ}} \to S$ be the unique ring homomorphisms so that $A \cong A_{\text{univ}} \otimes_{R_{\text{univ}}} R$ and $A_S \cong A_{\text{univ}} \otimes_{R_{\text{univ}}} S$ as framed R- and S-algebras, respectively. Then φ_S factors through φ_R, i.e., $\varphi_S = \psi \circ \varphi_R$.*

$$\begin{tikzcd}
& R_{\text{univ}} \arrow[ld, "\varphi_R"'] \arrow[rd, "\varphi_S"] & \\
R \arrow[rr, "\psi"'] & & S
\end{tikzcd}$$

Proof. Since $A \cong A_{\text{univ}} \otimes_{R_{\text{univ}}} R$, then

$$A_S = A \otimes_R S \cong A_{\text{univ}} \otimes_{R_{\text{univ}}} R \otimes_R S\,.$$

Then both $\varphi_S : R_{\text{univ}} \to S$ and $\psi \circ \varphi_R : R_{\text{univ}} \to S$ correspond to A_S. By the uniqueness statement in Proposition 3.2.1, then $\varphi_S = \psi \circ \varphi_R$.

□

We now show that the construction of I_C and I_E is functorial under ring homomorphisms.

Proposition 3.4.3. *Let R and S be commutative rings, let A be a framed R-algebra of rank 3 with modest basis e_1, e_2, e_3 and let $\psi : R \to S$ be a ring homomorphism. Then*

$A_S := A \otimes_R S$ is free of rank 3 with modest basis $e_1 \otimes 1, e_2 \otimes 1, e_3 \otimes 1$. Let $I_{C,R}, I_{E,R}$ and $I_{C,S}, I_{E,S}$ be the minimal ideals of R and S, respectively such that $A/I_{C,R}A$ and $A_S/I_{C,S}A_S$ are commutative and $A/I_{E,R}A$ and $A_S/I_{E,S}A_S$ are exceptional. Then $\psi(I_{C,R})S = I_{C,S}$ and $\psi(I_{E,R})S = I_{E,S}$, that is, $I_{C,S}$ and $I_{E,S}$ are the extensions along ψ of their counterparts over R.

Proof. Let $\varphi_R : R_{\text{univ}} \to R$ and $\varphi_S : R_{\text{univ}} \to S$ be the unique ring homomorphisms given by representability (Proposition 3.3.2). By Theorem 3.3.2, then

$$\begin{aligned} I_{C,R} &= \varphi_R(I_{\text{univ},C}) & \qquad I_{E,R} &= \varphi_R(I_{\text{univ},E}) \\ I_{C,S} &= \varphi_S(I_{\text{univ},C}) & \qquad I_{E,S} &= \varphi_S(I_{\text{univ},E})\,. \end{aligned}$$

Since $\varphi_S = \psi \circ \varphi_R$ by Lemma 3.4.2, then

$$\begin{aligned} \psi(I_{C,R})S &= \psi(\varphi_R(I_{\text{univ},C}))S = \varphi_S(I_{\text{univ},C})S = I_{C,S} \\ \psi(I_{E,R})S &= \psi(\varphi_R(I_{\text{univ},E}))S = \varphi_S(I_{\text{univ},E})S = I_{E,S} \end{aligned}$$

as desired. □

Section 3.5

The case of a sheaf of algebras over a scheme

We now pass to the most general version of our main result, treating the case of a sheaf of locally free algebras over a base scheme. For the remainder of this chapter, let X be a scheme and $\mathscr{A}$ be a sheaf of algebras on X.

We first show that commutativity and exceptionality can be detected locally.

Lemma 3.5.1. *Let R be a commutative ring and A an R-algebra, and let $\mathscr{A} = \widetilde{A}$ be the sheaf of algebras on $\mathrm{Spec}(R)$ induced by A. Suppose $a \in A$. The following are equivalent.*

(a) $a = 0$.

(b) $\mathrm{res}_U^{\mathrm{Spec}(R)}(a) = 0$ *for all open subsets* $U \subseteq \mathrm{Spec}(R)$.

(c) *There exist* $f_1, \ldots, f_m \in R$ *with* $(f_1, \ldots, f_m) = R$ *such that* $a/1 = 0$ *in* $R[1/f_i]$ *for all* $i = 1, \ldots, m$.

Proof. This follows immediately from the fact that $\mathscr{O}_{\mathrm{Spec}(R)}$ is a sheaf, hence two sections are equal if and only if they are locally equal everywhere. □

Lemma 3.5.2. *Let R be a commutative ring and A an R-algebra. The following are equivalent.*

(a) *A is commutative.*

(b) *There exist* $f_1, \ldots, f_m \in R$ *with* $(f_1, \ldots, f_m) = R$ *such that* $A \otimes_R R[1/f_i]$ *is commutative for all* $i = 1, \ldots, m$.

Proof. Suppose $a, b \in A$ and apply Lemma 3.5.1 to $ab - ba$. □

Lemma 3.5.3 (Lemma 3.7, [Voight, 2011c])**.** *An R-algebra A of rank > 2 is exceptional if and only if $A_{\mathfrak{p}}$ is exceptional for all primes $\mathfrak{p}$ of R.*

Remark 3.5.4. The above lemma shows that exceptionality can be detected on the level of stalks. One can show that this implies that it can also be detected on the level of distinguished Zariski open sets. This yields the following result.

Lemma 3.5.5. *Let R be a commutative ring and A a free R-algebra of rank > 2. The following are equivalent.*

(a) *A is exceptional.*

(b) *There exist $f_1, \ldots, f_m \in R$ with $(f_1, \ldots, f_m) = R$ such that $A \otimes_R R[1/f_i]$ is exceptional for all $i = 1, \ldots, m$.*

The theorem can be extended to a sheaf of locally free algebras over an arbitrary base scheme. We first extend our definitions of commutative and exceptional to sheaves of algebras.

Definition 3.5.6. A sheaf of algebras $\mathscr{A}$ is *commutative* if there exists a cover of X by affine open subsets $\{U_i\}_i$ such that $\mathscr{A}(U_i)$ is a commutative R_i-algebra for each i, where $U_i = \operatorname{Spec}(R_i)$.

Definition 3.5.7. A sheaf of algebras $\mathscr{A}$ is *exceptional* if there exists a cover of X by affine open subsets $\{U_i\}_i$ such that $\mathscr{A}(U_i)$ is an exceptional R_i-algebra for each i, where $U_i = \operatorname{Spec}(R_i)$.

Proposition 3.5.8. *The following are equivalent.*

(a) *$\mathscr{A}$ is commutative.*

(b) *$\mathscr{A}(U)$ is a commutative R-algebra, for every affine open subset $U = \operatorname{Spec}(R)$ of X.*

(c) *$\mathscr{A}_x$ is a commutative $\mathscr{O}_{X,x}$-algebra for every $x \in X$.*

Proof. (a) $\implies$ (b): We use the Affine Communication Lemma (Lemma 2.7.2) to show that commutativity is an affine-local property. For an affine open subset

$U = \operatorname{Spec}(R)$ of X, let P be the property that $A := \mathscr{A}(U)$ is a commutative R-algebra. Given an affine open $U = \operatorname{Spec}(R)$ such that $A := \mathscr{A}(U)$ is commutative, then certainly $\mathscr{A}(U_f) \cong A_f \cong A \otimes_R R_f$ is commutative for every $f \in R$ by Lemma 3.3.1, so (i) holds. By Lemma 3.5.2 (ii) holds as well, so commutativity is an affine local property. Then (a) $\implies$ (b) by the Affine Communication Lemma 2.7.2.

(b) $\implies$ (c): Given $a|_x, b|_x \in \mathscr{O}_{X,x}$, choose representatives (a, U), (b, V) for the germs $a|_x, b|_x$, where U and V are open subsets of X with $a \in \mathscr{A}(U)$ and $b \in \mathscr{A}(V)$. We may assume $U = V$ by replacing U and V by $U \cap V$. Moreover, since affine open subsets form a basis for the topology on X, there exists an affine open subset $\operatorname{Spec}(R) \subseteq U \cap V$ with $x \in \operatorname{Spec}(R)$. Thus we may assume that $U = V = \operatorname{Spec}(R)$ is affine. Then

$$a|_x\, b|_x - b|_x\, a|_x = (ab - ba)|_x = \operatorname{res}^U_x(ab - ba) = \operatorname{res}^U_x(0) = 0$$

so $\mathscr{O}_{X,x}$ is commutative.

(c) $\implies$ (b): Given an open subset U of X, and sections $a, b \in \mathcal{A}(U)$, then

$$a|_x\, b|_x - b|_x\, a|_x = (ab - ba)|_x = 0$$

for each $x \in U$. Choosing representatives (a, U_x) and (b, U_x) for these germs, then there exists an open set $U_x \subseteq U$ such that $\operatorname{res}^U_{U_x}(ab - ba) = 0$. Then $\{U_x\}_{x \in U}$ is open cover for U such that $ab - ba$ on U_x for each x, so $ab - ba = 0$ since $\mathscr{A}$ is a sheaf.

The implication (b) $\implies$ (a) is immediate, so this completes the proof. □

An analogous result holds for sheaves of exceptional algebras provided that the rank is > 2.

Proposition 3.5.9. *Let $\mathscr{A}$ be a sheaf of algebras on X that is locally free of rank > 2. The following are equivalent.*

(a) *$\mathscr{A}$ is exceptional.*

(b) *$\mathscr{A}(U)$ is an exceptional R-algebra for every affine open subset $U = \operatorname{Spec}(R)$ of X.*

Proof. The implication (b) $\implies$ (a) is immediate, so it remains to show the converse. Again we use the Affine Communication Lemma (Lemma 2.7.2) to show that exceptionality is an affine-local property. For an affine open subset $U = \operatorname{Spec}(R)$ of X, let P be the property that $A := \mathscr{A}(U)$ is a exceptional R-algebra. Given an affine open $U = \operatorname{Spec}(R)$ such that $A := \mathscr{A}(U)$ is exceptional, then $\mathscr{A}(U_f) \cong A_f \cong A \otimes_R R_f$ is exceptional for every $f \in R$ by Lemma 3.3.1, so (i) holds. By Lemma 3.5.5, (ii) holds as well, so exceptionality is an affine local property. Then (a) $\implies$ (b) by the Affine Communication Lemma 2.7.2. □

We also extend our definition of the nilproduct algebra.

Definition 3.5.10. Let $\mathscr{A}$ be a sheaf of algebras on X that is locally free of rank n. Then $\mathscr{A}$ is *nilproduct* if there is an affine open cover $\{\operatorname{Spec}(R_i)\}_i$ of X such that $A_i \cong \dfrac{R_i[x_1, \ldots, x_{n-1}]}{(x_1, \ldots, x_{n-1})^2}$ for each i, where $A_i = \mathscr{A}(\operatorname{Spec}(R_i))$.

Proposition 3.5.11. *Let $\mathscr{A}$ be a sheaf of algebras on X that is locally free of rank 3. Then $\mathscr{A}$ is nilproduct if and only if it is both commutative and exceptional.*

Proof. Let $\{\operatorname{Spec}(R_i)\}_i$ be an affine open cover of X as in the definition. Then $A_i \cong \dfrac{R_i[x, y]}{(x, y)^2}$ for each i, so A_i is both commutative and exceptional for each i. Thus $\mathscr{A}$ is both commutative and exceptional.

Conversely, suppose $\mathscr{A}$ is both commutative and exceptional. By Propositions 3.5.8 and 3.5.9, then $\mathscr{A}(U)$ is commutative and exceptional for every affine open subset U of X. By 3.4.1, then $\mathscr{A}(U)$ is nilproduct.

□

Theorem 3.5.12. *Let $\mathscr{A}$ be sheaf of algebras on X that is locally free of rank 3. Then there exist quasicoherent ideal sheaves $\mathscr{I}_C$ and $\mathscr{I}_E$ on X such that*

(a) $\mathscr{A} \otimes_{\mathscr{O}_X} \dfrac{\mathscr{O}_X}{\mathscr{I}_C}$ *is commutative;*

(b) $\mathscr{A} \otimes_{\mathscr{O}_X} \dfrac{\mathscr{O}_X}{\mathscr{I}_E}$ *is exceptional;*

and $\mathscr{I}_C$ and $\mathscr{I}_E$ are the minimal ideal sheaves with these properties in the following sense. If $\mathscr{J}$ is an ideal sheaf on $\mathscr{O}_X$ such that $\mathscr{A} \otimes_{\mathscr{O}_X} \dfrac{\mathscr{O}_X}{\mathscr{J}}$ is commutative (resp., exceptional), then $\mathscr{I}_C(U) \subseteq \mathscr{J}(U)$ (resp., $\mathscr{I}_E(U) \subseteq \mathscr{J}(U)$) for every affine open subset U of X.

Furthermore,

$$\mathscr{A} \otimes_{\mathscr{O}_X} \frac{\mathscr{O}_X}{\mathscr{I}_C} \otimes_{\mathscr{O}_X} \frac{\mathscr{O}_X}{\mathscr{I}_E}$$

is nilproduct.

We first prove some auxiliary lemmas.

Lemma 3.5.13. *Let $\mathscr{A}$ be a locally free sheaf of rank n algebras on X. Then the set $\mathcal{B}$ of affine open subsets of X over which $\mathscr{A}$ is free and has a modest basis, i.e.,*

$$\mathcal{B} = \{U \subseteq X : U \textit{ is affine open and } \mathscr{A}(U) \textit{ is free and has a modest basis}\}$$

is a basis for the topology on X.

Proof. Since $\mathscr{A}$ is locally free, then there is a cover $\mathcal{V}$ of X consisting of affine open subsets such that $\mathscr{A}(V)$ is free for all $V \in \mathcal{V}$. We show that we can cover each $V \in \mathcal{V}$ by elements of $\mathcal{B}$. Given $V \in \mathcal{V}$, let $A = \mathscr{A}(V)$ so A is a free R-algebra of rank n, where $V = \operatorname{Spec}(R)$. By Lemma 2.5.1, $A \cong R \oplus A/R$ and A/R is locally free. Thus there exists an open cover $\{D(f_i)\}_i$ of V by distinguished open subsets such that $(A/R)_{f_i}$ is free for each i. Then

$$\mathscr{A}(D(f_i)) \cong A_{f_i} \cong (R \oplus A/R)_{f_i} \cong R_{f_i} \oplus (A/R)_{f_i}\,.$$

Since $(A/R)_{f_i}$ is free and 1 is a basis for R_{f_i}, then for each i there is a basis of A_{f_i} containing 1. By Lemma 2.5.6, then A_{f_i} has a modest basis, so we have covered V by elements of $\mathcal{B}$. Thus $\mathcal{B}$ covers X.

Given $U, V \in \mathcal{B}$ with $U = \operatorname{Spec}(R)$, suppose $x \in U \cap V$. Since $U \cap V$ is an open subset of the affine scheme $\operatorname{Spec}(R)$ and distinguished open subsets form a basis for the Zariski topology on $\operatorname{Spec}(R)$, then there exists $f \in R$ such that $x \in D(f) \subseteq U \cap V$. Letting $A = \mathscr{A}(U)$, then

$$\mathscr{A}(D(f)) = A \otimes_R R[1/f] \cong \left(\bigoplus_{i=1}^{n} R\right) \otimes_R R[1/f] \cong \bigoplus_{i=1}^{n} R[1/f]$$

so $\mathscr{A}$ is free over $D(f)$. Moreover, denoting the modest basis of A by $(e_i)_i$, then $(e_i \otimes 1)_i$ is a modest basis for $A \otimes_R R[1/f]$. Thus $D(f) \in \mathcal{B}$, and this shows that $\mathcal{B}$ is a basis. $\square$

Proof of Theorem 3.5.12. We prove the result for X_C; the proof for X_E is analogous. Let $\mathcal{B}$ be the basis as in Lemma 3.5.13. For each $U = \operatorname{Spec}(R) \in \mathcal{B}$, let $\mathscr{I}_C(U) = I_{C,R}$ as in Theorem 3.4.1. By the functoriality result of Proposition 3.4.3, given $V =$

$\operatorname{Spec}(S) \in \mathcal{B}$ with $V \subseteq U$, we have

$$\operatorname{res}_V^U(\mathscr{I}_C(U)) = \operatorname{res}_V^U(I_{C,R}) = I_{C,S} = \mathscr{I}_C(V)\,,$$

so $\mathscr{I}_C$ is a presheaf on $\mathcal{B}$.

We now show $\mathscr{I}_C$ is a sheaf on $\mathcal{B}$. Since $\mathscr{I}_C$ is a sub-presheaf of $\mathscr{O}_X$, the local determination property is immediate, so it remains to show that compatible sections glue. Rather than showing this directly, we instead show that $\mathscr{I}_C|_U = \widetilde{I_{C,R}}$, the sheaf of ideals induced by $I_{C,R}$. To do so, it suffices to show they coincide on the distinguished basis of $U = \operatorname{Spec}(R)$. Let $D(f) = \operatorname{Spec}(R[1/f])$ be a distinguished open set of U and let $\varphi\colon R \to R[1/f]$ be the localization map. By definition, then

$$\mathscr{I}_C|_U(D(f)) = \mathscr{I}_C(D(f)) = I_{C,R[1/f]}\,.$$

On the other hand, by the definition of $\widetilde{I_{C,R}}$ we have

$$\widetilde{I_{C,R}}(D(f)) = \varphi(I_{C,R})R[1/f] = I_{C,R[1/f]}$$

where the last equality follows from the functoriality result given in Proposition 3.4.3. Thus $\mathscr{I}_C|_U$ and $\widetilde{I_{C,R}}$ agree on a basis for the topology, so $\mathscr{I}_C|_U = \widetilde{I_{C,R}}$.

Thus $\mathscr{I}_C$ is a sheaf on $\mathcal{B}$. By Lemma 2.6.4, then there exists a unique sheaf of ideals on X extending $\mathscr{I}_C$; abusing notation, we denote this sheaf again by $\mathscr{I}_C$.

We now show that $\mathscr{I}$ has the desired properties. Since $\mathscr{I}|_U = \widetilde{I_{C,R}}$ for each $U = \operatorname{Spec}(R) \in \mathcal{B}$, then $\mathscr{I}_C$ is quasicoherent. Since $\mathscr{O}_X$ is quasicoherent, then the quotient $\mathscr{O}_X/\mathscr{I}_C$ (which is the cokernel of the inclusion $\mathscr{I} \hookrightarrow \mathscr{O}_X$) is quasicoherent by

Proposition 2.7.8. Since $\mathscr{A}$ is locally free, then it is *a fortiori* quasicoherent. Given an affine open set $U = \operatorname{Spec}(R) \in \mathcal{B}$, then

$$\left(\mathscr{A} \otimes_{\mathscr{O}_X} \frac{\mathscr{O}_X}{\mathscr{I}_C}\right)(U) = \mathscr{A}(U) \otimes_{\mathscr{O}_X(U)} \frac{\mathscr{O}_X}{\mathscr{I}_C}(U)$$

by Proposition 2.7.8. We have

$$\frac{\mathscr{O}_X}{\mathscr{I}_C}(U) \cong \frac{\mathscr{O}_X(U)}{\mathscr{I}_C(U)}$$

by Proposition 2.7.7, so

$$\left(\mathscr{A} \otimes_{\mathscr{O}_X} \frac{\mathscr{O}_X}{\mathscr{I}_C}\right)(U) \cong \mathscr{A}(U) \otimes_{\mathscr{O}_X(U)} \frac{\mathscr{O}_X(U)}{\mathscr{I}_C(U)} = A \otimes_R \frac{R}{I_{C,R}}$$

where $A = \mathscr{A}(U)$. By Theorem 3.4.1 $A \otimes_R \dfrac{R}{I_{C,R}}$ is commutative, so this shows that $\mathscr{A} \otimes_{\mathscr{O}_X} \dfrac{\mathscr{O}_X}{\mathscr{I}_C}$ is commutative.

Applying Propositions 2.7.8 and 2.7.7 as above, the last two assertions follow from the corresponding statements for an algebra over a ring given in Theorem 3.4.1: minimality of $\mathscr{I}_C$ follows from the minimality of $I_{C,R}$, and

$$\left(\mathscr{A} \otimes_{\mathscr{O}_X} \frac{\mathscr{O}_X}{\mathscr{I}_C} \otimes_{\mathscr{O}_X} \frac{\mathscr{O}_X}{\mathscr{I}_E}\right)(U)$$

is nilproduct for every affine open $U \in \mathcal{B}$, hence is nilproduct. □

Corollary 3.5.14. *Let $\mathscr{A}$ be sheaf of algebras on X that is locally free of rank 3. Then there exist closed subschemes $\iota_C : X_C \hookrightarrow X$ and $\iota_E : X_E \hookrightarrow X$ of X such that*

(a) *$\iota_C^*(\mathscr{A})$ is commutative;*

(b) $\iota_E^*(\mathscr{A})$ *is exceptional*

and X_C *and* X_E *are the largest closed subschemes with these properties.*

Let $X_{CE} = X_C \cap X_E = X_C \times_X X_E$ *with closed embedding* $\iota_{CE} : X_{CE} \hookrightarrow X$*. Then* $\iota_{CE}^*(\mathscr{A})$ *is the nilproduct algebra.*

Proof. Let $\mathscr{I}_C$ and $\mathscr{I}_E$ be as in the previous theorem. As before, we prove the result only for $\mathscr{I}_C$. Since $\mathscr{I}_C$ is quasicoherent, then by Proposition 2.7.6 there is a unique closed subscheme X_C of X corresponding to $\mathscr{I}_C$, namely

$$X_C := \{x \in X : (\mathscr{I}_C)_x \neq \mathscr{O}_{X,x}\},$$

equipped with the sheaf of rings $\mathscr{O}_{X_C} := \iota_C^{-1}\left(\frac{\mathscr{O}_X}{\mathscr{I}_C}\right)$, where $\iota_C : X_C \hookrightarrow X$ is the inclusion map.

We claim that

$$\iota_{C*}\iota_C^*\mathscr{A} = \mathscr{A} \otimes_{\mathscr{O}_X} \frac{\mathscr{O}_X}{\mathscr{I}_C}.$$

Consider the associated map of sheaves $\iota_C^\# : \mathscr{O}_X \to \iota_{C*}(\mathscr{O}_{X_C})$. Since pushforward and inverse image are adjoint, the identity morphism

$$\mathrm{id} \in \mathrm{Hom}(\mathscr{O}_{X_C}, \mathscr{O}_{X_C}) = \mathrm{Hom}\left(\iota_C^{-1}\left(\frac{\mathscr{O}_X}{\mathscr{I}_C}\right), \mathscr{O}_{X_C}\right) \cong \mathrm{Hom}\left(\frac{\mathscr{O}_X}{\mathscr{I}_C}, \iota_{C*}\mathscr{O}_{X_C}\right)$$

corresponds to a natural map

$$\frac{\mathscr{O}_X}{\mathscr{I}_C} \to \iota_{C*}\ \iota^{-1}\left(\frac{\mathscr{O}_X}{\mathscr{I}_C}\right) = \iota_{C*}(\mathscr{O}_{X_C})$$

Moreover, since ι_C is a closed embedding then this map is an isomorphism. By the projection formula given in Proposition 2.7.10, then

$$\iota_{C*}\iota_C^*\mathscr{A} = \iota_{C*}(\mathscr{O}_{X_C} \otimes_{\mathscr{O}_{X_C}} \iota_C^*(\mathscr{A})) \cong \left(\iota_{C*}\iota_C^{-1}\frac{\mathscr{O}_X}{\mathscr{I}_C}\right) \otimes_{\mathscr{O}_X} \mathscr{A} \cong \frac{\mathscr{O}_X}{\mathscr{I}_C} \otimes_{\mathscr{O}_X} \mathscr{A}$$

as claimed. Since $\mathscr{A} \otimes_{\mathscr{O}_X} \dfrac{\mathscr{O}_X}{\mathscr{I}_C}$ is commutative, then $\iota_{C*}\iota_C^*\mathscr{A}$ and hence $\iota_C^*\mathscr{A}$ are commutative. Moreover, since the bijection between quasicoherent ideal sheaves and closed subschemes is inclusion-reversing, the fact that $\mathscr{I}_C$ is minimal implies that X_C is maximal. □

Corollary 3.5.15. *Let R be a commutative ring, and let A be an R-algebra that is locally free of rank* 3. *There exist closed subschemes* $\operatorname{Spec}(R_C)$ *and* $\operatorname{Spec}(R_E)$ *of* $\operatorname{Spec}(R)$ *such that*

(a) *$A \otimes_R R_C$ is commutative;*

(b) *$A \otimes_R R_E$ is exceptional;*

(c) *$A \otimes_R R_C \otimes_R R_E$ is nilproduct.*

and $\operatorname{Spec}(R_C)$ *and* $\operatorname{Spec}(R_E)$ *are the largest closed subschemes with these properties.*

Proof. This follows from applying Corollary 3.5.14 to $X = \operatorname{Spec}(R)$ and $\mathscr{A} = \widetilde{A}$, the sheaf of algebras induced by A. □

Section 3.6

Change of modest basis

Let A be a free, rank 3 R-algebra. If we consider the collection of all bases of A, then the possible change of basis transformations are given by the group $\mathrm{GL}_3(R)$. However, if we restrict ourselves to the collection of all *modest* bases of A, the restrictions $e_1 = 1$, $c_{23}^{(2)} = c_{32}^{(3)} = 0$ placed on a modest basis mean that we instead get an action of $\mathrm{GL}_2(R)$. Given a modest basis e_1, e_2, e_3 with associated structure constants $c_{ij}^{(k)}$, $\mathrm{GL}_2(R)$ acts on e_1, e_2, e_3 as follows. Given $P = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(R)$, define

$$\begin{pmatrix} e_1' \\ e_2' \\ e_3' \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ f & \alpha & \beta \\ g & \gamma & \delta \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \\ e_3 \end{pmatrix} \tag{3.6.1}$$

where $f, g \in \mathbb{Z}[c_{ij}^{(k)}]\left[\alpha, \beta, \gamma, \delta, \frac{1}{\alpha\delta - \beta\gamma}\right]$ are given by

$$\begin{aligned} f &= \frac{1}{\alpha\delta - \beta\gamma}\left(\alpha\gamma\delta(c_{23}^{(3)} - c_{22}^{(2)}) + \beta\gamma\delta(c_{33}^{(3)} - c_{32}^{(2)}) + \alpha\gamma^2 c_{22}^{(3)} - \beta\delta^2 c_{33}^{(2)}\right) \\ g &= \frac{1}{\alpha\delta - \beta\gamma}\left(\alpha\beta\gamma(c_{22}^{(2)} - c_{23}^{(3)}) + \alpha\beta\delta(c_{32}^{(2)} - c_{33}^{(3)}) - \alpha^2\gamma c_{22}^{(3)} + \beta^2\delta c_{33}^{(2)}\right) . \end{aligned}$$

The definitions of f and g follow from the fact that $c_{23}^{(2)\prime} = c_{32}^{(3)\prime} = 0$, where $(c_{ij}^{(k)\prime})_{i,j,k}$ are the structure constants associated to $(e_i')_i$.

In this way, $\mathrm{GL}_2(R)$ also acts on the structure constants: given $P \in \mathrm{GL}_2(R)$, and a modest basis $(e_i)_i$ with associated structure constants $(c_{ij}^{(k)})_{i,j,k}$, let $(e_i')_i = P(e_i)_i$, that is, as in equation (3.6.1). Letting $(c_{ij}^{(k)\prime})_{i,j,k}$ be the structure constants associated to $(e_i')_i$, define $P \cdot (c_{ij}^{(k)})_{i,j,k} = (c_{ij}^{(k)\prime})_{i,j,k}$.

Changing basis does not change the properties of commutativity or exceptionality. Thus the action of GL_2 preserves setwise the irreducible components X_C and X_E, or in algebraic terms, the corresponding ideals I_C and I_E.

In [Gross and Lucianovic, 2009, §2], the authors study the action of $\mathrm{GL}_2(R)$ on commutative, free, rank 3 R-algebras in the case where R is a PID or a local ring.

Proposition 3.6.1 ([Gross and Lucianovic, 2009, Proposition 2.1])**.** *Let R be a PID or a local ring and let N be free R-module of rank 2. There is a bijection between the set of orbits of the action of $\mathrm{GL}(N) \cong \mathrm{GL}_2(R)$ on the R-module $M = \mathrm{Sym}^3(N) \otimes \left(\bigwedge^2 N\right)^{-1}$ and the set of isomorphism classes of commutative cubic algebras A over R.*

We extend this result to exceptional algebras. Recall that $R_{\mathrm{univ},E} \cong \mathbb{Z}[\gamma_{23}^{(3)}, \gamma_{32}^{(2)}]$.

Lemma 3.6.2. *Let $N = \mathbb{Z}\gamma_{23}^{(3)} \oplus \mathbb{Z}\gamma_{32}^{(2)}$ and let $\mathrm{GL}_2(\mathbb{Z})$ act on N by the action induced by change of modest basis. The action of $\mathrm{GL}_2(\mathbb{Z})$ on N is isomorphic to the standard representation. That is,*

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \gamma_{23}^{(3)} = \alpha\gamma_{23}^{(3)} + \beta\gamma_{32}^{(2)} \qquad \textit{and} \qquad \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \gamma_{32}^{(2)} = \gamma\gamma_{23}^{(3)} + \delta\gamma_{32}^{(2)}$$

for all $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$.

This allows us to complete the description of the change of modest basis action on the moduli space, recovering a result of Voight.

Proposition 3.6.3 ([Voight, 2011c, Proposition 4.3])**.** *Let N be a free R-module of rank 2. Then there is a bijection between the set of orbits of $\mathrm{GL}(N)$ acting on N and the set of isomorphism classes of free R-algebras of rank 3 with a standard involution.*

These results constitute the first steps toward understanding the moduli space of rank 3 algebras *without* a choice of basis.

Section 3.7

Degenerations

As the moduli space $\mathfrak{M}_n^{\square}$ sits inside $\mathbb{A}^{n^3}$, it is natural to wonder what its closure inside $\mathbb{P}^{n^3}$ is, and what, if any, algebraic meaning we can give to the points on the hyperplane at infinity. In this section, we study the projective closure of $\mathfrak{M}_3^{\square}$ and the algebraic objects corresponding to the points on the hyperplane at infinity, which we call *degenerations* of cubic algebras.

Using Magma, we compute Gröbner bases for $I_{\mathrm{univ},C}$ and $I_{\mathrm{univ},E}$. We then homogenize them, obtaining

$$\begin{aligned}
&\{\gamma_{11}^{(1)} - Z, \gamma_{11}^{(2)}, \gamma_{11}^{(3)},\\
&\ \gamma_{12}^{(1)}, \gamma_{12}^{(2)} - Z, \gamma_{12}^{(3)},\\
&\ \gamma_{13}^{(1)}, \gamma_{13}^{(2)}, \gamma_{13}^{(3)} - Z,\\
&\ \gamma_{21}^{(1)}, \gamma_{21}^{(2)} - Z, \gamma_{21}^{(3)},\\
&\ \gamma_{23}^{(1)} - \gamma_{32}^{(1)}, \gamma_{23}^{(2)}, \gamma_{23}^{(3)},\\
&\ \gamma_{31}^{(1)}, \gamma_{31}^{(2)}, \gamma_{31}^{(3)} - Z,\\
&\ \gamma_{32}^{(2)}, \gamma_{32}^{(3)}\\
&\ \gamma_{22}^{(2)}\gamma_{32}^{(1)} + \gamma_{22}^{(3)}\gamma_{33}^{(1)}, \gamma_{22}^{(1)}\gamma_{33}^{(2)} + \gamma_{32}^{(1)}\gamma_{33}^{(3)},\\
&\ \gamma_{22}^{(2)}\gamma_{33}^{(2)} + \gamma_{33}^{(1)}Z, \gamma_{22}^{(3)}\gamma_{33}^{(2)} - \gamma_{32}^{(1)}Z, \gamma_{22}^{(3)}\gamma_{33}^{(3)} + \gamma_{22}^{(1)}Z\}
\end{aligned}$$

and

$$
\begin{aligned}
&\{\gamma_{11}^{(1)} - Z, \gamma_{11}^{(2)}, \gamma_{11}^{(3)},\\
&\gamma_{12}^{(1)}, \gamma_{12}^{(2)} - Z, \gamma_{12}^{(3)},\\
&\gamma_{13}^{(1)}, \gamma_{13}^{(2)}, \gamma_{13}^{(3)} - Z,\\
&\gamma_{21}^{(1)}, \gamma_{21}^{(2)} - Z, \gamma_{21}^{(3)},\\
&\gamma_{22}^{(1)}, \gamma_{22}^{(2)} - \gamma_{23}^{(3)}, \gamma_{22}^{(3)},\\
&\gamma_{23}^{(1)}, \gamma_{23}^{(2)},\\
&\gamma_{31}^{(1)}, \gamma_{31}^{(2)}, \gamma_{31}^{(3)} - Z,\\
&\gamma_{32}^{(1)}, \gamma_{32}^{(2)} - \gamma_{33}^{(3)}, \gamma_{32}^{(3)},\\
&\gamma_{33}^{(1)}, \gamma_{33}^{(2)}\}
\end{aligned}
$$

as Gröbner bases for the homogenized ideals $I^h_{\text{univ},C}$ and $I^h_{\text{univ},E}$, respectively. To examine the hyperplane at infinity we set $Z = 0$, which yields

$$\begin{aligned}
&\{\gamma_{11}^{(1)}, \gamma_{11}^{(2)}, \gamma_{11}^{(3)}, \\
&\gamma_{12}^{(1)}, \gamma_{12}^{(2)}, \gamma_{12}^{(3)}, \\
&\gamma_{13}^{(1)}, \gamma_{13}^{(2)}, \gamma_{13}^{(3)}, \\
&\gamma_{21}^{(1)}, \gamma_{21}^{(2)}, \gamma_{21}^{(3)}, \\
&\gamma_{23}^{(1)} - \gamma_{32}^{(1)}, \gamma_{23}^{(2)}, \gamma_{23}^{(3)}, \\
&\gamma_{31}^{(1)}, \gamma_{31}^{(2)}, \gamma_{31}^{(3)}, \\
&\gamma_{32}^{(2)}, \gamma_{32}^{(3)} \\
&\gamma_{22}^{(2)}\gamma_{32}^{(1)} + \gamma_{22}^{(3)}\gamma_{33}^{(1)}, \gamma_{22}^{(1)}\gamma_{33}^{(2)} + \gamma_{32}^{(1)}\gamma_{33}^{(3)}, \\
&\gamma_{22}^{(2)}\gamma_{33}^{(2)}, \gamma_{22}^{(3)}\gamma_{33}^{(2)}, \gamma_{22}^{(3)}\gamma_{33}^{(3)}\}
\end{aligned}$$

and

$$\begin{aligned}
&\{\gamma_{11}^{(1)}, \gamma_{11}^{(2)}, \gamma_{11}^{(3)}, \\
&\gamma_{12}^{(1)}, \gamma_{12}^{(2)}, \gamma_{12}^{(3)}, \\
&\gamma_{13}^{(1)}, \gamma_{13}^{(2)}, \gamma_{13}^{(3)}, \\
&\gamma_{21}^{(1)}, \gamma_{21}^{(2)}, \gamma_{21}^{(3)}, \\
&\gamma_{22}^{(1)}, \gamma_{22}^{(2)} - \gamma_{23}^{(3)}, \gamma_{22}^{(3)}, \\
&\gamma_{23}^{(1)}, \gamma_{23}^{(2)}, \\
&\gamma_{31}^{(1)}, \gamma_{31}^{(2)}, \gamma_{31}^{(3)}, \\
&\gamma_{32}^{(1)}, \gamma_{32}^{(2)} - \gamma_{33}^{(3)}, \gamma_{32}^{(3)}, \\
&\gamma_{33}^{(1)}, \gamma_{33}^{(2)}\}.
\end{aligned}$$

Let $I^{\infty}_{\mathrm{univ},C}$ and $I^{\infty}_{\mathrm{univ},E}$ be the ideals generated by these sets. Then $I^{\infty}_{\mathrm{univ},E}$ is prime and the corresponding closed subscheme is isomorphic to $\mathrm{Spec}(\mathbb{Z}[\gamma_{23}^{(2)}, \gamma_{32}^{(2)}])$. While this is the same closed subscheme corresponding to $I_{\mathrm{univ},E}$, the structure of the algebra over ${R_{\mathrm{univ},E}}^{\infty} := R_{\mathrm{univ}}/I^{\infty}_{\mathrm{univ},E}$ is quite different. Since $\gamma_{1j}^{k}, \gamma_{i1}^{k} \in I^{\infty}_{\mathrm{univ},E}$ for all $i, j, k \in \{1, 2, 3\}$, then e_1 acts as 0 in $A_{\mathrm{univ}} \otimes_{R_{\mathrm{univ}}} {R_{\mathrm{univ},E}}^{\infty}$, i.e., $e_1\alpha = 0$ for all α. Thus it is no longer clear that $A_{\mathrm{univ}} \otimes_{R_{\mathrm{univ}}} {R_{\mathrm{univ},E}}^{\infty}$ has a multiplicative identity at all, hence is not an algebra, but rather a nonunital algebra. On the other hand e_2 and e_3 behave as they did in $A_{\mathrm{univ}} \otimes_{R_{\mathrm{univ}}} R_{\mathrm{univ},E}$:

$$\begin{aligned} e_2^2 &= re_2 & \qquad e_2e_3 &= re_3 \\ e_3e_2 &= se_2 & \qquad e_3^2 &= se_3 \end{aligned}$$

where $r = \gamma_{22}^{(2)} = \gamma_{23}^{(3)}$ and $s = \gamma_{32}^{(2)} = \gamma_{33}^{(3)}$.

Recall that $A_{\mathrm{univ}} \otimes_{R_{\mathrm{univ}}} R_{\mathrm{univ},E} \cong R_{\mathrm{univ}} \oplus M$, where M is the ideal $R_{\mathrm{univ}}e_2 \oplus R_{\mathrm{univ}}e_3$ of R_{univ}. Thus in passing from $A_{\mathrm{univ}} \otimes_{R_{\mathrm{univ}}} R_{\mathrm{univ},E}$ to $A_{\mathrm{univ}} \otimes_{R_{\mathrm{univ}}} {R_{\mathrm{univ},E}}^{\infty}$ we in some sense "forget" about the copy of R_{univ} in this decomposition, and are simply left with $M = R_{\mathrm{univ}}e_2 \oplus R_{\mathrm{univ}}e_3$.

The situation for $I^{\infty}_{\mathrm{univ},C}$ is more complicated: $I^{\infty}_{\mathrm{univ},C}$ is no longer prime, or even primary. However, it is still radical and, computing its primary decomposition using Magma, we find that $I^{\infty}_{\mathrm{univ},C} = P_1^{\infty} \cap P_2^{\infty} \cap P_3^{\infty}$ where P_i^{∞} is a prime of dimension 4 for each $i = 1, 2, 3$. Their corresponding closed subschemes are isomorphic to

$$\begin{aligned}
\operatorname{Spec}(R^{\infty}_{C,1}) &= \operatorname{Spec}\left(\frac{\mathbb{Z}[\gamma^{(1)}_{22}, \gamma^{(2)}_{22}, \gamma^{(3)}_{22}, \gamma^{(1)}_{23}, \gamma^{(1)}_{33}]}{(\gamma^{(1)}_{33}\gamma^{(3)}_{22} + \gamma^{(1)}_{23}\gamma^{(2)}_{22})}\right), \\
\operatorname{Spec}(R^{\infty}_{C,2}) &= \operatorname{Spec}\left(\frac{\mathbb{Z}[\gamma^{(1)}_{22}, \gamma^{(1)}_{23}, \gamma^{(1)}_{33}, \gamma^{(2)}_{33}, \gamma^{(3)}_{33}]}{(\gamma^{(1)}_{22}\gamma^{(2)}_{33} + \gamma^{(1)}_{23}\gamma^{(3)}_{33})}\right), \text{ and} \\
\operatorname{Spec}(R^{\infty}_{C,3}) &= \operatorname{Spec}(\mathbb{Z}[\gamma^{(1)}_{22}, \gamma^{(2)}_{22}, \gamma^{(1)}_{33}, \gamma^{(3)}_{33}])\,.
\end{aligned}$$

Again, the base change of A_{univ} to each of these subschemes results in a nonunital algebra where e_1 acts as 0. Thus the multiplication in $A_{\text{univ}} \otimes_{R_{\text{univ}}} R^{\infty}_{C,1}$ is determined by

$$\begin{aligned}
e_2^2 &= \gamma^{(1)}_{22} e_1 + \gamma^{(2)}_{22} e_2 + \gamma^{(3)}_{22} e_3 & \qquad e_2 e_3 &= \gamma^{(1)}_{23} e_1 \\
e_3 e_2 &= \gamma^{(1)}_{23} e_1 & \qquad e_3^2 &= \gamma^{(1)}_{33} e_1\ .
\end{aligned}$$

The multiplication in $A_{\text{univ}} \otimes_{R_{\text{univ}}} R^{\infty}_{C,2}$ is given analogously, but interchanging e_2 and e_3. Finally multiplication in $A_{\text{univ}} \otimes_{R_{\text{univ}}} R^{\infty}_{C,3}$ is simply given by

$$\begin{aligned}
e_2^2 &= \gamma^{(1)}_{22} e_1 + \gamma^{(2)}_{22} e_2 & \qquad e_2 e_3 &= 0 \\
e_3^2 &= \gamma^{(1)}_{33} e_1 + \gamma^{(3)}_{33} e_3 & \qquad e_3 e_2 &= 0\,.
\end{aligned}$$

We hope that these degenerations may help us to better understand the moduli of framed algebras, and may allow us to define a compactified moduli functor.

Section 3.8

Future Work

In this section we mention some directions of investigation for future work.

3.8.1. Moduli of algebras

As mentioned in subsection 3.6, our true interest lies in understanding the moduli space of algebras, rather than modestly framed algebras. We can attempt to form the moduli stack of cubic algebras $\mathfrak{M}_3$ by taking the stack quotient of the moduli space of modestly framed algebras $\mathfrak{M}_3^{\square}$ by the action of GL_2 on modest bases.

3.8.2. Stratification by geometric degree

Our classification results fit into a larger classification problem that seeks to answer the following question: for which positive integers n and d are there algebras of rank n and geometric degree d? For these values of n and d, what does the moduli space of such algebras look like? As shown in Proposition 2.2.9, we must have $d \leq n$. One can easily resolve the question for special values of n and d (for instance, when $n = d$), but we have thus far been unable to extend our results to higher rank. The main obstacle has been that, in a polynomial ring of n^3 variables, computing Gröbner bases quickly becomes very expensive for increasing values of n. This prevents us from simply computing the primary decomposition of an ideal as before, as this requires the computation of a Gröbner basis.

Chapter 4

Computing Elliptic and Hyperelliptic Belyi Maps

Section 4.1

Introduction

In this chapter we present a numerical method for computing Belyi maps. We have used this method to compute an exhaustive database of Belyi maps of low degree. Our main results are observations on the features of the data, given in Theorems 4.4.8 and 4.5.8.

Section 4.2

Background

4.2.1. Conventions

Throughout this chapter we follow the algebro-geometric conventions and terminology laid out in [Silverman, 2009, Chapter 1]. In particular we adopt the following definition of a curve.

Definition 4.2.1. An *(algebraic) curve* is an (irreducible) projective variety of dimension 1 over a field.

Given a curve X over a field K, we denote by $\Omega(X)$ its space of holomorphic (or regular) differentials, as defined in [Shafarevich, 2013, Ch. 3, §5]. As a vector space over K, $\dim_K(\Omega(X)) = g$, where g is the genus of X, as discussed in [Shafarevich, 2013, Ch. 3, §6.3].

Given a discrete subgroup Γ of $\mathrm{PSL}_2(\mathbb{R})$ (called a *Fuchsian group*), we define a modular form for Γ as in [Voight and Zureick-Brown, 2015, §6.2]. Since all the Fuchsian groups we consider herein are cocompact, hence have no cusps, this means that a *modular form* for Γ of weight $k \in \mathbb{Z}_{\geq 0}$ is a holomorphic function $f\colon \mathcal{H} \to \mathbb{C}$ such that

$$f(\gamma z) = (cz+d)^k f(z) \qquad \text{for all} \quad \gamma = \pm \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma\,.$$

We denote the vector space of modular forms for Γ of a given weight k by $M_k(\Gamma)$ or $S_k(\Gamma)$. (The notation $S_k(\Gamma)$ is usually reserved for cusp forms, but as our Fuchsian groups have no cusps, then trivially $M_k(\Gamma) = S_k(\Gamma)$.) As described in [Voight and

Zureick-Brown, 2015, §6.2], there is an isomorphism

$$M_2(\Gamma) \xrightarrow{\sim} \Omega(X) \tag{4.2.1}$$

$$f(z) \mapsto f(z)\,\mathrm{d}z\,. \tag{4.2.2}$$

Most of the curves we will consider arise as quotients of hyperbolic 2-space. We denote by $\mathcal{H}$ the complex upper half-plane $\{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$, equipped with the hyperbolic metric

$$\frac{|\mathrm{d}z|^2}{|\mathrm{Im}(z)|^2} = \frac{(\mathrm{d}x)^2 + (\mathrm{d}y)^2}{y^2}$$

where $z = x + iy$. We denote by $\mathcal{D}$ the complex open unit disc $\{w \in \mathbb{C} : |w| < 1\}$ and equip it with the hyperbolic metric

$$4\frac{|\mathrm{d}w|^2}{(1-|w|^2)^2} = 4\frac{(\mathrm{d}x)^2 + (\mathrm{d}y)^2}{(1-x^2-y^2)^2}$$

where $w = x + iy$. (We will systematically use the variable z to denote the coordinate in $\mathcal{H}$ and w to denote the coordinate in $\mathcal{D}$.) Then $\mathcal{H}$ and $\mathcal{D}$ are isometrically isomorphic as Riemann surfaces via the map

$$\begin{aligned} \mathcal{H} &\to \mathcal{D} \\ z &\mapsto \frac{z-i}{z+i} \end{aligned}$$

with inverse

$$\begin{aligned} \mathcal{D} &\to \mathcal{H} \\ w &\mapsto i\frac{1+w}{1-w}\,. \end{aligned}$$

Under this map, the differential dz on $\mathcal{H}$ is mapped to the differential

$$\mathrm{d}\left(i\frac{1+w}{1-w}\right) = i\frac{1-w+1+w}{(1-w)^2}\,\mathrm{d}w = \frac{2i}{(1-w)^2}\,\mathrm{d}w \tag{4.2.3}$$

on $\mathcal{D}$. It is often convenient to pass between these two models for hyperbolic 2-space. Thus we identify $\mathcal{H}$ and $\mathcal{D}$ via the isomorphisms above and henceforth freely pass between them without further comment.

4.2.2. Motivation and history

The absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is arguably the most important group in algebraic number theory. In some sense it encodes all possible symmetries of algebraic numbers: for every number field K, the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ can be realized as a quotient of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. In his seminal work [Grothendieck, 1997], Grothendieck defined an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on a special class of topological graphs, which he compared to *dessins d'enfants*—children's drawings. His ambitious aim was to understand this mysterious and important group in terms of its action on these simple drawings.

Grothendieck's program springs from a theorem of Belyi, about which he marveled, "...never has a deep and disconcerting result been proven in so few lines!"

Theorem 4.2.2 ([Belyi, 1980, Theorem 4]). *A smooth projective curve X over $\mathbb{C}$*

can be defined over $\overline{\mathbb{Q}}$ *if and only if there exists a nonconstant morphism of algebraic curves* $\varphi\colon X \to \mathbb{P}^1_{\mathbb{C}}$ *unramified outside* $\{0, 1, \infty\}$.

Such a map is called a Belyi map.

Definition 4.2.3. A *Belyi map* over $\mathbb{C}$ is a nonconstant morphism of algebraic curves $\varphi\colon X \to \mathbb{P}^1_{\mathbb{C}}$ that is unramified outside $\{0, 1, \infty\}$. The *genus* of φ is the genus of the curve X, its domain.

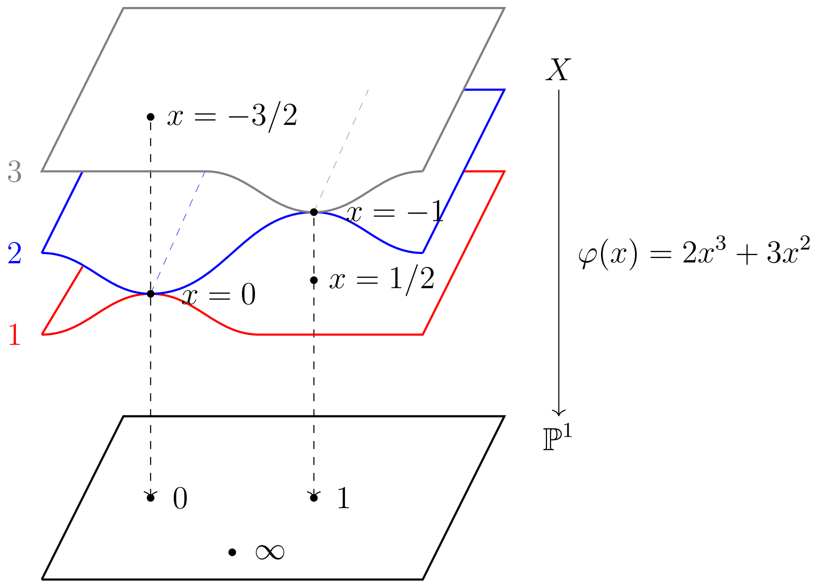
Example 4.2.4. Consider the map $\varphi\colon \mathbb{P}^1 \to \mathbb{P}^1$ given by $\varphi(x) = 2x^3 + 3x^2$.

Since $\varphi'(x) = 6x^2 + 6x = 6x(x+1)$, φ is only ramified above $0, 1, \infty$. The factorizations

$$\varphi(x) = 2x^3 + 3x^2 = x^2(2x+3)$$
$$\varphi(x) - 1 = 2x^3 + 3x^2 - 1 = (2x-1)(x+1)^2$$

show that $\varphi^{-1}(0) = \{0, -3/2\}$ and these points have ramification indices 2 and 1, respectively, and $\varphi^{-1}(1) = \{1/2, -1\}$ and these points have ramification indices 1 and 2, respectively.

We can visualize the map φ as a ramified cover of $\mathbb{P}^1$ as depicted in the following illustration.



Remark 4.2.5. Due to their ramification structure, Belyi maps are sometimes referred to as three-point branched covers.

Definition 4.2.6. Given Belyi maps $\varphi_1 \colon X_1 \to \mathbb{P}^1$ and $\varphi_2 \colon X_2 \to \mathbb{P}^1$, a *morphism* $\iota \colon \varphi_1 \to \varphi_2$ of Belyi maps is a morphism $\iota \colon X_1 \to X_2$ of algebraic curves such that $\varphi_1 = \varphi_2 \circ \iota$, i.e., such that the following diagram commutes.

$$\begin{tikzcd} X_1 \arrow[rr, "\iota"] \arrow[dr, "\varphi_1"'] & & X_2 \arrow[dl, "\varphi_2"] \\ & \mathbb{P}^1 & \end{tikzcd}$$

Belyi maps φ_1 and φ_2 are *isomorphic* if there exists a map ι as above that is an isomorphism of algebraic curves.

While we are primarily interested in Belyi maps due to the Galois action on their isomorphism clases (described in subsection 4.2.3 below), they also have a number of other applications. We briefly describe some of these applications below.

Belyi maps can be used to solve instances of the inverse Galois problem which, given a finite group G, aims to find a finite Galois extension $K/\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong G$. Indeed, in his original paper [Belyi, 1980], Belyi uses Belyi maps to construct extensions of $\mathbb{Q}$ with Galois groups isomorphic to specific families of Chevalley groups over finite fields. The basic idea is to use the notion of rigidity to produce an extension of the rational function field $\mathbb{Q}(t)$ with a given Galois group, and then specialize and apply Hilbert's irreducibility theorem to obtain an extension of $\mathbb{Q}$ with the same Galois group. For comprehensive treatments, see [Malle and Matzat, 1999], [Serre, 2016], and [Volklein, 1996].

Belyi maps have also been used to construct number fields with interesting ramification properties. In [Malle, 1994], Malle computes tables containing fields of definition of Belyi maps of degree at most 13. He notes that the number fields obtained in this way are remarkable in that they are ramified over only a few small primes. Specializing Belyi maps also yields interesting number fields. A Belyi map $\varphi\colon X \to \mathbb{P}^1$ defined over $\mathbb{Q}$ induces an extension $\mathbb{Q}(t) \hookrightarrow \mathbb{Q}(X)$ of function fields. By specializing the value of the parameter t, one can obtain number fields with small ramification set or root discriminant, an approach investigated in [Jones and Roberts, 2007], [Roberts, 2004], and [Roberts, 2016].

Belyi maps also have interesting dynamical properties. A Belyi map $\varphi\colon \mathbb{P}^1 \to \mathbb{P}^1$ is *dynamical* if it preserves the set $\{0, 1, \infty\}$, i.e., $\varphi(\{0, 1, \infty\}) \subseteq \{0, 1, \infty\}$. As described in [Zvonkin, 2008], dynamical Belyi maps give examples of rigid, postcritically finite dynamical systems. The properties of dynamical Belyi maps are further explored in [Anderson et al., 2018].

In [Elkies, 1991] Elkies shows that, given an effective version of the ABC conjecture, one can use Belyi maps to give an effective proof of the Mordell conjecture. (The Mordell conjecture is now perhaps better known as Faltings's theorem; cf., [Faltings, 1983] or its translation [Faltings, 1986].)

For an introduction to the theory of Belyi maps and dessins d'enfants, we refer the reader to [Jones and Wolfart, 2016], [Girondo and González-Diez, 2012], and [Schneps, 1994].

4.2.3. The Galois action on Belyi maps

We now consider the arithmetic of Belyi maps and the action of $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Given a Belyi map $\varphi\colon X \to \mathbb{P}^1$, then by Theorem 4.2.2 we can find a model for X with defining equations having coefficients in $\overline{\mathbb{Q}}$. Moreover, the proof of Belyi's theorem presented in [Belyi, 1980, Theorem 4] shows that the Belyi map itself can also be defined over $\overline{\mathbb{Q}}$. (For more on this, see [Girondo and González-Diez, 2012, Proposition 3.34]). Then the absolute Galois group $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on a Belyi map φ and its domain X simply by acting on the coefficients of their defining equations. We denote the action of $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the curve and Belyi map by X^σ and φ^σ, respectively. Note as well that the action of $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ preserves the genus, monodromy group, and ramification type of a Belyi map (cf., [Girondo and González-Diez, 2012, Theorem 3.28]).

The equations for a Belyi map—those for the curve X and those for the map φ itself—involve only finitely many coefficients. Thus, once we find equations for the map over $\overline{\mathbb{Q}}$, they will in fact belong to some finite extension K of $\mathbb{Q}$. Thus we seek to find equations for the Belyi map that belong to the number field of minimal degree, if such a field exists.

Definition 4.2.7. Let $\varphi\colon X \to \mathbb{P}^1$ be a Belyi map. The *field of moduli* $M(X, \varphi) \subseteq \overline{\mathbb{Q}}$

of φ is the subfield of $\overline{\mathbb{Q}}$ fixed by the group

$$\left\{\tau \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) : \varphi^\tau \cong \varphi\right\} .$$

The field of moduli is the intersection of all fields over which φ can be defined. However, it is not always the case that φ can be defined over $M(X, \varphi)$. The issue of descent of a Belyi map is subtle, as discussed in [Musty et al., 2019, §4]. In order to rigidify the situation and avoid these subtleties, we define a pointed variant of a Belyi map.

Definition 4.2.8. A *pointed Belyi map* $(X, \varphi; P)$ is a Belyi map $\varphi\colon X \to \mathbb{P}^1$ together with a point $P \in \varphi^{-1}(\{0, 1, \infty\}) \subseteq X(\overline{\mathbb{Q}})$. A *morphism* of pointed Belyi maps $(X_1, \varphi_1; P_1) \to (X_2, \varphi_2; P_2)$ is an morphism of Belyi maps ι such that $\iota(P_1) = P_2$. The pointed Belyi maps $(X_1, \varphi_1; P_1)$ and $(X_2, \varphi_2; P_2)$ are *isomorphic* if there exists a map ι as above that is an isomorphism of algebraic curves.

Definition 4.2.9. The *field of moduli* $M(X, \varphi; P) \subseteq \overline{\mathbb{Q}}$ of the pointed Belyi map$(X, \varphi; P)$ is the fixed field of

$$\left\{\tau \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) : \varphi^\tau \cong \varphi \text{ and } \tau(P) = P\right\} .$$

Theorem 4.2.10 ([Sijsling and Voight, 2016, Theorem 1.10], [Birch, 1994, Theorem 2])**.** *A pointed Belyi map $(X, \varphi; P)$ descends to $M(X, \varphi; P)$: the curve X, the map φ, and the point P can all be defined over $M(X, \varphi; P)$.*

In the next subsection we will bound the degree of $M(X, \varphi; P)$ over $\mathbb{Q}$ in terms of combinatorial data. This will prove to be useful for computing equations for X and φ.

4.2.4. Background: the big bijective picture

Our method makes use of a web of bijections that relate various collections of algebraic, combinatorial, topological, geometric, and algebro-geometric objects. We give only an overview here—see [Klug et al., 2014, §1] for more details.

We first introduce the classes of objects in this "big bijective picture."

Definition 4.2.11. A *permutation triple* of degree d is a triple $\sigma = (\sigma_0, \sigma_1, \sigma_\infty) \in S_d^3$ such that $\sigma_\infty \sigma_1 \sigma_0 = 1$. The permutation triple σ is *transitive* if $\langle \sigma_0, \sigma_1, \sigma_\infty \rangle \leq S_d$ is a transitive subgroup. Two permutation triples σ, σ' are *simultaneously conjugate* if there exists $\rho \in S_d$ such that

$$(\sigma_0', \sigma_1', \sigma_\infty') = (\rho\sigma_0\rho^{-1}, \rho\sigma_1\rho^{-1}, \rho\sigma_\infty\rho^{-1}) .$$

Remark 4.2.12. We choose the ordering $\sigma_\infty\sigma_1\sigma_0$ in the definition of permutation triples (while others might require $\sigma_0\sigma_1\sigma_\infty = 1$) to agree with our conventions on the action of an element of a triangle group; cf., Remark 4.2.25 below.

The notion of a passport allows us to organize permutation triples by their combinatorial data.

Definition 4.2.13. A *passport* consists of the data (g, G, λ) where

- $g \geq 0$ is an integer,
- $G \leq S_d$ is a transitive subgroup; and
- $\lambda = (\lambda_0, \lambda_1, \lambda_\infty)$ is a triple of partitions of d.

The passport of a permutation triple $\sigma \in S_d^3$ is (g, G, λ) where

(i) $\langle \sigma_0, \sigma_1, \sigma_\infty \rangle = G$; and

(ii) $\sigma_0, \sigma_1, \sigma_\infty$ have the cycle types specified by $\lambda_0, \lambda_1, \lambda_\infty$

(iii) $\displaystyle 2g - 2 = -2d + \sum_{s \in \{0,1,\infty\}} \sum_{\tau \text{ a cycle in } \sigma_s} (\operatorname{len}(\tau) - 1)$

where $\operatorname{len}(\tau)$ is the length of the cycle τ. In this case we say that σ *belongs* to the passport (g, G, λ). The *size* of a passport is the number of permutation triples belonging to it, up to simultaneous conjugacy.

Remark 4.2.14. The formula in criterion (c) of belonging is essentially a combinatorial avatar of the Riemann-Hurwitz formula. We will see that this means that for each σ belonging to the passport (g, G, λ) the Belyi map corresponding to σ has genus g.

Example 4.2.15. Consider the permutation triple $\sigma = (\sigma_0, \sigma_1, \sigma_\infty)$ where

$$\sigma_0 = (1\,3\,7)(2)(4\,5\,6)\,, \quad \sigma_1 = (1\,4\,5\,3)(2\,7)(6)\,, \quad \sigma_\infty = (1\,2\,7\,5)(3)(4\,6)\,.$$

Then σ belongs to the passport

$$(0, G, ((3,3,1),(4,2,1),(4,2,1)))$$

where $G = \langle (1\,2\,3\,4\,5\,6\,7), (1\,2)(3\,6) \rangle$ has transitive group label 7T5 and is isomorphic to $\mathrm{GL}_3(\mathbb{F}_2)$.

One can use a double coset computation show that this passport has size 2. (See [Musty et al., 2019, Lemma 2.2.1].) The other triple is $\sigma' = (\sigma'_0, \sigma'_1, \sigma'_\infty)$ with

$$\sigma'_0 = (1\,3\,7)(2)(4\,5\,6)\,, \quad \sigma'_1 = (1\,6\,3\,2)(4\,5)(7)\,, \quad \sigma'_\infty = (1\,7\,6\,4)(2\,3)(5)\,.$$

Remark 4.2.16. As the conjugacy class of a permutation in S_d is uniquely determined by its cycle type, the triple λ of partitions of d is equivalent to a triple of conjugacy classes of S_d.

We now introduce the combinatorial analogue of a pointed Belyi map.

Definition 4.2.17. A *pointed permutation triple* $(\sigma; c)$ is a permutation triple $\sigma \in S_d^3$ together with a distinguished cycle c in one of the permutations σ_s with $s = 0, 1, \infty$; we call s its *base point* and the length of the cycle c its *length.* We call $(\sigma; c)$ a *pointed refinement* of the permutation triple σ.

Two pointed permutation triples $(\sigma; c)$ and $(\sigma'; c')$ are *simultaneously conjugate* if the permutation triples σ, σ' are simultaneously conjugate by an element $\rho \in S_d$ such that $\rho c \rho^{-1} = c'$.

Remark 4.2.18. In our computations we always choose the distinguished cycle c of σ to be the cycle in σ_0 containing 1.

Definition 4.2.19. A *pointed passport* consists of the data $(g, G, \lambda; c)$ where (g, G, λ) is a passport and $c = (s, e, a)$ consists of the data:

(a) $s \in \{0, 1, \infty\}$;

(b) $e \in \mathbb{Z}_{\geq 1}$ a part in the partition λ_s; and

(c) $a \in \mathbb{Z}_{\geq 1}$.

The pointed passport of a pointed permutation triple $(\sigma; c)$ is the pointed passport $(g, G, \lambda; (s, e, a))$ where (g, G, λ) is the passport of σ, $s \in \{0, 1, \infty\}$ indicates which of $\sigma_0, \sigma_1, \sigma_\infty$ contains c, e is the length of c, and

$$a = \#\{\rho \in S_d : \rho \sigma_s \rho^{-1} = \sigma_s \ \forall s \in \{0, 1, \infty\} \text{ and } \rho c \rho^{-1} = c\}.$$

In this case we say that $(\sigma; c)$ *belongs* to the pointed passport $(g, G, \lambda; c)$. The *size* of a pointed passport is the number of pointed permutation triples belonging to it, up to simultaneous conjugacy.

Proposition 4.2.20 ([Musty et al., 2019, Corollary 4.3.2])**.** *A pointed Belyi map is defined over a field whose degree is at most the size of its pointed passport.*

Remark 4.2.21. This proposition allows us to bound the degree of the number field over which a (pointed) Belyi map is defined purely in terms of group theoretic and combinatorial data.

The next class of objects involved in this web of bijections are triangle subgroups.

Definition 4.2.22. A triple of integers $a, b, c \in \mathbb{Z}_{\geq 2}$ is *spherical*, *Euclidean*, or *hyperbolic* according to whether the value

$$\chi(a, b, c) := 1 - \frac{1}{a} - \frac{1}{b} - \frac{1}{c}$$

is respectively negative, zero, or positive. We associate the geometry

$$H = \begin{cases} \text{sphere } \mathbb{P}^1_{\mathbb{C}}, & \text{if } \chi(a, b, c) < 0; \\ \text{plane } \mathbb{C}, & \text{if } \chi(a, b, c) = 0; \\ \text{upper half-plane } \mathcal{H}, & \text{if } \chi(a, b, c) > 0. \end{cases}$$

Remark 4.2.23. In other words, H is the unique (classical) geometry permitting a triangle T with angles $\pi/a, \pi/b$, and π/c.

Definition 4.2.24. For $a, b, c \in \mathbb{Z}_{\geq 2}$ we define the *triangle group* by the presentation

$$\Delta(a,b,c) = \langle \delta_a, \delta_b, \delta_c \mid \delta_a^a = \delta_b^b = \delta_c^c = \delta_c\delta_b\delta_a = 1 \rangle \,.$$

The generators $\delta_a, \delta_b, \delta_c$ of $\Delta(a,b,c)$ can be interpreted as the isometries of H given by rotation about the vertices z_a, z_b, z_c of T by the angles $2\pi/a$, $2\pi/b$, $2\pi/c$, respectively, as shown in Figure 4.2.1.

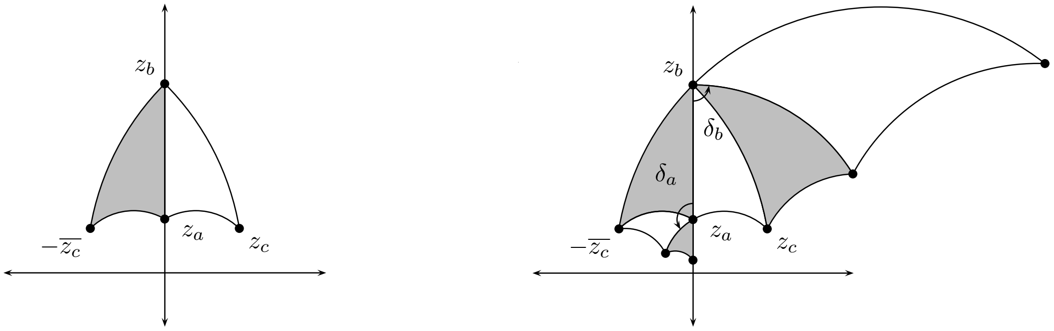


Figure 4.2.1: A fundamental domain for the action of $\Delta(a,b,c)$ on H. The action of δ_a and δ_b on the fundamental domain.

Remark 4.2.25. We choose the ordering $\delta_c\delta_b\delta_a$ in the definition of permutation triples (while others might require $\delta_a\delta_b\delta_c = 1$) so that δ_a, δ_b, and δ_c act by counterclockwise rotations of the appropriate angle. The opposite convention would require them to act as clockwise rotations.

Remark 4.2.26. Some authors allow $a, b, c \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$. With this convention, the full modular group $\mathrm{PSL}_2(\mathbb{Z})$ can be interpreted as the triangle group $\Delta(2, 3, \infty)$, as the usual fundamental domain for $\mathrm{PSL}_2(\mathbb{Z})$ consists of a triangle with angles $\pi/2, \pi/3, 0$ and with one vertex at infinity, together with its reflection across the imaginary axis. However, the triangle groups that arising from our method always have a, b, and c finite; henceforth we restrict to the case of triangle groups $\Delta(a,b,c)$ with a, b, and c

finite.

The objects in this bijective picture that most enchanted Grothendieck are graphs called dessins d'enfants (children's drawings). In contrast with the other classes of objects in consideration, these dessins are strikingly simple, just consisting of black and white dots connected by lines. In [Grothendieck, 1997], Grothendieck marveled at the fact that these seemingly simple drawings nonetheless capture all the structure of maps of complex algebraic curves:

"I don't think that a mathematical fact has ever struck me as much as this, nor had a comparable psychological impact. This surely stems from the very familiar, non-technical nature of the objects considered, of which any drawing scrawled on a scrap of paper...gives a perfectly explicit example."

Definition 4.2.27. A *dessin (d'enfant)* is a finite graph D embedded in an oriented compact connected topological surface X with the following properties:

(i) D is connected;

(ii) D is *bicolored*: each vertex is assigned the color black or white, and adjacent vertices have different colors; and

(iii) $X \setminus D$ has finitely many connected components, each of which is homeomorphic to a disc. (These are called the *faces* of D.)

Dessins D_1 and D_2 embedded in X_1 and X_2, respectively, are *equivalent* if there exists an orientation-preserving homeomorphism $\psi\colon X_1 \to X_2$ whose restriction to D_1 induces an isomorphism between the bicolored graphs D_1 and D_2.

Remark 4.2.28. The notion of equivalence of dessins can also be given in more combinatorial terms, without reference to the ambient topological surfaces. Given a dessin

D, we label the edges of D with the labels $1, 2, \ldots, d$. For each white (resp., black) vertex v, we give a cyclic ordering of the edges incident to v, which we then record as a cycle of a permutation O_0 (resp., O_1). The pair (O_0, O_1) is called an *orientation* of the dessin D.

We then define dessins D_1 and D_2 to be equivalent if there exists an isomorphism of graphs $\psi \colon D_1 \to D_2$ that preserves both the bicoloring and orientation of D_1. For more details, cf., [Sijsling and Voight, 2014, §1].

Lemma 4.2.29. *There are bijections between the following classes of objects.*

(a) *Belyi maps of degree d, up to isomorphism*

(b) *Transitive permutation triples in S_d, up to simultaneous conjugacy*

(c) *Subgroups of triangle groups of index d, up to conjugacy*

(d) *Dessins d'enfants with d edges, up to equivalence*

We will not give a full proof here, but will rather outline the correspondences that are important for our method. See [Klug et al., 2014, Lemma 1.1] for more details.

4.2.5. Belyi maps to permutation triples

Let $\varphi \colon X \to \mathbb{P}^1$ be a Belyi map of degree d, let $U = \mathbb{P}^1 \setminus \{0, 1, \infty\}$, and let $Y = \varphi^{-1}(U) = X \setminus \varphi^{-1}(\{0, 1, \infty\})$. Then the restriction $\varphi|_Y \colon Y \to U$ is an (unramified) covering map of topological surfaces. Choosing a basepoint $* \in U$, we have a presentation of the fundamental group as

$$\pi_1(U, *) = \langle \gamma_0, \gamma_1, \gamma_\infty \mid \gamma_\infty \gamma_1 \gamma_0 = 1 \rangle$$

where $\gamma_0, \gamma_1, \gamma_\infty$ are homotopy classes represented by loops based at $*$ around 0, 1, and ∞, respectively. Since φ is a covering map, then for each $x \in \varphi^{-1}(*)$, a path γ in U with initial point $*$ can be lifted to a unique path $\widetilde{\gamma}$ in Y with initial point x such that $f \circ \widetilde{\gamma} = \gamma$. Thus the terminal point of $\widetilde{\gamma}$ will be a unique $x' \in \varphi^{-1}(*)$, and this induces a right action of $\pi_1(U, *)$ on $\varphi^{-1}(*)$ by $x^\gamma = \widetilde{\gamma}(1)$. Labelling the d points in $\varphi^{-1}(*)$ with $\{1, \dots, d\}$, this action yields a permutation representation $\sigma \colon \pi_1(U, *) \to S_d$, called the *monodromy action* of φ. Letting $\sigma_0 = \sigma(\gamma_0)$, $\sigma_1 = \sigma(\gamma_1)$, and $\sigma_\infty = \sigma(\gamma_\infty)$ produces a permutation triple; moreover, since Y is path-connected, the group $\langle \sigma_0, \sigma_1, \sigma_\infty \rangle \leq S_d$ is transitive.

The triple $(\sigma_0, \sigma_1, \sigma_\infty)$ obtained in this way encodes several pieces of information about the associated Belyi map. The number of disjoint cycles in σ_0 (resp., σ_1, σ_∞) is the number of distinct points in the fiber above 0 (resp., 1, ∞), while ramification indices of the points in the fiber are given by the lengths of these cycles.

Remark 4.2.30. The basic idea of our method is to reverse this correspondence: given a permutation triple, we wish to compute the Belyi map associated to it. To do so, we pass first from permutation triples to triangle subgroups, and then from triangle subgroups to Belyi maps.

4.2.6. Permutation triples to triangle subgroups

Given a transitive permutation triple $\sigma = (\sigma_0, \sigma_1, \sigma_\infty) \in S_d^3$ with orders $a, b, c \in \mathbb{Z}_{\geq 2}$, let $\Delta = \Delta(a, b, c)$ be its associated triangle subgroup. Since the permutations

$\sigma_0, \sigma_1, \sigma_\infty$ satisfy the relations defining Δ, then there is a group homomorphism

$$\pi\colon \Delta \to S_d$$
$$\delta_a, \delta_b, \delta_c \mapsto \sigma_0, \sigma_1, \sigma_\infty\,.$$

This homomorphism allows us to define an action of Δ on the labels $\{1, 2, \ldots, d\}$: an element $\delta \in \Delta$ acts as $\pi(\delta) \in S_d$. Let

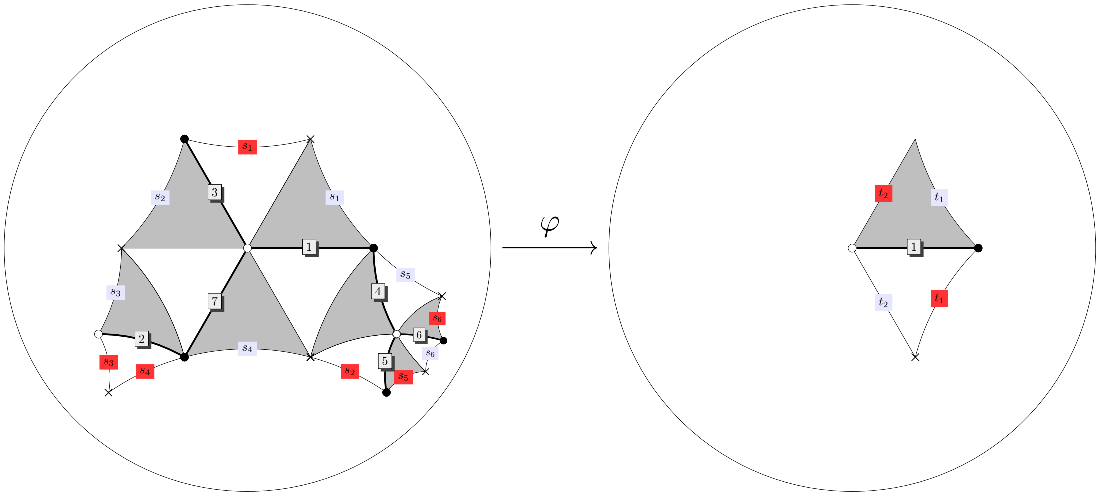
$$\Gamma = \mathrm{Stab}_\Delta(1) = \{\delta \in \Delta : 1^{\pi(\delta)} = 1\}$$

where $G = \langle \sigma \rangle \leq S_d$. Since G acts transitively on $\{1, 2, \ldots, d\}$, then the orbit of 1 has size d. Thus $[\Delta : \Gamma] = d$ by the orbit-stabilizer theorem.

4.2.7. Triangle subgroups to Belyi maps

Let Γ be a subgroup of a triangle group $\Delta = \Delta(a, b, c)$. Then Δ (and Γ) acts on its associated geometric space H (the sphere, Euclidean space, or hyperbolic space). The quotient space $X(\Delta) := \Delta\backslash H$ is homemorphic to a sphere and, after resolving quotient singularities, even isomorphic to $\mathbb{P}^1_\mathbb{C}$. Similarly, $X(\Gamma) = \Gamma\backslash H$ can be given the structure of a smooth projective curve. Moreover, since $\Gamma \leq \Delta$, there is a natural map $\Gamma\backslash H \to \Delta\backslash H$ taking equivalence classes mod Γ to equivalence classes mod Δ. Identifying $X(\Delta)$ with $\mathbb{P}^1(\mathbb{C})$, then this map is the Belyi map $\varphi\colon X(\Gamma) \to \mathbb{P}^1(\mathbb{C})$.

Remark 4.2.31. To pass from Belyi maps to dessins, consider the closed unit interval $[0, 1] \subseteq \mathbb{P}^1$, with 0 and 1 labelled with white and black dots, respectively. One can show that $\varphi^{-1}([0, 1])$, the graph embedded in X by pulling back along φ, is a dessin.



Section 4.3

Computing equations: generalities

There are a variety of methods for computing Belyi maps, using tools such as Gröbner bases, complex analytic techniques, and p-adic techniques. For a survey of these methods, see [Sijsling and Voight, 2014].

This section is based strongly on joint work with Klug, Musty, and Voight [Klug et al., 2014]. We employ a numerical method that uses power series expansions of modular forms for subgroups of triangle groups. In subsection 4.4.4 we augment this procedure with Newton's method, extending the approach in [Klug et al., 2014, Example 5.28] for genus 0 Belyi maps.

Below is an overview of our method for computing equations for Belyi maps. Our method takes as input a permutation triple $\sigma = (\sigma_0, \sigma_1, \sigma_\infty) \in S_d$ and produces as output equations for the curve X and the Belyi map $\varphi\colon X \to \mathbb{P}^1$ corresponding to σ. It is comprised of the following steps.

(1) Form the triangle subgroup $\Gamma \leq \Delta(a, b, c)$ associated to σ and compute its coset graph.

(2) Use a reduction algorithm for Γ and numerical linear algebra to compute numerical power series expansions of modular forms $f_i \in S_k(\Gamma)$ for an appropriate weight k.

(3) Embed the curve $X(\Gamma) = \Gamma \backslash \mathcal{D}$ in projective space using the modular forms f_i. Use numerical linear algebra and Riemann–Roch to find polynomial relations among the series f_i, yielding equations for the curve X and φ.

(4) Normalize the equations of X and φ so that the coefficients are algebraic and recognize these coefficients as elements of a number field $K \subseteq \mathbb{C}$.

(5) Verify that φ has the correct ramification and monodromy representation.

We will focus on steps 3 and 4 of the above method in the cases where $X(\Gamma)$ is an elliptic curve or a hyperelliptic curve. Below we provide brief summaries of the content of the other steps, along with references to more complete treatments.

In step 1, we examine the action of Δ on the coset space $\Gamma \backslash \Delta$. We record this action in a *coset graph*, which is defined similarly to the Cayley graph of a group. This allows us to construct a fundamental domain for Γ that is connected, and comprised of translates of the fundamental domain for Δ. This in turn leads to an efficient reduction algorithm for the group Γ. For more details on this step, we refer the reader to [Klug et al., 2014, §3].

In step 2, we use the reduction algorithm obtained in step 1, along with numerical linear algebra computations, to obtain numerical power series expansions for modular forms for the group Γ. For more details on this step, we refer the reader to [Klug, 2013], [Voight and Willis, 2014], and [Klug et al., 2014, §4].

In step 5, we can verify using Magma that our putative Belyi map φ has the desired ramification by computing its divisor. To verify that φ has the correct monodromy representation, we use the method described in [Bruin et al., 2019, subsection 2C].

Thus at the beginning of step 3 we have the following data:

(i) power series expansions for a basis of modular forms of the appropriate weight;

(ii) a power series expansion for the Belyi map φ as a function on $\Gamma\backslash\mathcal{D}$;

(iii) a fundamental domain in $\mathcal{D}$ for Γ with coordinates of the ramification points of φ; and

(iv) a list of *side pairing elements* of Δ that identify the sides of the fundamental domain that are equivalent under the action of Γ.

Section 4.4

Elliptic Belyi Maps

This section is based on joint work with Musty, Sijsling, and Voight, specifically [Musty et al., 2019, §5]. Our main result is a numerical method for computing elliptic Belyi maps, which we then use to compute an exhaustive database of Belyi maps of low degree. Throughout this section we assume that $X(\Gamma)$ has genus 1. We call a Belyi map whose domain is an elliptic curve an *elliptic Belyi map.*

Remark 4.4.1. Technically an elliptic curve over a field K is more than just a genus 1 curve over K; it comes equipped with a distinguished K-rational point. However, as discussed in subsection 4.2.3 we always compute pointed Belyi maps, which come with a distinguished point. Thus the genus 1 curves we encounter will always come equipped with a K-rational point, and hence are elliptic curves over K.

4.4.1. Setup

Recall from (4.2.1) that $\Omega(X(\Gamma))$ and $S_2(\Gamma)$ are isomorphic via the map $f(z) \mapsto f(z)\,\mathrm{d}z$. Since $X(\Gamma)$ has genus 1, then $S_2(\Gamma)$ has dimension 1, hence it is spanned by a form

$$f(z(w)) = (1-w)^2 \sum_{n=0}^{\infty} b_n w^n \in \mathbb{C}[[w]], \tag{4.4.1}$$

which is unique up to rescaling by $\mathbb{C}^\times$. Then $\omega := f(w)\,\mathrm{d}w$ is the unique (nonzero) holomorphic differential 1-form on the Riemann surface $X(\Gamma)$, up to rescaling by $\mathbb{C}^\times$.

In order to obtain a Weierstrass model for $X(\Gamma)$, we first compute the Abel-Jacobi map $X(\Gamma) \to \mathbb{C}/\Lambda$, where Λ is the period lattice of $X(\Gamma)$. Using our explicit description of a fundamental domain for Γ, we find a set of paths $\gamma_1, \dots, \gamma_t$ generating the homology $H^1(X(\Gamma), \mathbb{Z})$ and then compute the period integrals $\displaystyle\int_{\gamma_i} \omega$. To do so, we compute an antiderivative F for f by integrating the series representations for f term-by-term. Applying the fundamental theorem of calculus, we compute $F(q_i) - F(p_i)$ for $i = 1, \dots, t$, where p_i and q_i are the initial and terminal points, respectively, of the path γ_i. Given a fundamental domain for Γ constructed using the "petalling" variant of the coset graph method (cf., the paragraph preceding Algorithm 3.8 in [Klug et al., 2014]), we can simply take p_i and q_i ranging over all black dots (preimages of 1) in the fundamental domain that are incident to an edge involved in a side pairing. The numerical values computed form a spanning set for the period lattice Λ, which we then reduce to a basis ω_1, ω_2 using the LLL lattice reduction algorithm, as implemented in Magma's LinearRelation. Interchanging ω_1, ω_2 if necessary, we may assume that $\tau := \omega_1/\omega_2 \in \mathcal{H}$.

In computing power series expansions for modular forms we employ a "federalist approach," as described in [Klug et al., 2014, §4]. This entails, for each modular form f, computing a power series expansion for f centered at each white dot (preimage of 0) in the fundamental domain. This approach provides better numerical accuracy when evaluating a modular form f at a point in the fundamental domain, as we can choose the series expansion for f that minimizes the distance between the point and the center of the expansion.

Despite these benefits, the federalist approach leads to a more involved procedure for computing period integrals as above, as we must keep track of the various neighborhoods while using different power series expansions for a given modular form. We illustrate this with the following example.

Example 4.4.2. Consider the permutation triple $\sigma = (\sigma_0, \sigma_1, \sigma_\infty)$ where

$$\sigma_0 = (1\ 7\ 8\ 6)(2\ 4)(3\ 5), \qquad \sigma_1 = (1\ 5)(2\ 7)(3\ 4\ 8\ 6), \qquad \sigma_\infty = (1\ 8\ 2\ 3)(4\ 7\ 5\ 6)\,,$$

which belongs to the passport $(1, G, ((4,2,2),(4,2,2),(4,4)))$, where G is the transitive subgroup of S_8 with label 8T46. Let Γ be the corresponding triangle subgroup. As shown below in figure 4.4.1, the fundamental domain for Γ contains the 3 preimages of 0 (indicated by white dots)

$$v_1 = 0, \qquad v_2 \approx 0.32180 + 0.77689i, \qquad v_3 \approx 0.77689 - 0.32180i\,,$$

one for each cycle in σ_0. Let f be the unique (up to rescaling) weight 2 modular form for Γ. We compute a power series expansion for f centered at each preimage of 0, obtaining the series

$$\begin{aligned}
\frac{f_1(w_1)}{(1-w_1)^2} &\approx 1.00000 - (0.61087 - 0.61087i)w_1 - 0.20488i\, w_1^2 - (1.41241 + 1.41241i)w_1^3 + \cdots \\
\frac{f_2(w_2)}{(1-w_2)^2} &\approx (5.19539 - 2.81603i)w_2 - (5.65951 + 7.29719i)w_2^3 + \cdots \\
\frac{f_3(w_3)}{(1-w_3)^2} &\approx -(0.68929 - 0.50080i)w_3 - (0.02607 + 1.33116i)w_3^3 + \cdots .
\end{aligned}$$

In representing the series, we have applied an automorphism of the disc translating the center u_j of each expansion to the origin. We denote this translated coordinate by w_j. Let F_j be the antiderivative of f_j for $j = 1, 2, 3$.

To compute the period corresponding to the side pairing s_8, we compute the path integral from b_1 to b_4 as

$$\begin{aligned}
\int_{b_1}^{b_2} & f_2(w_2)\,\frac{2i\,\mathrm{d}w_2}{(1-w_2)^2} + \int_{b_2}^{b_3} f_1(w_1)\,\frac{2i\,\mathrm{d}w_1}{(1-w_1)^2} + \int_{b_3}^{b_4} f_3(w_3)\,\frac{2i\,\mathrm{d}w_3}{(1-w_3)^2} \\
&= (F_2(b_2) - F_2(b_1)) + (F_1(b_3) - F_1(b_2)) + (F_3(b_4) - F_2(b_3)) \\
&\approx 1.23941 - 0.20035i + 0.75370 + 0.75370i + (-0.20035 + 1.23941i) \\
&= 1.79276 + 1.79276i
\end{aligned}$$

where b_1, b_2, b_3, b_4 are as depicted in figure 4.4.1. Computing similarly for the other side pairings, we obtain the nonzero periods

$$-1.95468 + 1.95468i, \qquad -1.79276 - 1.79276i\,.$$

(In this example we find only two distinct periods up to numerical precision, so it is

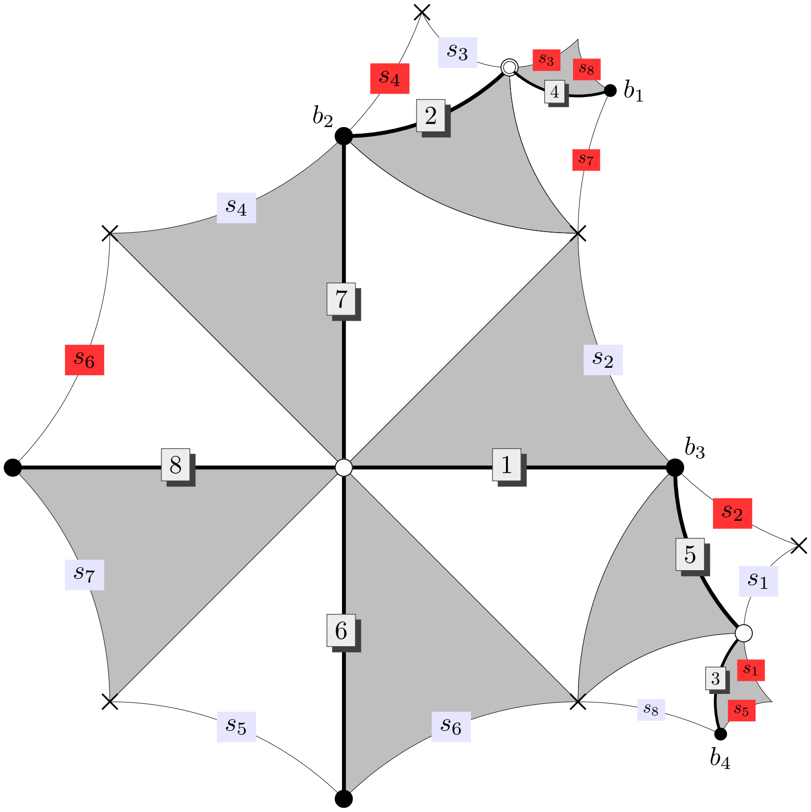


Figure 4.4.1: A fundamental domain for the triangle subgroup corresponding to the permutation triple $(1\ 7\ 8\ 6)(2\ 4)(3\ 5), (1\ 5)(2\ 7)(3\ 4\ 8\ 6), (1\ 8\ 2\ 3)(4\ 7\ 5\ 6)$.

not necessary to reduce the list of periods to a basis.)

With the period lattice $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ in hand, we can now compute the Abel-Jacobi map.

$$\begin{aligned} \alpha\colon X(\Gamma) &\to \mathbb{C}/\Lambda \\ w &\mapsto \int_0^w f(t)\,\frac{2i\,\mathrm{d}t}{(1-t)^2} \mod \Lambda \end{aligned}$$

(The factor of $2i/(1-t)^2$ appears because the differentials in $\mathcal{H}$ and $\mathcal{D}$ are related by

$$dz = \frac{2i}{(1-w)^2}\, dw\,;$$

cf., (4.2.3).) We then apply Weierstrass uniformization to obtain a model

$$E(\Gamma) : y^2 = x^3 - 27c_4x - 54c_6 \tag{4.4.2}$$

for the elliptic curve, along with an isomorphism

$$\begin{aligned} \mathbb{C}/\Lambda &\xrightarrow{\sim} E(\Gamma) \\ z &\mapsto \left(\wp(z), \frac{\wp'(z)}{2}\right) \end{aligned}$$

where $\wp$ is the Weierstrass $\wp$-function,

$$E_{2k}(\tau) = 1 + (-1)^k \frac{4k}{B_{2k}} \sum_{n=0}^{\infty} \sigma_{2k-1}(n) q^n$$

is the normalized Eisenstein series with B_{2k} the Bernoulli numbers, so that

$$\begin{aligned} E_4(\tau) &= 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n = 1 + 240q + 2160q^2 + 6720q^3 + \dots \\ E_6(\tau) &= 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n = 1 - 504q - 16632q^2 - 122976q^3 + \dots, \end{aligned}$$

and finally

$$c_{2k}(\Lambda) = \left(\frac{2\pi}{6\omega_2}\right)^{2k} E_{2k}(\tau). \tag{4.4.3}$$

We now describe how we efficiently compute the composition $X(\Gamma) \to \mathbb{C}/\Lambda \to E(\Gamma)$

of the above maps.

4.4.2. Recursion for power series

Once we have computed the periods ω_1, ω_2, the formulas for c_4 and c_6 in terms of Eisenstein series immediately give us a (numerical) equation for the curve $E(\Gamma)$. However, we also require an explicit map $X(\Gamma) \to E(\Gamma)$ in order to determine the images of the ramification points of φ. To achieve this, we compose the two isomorphisms discussed above and compute explicit Laurent series.

We compute series expansions for the coordinate functions $x, y \colon X(\Gamma) \to E(\Gamma)$ on the Weierstrass model as the composition of the maps mentioned above, i.e.,

$$x(w) = \wp(\alpha(w)), \qquad y(w) = \frac{\wp'(\alpha(w))}{2} = \frac{x'(w)}{2}\,.$$

Thus it remains to compute Laurent series expansions for $\wp$ and $\wp'$. In terms of $\wp$ and $\wp'$, equation (4.4.2) becomes the differential equation

$$\left(\frac{\wp'(u)}{2}\right)^2 = \wp(u)^3 - 27c_4\wp(u) - 54c_6 \tag{4.4.4}$$

where u is the coordinate in $\mathbb{C}$. Writing

$$\wp(w) = \frac{1}{u^2} + \frac{a_{-1}}{u} + \sum_{n=0}^{\infty} a_n u^n \tag{4.4.5}$$

for the Laurent series of $\wp$, given c_4, c_6, then equation (4.4.4) yields a recurrence for the coefficients a_n. We have the initial condition $a_{-2} = 1$ and a laborious but straightforward calculation shows that

$$a_n = \frac{1}{n+3}\left(\frac{1}{4}\sum_{k=1}^{n+1}(n-k)(k-2)a_{n-k}a_{k-2} \right.$$
$$\left. - \left(\sum_{\substack{i+j+k=n+2 \\ 0\le i,j,k\le n+1}} a_{i-2}a_{j-2}a_{k-2}\right) + 27c_4a_{n-4} + 54c_6\chi[n=4]\right) \tag{4.4.6}$$

for $n \geq -1$, where

$$\chi[n=4] = \begin{cases} 1, & \text{if } n = 4; \\ 0, & \text{otherwise.} \end{cases}$$

Thus, given the values for c_4 and c_6, equation 4.4.6 allows us to compute as many terms of $x(w)$ and $y(w)$ as desired, and hence allows us to compute the isomorphism $X(\Gamma) \to E(\Gamma)$ to arbitrary w-adic precision.

4.4.3. Computing the Belyi map

We compute the expression of the Belyi map φ as a rational function in x and y as follows.

(1) Determine an appropriate Riemann–Roch space $\mathscr{L}(D)$.

(2) Compute a basis of $\mathscr{L}(D)$ in terms of x and y.

(3) Using numerical linear algebra, express φ as a linear combination of functions in this basis.

We make this precise as follows, proceeding similarly to [Javanpeykar and Voight, 2019, Lemma 3.2]. Let $\sigma = (\sigma_0, \sigma_1, \sigma_\infty)$ be a transitive permutation triple of degree d with corresponding elliptic Belyi map $\varphi : X \to \mathbb{P}^1$. Let s be the length of the cycle containing 1 in σ_0 and let $k_1, \dots k_r$ be the lengths of the remaining cycles in σ_0. Then the divisor of zeroes of φ (which is also the divisor of poles of $1/\varphi$) is

$$\operatorname{div}_0(\varphi) = \operatorname{div}_\infty(1/\varphi) = s\infty + \textstyle\sum_{i=1}^r k_i P_i$$

for some points $P_1, \dots, P_r \in X(\mathbb{C})$.

Since we do not have control over the points $P_1, \dots, P_r$, we "cancel" these poles by multiplying φ by a suitable function φ_0 that has zeroes at $P_1, \dots, P_r$ and has poles only at ∞. Such a φ_0 will belong to the space $\mathscr{L}(D) \subseteq \mathscr{L}(t\infty)$ where

$$D := -\textstyle\sum_{i=1}^r k_i P_i + t\infty \tag{4.4.7}$$

for some (as of yet undetermined) $t \in \mathbb{Z}_{\geq 0}$. Once we have obtained φ_0, then $\varphi_0/\varphi \in \mathscr{L}((s+t)\infty)$. As we will describe in the next step, we can write down a basis for Riemann–Roch spaces for divisors of the form $m\infty$, which allows us to compute φ_0 and $\varphi_\infty := \varphi_0/\varphi \in \mathscr{L}((s+t)\infty)$ with respect to this basis. Thus we have $\varphi = \varphi_0/\varphi_\infty$ for some $\varphi_0 \in \mathscr{L}(t\infty)$ and $\varphi_\infty \in \mathscr{L}((s+t)\infty)$.

It remains to determine a value of t so that such a φ_0 exists. Let $t = d - s + 1$. Since $\displaystyle\sum_{i=1}^r k_i = d - s$, then

$$\deg(D) = -(d-s) + t = s - d + d - s + 1 = 1\,.$$

Since X has genus 1, then every canonical divisor K_X of X has degree $2 \cdot 1 - 2 = 0$. Since we may take K_X to be effective, then $K_X = 0$ is a canonical divisor for X (cf., [Silverman, 2009, Example 5.7]). Applying Riemann–Roch to the divisor D, we find

$$\ell(D) - \ell(K_X - D) = 1 - g + \deg(D) = 1 - 1 + 1 = 1\,. \tag{4.4.8}$$

Since $K_X - D = 0 - D = -D$ has degree $\deg(-D) = -1 < 0$, then $\ell(K_X - D) = 0$. Then (4.4.8) simply becomes $\ell(D) = 1$, so there is a unique $\varphi_0 \in \mathscr{L}(D)$ as above, up to rescaling.

Since x and y have poles at ∞ of orders 2 and 3, respectively, then a basis for $\mathscr{L}(m\infty)$ is

$$\begin{cases} 1, x, y, xy, x^2, \ldots, x^{m/2} & \text{if } m \text{ is even} \\ 1, x, y, xy, x^2, \ldots, x^{\frac{m-3}{2}}y & \text{if } m \text{ is odd}\,. \end{cases} \tag{4.4.9}$$

This allows us to express φ_0 and φ_∞ as linear combinations of monomials in x and y, and hence express φ as a rational function in x and y. We illustrate this in the following example.

Example 4.4.3. The smallest degree d for which there exists a hyperbolic passport of genus one is $d = 4$, and there is a unique such passport with $(a, b, c) = (4, 3, 4)$ and representative triple

$$\sigma_0 = (1\ 2\ 4\ 3), \quad \sigma_1 = (1\ 2\ 3), \quad \sigma_\infty = (1\ 2\ 3\ 4).$$

Then $s = 4$, so $t = d - s + 1 = 1$ and we have $\varphi_0 \in \mathscr{L}(\infty)$ and $\varphi_\infty \in \mathscr{L}(5\infty)$. Bases for these spaces are, respectively, 1 and $1, x, y, x^2, xy$. Thus we can write

$$\varphi = u\frac{1}{b_0 + b_2x + b_3y + b_4x^2 + xy}$$

for some $u, b_0, b_2, b_3, b_4 \in \mathbb{C}$. Rearranging, we find that

$$b_0\varphi + b_2x\varphi + b_3y\varphi + b_4x^2\varphi + xy\varphi - u = 0$$

and hence there is a linear relation among $\varphi, x\varphi, y\varphi, x^2\varphi, xy\varphi, 1$. To compute this relation we write the coefficients of the numerical Laurent series for each of these functions as the entries of the rows of a matrix, and then compute its numerical kernel.

4.4.4. Newton's method

In [Klug et al., 2014, Example 5.28], we describe how to use Newton's method in the case of genus 0 to achieve very accurate approximations of the coefficients of the Belyi map, allowing us to quickly pass from tens of digits of precision to tens of thousands. We now explain how Newton's method can be extended to the case of genus 1 Belyi maps.

Let $\varphi\colon E \to \mathbb{P}^1$ be a Belyi map with E of genus 1 with $E = E(\Gamma)$ as in 4.4.2. In the genus 0 case one can determine equations satisfied by the coefficients of the Belyi map by simply writing down the required factorization pattern. However, this approach relies on the fact that the coordinate ring $\mathbb{C}[x]$ of the affine line $\mathbb{A}^1$ is a UFD. By contrast, the affine coordinate ring

$$\mathbb{C}[E] := \frac{\mathbb{C}[x,y]}{\langle y^2 - (x^3 - 27c_4x - 54c_6)\rangle} \tag{4.4.10}$$

is not a UFD. Nevertheless, since E is a nonsingular curve then $\mathbb{C}[E]$ is locally factorial: the local rings $\mathbb{C}[E]_P$ are DVRs for each affine point $P \in E(\mathbb{C})$, and we will see that this is enough for our purposes.

Let $P = (x_P, y_P) \in E(\mathbb{C})$ be an affine point and let $\xi := x - x_P$ and $\zeta := y - y_P$. Insisting that φ have a zero or pole of a given order at P imposes equations that can be determined by working in the completed local ring $\widehat{\mathbb{C}[E]}_P$ as follows.

If P is not a 2-torsion point of X, then $y_P \neq 0$ and ξ is a uniformizer for $\widehat{\mathbb{C}[E]}_P$. We solve for ξ in terms of ζ by substituting $x = \xi + x_P$ and $y = \zeta + y_P$ into the equation for E, thereby obtaining a quadratic equation in ζ

$$0 = \zeta^2 + 2y_P\zeta + \xi^3 + 3x_P\xi^2(3x_P^2 - 27c_4)\xi$$

whose solution is

$$\zeta = -y_P + y_P\sqrt{1 + \frac{\xi^3 + 3x_P\xi^2 + (3x_P^2 - 27c_4)\xi}{y_P^2}}\,. \tag{4.4.11}$$

If instead P is a 2-torsion point, then ζ is a uniformizer for $\widehat{\mathbb{C}[E]}_P$; substituting as above, we obtain a cubic equation for ξ in terms of ζ, which we solve via Hensel lifting. In either case, we may express the numerator and denominator of φ as power series in the local parameter.

Once this has been accomplished, we obtain the equations imposed by a zero (resp., pole) at P of order e_P by insisting that the first e_P coefficients of the series for the numerator or denominator, respectively, of φ vanish.

However, the system of polynomial equations from these considerations—from insisting that the ramification points lie on the curve and that φ have the desired ramification indices at each point—may still be underdetermined. In practice, we have often found that the number of equations obtained as above will be one less than the number of variables. In this case, we obtain more equations as follows. Recall from subsection 4.4.3 that s is the cycle of σ_0 containing 1 and $t = d - s + 1$. Then the divisor $(s+t)\infty = (d+1)\infty$ has degree $d+1$, so $\varphi_\infty \in \mathscr{L}((s+t)\infty)$ has degree at most $d+1$. But φ has degree d, so this means that φ_0 and φ_∞ must have a common zero at a point P_s. This common zero allows us to obtain enough equations. We adjoin two more variables x_s and y_s for the coordinates of P_s and obtain three more equations: the equation $y_s^2 = x_s^3 - 27c_4x_s - 54c_6$ since P_s lies on the elliptic curve, and the equations $\varphi_0(P_s) = \varphi_\infty(P_s) = 0$. This results in a system with as many equations as variables, which (assuming independence of the equations) has a unique solution, hence can be solved using Newton's method.

Newton's method has proven invaluable in our computations: it has allowed us to compute genus 1 maps that were previously out of reach, and has also sped up our computations considerably.

4.4.5. Example

We illustrate the above method with an example.

Example 4.4.4. Consider the passport $(1, S_7, (6^1 1^1, 6^1 1^1, 2^2 3^1))$ of size 13. Its pointed refinement taking the 6-cycle over 0 also has size 13. A representative permutation triple is

$$\sigma_0 = (1\ 2\ 3\ 4\ 5\ 6)(7), \qquad \sigma_1 = (1)(2\ 7\ 6\ 3\ 4\ 5), \qquad \sigma_\infty = (1\ 7\ 2)(3\ 5)(4\ 6). \quad (4.4.12)$$

Given this ramification data, then $d = 7$, $s = 6$, and $t = d - s + 1 = 2$ in the notation of subsection 4.4.3. The Riemann–Roch calculation shows that φ can be written as the ratio of an element of $\mathscr{L}(2\infty)$ by an element of $\mathscr{L}(8\infty)$. Since $1, x$

and $1, x, y, x^2, xy, \dots, x^4$ are bases for $\mathscr{L}(2\infty)$ and $\mathscr{L}(8\infty)$, respectively, factoring out leading coefficients, we can write

$$\varphi = u\frac{\varphi_0}{\varphi_\infty} = u\frac{a_0 + x}{b_0 + b_2x + b_3y + \cdots + b_7x^2y + x^4} \tag{4.4.13}$$

for some $u, a_0, b_0, b_2 \dots, b_7 \in \overline{\mathbb{Q}} \subset \mathbb{C}$, so $\varphi \in \mathscr{L}(2\infty)$ and $\varphi_\infty \in \mathscr{L}(8\infty)$. Computing with 40 decimal digits of precision (but only displaying 5), after 20 seconds on a standard CPU we find the initial approximation for X and φ. After normalizing the coefficients (which we discuss in detail in the next subsection) to get $b_7(= b_8) = 1$, we obtain

$$\begin{aligned} c_4, c_6 &\approx -0.00031, 0.0000035 \\ \varphi &\approx 0.0024\frac{-0.18587 + x}{-0.00042 + 0.00112x + \cdots + 0.03839x^3 + x^2y + x^4}. \end{aligned} \tag{4.4.14}$$

Let $P = (x_P, y_P)$ be the point corresponding to the 3-cycle in σ_∞. Since $P \in X(\mathbb{C})$, our first equation is $y_P^2 = x_P^3 - 27c_4x_P - 54c_6$. Computing ζ as in (4.4.11), we find

$$\begin{aligned} \zeta = {} & \frac{\frac{3}{2}x_P^2 - \frac{27}{2}c_4}{y_P}\xi + \frac{-\frac{9}{8}x_P^4 + \frac{81}{4}c_4x_P^2 + \frac{3}{2}x_Py_P^2 - \frac{729}{8}c_4^2}{y_P^3}\xi^2 \\ & + \frac{\frac{27}{16}x_P^6 - \frac{729}{16}c_4x_P^4 + \cdots + \frac{81}{4}c_4x_Py_P^2 + \frac{1}{2}y_P^4 - \frac{19683}{16}c_4^3}{y_P^5}\xi^3 + O(t^4)\,. \end{aligned} \tag{4.4.15}$$

Substituting $x = \xi + x_P$ and $y = \zeta + y_P$ into the above expression for φ_∞ yields

$$\begin{aligned} \varphi_\infty = {} & x_P^4 + x_P^3b_6 + x_P^2y_Pb_7 + x_P^2b_4 + x_Py_Pb_5 + x_Pb_2 + y_Pb_3 + b_0 \\ & + \left(\tfrac{3}{2}x_P^4b_7 + 4x_P^3y_P + \tfrac{3}{2}x_P^3 + \cdots + b_5 + y_Pb_2 - \tfrac{27}{2}c_4b_3\right)\frac{\xi}{y_P} \\ & + \left(-\tfrac{9}{8}x_P^6b_7 - \tfrac{9}{8}x_P^5b_5 + \cdots + \tfrac{729}{8}c_4^2b_3\right)\frac{\xi^2}{y_P^3} + O(\xi^3)\,. \end{aligned} \tag{4.4.16}$$

To impose the condition that φ has a pole of order 3 at P, we set the first three coefficients of φ_∞ equal to 0, giving 3 equations.

Proceeding similarly with the other ramification points, we obtain 22 polynomial equations in the 23 variables $u, c_4, c_6, a_0, b_0, \ldots, b_7$ and x_P, y_P for each of the ramification points, other than the point corresponding to the cycle containing 1 in σ_0. (The point corresponding to this cycle is ∞, and we have already imposed the condition that φ vanishes to order 6 at ∞ by taking $\varphi_0 \in \mathscr{L}(2\infty) \setminus \mathscr{L}(\infty)$ and $\varphi_\infty \in \mathscr{L}(8\infty) \setminus \mathscr{L}(7\infty)$.) This system is underdetermined, so in order to apply Newton's method we must find at least one more equation. We observe that although φ is a degree 7 map, φ_∞ has degree 8, so there must be a common zero of φ_0 and φ_∞. Calling this point $P_s = (x_s, y_s)$, we obtain three more equations

$$\begin{gathered} y_s^2 = x_s^3 - (27c_4x_s - 54c_6) \qquad 0 = \varphi_0(P_s) = a_0 + x_s \\ 0 = \varphi_\infty(P_s) = b_0 + b_2x_s + b_3y_s + \cdots + b_7x_s^2y_s + x_s^4 \,. \end{gathered} \tag{4.4.17}$$

We have adjoined two more variables x_s, y_s and produced three more equations to ensure non-degeneracy. This produces a system of 25 equations in 25 variables. Applying Newton's method to this system, in 16.20 seconds we obtain approximations of coefficients with 2000 digits of precision, which allows us to recognize the coefficients of φ as algebraic numbers. After a change of variables to reduce the size of the output, we find the elliptic curve

$$X\colon y^2 = x^3 - (24\nu + 75)x + \tfrac{1}{2}(-657\nu^2 - 1014\nu + 3278) \tag{4.4.18}$$

and Belyi map $\varphi = u\varphi_0/\varphi_\infty$ where $u = 1/(2^9 3^2)$ and

$$\begin{aligned}
\varphi_0 &= (-419\nu^2 - 358\nu + 2947) + 49x \\
\varphi_\infty &= (-806361\nu^2 - 724014\nu + 5449304) + (-3150\nu^2 - 15652\nu + 84560)x \\
&\qquad + (-11310\nu^2 + 17940\nu + 118656)y + (-33180\nu^2 + 74760\nu - 55104)x^2 \\
&\qquad + (59556\nu^2 - 189336\nu + 233856)xy + (5166\nu^2 - 16380\nu + 20720)x^3 \\
&\qquad + (-59022\nu^2 + 184980\nu - 225792)x^2y + (25557\nu^2 - 80122\nu + 97832)x^4
\end{aligned}$$

over the number field $\mathbb{Q}(\nu)$ where $\nu^3 - 6\nu + 12 = 0$. It turns out that this passport decomposes into two Galois orbits, one of size 3 as shown above, and the other of size 10. The coefficients of the Belyi map for the size 10 orbit are too large for us to display here, but it is defined over the number field $\mathbb{Q}(\mu)$ where

$$\mu^{10} - 2\mu^9 + 15\mu^8 - 78\mu^7 + 90\mu^6 + 48\mu^5 + 90\mu^4 - 78\mu^3 + 15\mu^2 - 2\mu + 1 = 0\,. \quad (4.4.19)$$

One can find the full data for this Galois orbit at `http://beta.lmfdb.org/Belyi/7T7/%5B6%2C6%2C6%5D/61/61/322/g1/b`.

Remark 4.4.5. The "extra zero" phenomenon described in subsection 4.4.4 can be avoided in the special case when 0 is totally ramified (i.e., when σ_0 is a d-cycle).

4.4.6. Normalization

Once the coefficients of the curve and map have been computed to sufficiently high precision, it remains to normalize them and recognize them as algebraic numbers.

As shown in [Silverman, 2009, III §1], (cf., Table 3.1 and the discussion following it), given a Weierstrass model $y^2 = x^3 + Ax + B$ for an elliptic curve over $\mathbb{C}$, the only change of variables preserving the form of the equation is

$$x = \lambda^2 x' \quad \text{and} \quad y = \lambda^3 y' \tag{4.4.20}$$

for some $\lambda \in \mathbb{C}^\times$, which then rescales the coefficients and discriminant by

$$A = \lambda^4 A', \quad B = \lambda^6 B', \quad \Delta = \lambda^{12}\Delta' . \tag{4.4.21}$$

Since the curve $E : y^2 = x^3 - 27c_4x - 54c_6$ admits a Belyi map, then E has a model defined over $\overline{\mathbb{Q}}$ by Belyi's theorem (Theorem 4.2.2). Thus there exists $\lambda \in \mathbb{C}^\times$ such that $c_4/\lambda^4, c_6/\lambda^6 \in \overline{\mathbb{Q}}$. Moreover, the Belyi map φ itself can also be defined over $\overline{\mathbb{Q}}$, so we can find a rescaling factor λ so that the coefficients of φ also belong to $\overline{\mathbb{Q}}$.

Under such a change of variable, a monomial ax^iy becomes $a(\lambda^2x)^i(\lambda^3y) = \lambda^{2i+3}ax^iy$. Thus the coefficients of the Belyi map, when written as a ratio of linear combinations of monomials in x and y, belong to a weighted projective space, where the weight is given by the order of pole at ∞ (the identity of the group law) of the corresponding monomial.

For instance, suppose that the monomials a_4x^2 and a_5xy both appear in the expression for φ and a_4 and a_5 are nonzero. Considering $[a_4 : a_5]$ as an element of the weighted projective space $\mathbb{P}(4 : 5)$, then

$$[a_4 : a_5] = \lambda[a_4 : a_5] = [\lambda^4 a_4 : \lambda^5 a_5]$$

for any $\lambda \in \mathbb{C}^\times$. Since the weights 4 and 5 are relatively prime, then we can find a representative for $[a_4 : a_5]$ where the components are equal: insisting that λ is chosen so that $\lambda^4 a_4 = \lambda^5 a_5$, we solve for λ as

$$a_4/a_5 = \lambda^5/\lambda^4 = \lambda\,.$$

More generally, let $w_1, \dots, w_t$ be the weights of the (numerically) nonzero coefficients of the Belyi map. If $\gcd(w_1, \dots, w_t) = 1$ we can still compute the rescaling factor λ as the product of these coefficients raised to the appropriate powers. If instead $\gcd(w_1, \dots, w_t) = m > 1$, then all coefficients appearing in the Belyi map have weight divisible by m, hence will be rescaled by a power of λ^m. Then we need only determine λ^m, which again can be accomplished as in the case where $\gcd(w_1, \dots, w_t) = 1$. We illustrate the case where $\gcd(w_1, \dots, w_t) = 1$ in the following example.

Example 4.4.6. Consider the permutation triple $\sigma = (\sigma_0, \sigma_1, \sigma_\infty)$ where

$$\sigma_0 = (1\ 4\ 2\ 5\ 3), \qquad \sigma_1 = (1\ 2\ 3)(4\ 5), \qquad \sigma_\infty = (1\ 2\ 5)(3\ 4)\,.$$

Then σ belongs to the passport $(1, S_5, ((5), (3,2), (3,2))$ and one can show that this passport has pointed size 1, hence σ is the unique representative up to simultaneous conjugacy. Computing as described above, we find the corresponding Belyi map as the rational function

$$\varphi = \frac{a_0}{b_0 + b_3 y + b_5 xy}$$

defined on the elliptic curve $E : y^2 = x^3 - 27c_4x - 54c_6$ where

$$c_4 \approx -0.02600 + 0.01889i \quad c_6 \approx -0.00682 - 0.00495i \quad a_0 \approx 0.21234 - 0.46856i$$
$$b_0 \approx 0.10617 + 0.23427i \quad b_3 \approx -0.21576 - 0.23646i \quad b_5 \approx 0.68570 - 0.31074i\,.$$

(For this example we computed with 50 decimal digits of precision, but display only 5.) Letting $b_i' = b_i/a_0$ for $i = 0, 3, 5$, then

$$\varphi = \frac{1}{b_0' + b_3'y + b_5'xy}$$

and $b_0' \approx 0.5000$. Note that in this example there are no nonzero coefficients with consecutive weights. However the nonzero weights 3 and 5 have $\gcd(3, 5) = 1$, so we can still find a suitable rescaling factor. Since $2 \cdot 3 + (-1) \cdot 5 = 1$, we let

$$\lambda = b_5'/b_3'^2 \approx -2.22147 + 3.05758i\,.$$

Replacing (x, y) by $(\lambda^2 x, \lambda^3)$ has the effect of multiplying b_3' by λ^3 and b_5' by λ^5. Letting $b_i'' = \lambda^i b_i'$ for $i = 0, 3, 5$, then

$$b_3'' \approx -33.592320000000000000000000000000000000000002133650 + 10^{-43}i$$
$$b_5'' \approx -1128.44396298240000000000000000000000000001433485 + 10^{-41}i$$

which appear rational. Similarly, letting $c_4' = c_4/\lambda^4$ and $c_6' = c_6/\lambda^6$, then

$$c_4' \approx 0.000157542406720776195189821259040329175775729284508\,09 - 10^{-48}i$$

$$c_6' \approx -2.89206434122874872491856600183820761397346339254\,65 \cdot 10^{-6} + 10^{-49}i$$

which at least appear real, and turn out to be rational.

Once the coefficients of the curve and Belyi map have been normalized to be (putatively) algebraic, it remains to recognize them as such. We first find a bound on the degree of the number field containing the coefficients. As discussed in subsection 4.2.3, the degree of the number field over which the pointed Belyi map φ is defined is bounded by the size of its pointed passport. With this bound in hand, we can recognize the numerical approximations of the coefficients by using, for instance, LLL, as implemented in `Magma`'s `PowerRelation` command. We illustrate this by continuing Example 4.4.6, completing the computation.

Example 4.4.7. Recognizing the numerical approximations above, we find

$$b_0'' = \frac{1}{2} \qquad b_3'' = -\frac{104976}{3125} = -\frac{2^4 3^8}{5^5} \qquad b_5'' = -\frac{11019960576}{9765625} = -\frac{2^8 3^{16}}{5^{10}}$$

$$c_4' = \frac{1953125}{12397455648} = \frac{5^9}{2^5 3^{18}} \qquad c_6' = -\frac{45166015625}{15617223649253376} = -\frac{5^{13} 37}{2^{11} 3^{27}}$$

and thus obtain the Belyi map

$$\varphi = \frac{1}{\frac{1}{2} - \frac{104976}{3125} y - \frac{11019960576}{9765625} xy}$$

defined on the elliptic curve

$$E : y^2 = x^3 - \frac{1953125}{459165024}x + \frac{45166015625}{289207845356544}\,.$$

We can simplify the equations for the map and the curve by computing the minimal model $E_{\min}$ of the elliptic curve and pushing the Belyi map forward along the isomorphism $E \overset{\sim}{\to} E_{\min}$. Performing these calculations in Magma, we obtain the map

$$\varphi_{\min} = \frac{1}{\frac{1}{2} + \frac{5}{324}y + \frac{1}{324}xy} = \frac{324}{162 + 5y + xy}$$

defined on the elliptic curve

$$E_{\min} : y^2 = x^3 - 120x + 740\,,$$

which has discriminant $\Delta(E_{\min}) = -2^8 3^9 5^2$.

4.4.7. Results

Using the method described above, we have computed a large collection of elliptic Belyi maps in low degree. In particular, we have produced an exhaustive list of elliptic Belyi maps of degree $d \leq 7$. This data is available at `http://beta.lmfdb.org/Belyi/` and the raw text files comprising the database are available at `https://github.com/michaelmusty/BelyiDB`.

Theorem 4.4.8. *There are* 118 *Galois orbits of elliptic Belyi maps with degree* $d \leq 7$. *They are distributed with respect to degree as shown in the table below.*

Proof. This is an easy observation from our data, which includes equations for each

d	Number of orbits
3	1
4	2
5	7
6	35
7	73

of these Galois orbits. □

We conclude this section with a look at the completeness of our computations in higher degree. In the following table, the second column records the number of genus 1 passports in each degree $d \leq 9$. The last column records the number of passports that we have computed completely, i.e., such that we have computed equations for *every* isomorphism class in this passport.

d	Total number of passports	Computed
3	1	1
4	2	2
5	6	6
6	29	29
7	50	50
8	217	83
9	427	33

We hope to extend our computations to higher degree in future work.

One practical obstacle arises due to the "extra point" phenomenon described in subsection 4.4.4. To find an extra point we seek a common zero of two polynomials with coefficients in $\mathbb{C}$. Loss of numerical precision in factoring these polynomials may make it appear that the polynomials have no roots in common, preventing us from finding an extra point. And even when we succeed in finding an extra point, we often only know it to a much lower numerical precision. If the loss of precision is too large, it may cause our initial values to fall outside the basin of convergence for Newton's method.

The existence of large Galois orbits presents a genuine obstacle. If a passport contains a large Galois orbit, then the corresponding Belyi maps will be defined over a number field of large degree (the size of the orbit). The amount of numerical precision required to recognize these coefficients may figure in the thousands or tens of thousands of decimal digits. Our approach using Newton's method has helped in this regard, as it provides us with much higher numerical precision. For instance, it has allowed us to successfully compute all maps associated to the passport $(1, S_7, ((6,1),(6,1),(4,2,1)))$, which has size 32.

Section 4.5

Hyperelliptic Belyi Maps

This section is based on joint work with Musty, Sijsling, and Voight, specifically [Musty et al., 2019, §6]. Our main result is a numerical method for computing hyperelliptic Belyi maps, that is, Belyi maps defined on hyperelliptic curves. We then use this method to compute an exhaustive database of Belyi maps of low degree. Throughout this section we assume that $X(\Gamma)$ is hyperelliptic (and has genus ≥ 2).

4.5.1. Setup

Definition 4.5.1. Let K be a field of characteristic 0 and let X be a curve over K of genus ≥ 2. Then X is *hyperelliptic* if there exists a morphism $X \to \mathbb{P}^1_K$ of degree 2.

Remark 4.5.2. Some authors instead use a broader definition, defining X to be hyperelliptic if there is a degree 2 morphism $X \to C$ with C a smooth projective conic. As we compute *pointed* Belyi maps, this distinction will be inconsequential: we insist that the curve X has a K-rational point P, which maps to a K-rational point of C. A conic with a K-rational point is isomorphic to $\mathbb{P}^1_K$, and composing with this isomorphism yields a degree 2 map $X \to \mathbb{P}^1_K$.

Recall that a hyperelliptic curve H of genus $g \geq 2$ over K has a model

$$H\colon y^2 + u(x)y = v(x) \tag{4.5.1}$$

where $\deg(u) \leq g+1$ and $\deg(v) \leq 2g+2$. Letting $f(x) := u(x)^2 + 4v(x)$, we have $f(x)$ separable with $\deg f(x) = 2g+1$ or $2g+2$; we refer to the model as *even* or *odd* according to the parity of $\deg f(x)$. Note that an odd model has the single point $\infty = (1 : 0 : 0)$ at infinity while an even model has two, $\infty' = (1 : \sqrt{f_0} : 0)$ and $\infty = (1 : -\sqrt{f_0} : 0)$ where f_0 is the leading coefficient of $f(x)$, i.e., the point ∞ is a Weierstrass point if and only if the model is odd.) In constructing the Belyi map, in both cases we take ∞ to be the marked point (around which we expand series), and by convention it corresponds to the cycle containing 1 in σ_0.

For more background on hyperelliptic curves, we refer the reader to [Liu, 2002, §7.4.3].

4.5.2. Numerical test for hyperellipticity

Before we can apply our method for computing hyperelliptic Belyi maps, we must first determine whether the map at hand is indeed hyperelliptic. Below we describe a procedure for determining if the source curve $X(\Gamma)$ appears to be hyperelliptic (over $\mathbb{C}$) up to the working numerical precision.

Let Γ be a triangle subgroup with $X = X(\Gamma)$ of genus $g \geq 2$. We test if X is numerically hyperelliptic (in the sense the curve appears to be hyperelliptic to the precision computed) as follows. First, we compute power series expansions of an *echelonized* basis $f_1, f_2, \dots, f_g$ of $S_2(X(\Gamma))$. We have an isomorphism $S_2(X(\Gamma)) \cong \Omega(X(\Gamma))$ given by $f(z) \mapsto f(z)\,\mathrm{d}z$ where $\Omega(X(\Gamma))$ is the $\mathbb{C}$-vector space of holomorphic differential 1-forms on $X(\Gamma)$. If X is hyperelliptic with model a model H as in (4.5.1), since $f_1, \dots, f_g$ is an echelonized basis we have the further isomorphism

$$\begin{aligned} \Omega(X(\Gamma)) &\xrightarrow{\sim} \Omega(H) \\ f_i(z)\,\mathrm{d}z &\mapsto x^{g-i}\frac{\mathrm{d}x}{y} \end{aligned} \tag{4.5.2}$$

for $i = 1, \dots, g$. Thus, to recover x, y defined on $X(\Gamma)$, we can take

$$x := f_1/f_2 \qquad\qquad y := x'/f_g \tag{4.5.3}$$

since

$$\frac{f_1}{f_2} = \frac{x^{g-1}\,\mathrm{d}x/y}{x^{g-2}\,\mathrm{d}x/y} = x \qquad \frac{x'}{f_g} = \frac{\mathrm{d}x}{\mathrm{d}x/y} = y \tag{4.5.4}$$

where x' denotes the derivative of x with respect to z (the coordinate in $\mathcal{H}$). If the model is odd, then $\mathrm{ord}_\infty x = -2$ and $\mathrm{ord}_\infty y = -(2g+1)$; if the model is even, then $\mathrm{ord}_\infty x = -1$ and $\mathrm{ord}_\infty y = -(g+1)$.

Consider the rational map $X(\Gamma) \dashrightarrow \mathbb{A}^2_{\mathbb{C}}$ with coordinates x, y. We test if there is an approximate linear relation among

$$1, x, \dots, x^{2g+2}, y, xy, \dots, x^{g+1}y, y^2 \in \mathbb{C}[[w]] \tag{4.5.5}$$

by using numerical linear algebra on their series expansions. If there is such a relation, we obtain a rational map from X to a hyperelliptic curve $X' \subseteq \mathbb{A}^2$. If $g(X') = g(X)$, then the Riemann–Hurwitz formula implies that this map is birational, hence X' is a model of X as in (4.5.1). If no such relation exists, then we conclude that X is not numerically hyperelliptic.

Remark 4.5.3. If X has genus 2, then X is automatically hyperelliptic (and the above test will yield an equation). If X has genus 3, then X is hyperelliptic (over $\mathbb{C}$) if and only if the functions f_1, f_2, f_3 satisfy a quadratic relation (over $\mathbb{C}$), which shows that the (numerical) image of the canonical map is a plane conic.

Example 4.5.4. Consider the degree 7 triple

$$\sigma = ((1,2,3,4,5,6,7),(1,2,3,4,5,6,7),(1,6,4,2,7,5,3))$$

which belongs to the passport $(3, G, ((7),(7),(7)))$, where $G \cong \mathbb{Z}/7\mathbb{Z}$ has transitive group label $\mathsf{7T1}$.

We compute with 50 digits of precision. Defining the coordinate functions x and y as in (4.5.3), we then form the power series for the monomials $1, x, \dots, x^8, y, xy, \dots, x^4y$ and y^2. We record the first 30 terms of each of these series as a row of a 15×30 matrix. Computing the numerical kernel of this matrix, we find that the kernel is 1-dimensional. We obtain the numerical linear relation (displayed with 5 digits of precision)

$$0 \approx (3.99999)x - 0.99999x^8 + y^2$$

which we easily recognize as the equation $y^2 = x^8 - 4x$ for our curve. Thus the Belyi map corresponding to this triple is hyperelliptic.

Example 4.5.5. Consider the degree 7 triple

$$\sigma = ((1\ 4\ 7\ 3\ 6\ 2\ 5), (1\ 4\ 6\ 5\ 7\ 2\ 3), (1\ 6\ 2\ 4\ 3\ 5\ 7))$$

which belongs to the passport $(3, G, ((7), (7), (7)))$, where $G \cong \mathrm{GL}_3(\mathbb{F}_2)$ has transitive group label 7T5.

We proceed as in the previous example. However, this time we find that the numerical kernel of the matrix is trivial, indicating that, up to numerical precision, the Belyi map corresponding to σ is not hyperelliptic. Indeed, it turns out that the Belyi map corresponding to σ is defined on a (non-hyperelliptic) quartic plane curve; cf., [Klug et al., 2014, Example 5.27].

4.5.3. Computing the Belyi map

If the above test for hyperellipticity is positive, we obtain a (numerical) equation for the curve X, so it remains to compute the Belyi map. Suppose now that X is hyperelliptic with model as in (4.5.1). We compute the expression of the Belyi map φ as a rational function in x and y using the same strategy as in the genus 1 case, namely:

(1) Determine an appropriate Riemann–Roch space $\mathscr{L}(D)$.

(2) Compute a basis of $\mathscr{L}(D)$ in terms of x and y.

(3) Using numerical linear algebra, express φ as a linear combination of functions in this basis.

We again use the notation from subsection 4.4.3. Let $\sigma = (\sigma_0, \sigma_1, \sigma_\infty)$ be a transitive permutation triple of degree d with corresponding hyperelliptic Belyi map

$\varphi : X \to \mathbb{P}^1$ of genus g. Let s be the length of the cycle containing 1 in σ_0 and let $k_1, \ldots k_r$ be the lengths of the remaining cycles in σ_0. As before, we seek an integer t such that we may write $\varphi = \dfrac{\varphi_0}{\varphi_\infty}$ with $\varphi_0 \in \mathscr{L}(t\infty$ and $\varphi_\infty \in \mathscr{L}((s+t)\infty)$.

As before, let

$$D := -\textstyle\sum_{i=1}^{r} k_i P_i + t\infty\,. \tag{4.5.6}$$

Applying Riemann-Roch to D yields

$$\ell(D) \geq \ell(D) - \ell(K_X - D) = 1 - g + \deg(D) = 1 - g + (s - d + t)\,. \tag{4.5.7}$$

Thus to ensure that $\ell(D) \geq 1$, it suffices to have the inequality

$$1 - g + s - d + t \geq 1\,,$$

i.e., $t \geq d - s + g$. Thus we may take $t = d - s + g$. (This conclusion actually does not require X to be hyperelliptic.) Unlike in the elliptic case, with this choice of t we may still have $\ell(t\infty) > 1$. In this case, we can repeatedly replace t by $t-1$ until $\ell(t\infty) = 1$.

Next, we explain how to compute bases for $\mathscr{L}(t\infty)$ and $\mathscr{L}((s+t)\infty)$ as in step 2. In the case of an odd model, this basis is particularly simple: x and y have poles at ∞ of orders 2 and $2g+1$, respectively, so

$$1, x, x^2, \ldots, x^{\lfloor m/2 \rfloor}, y, xy, \ldots, x^{\lfloor \frac{m-(2g+1)}{2} \rfloor} y \tag{4.5.8}$$

is a basis for $\mathscr{L}(m\infty)$. In the case of an even model the situation is more complicated. Now $x, y \notin \mathscr{L}(m\infty)$ because they also have poles at ∞'. We compute a basis for

$\mathscr{L}(m\infty)$ as follows. Since x has a simple pole at ∞' we know $\xi := 1/x$ has a simple zero, and hence is a uniformizing parameter at ∞'. (At this stage in the computation we have only complex approximations to the coefficients of the curve $X = X(\Gamma)$, so Magma's built-in functions for computing Riemann–Roch bases, which require curves defined over an exact field, cannot be used.) Working in the completed local ring $\widehat{\mathscr{O}}_{X,\infty'} \simeq \mathbb{C}[[\xi]]$, we can express y as a Laurent series in ξ via

$$y = \frac{1}{2}\left(-u(1/\xi) \pm \sqrt{u(1/\xi)^2 + 4v(1/\xi)}\right). \tag{4.5.9}$$

We consider the series expansion for $y(w)$ in order to choose correct sign in (4.5.9). For each $j \in \{0, \ldots, m-(g+1)\}$ we compute the Laurent tail $P_j \in \mathbb{C}[1/\xi] = \mathbb{C}[x]$ of $x^j y$, so that $x^j y - P_j$ is holomorphic at ∞'. In this way we obtain the basis

$$1, y - P_0, xy - P_1, \ldots, x^{m-(g+1)}y - P_{m-(g+1)} \tag{4.5.10}$$

for $\mathscr{L}(m\infty)$. We illustrate the above procedure in the following example.

Example 4.5.6. Consider the passport $(2, G, (6^1, 6^1, 3^2))$, where $G := 2A_4(6) \cong A_4 \times C_2$ has transitive group label 6T6. The pointed passport has size 1, with representative triple

$$\sigma_0 = (1\ 6\ 2\ 4\ 3\ 5), \quad \sigma_1 = (1\ 3\ 5\ 4\ 6\ 2), \quad \sigma_\infty = (1\ 3\ 5)(2\ 4\ 6). \tag{4.5.11}$$

Computing the coordinate functions x, y as in (4.5.3) to 50 digits (displaying 5), we find approximate series

$$\begin{aligned} x &\approx 0.99999w^{-1} - 0.79370w - 0.31498w^3 + O(w^4) \\ y &\approx -0.99999w^{-3} - 0.79370w^{-1} - 0.94494w - 0.02142w^3 + O(w^4)\,. \end{aligned} \tag{4.5.12}$$

Since the series for y has a pole of order $3 = g + 1$, we are in the case of an even model. Forming the matrix of coefficients of the monomials

$$1, x, x^2, x^3, x^4, x^5, x^6, y, xy, x^3y, y^2\,, \tag{4.5.13}$$

we find a hyperelliptic equation as in (4.5.1) with $u = 0$ and

$$v \approx 1.00000x^6 + 6.34960x^4 + 15.11905x^2 + 11.99999 \tag{4.5.14}$$

This gives the local expansion

$$\begin{aligned} y &= \sqrt{v(1/\xi)} = \sqrt{1.00000\xi^{-6} + 6.34960\xi^{-4} + 15.11905\xi^{-2} + 11.99999} \\ &= 1.00000\xi^{-3} + 3.17480\xi^{-1} + 2.51984\xi - 1.99999\xi^3 + O(\xi^4)\,. \end{aligned} \tag{4.5.15}$$

Thus the Laurent tail of y is $1.00000x^3 + 3.17480x$, and the first nonconstant element of our basis for $\mathscr{L}(m\infty)$ for $m \geq 3$ is

$$\begin{aligned} &y - (1.00000x^3 + 3.17480x) \\ &\qquad \approx -2.00000w^{-3} - 1.58740w^{-1} + 0.62996w - 0.04285w^3 + O(w^4) \end{aligned} \tag{4.5.16}$$

and we compute the remaining elements of the basis similarly.

4.5.4. Normalization

As in the case of genus 1 Belyi maps considered in subsection 4.4.6, we can consider the coefficients of a Belyi map as belonging to a weighted projective space, with weights given by the order of pole at ∞ of the corresponding monomial. Again, provided the weights of the nonzero coefficients of the Belyi map have gcd 1, we can compute the rescaling factor λ as a product of these coefficients raised to appropriate powers. We illustrate this, continuing the computation from the previous example.

Example 4.5.7. Let σ be as in Example 4.5.6. Computing as described above, we find the corresponding Belyi map as the rational function

$$\varphi = \frac{a_0}{b_0 + b_4 f_4 + b_6 f_6} \approx \frac{-1.00000}{-1.99999 + 0.79370 f_4 + 0.50000 f_6}\,,$$

where

$$\begin{aligned} f_4 &\approx xy - (1.00000x^4 + 3.17480x^2) \\ f_4 &\approx x^3y - (1.00000x^6 + 3.17480x^4 + 2.51984x^2) \end{aligned}$$

defined on the hyperelliptic curve $X : y^2 = c_6x^6 + c_4x^4 + c_2x^2 + c_0$ where

$$c_0 \approx 12.00000 \qquad c_2 \approx 15.11905 \qquad c_4 \approx 6.34960 \qquad c_6 \approx 1.00000\,.$$

(For this example we computed with 50 decimal digits of precision, but display only 5.) We observe that all basis functions have poles at $w = 0$ (equivalently, at ∞) of even order, so it suffices to compute λ^2, the square of the rescaling factor. Since f_4

and f_6 have poles of orders 4 and 6, then we may take

$$\lambda^2 = \frac{b_4}{b_6} \approx 1.58740\,.$$

Replacing (f_4, f_6) by $(\lambda^4 f_4, \lambda^6 f_6)$ transforms the Belyi map by

$$\varphi = \frac{a_0}{b_0 + \lambda^4 b_4 f_4 + \lambda^6 b_6 f_6} \approx \frac{-1.00000}{-1.99999 + 1.99999 f_4 + 1.99999 f_6}$$

whose coefficients are easily recognized as rational numbers. Replacing (x, y) by $(\lambda x, \lambda^3 y)$ transforms the equation of the curve by

$$\lambda^6 y^2 = \lambda^6 c_6 x^6 + \lambda^4 c_4 x^4 + \lambda^2 c_2 x^2 + c_0$$

and dividing through by λ^6 to maintain a Weierstrass equation, we have

$$\begin{aligned} y^2 &= c_6 x^6 + \lambda^{-2} c_4 x^4 + \lambda^{-4} c_2 x^2 + \lambda^{-6} c_0 \\ &\approx 1.00000 x^6 + 4.00000 x^4 + 6.00000 x^2 + 3.00000 \end{aligned}$$

which is easily recognized as $y^2 = x^6 + 4x^4 + 6x^2 + 3$. We recompute the Riemann-Roch basis as before, now using this curve, and obtain

$$f_4 = xy - (x^4 + 2x^2) \quad \text{and} \quad f_6 = x^3 y - (x^6 + 2x^4 + x^2)\,.$$

Using the coefficients for the Belyi map computed above, we have

$$\begin{aligned}\varphi &= \frac{-1}{-2+2(xy-(x^4+2x^2))+2(x^3y-(x^6+2x^4+x^2))} \\ &= \frac{1}{1+3x^2+3x^4-xy+x^6-x^3y} = \frac{x^4+2x^2+xy+1}{2(x^2+1)^2}\,.\end{aligned}$$

To show that this map has the correct ramification, we compute the divisors of φ and $\varphi-1$, obtaining

$$\begin{aligned}\operatorname{div}(\varphi) &= 6(1:-1:0)-3(i:0:1)-3(-i:0:1) \\ \operatorname{div}(\varphi-1) &= 6(1:1:0)-3(i:0:1)-3(-i:0:1)\end{aligned} \tag{4.5.17}$$

where $i^2+1=0$.

4.5.5. Results

Using the method described above, we have computed a modest collection of hyperelliptic Belyi maps in low degree. In particular, we have produced an exhaustive list of hyperelliptic Belyi maps of degree $d \le 6$.

Theorem 4.5.8. *There are* 12 *Galois orbits of hyperelliptic Belyi maps with degree* $d \le 6$*. There are* 4 *orbits of Belyi maps in degree* 5 *and 8 orbits in degree* 6*.*

Proof. Again, this is an easy observation from our data, available at `http://beta.lmfdb.org/Belyi/`. □

Example 4.5.9. The passport $(3, C_7, (7^1, 7^1, 7^1))$ produces interesting results. It has size 5 and decomposes into 5 Galois orbits, each of size 1. Three of these orbits produce the hyperelliptic Belyi maps

$$\begin{aligned} X : y^2 &= x^8 - 2x, & \varphi &= \frac{y + x^4}{2x^4} \\ X : y^2 &= x^8 + 16x, & \varphi &= -\frac{x^3 y + x^7}{8} \\ X : y^2 &= x^8 + 2x, & \varphi &= x^3 y + x^7 + 1 \end{aligned}$$

while the remaining two are defined on the Klein quartic $X\colon xy^3 + x^3 + y = 0$, one given by $\varphi = -xy^2$ and the other by $\varphi = xy^2 + 1$. (Note that these maps are related by the automorphism $x \mapsto 1 - x$ of $\mathbb{P}^1$.)

We conclude this section with a look at the completeness of our computations in higher degree. In the following table, each entry records our computation of passports in a given degree $d \leq 7$ and genus $g \in \{2, 3\}$. The denominator is the total number of passports for the given genus and degree, while the numerator is the number of passports that we have computed completely, i.e., such that we have computed equations for *every* isomorphism class in this passport.

d \ g	2	3
5	2/2	0
6	7/7	0
7	7/13	2/3

As in the case of elliptic Belyi maps, the main obstruction to completing the computations indicated in the table above is the presence of large passports. In degree 7 and genus 2, the passports that remain to be computed have sizes 12, 20, 20 24, 24, and 38, and the remaining passport in degree 7 and genus 3 has size 23. Some of these passports decompose into Galois orbits, some of which are of moderate size, but the larger orbits require too much numerical precision for us to compute equations for the entire passport.

We conclude this section with an examination of the completeness of our computations in low degree for all genera. The denominator of each entry gives the total number of passports in a given degree and genus, while the numerator specifies how many these passports we have computed completely, i.e., such that we have computed equations for *every* isomorphism class in the passport.

$d \backslash g$	0	1	2	3	≥ 4	total
1	1/1	0	0	0	0	1/1
2	1/1	0	0	0	0	1/1
3	2/2	1/1	0	0	0	3/3
4	6/6	2/2	0	0	0	8/8
5	12/12	6/6	2/2	0	0	20/20
6	38/38	29/29	7/7	0	0	74/74
7	89/89	50/50	7/13	2/3	0	148/155
8	243/261	83/217	0/84	0/11	0	326/573
9	410/583	33/427	0/163	0/28	0/6	443/1207
total	802/993	204/732	16/269	2/42	0/6	1024/2042

We hope to extend our computations to higher degree in future work. In particular, we hope to implement an approach using Newton's method for hyperelliptic Belyi maps similar to the one used in the case of elliptic Belyi maps. Such an implementation would allow us to overcome the presence of large passports and compute a much larger range of degrees, in addition to speeding up our computations.

In the longer term, we hope to further analyze the data we have computed, especially concerning the Galois action. In particular, for each passport that decomposes into multiple Galois orbits, we seek to find some sort of explanation for this reducibility. For instance, suppose that (g, G, λ) is a passport and C is the triple of conjugacy classes of S_d corresponding to λ. Suppose $\widetilde{G}$ is a central extension of G. If one or more of the conjugacy classes in C split into several conjugacy classes when considered in $\widetilde{G}$, then we expect that the passport (g, G, λ) will decompose into multiple Galois orbits. This approach is studied extensively in [Roberts, 2018], which includes many examples.

We hope that such analysis may help us to better understand this important and mysterious group, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Bibliography

[Anderson et al., 2018] Anderson, J., Bouw, I. I., Ejder, O., Girgin, N., Karemaker, V., and Manes, M. (2018). Dynamical belyi maps. In *Women in Numbers Europe II*, pages 57–82. Springer.

[Assem et al., 2006] Assem, I., Simson, D., and Skowroński, A. (2006). *Elements of the representation theory of associative algebras. Vol. 1*, volume 65 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge. Techniques of representation theory.

[Belyi, 1980] Belyi, G. (1980). On Galois extensions of a maximal cyclotomic field. *Mathematics of the USSR-Izvestiya*, 14(2):247.

[Benson, 1998] Benson, D. J. (1998). *Representations and cohomology. I*, volume 30 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition. Basic representation theory of finite groups and associative algebras.

[Birch, 1994] Birch, B. (1994). Noncongruence subgroups, covers and drawings. In Schneps, L., editor, *The Grothendieck Theory of Dessins d'Enfants*, London Mathematical Society Lecture Note Series, page 2546. Cambridge University Press.

[Bourbaki, 1998] Bourbaki, N. (1998). *Algebra I. Chapters 1–3*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin. Translated from the French, Reprint of the 1989 English translation [MR0979982 (90d:00002)].

[Bruin et al., 2019] Bruin, N., Sijsling, J., and Zotine, A. (2019). Numerical computation of endomorphism rings of Jacobians. *The Open Book Series*, 2(1):155–171.

[Cannon et al., 2006] Cannon, J., Bosma, W., Fieker, C., and Steel, A. (2006). Handbook of Magma functions.

[Delone and Faddeev, 1940] Delone, B. N. and Faddeev, D. K. (1940). Theory of irrationalities of third degree. *Trudy Matematicheskogo Instituta imeni VA Steklova*, 11:3–340.

[Eisenbud, 2013] Eisenbud, D. (2013). *Commutative Algebra: with a view toward algebraic geometry*, volume 150. Springer Science & Business Media.

[Elkies, 1991] Elkies, N. D. (1991). ABC implies Mordell. *International Mathematics Research Notices*, 1991(7):99–109.

[Faltings, 1983] Faltings, G. (1983). Endlichkeitssätze für abelsche varietäten über zahlkörpern. *Inventiones mathematicae*, 73(3):349–366.

[Faltings, 1986] Faltings, G. (1986). Finiteness theorems for abelian varieties over number fields. In *Arithmetic geometry*, pages 9–26. Springer.

[Fialowski and Penkava, 2009] Fialowski, A. and Penkava, M. (2009). The moduli space of 3-dimensional associative algebras. *Comm. Algebra*, 37(10):3666–3685.

[Flanigan, 1968] Flanigan, F. J. (1968). Algebraic geography: Varieties of structure constants. *Pacific J. Math.*, 27:71–79.

[Gabriel, 1974] Gabriel, P. (1974). Finite representation type is open. pages 23 pp. Carleton Math. Lecture Notes, No. 9.

[Gerstenhaber, 1964] Gerstenhaber, M. (1964). On the deformation of rings and algebras. *Ann. of Math. (2)*, 79:59–103.

[Girondo and González-Diez, 2012] Girondo, E. and González-Diez, G. (2012). *Introduction to compact Riemann surfaces and dessins d'enfants*, volume 79. Cambridge University Press.

[Gross and Lucianovic, 2009] Gross, B. H. and Lucianovic, M. W. (2009). On cubic rings and quaternion rings. *Journal of Number Theory*, 129(6):1468 – 1478.

[Grothendieck, 1997] Grothendieck, A. (1997). Esquisse d'un programme. *London Mathematical Society Lecture Note Series*, pages 5–48.

[Hartshorne, 2013] Hartshorne, R. (2013). *Algebraic geometry*, volume 52. Springer Science & Business Media.

[Jacobson, 1963] Jacobson, N. (1963). Generic norm of an algebra. *Osaka Mathematical Journal*, 15(1):25–50.

[Javanpeykar and Voight, 2019] Javanpeykar, A. and Voight, J. (2019). The Belyi degree of a curve is computable. *Arithmetic Geometry: Computation and Applications*, 722:43.

[Jones and Wolfart, 2016] Jones, G. A. and Wolfart, J. (2016). *Dessins d'enfants on Riemann surfaces*. Springer.

[Jones and Roberts, 2007] Jones, J. W. and Roberts, D. P. (2007). Galois number fields with small root discriminant. *Journal of Number Theory*, 122(2):379–407.

[Klug et al., 2014] Klug, M., Musty, M., Schiavone, S., and Voight, J. (2014). Numerical calculation of three-point branched covers of the projective line. *LMS Journal of Computation and Mathematics*, 17(1):379–430.

[Klug, 2013] Klug, M. R. (2013). *Computing rings of modular forms using power series expansions*. PhD thesis, University of Vermont.

[Levin, 2013] Levin, A. S. (2013). On the classification of algebras. *arXiv preprint arXiv:1312.6612*.

[Liu, 2002] Liu, Q. (2002). *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford. Translated from the French by Reinie Erné, Oxford Science Publications.

[Malle, 1994] Malle, G. (1994). Noncongruence subgroups, covers and drawings. In Schneps, L., editor, *The Grothendieck Theory of Dessins d'Enfants*, London Mathematical Society Lecture Note Series, pages 147–168. Cambridge University Press.

[Malle and Matzat, 1999] Malle, G. and Matzat, B. H. (1999). *Inverse Galois Theory*. Springer.

[Mazzola, 1979] Mazzola, G. (1979). The algebraic and geometric classification of associative algebras of dimension five. *Manuscripta Math.*, 27(1):81–101.

[Musty et al., 2019] Musty, M., Schiavone, S., Sijsling, J., and Voight, J. (2019). A database of Belyi maps. *The Open Book Series*, 2(1):375–392.

[Peirce, 1881] Peirce, B. (1881). Linear Associative Algebra. *Amer. J. Math.*, 4(1-4):97–229.

[Poonen, 2008] Poonen, B. (2008). The moduli space of commutative algebras of finite rank. *J. Eur. Math. Soc. (JEMS)*, 10(3):817–836.

[Roberts, 2004] Roberts, D. P. (2004). An abc construction of number fields. In *Number theory, CRM Proc. Lecture Notes*, volume 36, pages 237–267.

[Roberts, 2016] Roberts, D. P. (2016). Lightly ramified number fields with galois group sm 12. a. *Journal de Théorie des Nombres de Bordeaux*, 28(2):435–460.

[Roberts, 2018] Roberts, D. P. (2018). Hurwitz-Belyi maps. In *Publications mathématiques de Besançon. Algèbre et théorie des nombres. 2018*, volume 2018 of *Publ. Math. Besançon Algèbre Théorie Nr.*, pages 25–67. Presses Univ. Franche-Comté, Besançon.

[Schneps, 1994] Schneps, L., editor (1994). *The Grothendieck Theory of Dessins d'Enfants*. London Mathematical Society Lecture Note Series. Cambridge University Press.

[Serre, 2016] Serre, J.-P. (2016). *Topics in Galois theory*. AK Peters/CRC Press.

[Shafarevich, 2013] Shafarevich, I. R. (2013). *Basic algebraic geometry. 1*. Springer, Heidelberg, third edition. Varieties in projective space.

[Sijsling and Voight, 2014] Sijsling, J. and Voight, J. (2014). On computing Belyi maps. *Publications mathématiques de Besançon*, (1):73–131.

[Sijsling and Voight, 2016] Sijsling, J. and Voight, J. (2016). On explicit descent of marked curves and maps. *Research in Number theory*, 2(1):27.

[Silverman, 2009] Silverman, J. H. (2009). *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media.

[Stacks Project Authors, 2019] Stacks Project Authors, T. (2019). *Stacks Project*. `https://stacks.math.columbia.edu`.

[Vakil, 2015] Vakil, R. (2015). The rising sea: foundations of algebraic geometry.

[Venkata Balaji, 2007] Venkata Balaji, T. E. (2007). Line-bundle-valued ternary quadratic forms over schemes. *J. Pure Appl. Algebra*, 208(1):237–259.

[Voight, 2011a] Voight, J. (2011a). Characterizing quaternion rings over an arbitrary base. *J. Reine Angew. Math.*, 657:113–134.

[Voight, 2011b] Voight, J. (2011b). Characterizing quaternion rings over an arbitrary base. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 2011(657):113–134.

[Voight, 2011c] Voight, J. (2011c). Rings of low rank with a standard involution. *Illinois Journal of Mathematics*, 55(3):1135–1154.

[Voight and Willis, 2014] Voight, J. and Willis, J. (2014). Computing power series expansions of modular forms. In *Computations with modular forms*, pages 331–361. Springer.

[Voight and Zureick-Brown, 2015] Voight, J. and Zureick-Brown, D. (2015). The canonical ring of a stacky curve. *arXiv preprint arXiv:1501.04657*.

[Volklein, 1996] Volklein, H. (1996). *Groups as Galois groups: an introduction*. Number 53. Cambridge University Press.

[Zvonkin, 2008] Zvonkin, A. (2008). Belyi functions: examples, properties, and applications. In *Proceedings AAECC*, volume 11, pages 161–180.