CONTROLLING RAMIFICATION IN NUMBER FIELDS

A DISSERTATION
SUBMITTED TO THE DEPARTMENT OF MATHEMATICS
AND THE COMMITTEE ON GRADUATE STUDIES
OF STANFORD UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

Simon Rubinstein-Salzedo

August 2012

I certify that I have read this dissertation and that, in my opinion, it is fully adequate in scope and quality as a dissertation for the degree of Doctor of Philosophy.

(Akshay Venkatesh) Principal Adviser

I certify that I have read this dissertation and that, in my opinion, it is fully adequate in scope and quality as a dissertation for the degree of Doctor of Philosophy.

(Brian Conrad)

I certify that I have read this dissertation and that, in my opinion, it is fully adequate in scope and quality as a dissertation for the degree of Doctor of Philosophy.

(Persi Diaconis)

Approved for the University Committee on Graduate Studies

Abstract

This thesis focuses on two aspects of limited ramification and is split up into two independent sections. The first section (which comprises the second and third chapters) is on the distribution of class groups of cyclic cubic fields. We propose an explanation for the discrepancy between the observed number of cyclic cubics whose 2-class group is $C_2 \times C_2$ and the number predicted by the Cohen-Lenstra heuristics, in terms of an invariant living in a quotient of the Schur multiplier group. We also show that, in some cases, the definition of the invariant can be simplified greatly, and we compute 10^5 examples.

The second section (which comprises the fourth and fifth chapters) discusses branched covers of algebraic curves, especially covers of elliptic curves with one branch point. We produce some techniques that allow us to write down explicit equations for such maps, and then we give examples of number fields which arise from such covers.

Finally, we present some possibilities for future works that the author hopes to pursue.

Acknowledgements

I would like to thank my advisor, Akshay Venkatesh, for teaching me so many things, suggesting interesting problems that were delightful to work on, helping me make progress on the frequent occasions when I encountered difficulties, and always being infectiously enthusiastic about mathematics. I would also like to thank the mathematics department at Stanford University as a whole; it is exciting to be around so many people who also like mathematics and who are likely to tell me exciting new things at any moment. I am honored to have been able to work with and among such people.

I would like to thank the people who have helped me with my thesis. In addition to Akshay Venkatesh, who helped a tremendous amount, I would like to thank Dan Boneh, Brian Conrad, Persi Diaconis, and Ronen Mukamel for serving on my committee and reading my thesis. Many other people also gave me valuable feedback and mathematical suggestions about my work, including Rebecca Bellovin, Greg Brumfiel, Otis Chodosh, Jeff Danciger, Jordan Ellenberg, Ilya Grigoriev, Julio Gutiérrez, John Jiang, Silas Johnson, Jürgen Klüners, Hendrik Lenstra, Sam Lichtenstein, Michael Lipnowski, Daniel Litt, Jeremy Miller, Dan Murphy, David Roberts, David Sher, Soarer Ho Chung Siu, Nisan Stiennon, Frank Thorne, Ravi Vakil, and Melanie Matchett Wood. Thanks to all of them!

I am also grateful for earlier mathematical opportunities I have had in my life. Many thanks to the College of Creative Studies at the University of California, Santa Barbara and the mathematics department there. I could not possibly have had a better undergraduate experience than I had there. There were many people there who supported me, but I would like to single out Birge Huisgen-Zimmermann, Mihai

Putinar, and Charles Ryavec from the mathematics department, and Joel Feigin from the music department for being particularly helpful to me.

Thanks also to the mathematics contest community in the San Francisco Bay Area, 1999–2003. I shudder to think about how I would have escaped high school with my love of mathematics intact were it not for the stimulating environment I received at contests. Thanks also to Steve Headley, for being the primary teacher at my high school to take an active role in improving my mathematical education; he went far above and beyond the call of duty required of any teacher and deserves much credit for doing so.

I am also appreciative of all the students I have had over the years. Through them I remain convinced that I am helping to improve the world, even in those rough times when I sit at my desk day after day making no progress on my research and thus contributing nothing to the totality of human knowledge. When I teach, I can remind myself that my years of study can help to make someone else's life better. Thanks especially to four years of SUMaC students, who have indulged me by allowing me to tell numerous mathematical stories that fascinate me; I hope some of them were similarly interested. Some of them are still willing to talk to me, so I'll take that as a positive sign.

Finally, I would like to thank my family for supporting me throughout my entire life. They have always encouraged me to pursue intellectual endeavors and to learn as much as possible.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

This thesis is comprised of work on two projects. The first project, discussed in chapters 2 and 3, is on the Cohen-Lenstra heuristics. The Cohen-Lenstra heuristics are concerned with the distribution of class groups in number fields. Papers by Cohen, Lenstra, and Martinet from the 1980s provide conjectural probability distributions for the Sylow p-subgroups of class groups of number fields of certain types. For the most part, these conjectured distributions match the available data well, but they do not match the data at a few primes.

In Chapter 2, we give some background on algebraic number theory and the Cohen-Lenstra heuristics. There is nothing original in this chapter; it is only intended to give the reader an overview of previous work in the field. In Chapter 3, we present the author's contributions to the subject. In particular, we focus on the case of cyclic cubic fields for which the Sylow 2-subgroup of their class groups are $C_2 \times C_2$, the first case in which the Cohen-Lenstra distribution does not match available data. We propose an explanation for the failure of the Cohen-Lenstra heuristic in this case, which is described in Sections 3.4 and 3.5.

Briefly, what we do is to construct an invariant associated to cyclic cubic fields with Sylow 2-subgroup of the class group isomorphic to $C_2 \times C_2$, valued in C_2. We conjecture that the invariant is equidistributed in these two classes as the discriminant of the fields goes to infinity, and the remainder of Chapter 3 is devoted to giving numerical evidence to support this conjecture. For the purpose of computation, the

most useful pieces can be found in Theorem 3.5.4 and Algorithm 3.5.6. From there, we compute invariants for 10^5 examples of fields of this type, and we find that the invariant is roughly equidistributed, but with a small bias in favor of invariant 1 which appears to drop off gradually.

The second project, discussed in chapters 4 and 5, is on explicit branched covers of algebraic curves. This problem has been carefully studied in the case of maps from $\mathbb{P}^1$ to $\mathbb{P}^1$, especially in the form of dessins d'enfants and Belyĭ maps. We present a brief overview of known results in this field in Chapter 4. There is little new material in this chapter. The author computed the examples independently, but they are presumably known, in some form, by many other people.

In Chapter 5, we study explicit branched covers of elliptic curves. Surprisingly little work has been done in this area in the past, even though it is a natural follow-up to the study of Belyĭ maps and dessins d'enfants. We present several techniques for constructing these covers.

The most interesting techniques are probably those found in Section 5.3. In this section, we construct an explicit degree-5 cover of an elliptic curve by a genus-2 curve ramified only above one point. While the main result of the section, Theorem 5.3.1, is easy to verify once it is handed to us, it is interesting to come up with the equation of the curve independently. Hence, the techniques that go into coming up with and conjecturing Theorem 5.3.1 are far more exciting than is the actual statement of the theorem.

The main theme running through both projects is that of ramification. Our work on the Cohen-Lenstra heuristics involves constructing unramified or minimally ramified extensions of number fields. Our work on covers of algebraic curves involves constructing covers which are ramified only at a few specified points, and with specified ramification types. From such covers, it is possible to find number fields which are ramified only at specified sets of primes.

The number fields we construct give positive answers in certain cases to the following natural extension of the inverse Galois problem: given a finite group G and a finite set S of primes, is it possible to find a Galois extension $K/\mathbb{Q}$ with Galois group G so that $K/\mathbb{Q}$ is unramified outside S?

The classical inverse Galois problem asks the following:

Question 1.0.1. *Let G be a finite group. Is there a Galois extension $K/\mathbb{Q}$ so that* $\mathrm{Gal}(K/\mathbb{Q}) \cong G$*?*

In what follows, I shall present a small sample of the work that has been done on this problem. Note that it is far from being complete.

This problem goes back to the 19^{th} century, and it still remains an open problem, and one that attracts much attention today. There is no finite group G for which the inverse Galois problem for G is known to have a negative answer, but the question remains unknown for large classes of groups G.

Hilbert attempted this problem by constructing algebraic curves over $\mathbb{Q}$. Such curves give function fields $K/\mathbb{Q}(t)$. If $\mathrm{Gal}(K/\mathbb{Q}(t)) \cong G$, then Hilbert was able to construct number fields over $\mathbb{Q}$ with Galois group G. Hilbert was then able to answer the inverse Galois problem in the affirmative for all the symmetric and alternating groups. This is the approach taken in chapter 4, so we will postpone further discussion of this method until then.

For many other classes of finite groups G, the inverse Galois problem is known to have a positive solution. It is easy to show that if G is an abelian group, then we can find a suitable K; we can construct it as a subfield of some cyclotomic field.

A much deeper result, due to Shafarevich in [Šaf54], is that the inverse Galois problem holds for all solvable groups G. Once the solvable groups were taken care of, focus shifted toward simple groups.

Since Hilbert had already answered the inverse Galois problem for alternating groups, the next case to look at was that of $\mathrm{PSL}_2(\mathbb{F}_p)$. Shih in [Shi74] was able to prove the following result:

Theorem 1.0.2 (Shih)**.** *Let p be an odd prime for which at least one of 2, 3, and 7 is a quadratic non-residue modulo p. Then* $\mathrm{PSL}_2(\mathbb{F}_p)$ *occurs as a Galois group over* $\mathbb{Q}$.

Starting with the surprising discovery in 1965 of a new sporadic simple group, the race was on to find more of them; by 1982, the 21 new sporadic groups had

all been found. Number theorists naturally turned to the sporadic groups as a new source of special cases of the inverse Galois problem. In the mid-1980s, several papers including [MZM86], came out constructing the small Mathieu groups M_{11} and M_{12} as Galois groups.

At around the same time, Thompson developed a new technique, known as rigidity, to tackle the inverse Galois problem. In [Tho84], he was able to prove the following result:

Theorem 1.0.3. *Let G be a finite group, $C = (C_1, \ldots, C_s)$ a sequence of conjugacy classes of G, and*

$$A_G(C) = \{(g_1, \ldots, g_s) \in C_1 \times \cdots \times C_s : g_1 \cdots g_s = 1\}.$$

Suppose that $A_G(C)$ is nonempty. Then G acts on $A_G(C)$ by $g(g_1, \ldots, g_s) = (gg_1g^{-1}, \ldots, gg_sg^{-1})$. If G acts transitively on $A_G(C)$, and one (hence every) element of $A_G(C)$ generates G, then G occurs as a Galois group over $\mathbb{Q}$.

Using this theorem, Thompson showed that the Monster group occurs as a Galois group over $\mathbb{Q}$.

After much work on sporadic groups, the inverse Galois problem is almost complete in this case: of the 26 sporadic groups, it remains open only for M_{23}.

More recently, several people have become interested in the question of number fields with limited ramification (and perhaps given Galois group). This question has a geometric interpretation in terms of the étale fundamental group. If S is a scheme, then there is a profinite group $\pi_1^{\text{ét}}(S)$ which serves a similar function to the (profinite completion of the) topological fundamental group; that is, it classifies finite connected covers (or covering spaces) of S. If we let $\pi_A^{\text{ét}}(S)$ denote the set of abstract finite groups which occur as quotients of $\pi_1^{\text{ét}}(S)$, then $\pi_A^{\text{ét}}$ measures the Galois groups (or groups of deck transformations) which can occur for finite covers.

To use this machinery in the case of Galois groups over $\mathbb{Q}$, we let $S = \text{Spec}(\mathbb{Z}[1/N])$, where N is the product of the primes at which we allow ramification. The question of whether G occurs as a Galois group over $\mathbb{Q}$ of a field unramified

at primes not dividing N is then equivalent to asking whether $G \in \pi_A^{\text{ét}}(\text{Spec}(\mathbb{Z}[1/N]))$. An interesting discussion along these lines can be found in [Har94].

One concrete question, posed by Gross in [Gro98], is the following:

Question 1.0.4. *Let p be a prime. Is there a number field K, Galois over $\mathbb{Q}$, unramified away from p and ∞, so that $\text{Gal}(K/\mathbb{Q})$ is nonsolvable?*

This question has now been solved, in the affirmative. For primes $p \geq 11$, this question was answered by Serre in [Ser73], by Dembélé for $p = 2$ in [Dem09], by Dembélé, Greenberg, and Voight for $p = 3$ and 5 in [DGV11] and by Roberts for $p = 5$ with an explicit polynomial in [Rob11]. Very recently, Dieulefait in [Die12] solved this question for $p = 7$, finally answering the question completely. These papers used modular forms to construct the relevant fields.

The general question, of which pairs (G, S) of a Galois group and a set of ramified primes, can occur in a number field, is still very much open. It is this question that inspires the work done in this thesis, and to which I hope to be able to contribute. But at the moment, there is still much to be done before I will be able to construct many new examples.

Chapter 2

An Introduction to the Cohen-Lenstra Heuristics

2.1 Introduction

Before we begin our discussion of the Cohen-Lenstra heuristics, it will be helpful to recall some basic definitions and results from algebraic number theory and class field theory.

Definition 2.1.1. Let K be a number field with ring of integers $\mathfrak{o}_K$. A fractional ideal of K is a nonzero finitely generated $\mathfrak{o}_K$-submodule of K. Let $I(K)$ denote the set of fractional ideals of K.

The fractional ideals of K form a group under multiplication. The identity element is the fractional ideal $\mathfrak{o}_K$ itself.

Definition 2.1.2. A principal fractional ideal of K is a fractional ideal of the form $a\mathfrak{o}_K$, for some $a \in K^\times$. Let $P(K)$ denote the set of principal fractional ideals.

The principal fractional ideals form a subgroup of the group of fractional ideals.

Definition 2.1.3. The class group of K is the quotient $\mathrm{Cl}(K) = I(K)/P(K)$.

One of the most important theorems in basic algebraic number theory is the following:

Theorem 2.1.4. *If K is a number field, then $\mathrm{Cl}(K)$ is a finite group.*

See §17, page 71, of [CF86] for a proof, or the discussion in §IV.3 of [FT93] for an effective version, providing a bound on its size.

Definition 2.1.5. The class number $h(K)$ is defined to be the order of $\mathrm{Cl}(K)$.

The class group was first studied in connection with Fermat's Last Theorem, by Ernst Kummer in the middle of the 19^{th} century, based on a failed attempt by Gabriel Lamé to give a proof of this celebrated then-conjecture. The idea was as follows. Let $p \geq 3$ be a prime. We wish to show that $x^p + y^p = z^p$ has no solutions in positive integers. So, we try to factor the left side as

$$\prod_{i=0}^{p-1}(x + \zeta^i y),$$

where ζ is a primitive p^{th} root of unity. Since the right side is a p^{th} power, if all the factors in the product are pairwise relatively prime, then each one of them must be a p^{th} power as well. One can then attempt to show that this is impossible. A careful exposition of this approach can be found in [Was97].

However, this approach implicitly assumes that $\mathbb{Z}[\zeta]$ is a unique factorization domain, and this is false in general. (In fact, it is false for all primes $p \geq 23$.)

It it not too difficult to show that K has class number 1 exactly when $\mathfrak{o}_K$ is a unique factorization domain. Hence, the class number is a measure of the failure of $\mathfrak{o}_K$ to be a unique factorization domain. More concretely, if we have some element $x \in \mathfrak{o}_K$ with nonunique factorization, we can construct a nonprincipal ideal.

Example. Let $K = \mathbb{Q}(\sqrt{-5})$, so that $\mathfrak{o}_K = \mathbb{Z}[\sqrt{-5}]$. Then K has class number 2. We can give an explicit element of $\mathfrak{o}_K$ which has nonunique factorization:

$$6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

We can use this factorization to give us an example of a nonprincipal ideal, namely $(2, 1 + \sqrt{-5})$. (Any other similar pair of factors would also do. Any two such pairs provide ideals in the same ideal class, however.)

It will also be helpful for this chapter to recall various facts about ramification in number fields. We begin by recalling the following theorem, known as the efg Theorem:

Theorem 2.1.6 (efg Theorem)**.** *Let L/K be an extension of number fields of degree n, and let $\mathfrak{p} \subset \mathfrak{o}_K$ be a prime ideal. Suppose $\mathfrak{p}\mathfrak{o}_L$ factors in $\mathfrak{o}_L$ as*

$$\mathfrak{p}\mathfrak{o}_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i},$$

where the $\mathfrak{P}_i$ are distinct primes in $\mathfrak{o}_L$. Let $f_i = [\mathfrak{o}_L/\mathfrak{P}_i : \mathfrak{o}_K/\mathfrak{p}]$. Then

$$n = \sum_{i=1}^{g} e_i f_i.$$

If, furthermore, L/K is a Galois *extension, then all the e_i's and f_i's are equal, so we write these common values as e and f, respectively. We then have*

$$n = efg.$$

This is Theorem 20 in [FT93]. A proof can be found there.

An important invariant associated to a number field is its discriminant, defined as follows:

Definition 2.1.7. Let K be a number field with ring of integers $\mathfrak{o}_K$. Let $\{\alpha_i\}$ be an integral basis for K, i.e.,

$$\mathfrak{o}_K = \bigoplus_i \mathbb{Z}\alpha_i$$

as a $\mathbb{Z}$-module.

1. If $\alpha \in K$, then we define the trace of α to be the trace of the multiplication by α map with respect to the basis $\{\alpha_i\}$ of K. (Of course, this is independent of choice of basis.) We denote this number by $\mathrm{Tr}(\alpha)$.

2. The discriminant of K is defined to be

$$\mathrm{disc}(K) = \det(\mathrm{Tr}(\alpha_i \alpha_j))_{i,j}.$$

We can also define the discriminant of an extension of number fields L/K, but the situation is a little bit more subtle, since $\mathfrak{o}_L$ need not be a free $\mathfrak{o}_K$-module. To remedy this, we define the discriminant of L/K to be the ideal of $\mathfrak{o}_K$ defined as follows: suppose $[L : K] = n$, and suppose that $\mathcal{A} = \{\alpha_1, \ldots, \alpha_n\} \subset \mathfrak{o}_L$ generates a finite-index free $\mathfrak{o}_K$-subalgebra of $\mathfrak{o}_L$. Let $\mathrm{disc}_{\mathcal{A}}(L/K) = \det(\mathrm{Tr}(\alpha_i \alpha_j))_{i,j}$. Then the discriminant ideal of L/K is the ideal of $\mathfrak{o}_K$ generated by all the $\mathrm{disc}_{\mathcal{A}}(L/K)$'s.

Definition 2.1.8. Let L/K be an extension of number fields, and let $\mathfrak{p} \subset \mathfrak{o}_K$ be a prime ideal. We say that $\mathfrak{p}$ is ramified in L if, in the factorization given by the efg Theorem, some $e_i > 1$.

It turns out that, for any extension, there are only finitely many ramified primes. These are exactly the primes dividing the discriminant of L/K.

It is also possible to talk about a field being ramified or unramified at ∞.

Definition 2.1.9. An extension L/K of number fields of degree n is said to be unramified at ∞ if, whenever $\iota : K \to \mathbb{R}$ is an embedding, then there exist n embeddings $\tilde{\iota} : L \to \mathbb{R}$ whose restriction to K is equal to ι. Otherwise, the extension is said to be ramified at ∞.

In particular, if K is totally real, then L/K is unramified at ∞ if and only if L is also totally real.

One of the most remarkable achievements of twentieth century mathematics was the development of class field theory. Global class field theory relates abelian extensions of number fields (and function fields) to certain generalizations of class groups. We briefly describe some of the key results in class field theory now.

Theorem 2.1.10. *Let K be a number field. Then there exists a unique (up to isomorphism) maximal Galois extension L/K which is unramified at all prime ideals $\mathfrak{p}$ as well as at ∞, and so that $\mathrm{Gal}(L/K)$ is abelian. Furthermore, in this case, $\mathrm{Gal}(L/K) \cong \mathrm{Cl}(K)$.*

See page 61 of [Chi09] for more information and generalizations of this theorem.

Example. 1. If $K = \mathbb{Q}$, then its class group is trivial, so there are no unramified abelian extensions of $\mathbb{Q}$.

2. If $K = \mathbb{Q}(\sqrt{-5})$, then $\mathrm{Cl}(K) = C_2$, so there is a unique unramified quadratic extension of K. This extension is $\mathbb{Q}(\sqrt{-5}, \sqrt{-1})$.

3. If $K = \mathbb{Q}(\sqrt{-23})$, then $\mathrm{Cl}(K) = C_3$, so there is a unique unramified cyclic cubic extension of K. This extension is $\mathbb{Q}(\sqrt{-23}, \alpha)$, where α is a root of $x^3 - x - 1$.

This extension L is known as the Hilbert class field of K and is frequently denoted by $H(K)$. It is perhaps worth noting that the isomorphism given in the theorem is not merely an abstract isomorphism; rather, by using some powerful theorems in class field theory such as (a very weak version of) the Chebotarev density theorem, we can describe the map quite explicitly. The map in question is known as the Artin map.

We can also construct variants of the Hilbert class field. For instance, the maximal Galois unramified abelian extension of K for which the Galois group is abelian and for which $[L : K]$ is a p^{th} power corresponds via the Artin map in class field theory (or simply by Galois theory) to the Sylow p-subgroup of $\mathrm{Cl}(K)$.

There is also a variant of the class group known as the narrow class group, and it will be used later in this section. Let $P^+(K)$ denote the group of principal fractional ideals (a) of K for which a is totally positive, i.e., so that $\iota(a) > 0$ for every embedding $\iota : K \hookrightarrow \mathbb{R}$. Let $\mathrm{Cl}^+(K) = I(K)/P^+(K)$. We call $\mathrm{Cl}^+(K)$ the narrow class group of K.

As we saw above, there is a field (the Hilbert class field) associated to the class group of a number field. Similarly, there is a field, called the narrow class field, associated to the narrow class group. The narrow class field of K is the maximal abelian extension of K that is unramified at all *finite* primes.

Example. Let $K = \mathbb{Q}(\sqrt{3})$. Then $\mathrm{Cl}(K) = 1$, and $\mathrm{Cl}^+(K) = C_2$. Hence, there exists a quadratic extension L/K which is unramified at all finite places, but is ramified at infinity. This field is $L = \mathbb{Q}(\sqrt{3}, \sqrt{-1})$.

2.2 The Cohen-Lenstra Heuristics

Cohen and Lenstra in [CL84] were interested in studying the distribution of class groups of quadratic fields, and perhaps, abelian extensions of $\mathbb{Q}$ more generally. These heuristics were extended by Cohen and Martinet in [CM87] and [CM90] in 1987 and 1990 to fields of more general type.

Since class groups are finite abelian groups, we can attempt to understand them by understanding their p-Sylow subgroups. Assuming that the distributions of the p-Sylow subgroups are independent for different p, we can then patch together the distribution of class groups from the distribution of the p-Sylow subgroups for all p. (The independence of distributions at each prime is conjectural, but it is well-supported by numerical data.)

Therefore, we will restrict ourselves to looking at the distribution of the p-Sylow subgroups of the class groups of number fields. Let K be a number field. Then we let $\mathrm{Cl}_p(K)$ denote the p-Sylow subgroup of $\mathrm{Cl}(K)$, and we let $h_p(K)$ denote its order.

In the case of quadratic fields, Cohen and Lenstra made the following conjecture:

Conjecture 2.2.1 (Cohen-Lenstra)**.** *Let p be an odd prime. Let $D^{\pm}(X)$ denote the set of real (respectively imaginary) quadratic fields K with $|\operatorname{disc}(K)| < X$. Let A be a finite abelian p-group. Then*

$$\lambda^{\pm}(A) = \lim_{X\to\infty} \frac{\#\{K \in D^{\pm}(X) : \mathrm{Cl}_p(K) \cong A\}}{\#D^{\pm}(X)}$$

exists, and we have

$$\lambda^{+}(A) = c^{+}|\operatorname{Aut}(A)|^{-1} \times |A|^{-1}, \qquad \lambda^{-}(A) = c^{-}|\operatorname{Aut}(A)|^{-1}$$

for certain explicit constants c^{+} and c^{-}, which are independent of A.

The statement of this conjecture suggests many further questions. One such question is why we need to restrict to the case of of an odd prime p. The reason is that the 2-torsion in the class group is controlled by a different phenomenon, namely genus theory. In the general case, genus theory is quite involved (see [Frö83] for a complete

treatment), but in the case of 2-torsion in a quadratic field, it is readily understood: if K is a quadratic field and r is the number of primes dividing $\mathrm{disc}(K)$, then the 2-torsion of $\mathrm{Cl}(K)$ is isomorphic to C_2^{r-1} or C_2^{r-2} (see [FT93], Corollary 1 to Theorem 39, for a more precise statement and a proof). In particular, the 2-torsion in quadratic fields is rarely equal to 0 and can easily become arbitrarily large.

Another question that is likely to arise is what sort of heuristic evidence we have that suggests such a result might be true, or even a reasonable guess. One answer, supported by analogies in other areas of mathematics (especially the theory of stacks in algebraic geometry) is that objects in general are best and most uniformly treated when we take a quotient by the automorphism group of each object. An instance of this phenomenon that will become increasingly relevant in later chapters is that of elliptic curves. Most elliptic curves (over the complex numbers) have automorphism group C_2, but those with j-invariant 0 or 1728 have larger automorphism groups. The moduli stack of elliptic curves is then the quotient of the coarse moduli space $\mathbb{A}^1$ of elliptic curves by automorphism groups, and this is the best object to use to study families of elliptic curves, since there are unexpected phenomena that occur for these j-invariants.

It is also worth at this point giving a plausibility argument for this conjecture, which comes from a result of Friedman and Washington in [FW89]. Suppose we have a (large) collection of ideals $I_1, \ldots, I_n$ in a number field K. Then their images in $\mathrm{Cl}(K)$ satisfy various relations. In fact, we expect them to satisfy n or $n+1$ relations, depending on whether K is imaginary quadratic or real quadratic, respectively. Assuming we have chosen enough ideals to generate the class group, the class group will then be the cokernel of this matrix, considered as a map of free $\mathbb{Z}$-modules. Hence, the class group should be well-modeled by the cokernel of a random matrix of the right size.

Unfortunately, this approach does not make any sense as stated, since there is no obvious measure to put on these matrices. To fix this problem, we restrict to the p-power torsion and consider the matrices to have entries in $\mathbb{Z}_p$. Now, if we assume that the entries are distributed identically and independently according to the Haar measure on $\mathbb{Z}_p$, then we have a well-defined distribution on their cokernels. Friedman

and Washington showed that, as $n \to \infty$, a limiting distribution exists and is equal to the distribution in the above conjecture.

Here, it is necessary to try to justify the difference between the imaginary quadratic and real quadratic cases, but it is clear from even the most casual glance at a table of class numbers that imaginary and real quadratic fields behave very differently. Indeed, there are exactly nine imaginary quadratic fields with class number one, while there appear to be infinitely many (and in fact, around 75% of) real quadratic fields with class number one. It is hard to give very compelling reasons to believe that the rank of the unit group should be a determining factor in the distribution of class groups, but let us try to demonstrate that at least there ought to be some connection.

One place in which it becomes clear that there is a serious difference between real and imaginary quadratic fields is in the analytic class number formula. If K is any number field, and ζ_K is the Dedekind ζ function for K, then we have the formula

$$\zeta_K(0) = -\frac{hR}{w},$$

where h is the class number, R is the regulator, and w is the number of roots of unity in K. For all but finitely many quadratic fields, $w = 2$, so that term is not so critical. However, in the case of an imaginary quadratic field, $R = 1$, while for real quadratic fields, R depends on the fundamental unit of K. We should think of hR as being one block from an analytic point of view; it is hard to write down an analytic expression that separates h from R. If we were to study the distribution of hR in place of h, then we should expect much greater similarities between the real quadratic and imaginary quadratic situations.

Another place the unit group comes into consideration in the study of class groups is in the construction of class groups of quadratic fields in terms of binary quadratic forms. For imaginary quadratic fields K with discriminant $-\Delta$, the class group is exactly the group of reduced binary quadratic forms with discriminant $-\Delta$. For real quadratic fields, the analogous construction only gives us the narrow class group, which is either equal to the class group or else twice as large (in the case of real

quadratic fields).

In order to remedy this, we might think of the class group of a real quadratic field as being the narrow class group modulo the cyclic subgroup generated by a uniformly chosen element. (This is far from being actually true, but it is reasonable intuition.) Quotienting out by one element of a group modeled after the narrow class group should correspond to allowing one extra relation in the matrix. This should be our intuition for why the class group of a real quadratic field should be modeled by n generators and $n+1$ relations.

Of course, we need not lose interest in class groups as soon as we step beyond quadratic fields: we could ask the same question for fields of other types. Furthermore, in this case, the 2-power torsion will not necessarily be governed by genus theory, so we might also allow p to be 2. So, we could make the following guess, by attempting to apply the Cohen-Lenstra heuristics to situations for which we have no *a priori* reason for believing that they are appropriate, apart from a random matrix-type argument or a fuzzy argument of the type given just above.

Heuristic 2.2.2 (Proto-Cohen-Lenstra Heuristics)**.** *Let n be a positive integer, and let G be a transitive permutation group on a set of size n. Furthermore, let (r_1, r_2) be a signature, with $r_1 + 2r_2 = n$. Let $D(X)$ be the set of number fields K the absolute value of whose discriminant is less than X, and so that the Galois group $\mathrm{Gal}(K^\sharp/\mathbb{Q})$ of the Galois closure of K is isomorphic to G, and K has r_1 real embeddings and r_2 pairs of complex conjugate embeddings. Finally, let p be a prime not dividing $|G|$ and let A be a finite abelian p-group. Then*

$$\lim_{X\to\infty} \frac{\#\{K \in D(X) : \mathrm{Cl}_p(K) \cong A\}}{\#D(X)}$$

exists, and is inversely proportional to $|\operatorname{Aut}(A)| \times |A|^{r_1+r_2-1}$.

However, the proto-Cohen-Lenstra heuristics sometimes fail for silly reasons. Here's an example:

Lemma 2.2.3. *Let $n = 3$ and $G = C_3$ in the above heuristics. If $p \equiv 2 \pmod 3$, then the p-rank of K, $r_p(K) := \dim_{\mathbb{F}_p}(\mathrm{Cl}(K)/p\,\mathrm{Cl}(K))$, is even for all such K.*

Proof. The Galois group $C_3 = \{1, \sigma, \sigma^2\}$ of K over $\mathbb{Q}$ acts on $\mathrm{Cl}_p(K)$. The number of ideal classes of order p is $p^{r_p(K)} - 1$, which is congruent to 0 (mod 3) if and only if $r_p(K)$ is even. Hence, if $r_p(K)$ is odd, then there must be a nontrivial p-torsion ideal class C fixed by the Galois action. In particular, there's a nonprincipal ideal $\mathfrak{a} \in C$ of order p so that $\mathfrak{a}$, $\mathfrak{a}^\sigma$, and $\mathfrak{a}^{\sigma^2}$ are all in the same ideal class. We now show that their product $\mathfrak{a}^{1+\sigma+\sigma^2}$ is equal to the principal ideal $(N\mathfrak{a})\mathfrak{o}_K$. For any $a \in \mathfrak{a}$, $Na = a^{1+\sigma+\sigma^2} \in \mathfrak{a}^{1+\sigma+\sigma^2}$, and the Na generate $(N\mathfrak{a})\mathfrak{o}_K$ as an $\mathfrak{o}_K$-module, so $(N\mathfrak{a})\mathfrak{o}_K \subset \mathfrak{a}^{1+\sigma+\sigma^2}$. Now, the norms of both ideals $\mathfrak{a}^{1+\sigma+\sigma^2}$ and $(N\mathfrak{a})\mathfrak{o}_K$ are $(N\mathfrak{a})^3$. Hence, they are equal. Furthermore, $(N\mathfrak{a})\mathfrak{o}_K$ is principal, since it is generated by the element $N\mathfrak{a}$. Hence $C^3 = 1$ in $\mathrm{Cl}_p(K)$. But this is impossible, as $3 \nmid p$. ■

We can patch the proto-Cohen-Lenstra heuristics by excluding those A that are ruled out by this Lemma and related ones. Furthermore, as the proof of the lemma hints, for those A that are allowable, we need the automorphisms to be compatible with the Galois action, in the case that K is actually a Galois number field. More precisely, if $G = C_\ell$, then we need A to be a $\mathbb{Z}[\zeta_\ell]$-module. This suggests the following refinement of the proto-Cohen-Lenstra heuristics, at least in the case where $n = \ell$ is a prime, and $G = C_\ell$:

Heuristic 2.2.4 (Refined Cohen-Lenstra Heuristics)**.** *Let ℓ be an odd prime, and let $G = C_\ell$. Let $D(X)$ be the set of C_ℓ number fields with absolute discriminant less than X. (Such fields are necessarily totally real.) Also, let p be a prime different from ℓ and A an abelian p-group with the structure of a $\mathbb{Z}[\zeta_\ell]$-module. Then*

$$\lim_{X\to\infty} \frac{\#\{K \in D(X) : \mathrm{Cl}_p(K) \cong A\}}{\#D(X)}$$

exists, and is inversely proportional to $|\operatorname{Aut}_{\mathbb{Z}[\zeta_\ell]}(A)| \times |A|^{\ell-1}$.

Another, more modern and sometimes cleaner, way to interpret the refined Cohen-Lenstra heuristics is based on the following idea from probability theory. Let μ be a probability distribution on $\mathbb{R}$. Define the k^{th} moment of μ to be

$$a_k = \int_{-\infty}^{\infty} x^k \, d\mu.$$

From knowing the sequence of moments $a_1, a_2, \ldots$, it is possible to reconstruct μ under fairly mild hypotheses. To be more precise, define the moment generating function to be the power series

$$A(x) = \sum_{k=1}^{\infty} a_k \frac{x^k}{k!}.$$

Then assuming that $A(x)$ has positive radius of convergence, μ is the only probability distribution having moment generating function $A(x)$. (See [Bil95], Chapter 30, for a proof.)

In the context at hand, we can define an analogue of a moment for a probability distribution f of finite abelian p-groups as follows. Fix a finite abelian p-group A, and look at the expected number of surjections (in whichever category is appropriate) from an f-random finite abelian p-group X to A. This number behaves as the "A^{th} moment of X." Just as in the situation for classical moments of probability distributions, these A^{th} moments of X determine f, assuming that f is fairly well-behaved.

We now put this in proper context. If A is a finite abelian p-group that also has the structure of a $\mathbb{Z}[\zeta_\ell]$-module, then we would like to understand the number

$$\mathbb{E}(\#\operatorname{Surj}_{\mathbb{Z}[\zeta_\ell]}(\operatorname{Cl}(K), A)).$$

Here Surj is the set of surjective maps, and $\mathbb{E}$ denotes the expected value. Let's look at the case of $n = 3$ and $G = C_3$. Then the refined Cohen-Lenstra heuristics are equivalent to

$$\lim_{X\to\infty} \frac{1}{\#D(X)} \sum_{K\in D(X)} p^{r_p(K)} = \begin{cases} \left(1+\frac{1}{p}\right)^2 & p \equiv 1 \pmod 3, \\ 1+\frac{1}{p^2} & p \equiv 2 \pmod 3. \end{cases} \tag{2.2.1}$$

In the case when $A = C_p$ (if $p \equiv 1 \pmod 3$) or $A = C_p \times C_p$ (if $p \equiv 2 \pmod 3$), then

$$\mathbb{E}(\#\operatorname{Surj}_{\mathbb{Z}[\zeta_3]}(\operatorname{Cl}(K), A)) = \lim_{X\to\infty} \frac{1}{\#D(X)} \sum_{K\in D(X)} (p^{r_p(K)} - 1).$$

So, in particular, if $p = 2$, we'd expect the number of surjections from the class group of a random C_3 field to $C_2 \times C_2$ to be $1/4$. As we shall see shortly, however, this

appears not to be the case.

2.3 Malle's computations

Notation. We use the following notation: for $q, k \in \mathbb{N}$, let

$$(q)_k = \prod_{i=1}^{k}(1-q^{-1}), \qquad (q)_\infty = \prod_{i=1}^{\infty}(1-q^{-1}).$$

After performing many tests, Malle proposed a list of cases in which the Cohen-Lenstra heuristics are expected to fail. In particular, when $p = 2$, they should always fail. In the case of C_3 fields, the Cohen-Lenstra heuristics predict that the Sylow 2-subgroup of the class group should be isomorphic to $C_2 \times C_2$ with probability

$$\frac{1}{12}\frac{(4)_\infty}{(4)_1} \approx .0765.$$

Instead, in his sample of over 16 million fields, he finds that the actual probability is closer to .13, nearly twice as large as expected. Similarly, equation (2.2.1) does not seem to hold when $p = 2$: equation (2.2.1) predicts that the average size of the maximal elementary abelian 2-subgroup of $\mathrm{Cl}(K)$ be $\frac{5}{4}$, but Malle's computations suggest that the correct number is $\frac{3}{2}$.

In terms of expected number of surjections, it appears that

$$\mathbb{E}(\#\operatorname{Surj}_{\mathbb{Z}[\zeta_3]}(\mathrm{Cl}(K), C_2 \times C_2)) = 1/2, \tag{2.3.1}$$

rather than $1/4$, as mentioned in the previous section.

In general, Malle expects the Cohen-Lenstra heuristics to fail at the prime p when the ground field contains p^{th} roots of unity. In this case, he expects that if A is a nontrivial abelian p-group, then $\mathrm{Cl}_p(K) \cong A$ more often than the Cohen-Lenstra heuristics predict.

Remark 2.3.1. For C_3 fields, the Cohen-Lenstra prediction also fails for $p = 3$, since the 3-torsion in the class group is governed by genus theory, just as in the case of

$p = 2$ for quadratic fields. More generally, the Cohen-Lenstra predictions at a prime p do not hold for fields with Galois group G if p divides $|G|$ because of genus theory. In this thesis, we are not especially interested in the failure for that reason, since genus theory is well-understood. Thus, we will only be concerned with deviations due to the existence of p^{th} roots of unity.

In the case of quadratic fields, it is still interesting to look at the 4-ranks of class groups; that is, the maximum value of r so that $\mathrm{Cl}(K)$ contains a subgroup isomorphic to C_4^r. These are no longer controlled by genus theory, except that we have an obvious bound for the 4-rank in that it cannot exceed the 2-rank. In [Ger89], Gerth investigates the following situation. Let F be an imaginary quadratic field with odd class group. He then wishes to determine the distribution of 4-ranks of class groups of quadratic extensions K of F, ordered by the absolute norm of the relative discriminant of K over F. He proves the following theorem:

Theorem 2.3.2 (Gerth, [Ger89]). *1. If $F \neq \mathbb{Q}(\sqrt{-1})$, then the probability that the 4-rank of $\mathrm{Cl}(K)$ is equal to r is*

$$\frac{(2)_\infty}{2^{j(j+1)}(2)_j(2)_{j+1}}.$$

2. If $F = \mathbb{Q}(\sqrt{-1})$, then the probability that the 4-rank of $\mathrm{Cl}(K)$ is equal to r is

$$\frac{3}{2^{(j+1)(j+2)/2}(4)_\infty}.$$

Of particular importance is the difference in behavior when F contains a fourth root of unity and when F does not contain a fourth root of unity. Inspired by this and related results, Malle conjectured that deviations from the Cohen-Lenstra heuristics occur when the ground field contains roots of unity.

Chapter 3

The Cohen-Lenstra Heuristics and Roots of Unity

3.1 A Concise Guide to the Chapter

The goal of this chapter is to explain the discrepancy in (2.3.1): the class group of a C_3 field tends to contain more copies of $C_2 \times C_2$ than the Cohen-Lenstra heuristics predict. In this chapter, we will not work directly with C_3 fields, but rather with quartic A_4 fields, which will be slightly more convenient. However, this is only a minor distinction as there is a natural bijection between totally real A_4 fields and C_3 fields K with a Galois-equivariant surjection from $\mathrm{Cl}(K)$ to $C_2 \times C_2$.

The chapter begins with some preliminary material in §3.2 on the Schur multiplier and a variant of it called the reduced Schur multiplier. After that, we present some background material on lifting invariants in §3.3. This material is motivational: we do not use the results of this section in our new results or computations. However, much of what we do is heavily inspired by the results of §3.3. Thus, we include this section in order to make future constructions not seem like a bolt from the blue.

The new material begins in §3.4. Here we present an invariant associated to an A_4 field which is expected to explain the discrepancy in (2.3.1). In §3.5, we present an algorithm to compute the invariant, and we show that in certain circumstances, the invariant has a simple interpretation as the parity of the class group of a certain

field. In §3.6, we perform an explicit computation of the invariant for the smallest A_4 field. Finally, we end this chapter with Table 3.1, which summarizes the data collected from 10^5 fields.

3.2 Schur Multipliers and Variants

Our proposed correction to the Cohen-Lenstra heuristics in the presence of roots of unity can be described in terms of the reduced Schur multiplier. We first recall the definition of the Schur multiplier, then move on to the reduced Schur multiplier.

Definition 3.2.1. Let G be a group.

1. The Schur multiplier group of G is defined to be the second homology group $H_2(G, \mathbb{Z})$.

2. A central extension of G is a short exact sequence

$$0 \to A \to \widetilde{G} \to G \to 1,$$

   where A is an abelian group, and A is contained in the center of $\widetilde{G}$.

3. A stem extension of G is a central extension

$$0 \to A \to \widetilde{G} \to G \to 1$$

   so that A is contained in the intersection of the center of $\widetilde{G}$ and the derived subgroup of $\widetilde{G}$.

If G is finite, there is a stem extension $\widetilde{G}$ of maximal order; in fact, there may be more than one of maximal order, and such $\widetilde{G}$ need not be isomorphic. However, as $\widetilde{G}$ varies over maximal stem extensions, the corresponding A are all isomorphic, and they are isomorphic to the Schur multiplier group $H_2(G, \mathbb{Z})$. If, in addition, G is a perfect group (i.e., $G = [G, G]$ is its own commutator subgroup), then there is a unique such group $\widetilde{G}$.

Suppose G is a finite group. Then $H_2(G,\mathbb{Z})$ is a finite group all of whose elements have order dividing the order of G. Also, for a prime p, the Sylow p-subgroup of $H_2(G,\mathbb{Z})$ is trivial if the Sylow p-subgroup of G is cyclic. For convenience, we provide a few examples of Schur multiplier groups.

Proposition 3.2.2. *1. (Schur 1907, also Corollary 2.2.12 in [Kar87]) Let G be the finite abelian group*

$$G \cong C_{n_1} \times C_{n_2} \times \cdots \times C_{n_k},$$

with $n_{i+1} \mid n_i$ for $1 \leq i \leq k-1$. Let $C_n^{(m)}$ denote the direct product of m copies of C_n. Then

$$H_2(G,\mathbb{Z}) \cong C_{n_2} \times C_{n_3}^{(2)} \times \cdots \times C_{n_k}^{(k-1)}.$$

2. Let $G = C_2 \times C_2$. Then $H_2(G,\mathbb{Z}) \cong C_2$. There are two stem extensions of G:

$$0 \to C_2 \to D_8 \to C_2 \times C_2 \to 0$$

and

$$0 \to C_2 \to Q_8 \to C_2 \times C_2 \to 0. \tag{3.2.1}$$

3. Let $G = A_n$ be the alternating group on n letters. Then

$$H_2(G,\mathbb{Z}) = \begin{cases} 1 & n \leq 3, \\ C_2 & n \geq 4 \text{ and } n \neq 6,7, \\ C_6 & n = 6,7. \end{cases}$$

If $n = 4$, then we have $A_4 \cong \mathrm{PSL}_2(\mathbb{F}_3)$, and the unique stem extension of A_4 is

$$0 \to C_2 \to \mathrm{SL}_2(\mathbb{F}_3) \to A_4 \to 1. \tag{3.2.2}$$

Furthermore, the sequence (3.2.1) is the sequence of Sylow 2-subgroups of (3.2.2). If $n = 5$, we have $A_5 \cong \mathrm{PSL}_2(\mathbb{F}_5)$, and the unique stem extension

of A_5 is

$$0 \to C_2 \to \mathrm{SL}_2(\mathbb{F}_5) \to A_5 \to 1.$$

We write $\widetilde{A}_n$ for the maximal stem extension of A_n.

4. *Let $G = S_n$ be the symmetric group on n letters. Then*

$$H_2(G, \mathbb{Z}) = \begin{cases} 1 & n \leq 3, \\ C_2 & n \geq 4. \end{cases}$$

For $n \geq 4$, there are two nonisomorphic double covers of S_n.

In fact, what we really need is not the full Schur multiplier group, but a certain quotient of it, associated to a certain union of conjugacy classes of G. To this end, fix a union of conjugacy classes $c \subset G$. Let

$$0 \to H_2(G, \mathbb{Z}) \to \widetilde{G} \to G \to 1$$

be a Schur cover. Suppose $x \in c$ and $y \in G$ commute. Lift x and y to $\widetilde{x}$ and $\widetilde{y}$, respectively, in $\widetilde{G}$. (This can be done in multiple ways; choose one arbitrarily.) Then the commutator $[\widetilde{x}, \widetilde{y}]_{\widetilde{G}}$ lies in $H_2(G, \mathbb{Z})$, and this element is independent of the choice of lifts. Call this element $\langle x, y \rangle_{\widetilde{G}}$. Let Q_c denote the subgroup of $H_2(G, \mathbb{Z})$ generated by all the $\langle x, y \rangle_{\widetilde{G}}$'s.

Definition 3.2.3. The reduced Schur multiplier of a pair (G, c) is the quotient

$$H_2(G, c, \mathbb{Z}) = H_2(G, \mathbb{Z})/Q_c.$$

A reduced Schur cover of (G, c) is the quotient $\widetilde{G}_c = \widetilde{G}/Q_c$.

A reduced Schur cover is a largest stem extension of G so that c lifts bijectively to a union of conjugacy classes $\widetilde{c} \subset \widetilde{G}_c$.

Remark 3.2.4. We will tend to be slightly sloppy with our terminology when referring to reduced Schur covers. In the future, when we refer to a reduced Schur cover

$\widetilde{G}_c$, we shall assume that it comes packaged with a union of conjugacy classes $\widetilde{c} \subset \widetilde{G}_c$ which bijects onto c, even when no explicit choice of $\widetilde{c}$ is provided.

Example. Suppose $G = A_5$. If c is the conjugacy class of 3-cycles, then $H_2(G, c, \mathbb{Z}) \cong C_2$, and the corresponding extension is

$$0 \to C_2 \to \widetilde{A}_5 \to A_5 \to 1.$$

However, if c is the conjugacy class of $(12)(34)$, then $H_2(G, c, \mathbb{Z})$ is trivial. To see this, it suffices to show that the two lifts of an element of order 2 in A_5 to $\widetilde{A}_5$ are conjugate in $\widetilde{A}_5$. Since $A_5 \cong \mathrm{PSL}_2 \mathbb{F}_5$ and $\widetilde{A}_5 \cong \mathrm{SL}_2 \mathbb{F}_5$, it suffices to work with matrices. Let $g \in \mathrm{PSL}_2 \mathbb{F}_5$ be the image of the matrix

$$\begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix}.$$

Its two lifts to $\mathrm{SL}_2 \mathbb{F}_5$ are

$$\widetilde{g}_1 = \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix}, \qquad \widetilde{g}_2 = \begin{pmatrix} -2 & 0 \\ 0 & 2 \end{pmatrix}.$$

In $\mathrm{SL}_2 \mathbb{F}_5$, $\widetilde{g}_1$ and $\widetilde{g}_2$ are conjugate, since if

$$s = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

then

$$s^{-1} \widetilde{g}_1 s = \widetilde{g}_2.$$

3.3 Lifting Invariants for Hurwitz Spaces

This section is provided for motivation, as §3.4 would not seem to be very natural without the knowledge of the material in this section. However, it is not logically necessary to read this section in order to understand the new results.

In this section, we describe lifting invariants for branched covers of the disk. That is, we describe a combinatorial algorithm to determine whether or not two covers are in the same connected component of the space of all such covers. Before we do that, we need to recall the definition of a monodromy group of a finite cover.

Definition 3.3.1. Let X be a connected topological space, and let $f : Y \to X$ be a (not necessarily connected) finite cover of X, of degree d. Let $x \in X$ be a basepoint, and let $f^{-1}(x) = \{y_1, \ldots, y_d\} \subset Y$. Suppose γ is a loop in X based at x. For each i with $1 \leq i \leq d$, there is a unique lift $\widetilde{\gamma}_i$ of γ with $\widetilde{\gamma}_i(0) = y_i$. We now define a permutation $\pi_\gamma \in S_d$ to be the permutation which sends i to j, where $\widetilde{\gamma}_i(1) = y_j$. The map $\gamma \mapsto \pi_\gamma$ induces a map $\pi_1(X, x) \to S_d$, called the monodromy representation. Its image is called the monodromy group of f.

We recall some information about Hurwitz spaces, all of which can be found in greater detail in [EVW12].

Pick a basepoint x on the boundary of the disk, and let Conf_n denote the configuration space of n distinct unlabeled points in the interior of the disk. We are interested in branched covers of the disk with n branch points. We say two such covers $f_1 : Y_1 \to D$ and $f_2 : Y_2 \to D$ are isomorphic if there exists a homeomorphism $g : Y_1 \to Y_2$ so that the triangle

$$\begin{array}{ccc} Y_1 & \xrightarrow{\quad g \quad} & Y_2 \\ & {\scriptstyle f_1}\searrow \quad \swarrow{\scriptstyle f_2} & \\ & D & \end{array}$$

commutes. In particular, f_1 and f_2 must have the same branch points.

Fix a positive integer d and a finite group $G \leq S_d$, and let $\mathrm{Hur}_{G,n}$ denote the moduli space of branched covers of the disk with n branch points and monodromy group a subgroup of G. Equivalently, a point in $\mathrm{Hur}_{G,n}$ is a point $\{P_1, \ldots, P_n\} \in \mathrm{Conf}_n$, together with a homomorphism

$$\rho : \pi_1(D^2 - \{P_1, \ldots, P_n\}, x) \to G. \tag{3.3.1}$$

There are some variants of $\mathrm{Hur}_{G,n}$ which will also be important for us.

- Let $\mathrm{CHur}_{G,n}$ be the subspace of $\mathrm{Hur}_{G,n}$ consisting of the *connected* covers. Equivalently, a cover is connected if and only if the map ρ in (3.3.1) is surjective.

- If $c \subset G$ is a union of conjugacy classes of G, let $\mathrm{Hur}^c_{G,n}$ be the subspace of $\mathrm{Hur}_{G,n}$ consisting of covers for which all the local monodromies around the P_i lie in c. Define $\mathrm{CHur}^c_{G,n}$ similarly.

- Let $\mathbb{Z}^{c/G}$ be the free abelian group on the conjugacy classes inside c. If $\mathbf{m} \in \mathbb{Z}^{c/G}$ is a multi-index, we let $\mathrm{Hur}^c_{G,\mathbf{m}}$ be the subspace of $\mathrm{Hur}^c_{G,|\mathbf{m}|}$ consisting of covers for which there are $\mathbf{m}_i$ branch points with local monodromy inside c_i for each conjugacy class $c_i \subset c$.

- We define other variants similarly.

In this section, we will be interested in understanding the connected components of $\mathrm{Hur}^c_{G,n}$. Note that, since a cover is determined up to isomorphism by its monodromy at the branch points, we can express $\pi_0 \mathrm{Hur}_{G,n}$ and $\pi_0 \mathrm{Hur}^c_{G,n}$ in terms of quotients of G^n and c^n, respectively. To do this, we need to define the braid group and its action on G^n (and c^n).

Definition 3.3.2.

- Let $n \geq 2$ be an integer. The braid group Br_n on n strands is the group generated by elements $\sigma_1, \ldots, \sigma_{n-1}$, subject to the relations $[\sigma_i, \sigma_j] = 1$ if $|i-j| \geq 2$, and
$$\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$$
for $1 \leq i \leq n-2$.

- There is an action of the braid group Br_n on G^n and c^n. If σ_i is the i^{th} generator in the presentation above, then its action on $(g_1, \ldots, g_n)$ is given by
$$\sigma_i(g_1, \ldots, g_n) = (g_1, \ldots, g_{i-1}, g_i g_{i+1} g_i^{-1}, g_i, \ldots, g_n).$$

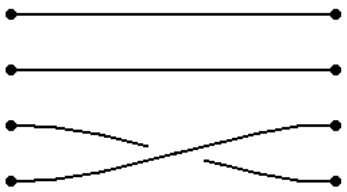


Figure 3.1: This denotes $\sigma_1 \in \mathrm{Br}_4$, where the strands are labeled 1 through 4, from bottom to top, and are considered as going from left to right.

The term "braid group" comes from making braids with n strands. We show a sample braid on four strands in Figure 3.1.

With this definition, we can make a precise statement equating connected components of Hurwitz space to n-tuples of elements of G: we have

$$\pi_0 \operatorname{Hur}_{G,n} \cong G^n / \operatorname{Br}_n, \qquad \pi_0 \operatorname{Hur}^c_{G,n} \cong c^n / \operatorname{Br}_n .$$

The maps $\pi_0 \operatorname{Hur}_{G,n} \to G^n / \operatorname{Br}_n$ and $\pi_0 \operatorname{Hur}^c_{G,n} \to c^n / \operatorname{Br}_n$ send a cover to the n-tuple of local monodromies at the branch points.

The key result is the following, based on unpublished work of Conway and Parker.

Theorem 3.3.3 (Conway-Parker)**.** *There exists a constant N, depending on G, c, and n, so that if $\mathbf{m}_i \geq N$ for all i, then*

$$\pi_0 \operatorname{CHur}^c_{G,\mathbf{m}} \xrightarrow{\sim} \widetilde{G}_c.$$

The map in the theorem has a very concrete, combinatorial description. Let $(g_1, \ldots, g_n)$ represent a class in $\pi_0 \operatorname{CHur}^c_{G,\mathbf{m}}$. Lift $g_1, \ldots, g_n \in c$ to $\widetilde{g}_1, \ldots, \widetilde{g}_n \in \widetilde{c}$. Then the lifting invariant associated to $(g_1, \ldots, g_n)$ is the product $\prod \widetilde{g}_i \in \widetilde{G}_c$.

We can give a similar description of the connected components of the space of branched covers of $\mathbb{P}^1$. The only difference is that the product of all the g_i's must be equal to 1, so we instead get a map from the connected components to $H_2(G, c, \mathbb{Z})$.

Example. Let $G = \mathrm{PSL}_2 \mathbb{F}_{11} \leq S_{12}$, and let c be the set of elements of order 3, 5, and 11. Then $H_2(G, c, \mathbb{Z}) = C_2 = \{\pm 1\}$, $\widetilde{G}_c = \mathrm{SL}_2 \mathbb{F}_{11}$, and $\widetilde{c}$ is the set of elements of

order 3, 5, and 11 inside $\mathrm{SL}_2 \mathbb{F}_{11}$. Consider two covers given by the following triples of elements of c: (g_1, g_2, g_3) and (h_1, h_2, h_3), where

$$g_1 = \begin{pmatrix} -1 & 4 \\ -1 & 3 \end{pmatrix} \qquad g_2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \qquad g_3 = \begin{pmatrix} -3 & -1 \\ -2 & -1 \end{pmatrix}$$
$$h_1 = \begin{pmatrix} -1 & 4 \\ -1 & 3 \end{pmatrix} \qquad h_2 = \begin{pmatrix} -1 & 3 \\ -4 & 0 \end{pmatrix} \qquad h_3 = \begin{pmatrix} -4 & -3 \\ 0 & -3 \end{pmatrix}$$

Then the invariant for the triple (g_1, g_2, g_3) is $1 \in H_2(G, c, \mathbb{Z})$, whereas the invariant for the triple (h_1, h_2, h_3) is $-1 \in H_2(G, c, \mathbb{Z})$. Hence (g_1, g_2, g_3) and (h_1, h_2, h_3) do not lie in the same connected component of Hurwitz space.

3.4 Invariants for Number Fields

We now introduce the invariant of Ellenberg and Venkatesh as described in [EV10]. This will be an attempt to explain (2.3.1), as follows: Ordinarily, we would expect the right-hand side of (2.3.1) to be $1/4$, but in this case, it is twice as large as we anticipate. To each surjection $\varphi : \mathrm{Cl}(K) \twoheadrightarrow C_2 \times C_2$ of $\mathbb{Z}[\zeta_3]$-modules, we associate an invariant $\mathfrak{z}(\varphi) \in \{0, 1\}$. We then hope that

$$\mathbb{E}(\#\{\varphi \in \mathrm{Surj}_{\mathbb{Z}[\zeta_3]}(\mathrm{Cl}(K), C_2 \times C_2) : \mathfrak{z}(\varphi) = 0\}) = \frac{1}{4}$$

and

$$\mathbb{E}(\#\{\varphi \in \mathrm{Surj}_{\mathbb{Z}[\zeta_3]}(\mathrm{Cl}(K), C_2 \times C_2) : \mathfrak{z}(\varphi) = 1\}) = \frac{1}{4}.$$

(For convenience, we'll overuse the notation $\mathfrak{z}$ a little bit: sometimes, we'll write $\mathfrak{z}(\varphi)$ to denote the invariant of a surjection, and sometimes we'll write $\mathfrak{z}(\rho)$ to denote the invariant of a field corresponding to a representation $\rho : G_K \to C_2 \times C_2$.)

The motivation for this comes from the case of function fields, which was studied by Ellenberg, Venkatesh, and Westerland in [EVW09]. In this case, the extensions are parametrized by a Hurwitz space, which may have several connected components. On each connected component, the number of extensions agrees (asymptotically) with

the Cohen-Lenstra predictions, but there is a discrepancy when there are multiple connected components. This is discussed at the end of [EVW12]. The invariant used there for classifying connected components of Hurwitz space is essentially the Conway-Parker invariant of §3.3.

In the number field case, we have no Hurwitz space to parametrize the extensions, but we are left with a vestige of the connected components, which are given in terms of the Schur multiplier. These vestiges of connected components are parametrized in a manner quite similar to the way connected components were parametrized in §3.3.

We now consider the following scenario, which is a modification of that considered by Ellenberg and Venkatesh in [EV10]. Let K be a number field or function field, let G be a finite group, and let $c = c_1 \cup \cdots \cup c_r \subset G$ be a union of conjugacy classes. Then, we assume that the following conditions hold:

Conditions 3.4.1.

1. G has trivial center.
2. c generates G.
3. If n is prime to the order of an element $g \in c$, then $g^n \in c$.

Example. These conditions hold if $G = A_4$ and c is the union of the two conjugacy classes of 3-cycles. They also hold if $G = A_5$ and c either the conjugacy class of 3-cycles or the conjugacy class of a product of two disjoint 2-cycles.

Lemma 3.4.2 (Ellenberg-Venkatesh)**.** *Let K be a totally real number field, let G be a finite group, and let c be a union of conjugacy classes of G, satisfying Conditions 3.4.1 above, and let $\rho : G_K \to G$ be a homomorphism so that*

1. *ρ is trivial at all infinite places.*
2. *ρ is tamely ramified, and the image of each inertia group $I_{\mathfrak{P}}$ in G_K is a cyclic subgroup contained in $c \cup \{1\}$.*

Furthermore, we assume that $2H_2(G, c, \mathbb{Z}) = 0$. Then ρ lifts to an extension $\widetilde{\rho} : G_K \to \widetilde{G}_c$ which is trivial at all infinite places and tamely ramified.

Remark 3.4.3. The conclusion of the Lemma is sometimes still valid even when the hypotheses are not all satisfied. In particular, if $G = C_2 \times C_2$ and c consists of just the identity, the conclusion still holds, even though c does not generate G. This particular case will show up again shortly.

We may now define the invariant $\mathfrak{z}(\rho) \in H_2(G, c, \mathbb{Z})$. If $H_2(G, c, \mathbb{Z}) = 0$, set $\mathfrak{z}(\rho) = 0$. Otherwise, assume that $H_2(G, c, \mathbb{Z}) \neq 0$. For each finite place v of K, let $\mathfrak{p}_v$ be the corresponding prime and k_v the residue field at v, and let q_v be the size of k_v. Let I_v be the inertia group of G_K at v, and fix an element $\pi \in \mathfrak{p}_v - \mathfrak{p}_v^2$. We have a map $I_v \to k_v^\times$, given by $\sigma \mapsto \sigma(\pi)/\pi \mod \mathfrak{p}_v$. Let g_v be any inverse image of -1 so that g_v topologically generates a subgroup of I_v^{tame} of index $\frac{q_v-1}{2}$. Now, each $x \in c$ is the image of a unique $x^* \in \widetilde{c}$.

Definition 3.4.4. The invariant $\mathfrak{z}(\rho)$ is defined to be

$$\mathfrak{z}(\rho) = \prod_{v \text{ finite}} \widetilde{\rho}(g_v)(\rho(g_v)^*)^{-1} \in H_2(G, c, \mathbb{Z}). \tag{3.4.1}$$

This invariant is independent of choice of $\widetilde{\rho}$, g_v, and I_v.

Remark 3.4.5. Definition 3.4.4 is heavily inspired by the invariant of Theorem 3.3.3. The ramified places v of K, i.e., those for which the image of inertia at v is nontrivial, are analogous to the branch points in the disk. In the Conway-Parker theorem, we define the invariant to be the product of the lifts of the local monodromies. In Definition 3.4.4, $\widetilde{\rho}(g_v)$ is analogous to the local monodromy, and $\rho(g_v)^*$ is analogous to a lift to $\widetilde{c} \subset \widetilde{G}_c$.

Definition 3.4.6. If L/K is a Galois extension with group G, we say that all ramification of L/K is of type c if L/K is tamely ramified, and for each prime $\mathfrak{P}$ of L, either $\mathfrak{P}$ is unramified, or else a generator of the inertia group at $\mathfrak{P}$ is contained in c.

We consider Galois extensions L/K with Galois group G with the following properties:

Conditions 3.4.7. 1. G and c satisfy Conditions 3.4.1 above.

2. All ramification of L/K is of type c.

3. K and L are totally real number fields.

In the case where $G = A_5$ and $K = \mathbb{Q}$, if c is the conjugacy class of 3-cycles so that $H_2(G, c, \mathbb{Z}) \cong C_2$, we can define the invariant in more down-to-earth terms. In this case, $\widetilde{G}_c = \widetilde{A}_5$ and $\widetilde{c}$ is the conjugacy class of elements of order 3 in $\widetilde{G}_c$.

Claim 3.4.8. *If $L/\mathbb{Q}$ is the A_5-field which is the fixed field of the kernel of ρ and $\widetilde{L}$ is the fixed field of the kernel of $\widetilde{\rho}$, then the invariant $\mathfrak{z}(\rho)$ is the number of primes $p \equiv 3 \pmod 4$ with even ramification degree in $\widetilde{L}$, modulo 2.*

Proof. We check the contribution to (3.4.1) at each prime. If $\widetilde{L}/L$ is unramified above v, then the contribution to the product is $1 \in \{\pm 1\}$. If $v \equiv 3 \pmod 4$ and $\widetilde{L}/L$ is ramified above v, then $\widetilde{\rho}(g_v)$ has even order in $\widetilde{G}_c$, and $\rho(g_v)^*$ has odd order, so the contribution to the product is -1. If $v \equiv 1 \pmod 4$ and $\widetilde{L}/L$ is ramified above v, then $\widetilde{\rho}(g_v)$ has odd order, as does $\rho(g_v)^*$, so they are equal. Hence in this case, the contribution to the product is 1. Thus, the product is -1 to the number of primes congruent to 3 mod 4 which ramify in $\widetilde{L}/L$. Since all ramified primes in L have odd ramification degree and all ramified primes in $\widetilde{L}/L$ have ramification degree 2, the claim is valid. ■

Remark 3.4.9. The invariant is independent of the choice of $\widetilde{L}$. Suppose we have another lift $\widetilde{L}'$. Then $\widetilde{L}$ and $\widetilde{L}'$ differ by a totally real quadratic twist $G_{\mathbb{Q}} \to C_2$ unramified at 2, and in any real quadratic field, the number of ramified primes congruent to 3 (mod 4) is even.

In the case where $G = A_4$ and $K = \mathbb{Q}$, we can take c to be the union of two conjugacy classes consisting of all 3-cycles of G. Then $H_2(G, c, \mathbb{Z}) \cong C_2$, and we take $\widetilde{G}_c = \widetilde{A}_4$ and $\widetilde{c}$ the collection of elements of order 3 in $\widetilde{G}_c$. The invariant is defined just like in the case of $G = A_5$ above: if $L/\mathbb{Q}$ is the A_4-field over $\mathbb{Q}$ which is the fixed field of a homomorphism $\rho : G_{\mathbb{Q}} \to A_4$, we can lift to an $\widetilde{A}_4$-field $\widetilde{L}$ which is tamely ramified and totally real. The invariant $\mathfrak{z}(\rho)$ is again the number of primes $p \equiv 3$ (mod 4) with even ramification degree in $\widetilde{L}$, modulo 2.

Much of the value of the invariant rests on our belief in the following conjecture:

Conjecture 3.4.10. *Assume Conditions 3.4.7 hold. As we vary L by discriminant, $\mathfrak{z}(\rho)$ is equidistributed over $H_2(G, c, \mathbb{Z})$.*

Remark 3.4.11. We can think about A_4 invariants in one of two ways. First, of course, they are invariants of A_4 fields. But an A_4 field also corresponds to a Galois cubic field K together with a Galois-equivariant surjection $\varphi : \mathrm{Cl}(K) \twoheadrightarrow C_2 \times C_2$: given such a field K and a surjection φ, we construct an unramified $C_2 \times C_2$ cover H of K, so that H is Galois over $\mathbb{Q}$ (and hence K), with $\mathrm{Gal}(H/K) \cong C_2 \times C_2$ and $\mathrm{Gal}(H/\mathbb{Q}) \cong A_4$. (This construction is described in section 3.5, and an example is given in detail in section 3.6.) Now, let c be the trivial conjugacy class in $C_2 \times C_2$. Although c does not generate $C_2 \times C_2$, the conclusion of Lemma 3.4.2 still holds. In this case, we have $H_2(G, c, \mathbb{Z}) \cong C_2$, so H lifts to fields $\widetilde{H}_1$ and $\widetilde{H}_2$, with $\mathrm{Gal}(\widetilde{H}_1/K) \cong D_8$ and $\mathrm{Gal}(\widetilde{H}_2/K) \cong Q_8$ which are tamely ramified and totally real. Since the Sylow 2-subgroup of $\widetilde{A}_4$ is isomorphic to Q_8, $\widetilde{H}_2$ is an $\widetilde{A}_4$-field. If, furthermore, all ramification in H is of type 3-cycle, then $\widetilde{H}_2$ is a lift of H of the type described above. Hence, we can also think of the invariant associated to an A_4 field H as being the invariant associated to a pair (K, φ), where K is a C_3 field an φ a surjection from $\mathrm{Cl}(K)$ to $C_2 \times C_2$.

3.5 Computing the invariant

In this section, we present an algorithm that takes an A_4 field ramified at one prime and produces an $\widetilde{A}_4$ lift of it. We then prove that the invariant associated to an A_4 field is closely related to the class group; this will help us compute tables of invariants much more quickly than if we had to construct the $\widetilde{A}_4$ field in every case.

We are now in a position to calculate the invariant associated to a totally real A_4 field H. Let c be set of all 3-cycles in A_4; this is a union of two conjugacy classes in A_4. If H is ramified at exactly one prime, we will prove below that all ramification in H is of type c, so the Lemma in the previous section tells us that we can lift H to a tamely ramified and totally real extension $\widetilde{H}$ with Galois group $\widetilde{A}_4 \cong \mathrm{SL}_2(\mathbb{F}_3)$. If H is ramified at more than one prime, all we can say is that the ramification of *some* prime is of type c.

Proposition 3.5.1. *If $E/\mathbb{Q}$ is an A_4 field ramified at exactly one rational prime, then all ramification is of type 3-cycle.*

This follows quickly from the following more general Lemma:

Lemma 3.5.2. *If $E/\mathbb{Q}$ is a finite Galois extension with Galois group G, then the inertia groups at the ramified finite places of E generate G.*

Proof. Let E_0 be the intersection of the fixed fields of all the inertia groups. Then $E_0/\mathbb{Q}$ is a finite Galois extension unramified at all finite places. Hence $E_0 = \mathbb{Q}$, and so the inertia groups generate G. ■

Proof of Proposition. There are no wildly ramified A_4 extensions of $\mathbb{Q}$ ramified at exactly one rational prime (see [Jon]), so E must be tamely ramified. Hence, its ramification type must either be that of 3-cycles, or that of products of two disjoint 2-cycles. The latter case cannot happen by the Lemma, because the products of two disjoint 2-cycles do not generate A_4. ■

Now, we shall see how to lift a totally real A_4 field H ramified at exactly one rational prime to a tamely ramified and totally real $\widetilde{A}_4$ field $\widetilde{H}$. Note that, since $\widetilde{H}/H$ will be a quadratic extension, tamely ramified is equivalent to being unramified above 2.

Algorithm 3.5.3

Input: A quartic polynomial f defining a quartic field L with Galois closure a totally real A_4 field H ramified at exactly one prime.

Output: An element $\alpha \in L$ so that $L(\sqrt{\alpha})$ with Galois closure $\widetilde{H}$, so that $\widetilde{H}$ has Galois group $\widetilde{A}_4$, and so that $\widetilde{H}$ is totally real and tamely ramified.

1. Let $\{\alpha_i\}$ be a set of representatives of $\mathfrak{o}_L^\times/\mathfrak{o}_L^{\times 2}$ which includes 1.
2. Let $\{C_j\}_{j\in J}$ be the 2-torsion ideal classes of L.
3. For $j \in J$, let I_j denote an integral ideal in C_j. Let the ideal (1) be the representative of the trivial ideal class.
4. Each I_j^2 is a principal ideal; let β_j be a generator for I_j^2.
5. Let $\gamma_1 = 1$.

6. Let p be the rational prime at which L is ramified. Then $p\mathfrak{o}_L$ splits as $\mathfrak{p}_1\mathfrak{p}_2^3$, for some prime ideals $\mathfrak{p}_1, \mathfrak{p}_2 \subset \mathfrak{o}_L$. Let $J = \mathfrak{p}_1\mathfrak{p}_2$. Suppose that the order of J in the class group is r. Let γ_2 be a generator for the principal ideal J^r.
7. Let $\Delta = \{\alpha_i\beta_j\gamma_k\}$.
8. For $\delta \in \Delta$, check if $L(\sqrt{\delta})$ has Galois group $\widetilde{A}_4$. Stop once we have found one that does, and call this element δ.
9. If $L(\sqrt{\delta})$ is tamely ramified and totally real, let $\alpha = \delta$.
10. If $L(\sqrt{\delta})$ is tamely ramified and totally complex, let q be a rational prime with $q \equiv 3 \pmod 4$ so that $L(\sqrt{\delta})$ is unramified at q. Let $\alpha = -q\delta$.
11. If $L(\sqrt{\delta})$ is wildly ramified and totally real, let q be a rational prime with $q \equiv 3 \pmod 4$ so that $L(\sqrt{\delta})$ is unramified at q. Let $\alpha = q\delta$.
12. If $L(\sqrt{\delta})$ is wildly ramified and totally complex, let $\alpha = -\delta$.
13. Return α.

Proof of Algorithm 3.5.3. By Lemma 3.4.2, we know that there is an $\alpha \in H$ so that $H(\sqrt{\alpha})$ is Galois over $\mathbb{Q}$ with Galois group $\widetilde{A}_4$. Suppose we have such an α. Let q be a rational prime different from p, and let $q\mathfrak{o}_H = \mathfrak{q}_1 \cdots \mathfrak{q}_g$. In order for $H(\sqrt{\alpha})$ to be Galois over $\mathbb{Q}$ it is necessary and sufficient that the class of α in $H^\times/H^{\times 2}$ is stable under the action of $\mathrm{Gal}(H/\mathbb{Q})$. If the class of α in $H^\times/H^{\times 2}$ is $\mathrm{Gal}(H/\mathbb{Q})$-stable, then the parity of $v_{\mathfrak{q}_i}(\alpha)$ must be the same for all i. If $v_{\mathfrak{q}_i}(\alpha) \equiv 1 \pmod 2$ for all i and the class of α is $\mathrm{Gal}(H/\mathbb{Q})$-stable, then $v_{\mathfrak{q}_i}(\alpha/q) \equiv 0 \pmod 2$ for all i, and the class of α/q is still $\mathrm{Gal}(H/\mathbb{Q})$-stable. Hence, we may assume that $v_{\mathfrak{q}}(\alpha) \equiv 0 \pmod 2$ for all primes $\mathfrak{q}$ of H lying over a rational prime different from p. Furthermore, the parities of $v_{\mathfrak{p}_i}(\alpha)$ are equal for all primes $\mathfrak{p}_i$ of H lying over p. Let Ξ be the set of square classes of H with even valuation at all primes not lying over p, and with all valuations at primes over p having the same parity.

Let B be the kernel of the map $\widetilde{A}_4 \twoheadrightarrow A_4$. Then $\widetilde{A}_4$ acts transitively and faithfully on a set of 8 objects partitioned into blocks of size 2 so that B fixes the blocks. The quotient $A_4 \cong \widetilde{A}_4/B$ acts on the blocks in the usual way that A_4 acts on 4 objects. Hence any $\widetilde{A}_4$ field is the Galois closure of an octic field obtained by adjoining the square root of some square class in a quartic field. Hence, we may restrict our list of square classes to check still further by letting Δ be the set of square classes in Ξ

which contain a representative in L. This shows that we can find a δ in Step 8 so that $L(\sqrt{\delta})$ has Galois group $\widetilde{A}_4$.

The remaining steps explain how we can twist by a quadratic character in order to remove wild ramification and ramification at ∞. Let $\widetilde{\rho} : G_{\mathbb{Q}} \to \widetilde{A}_4$ be the Galois representation corresponding to the number field $H(\sqrt{\delta})$. We can find some quadratic character $\chi : G_{\mathbb{Q}} \to C_2$ so that the representation $\chi\widetilde{\rho}$ is tamely ramified and unramified at ∞. This completes the proof. ■

Once we have found the desired $\widetilde{L}$, we can simply count the number of ramified primes congruent to 3 (mod 4) in $\widetilde{L}$ in order to determine the invariant $\mathfrak{z}(\rho)$.

Frequently, it is possible to compute the invariant without constructing an explicit lift to an $\widetilde{A}_4$ field. (Still, as a matter of good discipline and for the sake of generality, it is good to know how to perform the explicit construction.) We recall that $\mathrm{Cl}_2(K)$ denotes the Sylow 2-subgroup of $\mathrm{Cl}(K)$. We define variants such as $\mathrm{Cl}_2^+(K)$ to mean the Sylow 2-subgroup of $\mathrm{Cl}^+(K)$, and in general, a subscript of 2 in any sort of class group will denote the Sylow 2-subgroup of that class group. In the situation at hand, we have the following characterization of the invariant:

Theorem 3.5.4. *Let K be a C_3 field with prime conductor so that $\mathrm{Cl}_2(K) \cong C_2 \times C_2$, and let H be the everywhere unramified $C_2 \times C_2$ extension of K, so that H is an A_4 field. Let $L \subset H$ be the fixed field of any 3-cycle in $\mathrm{Gal}(H/\mathbb{Q})$, so that L is a non-Galois quartic field over $\mathbb{Q}$ with Galois closure H. Suppose furthermore that $\mathrm{Cl}_2^+(L)$ is cyclic. Then the invariant associated to H is equal to $\#\,\mathrm{Cl}(L) \pmod 2$.*

Proof. By the above, we have an $\widetilde{A}_4$ field $\widetilde{H}$ containing H so that $\widetilde{H}$ is totally real and tamely ramified. While the construction of $\widetilde{H}$ is not unique, any two such $\widetilde{H}$'s differ only by a quadratic twist $\chi : G_{\mathbb{Q}} \to C_2$. Let $\widetilde{\rho} : G_{\mathbb{Q}} \to \widetilde{A}_4$ be the Galois representation associated to one such $\widetilde{H}$. Suppose that $\widetilde{H}/H$ were ramified at two primes of H above two distinct primes p_1 and p_2 of $\mathbb{Q}$, so that $p_1 \equiv p_2 \equiv 3 \pmod 4$. Let $\chi : G_{\mathbb{Q}} \to C_2$ be the quadratic character associated to the number field $\mathbb{Q}(\sqrt{p_1 p_2})$. Then the number field associated to the representation $\chi\widetilde{\rho}$ is again an $\widetilde{A}_4$ field which is still tamely ramified, totally real, and contains H, and the corresponding quadratic extension of H is ramified at exactly the primes at which $\widetilde{H}$ ramifies, with the exception of the

primes above p_1 and p_2, where it is now unramified. Similarly, if $\widetilde{H}/H$ were ramified at a prime in H above some rational prime $q \equiv 1 \pmod 4$, then if χ is the quadratic character associated to $\mathbb{Q}(\sqrt{q})$, then the number field associated to the representation $\widetilde{\rho}\chi$ is now unramified at the primes above q. Hence, we may assume that there are no primes congruent to 1 (mod 4) for which the primes in H above p are ramified in $\widetilde{H}/H$, and there is at most one such prime congruent to 3 (mod 4). If we have a prime $q \equiv 3 \pmod 4$ for which the primes above q are ramified in $\widetilde{H}/H$, let χ be the quadratic character associated to $\mathbb{Q}(\sqrt{-q})$. Then the field associated to $\chi\widetilde{\rho}$ is unramified at the primes above q in H.

The above paragraph shows us how to produce a quadratic extension $\widetilde{H}/H$ unramified at all finite places, so that $\mathrm{Gal}(\widetilde{H}/\mathbb{Q}) \cong \widetilde{A}_4$. By the argument in the proof of Algorithm 3.5.3, $\widetilde{H}$ descends to a quadratic extension $\widetilde{L}$ of L, unramified at all finite places, so that the Galois closure of $\widetilde{L}$ over $\mathbb{Q}$ is $\widetilde{H}$. Hence, $\mathrm{Cl}_2^+(L)$ is nontrivial. If $\mathrm{Cl}_2^+(L)$ is cyclic, then there is a *unique* nontrivial quadratic extension of L unramified at all finite places, so this extension must be $\widetilde{L}$. In this case, $\widetilde{L}$ and hence $\widetilde{H}$ are totally real if and only if $\mathrm{Cl}_2(L)$ is nontrivial. If this happens, then $\widetilde{H}/H$ is everywhere unramified (including at infinity), so the invariant is 0. If $\mathrm{Cl}_2(L)$ is trivial, then $\widetilde{H}/H$ is ramified only at infinity, so we can twist by some character associated to a field $\mathbb{Q}(\sqrt{-p})$ for some $p \equiv 3 \pmod 4$ to obtain a totally real $\widetilde{H}$ ramified only at p. Hence, the invariant in this case is 1. In either case, the invariant is $\#\,\mathrm{Cl}_2(L) \pmod 2$. ■

Remark 3.5.5. The hypothesis that $\mathrm{Cl}_2^+(L)$ is cyclic holds very frequently. In fact, there are no exceptions in the 10^5 fields we tested for inclusion in the data given in Table 3.1.

In §3.6, we will need to start with a C_3 field K with $\mathrm{Cl}_2(K) \cong C_2 \times C_2$ and construct an A_4 field H containing K so that H/K is everywhere unramified. We now explain how that is done.

Algorithm 3.5.6

Input: A cubic polynomial f defining a Galois cubic field K.

Output: A quartic polynomial g so that the Galois closure of g is an A_4 field H containing K, with H/K everywhere unramified.

1. Let $\{\alpha_i\}$ be a set of representatives of $\mathfrak{o}_K^\times/\mathfrak{o}_K^{\times 2}$.
2. Let $\{C_j\}_{j\in J}$ be the 2-torsion ideal classes of K.
3. For $j \in J$, let I_j denote an integral ideal in C_j. Let the ideal (1) be the representative of the trivial ideal class.
4. Each I_j^2 is a principal ideal; let β_j be a generator for I_j^2.
5. Let $\Delta = \{\alpha_i\beta_j\}$.
6. For $\delta \in \Delta$, let K_δ be the Galois closure over $\mathbb{Q}$ of $K(\sqrt{\delta})$. If K_δ has Galois group A_4 and is totally real and unramified at 2, let $\alpha = \delta$ and stop.
7. Let $x^3 - a_2x^2 + a_1x - a_0$ be the minimal polynomial of α over $\mathbb{Q}$.
8. Let $b_2 = -2a_2$, $b_1 = -8\sqrt{a_0}$, $b_0 = a_2^2 - 4a_1$.
9. Let $h(x) = x^4 + b_2x^2 + b_1x + b_0$.
10. (Optional.) Using the LLL algorithm, find a polynomial g with smaller coefficients than h so that g and h generate the same field; this is implemented in PARI/GP [The08] as `polredabs`.
11. Return g.

Proof of Algorithm 3.5.6. We first show that there is some $\alpha \in \Delta$ so that the Galois closure H of $K(\sqrt{\alpha})$ has Galois group A_4 over $\mathbb{Q}$ and so that H/K is everywhere unramified. By class field theory, we know that there is some such $\alpha \in K^\times$, so it suffices to show that if $\alpha \notin \Delta K^{\times 2}$, then $K(\sqrt{\alpha})/K$ is ramified somewhere. Observe that for $K(\sqrt{\alpha})/K$ to be unramified, it is necessary (but not sufficient) that α have even valuation at all places of K. Those elements of $K^\times$ which have even valuation at all places of K are precisely the elements of $\Delta K^{\times 2}$, so this shows that we can find such an $\alpha \in \Delta$.

Now we explain the construction of $h(x)$. The A_4 field H is the Galois closure of a quartic field L over $\mathbb{Q}$. Since α has degree 3 over $\mathbb{Q}$ and is not a square, $\sqrt{\alpha}$ has degree 6. Let us call its Galois conjugates $\pm\sqrt{\alpha}, \pm\sqrt{\beta}, \pm\sqrt{\gamma}$. Now, L is generated by $r = \sqrt{\alpha}+\sqrt{\beta}+\sqrt{\gamma}$. The conjugates of r are $r_2 = \sqrt{\alpha}-\sqrt{\beta}-\sqrt{\gamma}$, $r_3 = -\sqrt{\alpha}+\sqrt{\beta}-\sqrt{\gamma}$, and $r_4 = -\sqrt{\alpha} - \sqrt{\beta} + \sqrt{\gamma}$, and so we can check explicitly that h as constructed in Algorithm 3.5.6 is the minimal polynomial of r. ∎

Suppose now that K is a C_3 field ramified at exactly one rational prime p. Then H

as constructed in Algorithm 3.5.6 is also ramified at p and nowhere else. Furthermore, H is totally real.

3.6 A sample invariant computation

Let us compute the invariant for the smallest A_4 field ramified at one prime. In order to build this A_4 field, we start with the smallest C_3 field with prime conductor and class group $C_2 \times C_2$. A polynomial generating this field is $p(x) = x^3 - x^2 - 54x + 169$. Let K denote this field, and let α be a root of p in K. The unit group is

$$\mathfrak{o}_K^\times = (\alpha - 4)^{\mathbb{Z}} \times (\alpha^2 + 4\alpha - 33)^{\mathbb{Z}} \times \{\pm 1\}.$$

Two ideals whose ideal classes generate the class group are $(5, \alpha - 2)$ and $(5, \alpha - 1)$, and the squares of these ideals are $(\alpha^2 + 4\alpha - 32)$ and $(\alpha^2 + 4\alpha - 35)$, respectively.

To find the Hilbert class field of K, it suffices to look at $K(\sqrt{\beta})$, where β is the product of elements of some subset of $\{-1, \alpha-4, \alpha^2+4\alpha-33, \alpha^2+4\alpha-32, \alpha^2+4\alpha-35\}$. We find that, if β is one of $\{\gamma_1, \gamma_2, \gamma_3\}$, where $\gamma_1 = \alpha^2 + 4\alpha - 32$, $\gamma_2 = (\alpha - 4)(\alpha^2 + 4\alpha - 33)(\alpha^2 + 4\alpha - 35) = 12\alpha^2 + 48\alpha - 395$, and $\gamma_3 = (\alpha - 4)(\alpha^2 + 4\alpha - 33)(\alpha^2 + 4\alpha - 32)(\alpha^2 + 4\alpha - 35) = 169\alpha^2 + 688\alpha - 5612$, then $K(\sqrt{\beta})$ is an unramified extension of K. Hence, if β is one of these elements, then the Hilbert class field $H(K)$ of K is the Galois closure of $K(\sqrt{\beta})$.

Now, we find an equation for a quartic field L whose Galois closure is $H(K)$. Take β as in the above paragraph, so that $H(K)$ is the Galois closure of $K(\sqrt{\beta})$. Suppose the Galois conjugates of β in K are $\beta_1 = \beta, \beta_2, \beta_3$. Then the minimal polynomial of $\sqrt{\beta}$ over $\mathbb{Q}$ has roots $\pm\sqrt{\beta_1}$, $\pm\sqrt{\beta_2}$, and $\pm\sqrt{\beta_3}$. An example of a quartic polynomial with the same Galois closure has roots $\sqrt{\beta_1}+\sqrt{\beta_2}+\sqrt{\beta_3}$, $\sqrt{\beta_1}-\sqrt{\beta_2}-\sqrt{\beta_3}$, $-\sqrt{\beta_1}+\sqrt{\beta_2}-\sqrt{\beta_3}$, and $-\sqrt{\beta_1}-\sqrt{\beta_2}+\sqrt{\beta_3}$. A polynomial with these roots is $x^4 - 34x^2 - 40x + 121$. Using the PARI/GP function `polredabs`, we find that another polynomial that generates the same field is $f(x) = x^4 - x^3 - 7x^2 + 2x + 9$. Let L be the field $\mathbb{Q}[x]/(f(x))$, and let γ be a root of f in L.

Now, we must construct a degree-8 extension of L whose Galois group is isomorphic to $\widetilde{A}_4$. First, we must find generators for the unit group of L. The unit group of L is isomorphic to $\mathbb{Z}^3 \times \{\pm 1\}$, and a basis for the torsion-free part is $\{\gamma^2 - 2, \gamma + 2, \gamma^2 - 2\gamma - 4\}$. The class group of L is trivial, so we get no contribution from 2-torsion ideal classes. Finally, L is ramified exactly at the prime 163, and (163) factors as $\mathfrak{p}_1\mathfrak{p}_2^3$, where $\mathfrak{p}_1 = (\gamma^3 - 4\gamma - 4)$ and $\mathfrak{p}_2 = (-4\gamma^3 + 9\gamma^2 + 16\gamma - 26)$. Hence, $\mathfrak{p}_1\mathfrak{p}_2 = (6\gamma^3 - 11\gamma^2 - 23\gamma + 23)$. Thus, some field of the form $L(\sqrt{\delta})$, where δ is the product of elements of some subset of $\{\gamma^2-2, \gamma+2, \gamma^2-2\gamma-4, 6\gamma^3-11\gamma^2-23\gamma+23\}$, has Galois group $\widetilde{A}_4$. We find that, if $\delta = \gamma+2$, then the Galois closure of $L_1 = L(\sqrt{\delta})$ has Galois group $\widetilde{A}_4$ over $\mathbb{Q}$. Now, L_1 is totally real, but it is ramified at 2, and hence not tamely ramified. Thus, we need to twist by a character that is ramified at one prime congruent to 3 (mod 4). In particular, $L_2 = L(\sqrt{3\delta})$ has Galois group $\widetilde{A}_4$, is totally real, and is tamely ramified, so it is a lift of the desired form. Now, in order to compute $\mathfrak{z}(\rho)$, we need to determine the number of primes congruent to 3 (mod 4) that are ramified to even order. There are two ramified primes of L_2, namely 3 and 163. Only 3 is ramified to even order, so $\mathfrak{z}(\rho) = 1$.

This computation, and all others in this paper, were done using Sage [S+10] and PARI/GP [The08].

3.7 The data

We collected data from the first 10^5 C_3 fields K ramified at exactly one prime such that the Sylow 2-subgroup of the class group is K is isomorphic to $C_2 \times C_2$ and constructed the associated A_4 fields. Of these, 53891 have invariant 1 and 46109 have invariant 0. So, while we might be forgiven for expecting that the invariant equidistributes among the two classes, the data seems to exhibit a slight bias that gradually goes away. Table 3.1 gives incremental data for the invariants.

The first column denotes the number of fields, the second denotes the number with invariant 1, and the third denotes the proportion with invariant 1. Hence, we

Table 3.1: Invariant Data

N	Invariant 1	Proportion with invariant 1
100	55	.5500
200	104	.5200
300	160	.5333
400	212	.5300
500	266	.5320
1000	536	.5360
2000	1063	.5315
4000	2183	.5458
6000	3279	.5465
8000	4372	.5465
10000	5456	.5456
20000	10862	.5431
30000	16267	.5422
40000	21638	.5410
50000	27064	.5413
60000	32400	.5400
70000	37768	.5395
80000	43176	.5397
90000	48578	.5398
100000	53891	.5389

suspect, somewhat hesitantly, that the two classes do equidistribute, but that there is a secondary term of slightly lower order that leads to an apparent bias that persists for a long time. Based on the numerical evidence, and the fact that the number of cubic fields with absolute value of the discriminant at most x is of the form

$$ax + bx^{5/6} + o(x^{5/6})$$

for certain explicitly known constants a and b (see [BST10] and [TT11]), we might conjecture that the proportion of these C_3 fields with invariant 1 among the first x by discriminant is

$$1/2 + cx^{-1/6} + o(x^{-1/6}),$$

where $c \approx 0.27$, perhaps with some logarithms thrown in because we are parametrizing fields in a slightly different manner from [BST10] and [TT11]. Still, there is not yet enough data to be able to distinguish between an error term of the form $cx^{-1/6}$ and, perhaps, $c'x^{-1/8}$, so this conjecture ought to be taken with more than a grain of salt.

Chapter 4

Background on Belyĭ maps

4.1 Introduction

In this section, we construct explicit maps of smooth projective complex algebraic curves $f : X \to Y$ that are unramified away from a few specified points. Recall that a map $f : X \to Y$ of algebraic curves of degree n is said to be unramified at $y \in Y$ if $f^{-1}(y)$ consists of exactly n distinct points, and that f is said to be unramified if it is unramified at all $y \in Y$.

Let $y \in Y$ be a point, and let $x_1, \ldots, x_r$ be the distinct preimages of y under f. (So, if f is unramified at y, then $r = n$; otherwise $r < n$.) There exists a neighborhood $U \subset Y$ of y on which f is unramified except perhaps at y. If U is sufficiently small in the analytic topology, then the x_i's are in pairwise disjoint components of $f^{-1}(U)$; write e_i for the degree (as a map of topological spaces) of the map from the component containing x_i in $f^{-1}(U)$ to U. The e_i's are called the ramification indices.

Ramification indices can be defined more precisely, and more generally, in terms of local rings. As before, let $f : X \to Y$ be a degree n map of algebraic curves (now over an arbitrary algebraically closed field k), and let $y \in Y$ be a point with $f^{-1}(y) = \{x_1, \ldots, x_r\}$. Fix some $x_i \in f^{-1}(y)$. Let $A = \mathcal{O}_{y,Y}$ be the ring of rational functions on Y regular at y; similarly, let $B = \mathcal{O}_{x_i,X}$. Both A and B are local rings, so they have unique maximal ideals $\mathfrak{p}$ and $\mathfrak{P}$, respectively. The map f induces a map $f^* : A \to B$. Now, since f^* is a *local* homomorphism, there is a unique number e_i so

that

$$f^*(\mathfrak{p})B = \mathfrak{P}^{e_i}.$$

This number e_i is the ramification index; when $k = \mathbb{C}$, this definition agrees with the preceding one.

In algebraic number theory and algebraic geometry, we tend to think of ramification as a menace. While there are only finitely many ramified points (in the case of a map of algebraic curves) or ramified primes (in the case of number fields), it is typically quite difficult to control which primes are ramified. For instance, we might try to construct number fields of degree n by writing down a "random" polynomial $f(x)$ of degree n over $\mathbb{Q}$ (which will almost certainly be irreducible, assuming our randomized selection is reasonable) and defining a number field $F = \mathbb{Q}[x]/(f(x))$. In this case, the ramified primes will be a subset of the primes dividing the discriminant of f. But trying to control the discriminant of f based on its coefficients requires us to solve a very difficult Diophantine equation.

Instead, we look for other methods to control ramification. Here, we are mostly interested in the case of algebraic curves, and the story begins with a theorem of Riemann, which we will state shortly after a brief discussion on monodromy.

Definition 4.1.1. Let $f : X \to Y$ be a covering map of degree n of topological spaces, and let $y \in Y$ be a base point. Let $f^{-1}(y) = \{x_1, \ldots, x_n\}$. Then we obtain a homomorphism $\rho : \pi_1(Y, y) \to S_n$ as follows: let γ be a loop in Y based at y. Then, for each $1 \leq i \leq n$, γ lifts uniquely to a path $\widetilde{\gamma}_i$ in X with $\widetilde{\gamma}_i(0) = x_i$. Suppose $\widetilde{\gamma}_i(1) = x_j$. Then we set $\rho([\gamma])(i) = j$. This is independent of the choice of γ in its homotopy class, and relabeling the points in $f^{-1}(y)$ is conjugation in S_n. The map ρ, defined up to conjugation in S_n, is called the monodromy representation of f, and the image of ρ is called the monodromy group of f.

In the case of a branched cover of Riemann surfaces, we also have a notion of local monodromy.

Definition 4.1.2. Let $f : X \to Y$ to be a branched cover of Riemann surfaces of degree n. Let $y_1, \ldots, y_r$ be the branch points, and pick a base point $v \in Y$

distinct from the branch points. For each branch point $y_i \in Y$, fix a loop $\gamma_i \in \pi_1(Y - \{y_1, \ldots, y_r\}, v)$ which has winding number 1 around y_i and winding number 0 around y_j for $j \neq i$. Let $x_1, \ldots, x_n$ be the preimages of v under f. Then each γ_i induces a permutation $\sigma_i \in S_n$, defined as follows. For each $j = 1, \ldots, n$, lift γ_i to $\widetilde{\gamma}_{ij}$ in such a way that $\widetilde{\gamma}_{ij}(0) = x_j$. Define $\sigma_i(j)$ by the rule $\widetilde{\gamma}_{ij}(1) = x_{\sigma_i(j)}$. The permutation σ_i is called the local monodromy around y_i with respect to γ_i.

Note that the local monodromies do depend on the choice of γ_i.

Riemann's Existence Theorem tells us that if we start with a (possibly punctured) Riemann surface Y and a homomorphism $\rho : \pi_1(Y, y) \to S_n$, then we can build an X and a map $f : X \to Y$ of degree n so that the monodromy representation of f is ρ. More precisely:

Theorem 4.1.3 (Riemann's Existence Theorem)**.** *Suppose Y is a connected Riemann surface (possibly with several punctures). If $n \geq 1$ and $\rho : \pi_1(Y) \to S_n$ is a homomorphism whose image is a transitive permutation group, then there exists a connected Riemann surface X (possibly with several punctures) and a map $f : X \to Y$ realizing ρ as its monodromy. Furthermore, X and f are unique up to isomorphism.*

We can also fill in the punctures to obtain a branched covering $X' \to Y'$, so that X' and Y' are compact Riemann surfaces. The relevance of this result for our purposes is that not only do X' and Y' have the structure of compact Riemann surfaces, but they actually have the structure of algebraic curves. More precisely:

Theorem 4.1.4. *There is an equivalence of categories between the category of compact Riemann surfaces and the category of smooth projective algebraic curves over the complex numbers.*

Hence, we are free to study either compact Riemann surfaces or smooth projective complex algebraic curves, whichever happens to be more convenient.

There are many other versions of Riemann's Existence Theorem. The version quoted in Theorem 4.1.3 can be found in [Don11], §4.2.2. Theorem 4.1.4 is a deep result. See [Har77], page 441, and the references found there for a discussion of this theorem.

4.2 Connection to Number Theory

In 1979, Belyĭ proved the following remarkable theorem:

Theorem 4.2.1 (Belyĭ, [Bel79]). *An algebraic curve C, defined initially over a field of characteristic zero, can be defined over $\overline{\mathbb{Q}}$ if and only if there exists a map $f : C \to \mathbb{P}^1$ which is ramified above three points.*

In fact, such a curve C with a map $f : C \to \mathbb{P}^1$ ramified above three points isn't just defined over $\overline{\mathbb{Q}}$; rather, both C and f can be defined over some number field, which we call a field of definition for C. However, the field of definition is not quite the correct object to study, since a curve and map may be definable over many fields. To define the correct object, we need to put a Galois action on the set of equivalence classes of Belyĭ pairs.

For $i \in \{0, 1, \infty\}$, fix loops γ_i around $i \in \mathbb{P}^1$ so that $\gamma_0\gamma_1\gamma_\infty$ is the trivial element of $\pi_1(\mathbb{P}^1 - \{0, 1, \infty\})$. Let $f : C \to \mathbb{P}^1$ and $g : D \to \mathbb{P}^1$ be two Belyĭ pairs. We say that (C, f) and (D, g) are equivalent if f and g have the same degree n, and the local monodromies $\sigma_0, \sigma_1, \sigma_\infty$ and $\sigma_0', \sigma_1', \sigma_\infty'$ around 0, 1, and ∞ with respect to the γ_i of f and g, respectively, are simultaneously conjugate, i.e., there is some $\tau \in S_n$ so that $\tau^{-1}\sigma_i\tau = \sigma_i'$ for $i = 0, 1, \infty$. There is an action of $\Gamma = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the set of Belyĭ pairs, given by acting on all coefficients of the curve and the map; this action descends to an action on the set of equivalence classes of Belyĭ pairs.

Definition 4.2.2. Let (C, f) be a Belyĭ pair. Then the field of moduli of (C, f) is the fixed field of the stabilizer of the equivalence class of (C, f).

The field of moduli, which can also be described as the intersection of all the fields of definition for C inside a fixed algebraic closure of $\mathbb{Q}$, is a better-behaved object than a field of definition. Such fields are of considerable arithmetic interest, thanks to the following result of Beckmann:

Theorem 4.2.3 (Beckmann, [Bec89]). *Let $f : X \to \mathbb{P}^1$ be a Belyĭ map, and let M be the field of moduli for X and f. Let G be the monodromy group of f. Then if p is a prime not dividing the order of G, then X and f have good reduction at p, and p is unramified in M.*

The converse fails, although somewhat infrequently: if p divides the order of G, then p might still be unramified in M. This turns out to be an important point: if we wish to construct fields which are unramified outside a finite set of primes, we may wish to allow monodromy groups whose orders have more prime factors, with the hope that some of these extra primes will accidentally turn out to be unramified. This situation is analogous to the difference between field discriminants and polynomial discriminants: the primes dividing the field discriminant are exactly the ramified primes. The field discriminant divides the polynomial discriminant for any defining polynomial of the field, but there may be extraneous primes dividing the polynomial discriminant which are nevertheless unramified in the field.

In fact, Beckmann's Theorem also works for more general branched covers of curves over number fields.

Theorem 4.2.4 (Beckmann, [Bec89])**.** *Let Y be an algebraic curve over a number field K and $f : X \to Y$ a branched cover with monodromy group G. Then if $\mathfrak{p}$ is a prime of K lying outside the union of*

1. *the set of primes $\mathfrak{q}$ dividing the order of G,*
2. *the set of primes of bad reduction of Y,*
3. *the set of primes $\mathfrak{q}$ for which the branch locus becomes singular modulo $\mathfrak{q}$,*

then X and f have good reduction at $\mathfrak{p}$, and $\mathfrak{p}$ is unramified in the field of moduli of X and f.

Roberts in [Rob04] has used this theorem to great effect to construct several fields of moderately large degree which are unramified outside $\{2, 3\}$. The point, as we shall soon see, is that writing down explicit Belyĭ maps of moderately large degree can be done relatively quickly with a computer. We shall work out some examples later.

4.3 Generalities on Belyĭ maps

We quickly give just enough background for what we'll need regarding Belyĭ maps; a delightful and more leisurely exposition of this material can be found in [LZ04], and

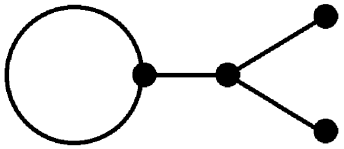


Figure 4.1: A sample dessin on $\mathbb{P}^1$. The black dots are points in $f^{-1}(1)$, and the elements of $f^{-1}(0)$ are in bijection with the edges between two black dots. We will soon see how to compute f from looking at the diagram.

reading it comes with this author's highest recommendation.

Following Belyĭ, Grothendieck noted in his famous "Esquisse d'un Programme" [Gro97] that, corresponding to an algebraic curve C (defined over the complex numbers initially, and over $\overline{\mathbb{Q}}$ by Belyĭ's Theorem) together with a Belyĭ map $f : C \to \mathbb{P}^1$ ramified above three points (which we can allow to be 0, 1, and ∞), we can associate a diagram called a dessin d'enfant, or simply a dessin. The dessin of f is defined to be $f^{-1}([0,1]) \subset C(\mathbb{C})$. Typically, we think of a dessin as being a (fat) graph on the Riemann surface $C(\mathbb{C})$, and it is tempting to draw a picture of it, as we have in Figure 4.1.

Remark 4.3.1. When we draw such a picture, we typically do not wish to think of its edges and vertices as consisting of specific points in $C(\mathbb{C})$; rather, we consider it only as a representative of an isomorphism class of fat graphs on $C(\mathbb{C})$. Hence, the picture of the actual points in $C(\mathbb{C})$ may look different; for example, they may be rotated, and some parts of the diagram may be scaled differently.

We can read off a fair bit of combinatorial data from looking at a dessin. Most importantly, we can determine the local monodromies around 0, 1, and ∞ of the target $\mathbb{P}^1$.

As an example, let us compute the local monodromies around 0, 1, and ∞ of the dessin in Figure 4.1. In figure 4.2, we have drawn white dots to represent the elements of $f^{-1}(0)$, and we have arbitrarily labeled the edges and placed the number to the right of the corresponding edge when we think of the edge as being directed from the black dot to the white dot. To obtain the local monodromy around 0, consider traversing a

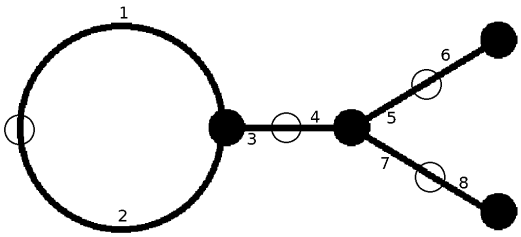


Figure 4.2: The same dessin as in Figure 4.1, but now with the white dots representing the elements of $f^{-1}(0)$, and with the edges labeled (in an arbitrary manner).

small counterclockwise circle around each white dot. Each circle will intersect several edges; the edges it intersects will form a cycle in the cycle decomposition of the local monodromy. Multiply these cycles together for all such white points to obtain the full local monodromy around 0. In this case, the local monodromy around 0 is

$$\sigma_0 = (12)(34)(56)(78).$$

Similarly, to obtain the local monodromy around 1, we traverse small counterclockwise circles around each black point to obtain the cycle decomposition. Hence, the local monodromy around 1 is

$$\sigma_1 = (123)(475)(6)(8).$$

One way to obtain the local monodromy around ∞ would be to use the relation $\sigma_0\sigma_1\sigma_\infty = 1$ to see that

$$\sigma_\infty = (1465873)(2).$$

Alternatively, we could look at each connected component of the complement of the dessin and travel around the boundary of that component in the *clockwise* direction and record the cycle consisting of the edge numbers we encounter in order. (This is why we have insisted on placing the edge numbers on the right!) This of course also tells us that

$$\sigma_\infty = (1465873)(2).$$

From here, we can determine the monodromy group of our dessin: it is the subgroup of the symmetric group (in this case, S_8) generated by σ_0 and σ_1. In this case, the monodromy group is the unique simple group of order 168, namely $\mathrm{GL}_3(\mathbb{F}_2) \cong \mathrm{PSL}_2(\mathbb{F}_7)$.

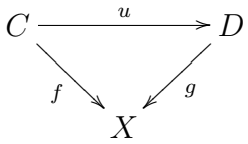
Conversely, if we are given three permutations $\sigma_0, \sigma_1, \sigma_\infty \in S_n$ with the property that $\sigma_0\sigma_1\sigma_\infty = 1$, we can find some algebraic curve C together with a Belyĭ function $f : C \to \mathbb{P}^1$ realizing these three permutations. For $i \in \{0, 1, \infty\}$, let p_i denote the cycle type of σ_i; we think of p_i as a partition of n. The curve C will be connected if and only if $\langle \sigma_0, \sigma_1, \sigma_\infty \rangle \leq S_n$ is a transitive permutation group. In the case that C is connected, the Riemann-Hurwitz formula tells us that if there are a total of r parts in p_0, p_1, p_∞, then C has genus $\frac{1}{2}(n + 2 - r)$.

The following definitions will be useful in the remainder of this section.

Definition 4.3.2. The triple $(\sigma_0, \sigma_1, \sigma_\infty)$ of permutations is called the constellation of the dessin (or the Belyĭ function). The triple (p_0, p_1, p_∞) of partitions of n is called the passport.

Note that the monodromy group is the group generated by σ_0, σ_1, and σ_∞.

Definition 4.3.3. Let $f : C \to X$ and $g : D \to X$ be two branched coverings of algebraic curves. We say that f and g are isomorphic if there exists an isomorphism $u : C \to D$ of algebraic curves so that the diagram



is commutative.

4.4 Computations of Belyĭ maps

In the case when $C = \mathbb{P}^1$, it is frequently possible to compute Belyĭ maps explicitly in a rather short amount of time. The process is perhaps best illustrated with an example.

Example. Let us suppose that we wish to find a Belyĭ map f of degree 6 on an algebraic curve C realizing the passport $p_0 = (4+1+1)$, $p_1 = (3+2+1)$, and $p_\infty = (4+2)$. By the genus formula given in the introduction, we know that C has genus 0. Hence, we can write f as a rational function in one variable. Such a function f has a quadruple zero at one point together with two simple zeros, and also has a quadruple pole at one point, and a double pole at another. After applying a suitable Möbius transformation, we may assume that the quadruple zero is at 0 and the quadruple pole is at ∞. Furthermore, if we let $g(x) = f(x) - 1$, then we know that g must have a triple zero at some point, a double zero at another point, and a simple zero at yet another one. We may also assume that the triple zero of g is at 1. Hence, there are eight points of interest to us, of which we have fixed three. So, there are five points left to locate, as well as a scaling constant.

Putting all this information together tells us that we can write

$$f(x) = K\frac{x^4(x^2+ax+b)}{(x-e)^2}$$

and

$$g(x) = f(x) - 1 = K\frac{(x-1)^3(x-c)^2(x-d)}{(x-e)^2}$$

for suitable constants a, b, c, d, e, K. These constraints yield a system of equations

$$\begin{aligned}
e^2 + c^2dK &= 0\\
-2e - c^2K - 2cdK - 3c^2dK &= 0\\
1 + 2cK + 3c^2K + dK + 6cdK + 3c^2dK &= 0\\
-K - 6cK - 3c^2K - 3dK - 6cdK - c^2dK &= 0\\
3K + 6cK + c^2K + 3dK + 2cdK &= bK\\
-3K - 2cK - dK &= aK.
\end{aligned}$$

This system of equations is sufficiently straightforward that Mathematica can solve it in a matter of seconds, but the resulting algebraic numbers ought not be displayed in full in polite society. However, we can write down the minimal polynomials in

concise form, and all the coefficients are defined over the quartic field defined by $x^4 - 2x^3 + 6x^2 - 6$, which has discriminant $-2^6 \cdot 3^3 \cdot 5$.

Let $p = (p_0, p_1, p_\infty)$ be a passport, and let Σ be the set of constellations $(\sigma_0, \sigma_1, \sigma_\infty)$ in S_n. We define an equivalence relation $\sim$ on Σ by saying that $(\sigma_0, \sigma_1, \sigma_\infty) \sim (\tau_0, \tau_1, \tau_\infty)$ if there is some $\rho \in S_n$ so that $\rho^{-1}\sigma_i\rho = \tau_i$ for all $i \in \{0, 1, \infty\}$. One can verify that two dessins are isomorphic if and only if they have equivalent constellations, as is done in [LZ04], Proposition 1.2.16.

Example. Let's return to the case of Figure 4.1. To determine the equation here, we must first work out the passport. In a neighborhood of each point in $f^{-1}(0)$, the image of f contains two copies of $[0, \varepsilon]$, for ε sufficiently small. Since there are four such points, $p_0 = (2 + 2 + 2 + 2)$. Similarly, in a neighborhood of each point in $f^{-1}(1)$, the image of f contains several copies of $[1 - \varepsilon, 1]$ for ε sufficiently small; the number of copies is equal to the number of edges emanating from that vertex. Hence $p_1 = (3+3+1+1)$. Finally, the elements of $f^{-1}(\infty)$ are in bijection with the faces of the diagram, and the degrees are equal to the number of vertices we reach traveling around the face (counted with multiplicity). Hence $p_\infty = (7 + 1)$.

Since the automorphism group of $\mathbb{P}^1$ is 3-transitive, we are allowed three normalization conditions for the function, so we can assume that the pole of order 7 is at ∞, the simple pole is at 1, and that the sum of the four double zeros is 0. Hence, we can write

$$f(x) = K\frac{(x^4 + ax^2 + bx + c)^2}{x - 1}$$

and

$$f(x) - 1 = K\frac{(x^2 + dx + e)^3(x^2 + fx + g)}{x - 1}.$$

Mathematica solves the system of equations easily, giving us

$$\begin{aligned} a &= -\frac{6}{7}, \\ b &= -\frac{32}{49}, \\ c &= \frac{159}{343}, \\ d &= -\frac{4}{7}, \\ e &= -\frac{17}{49}, \\ f &= \frac{12}{7}, \\ g &= \frac{9}{7}, \\ K &= -\frac{823543}{221184}. \end{aligned}$$

(We could, of course, choose different normalization conditions, for instance, by putting the simple pole somewhere else, which would give us different Belyĭ maps, but they would all be isomorphic.)

4.5 Extracting Number Fields with Limited Ramification from Dessins

As we mentioned in section 4.2, it is possible to construct number fields unramified outside primes dividing $|G|$ and ∞ with Galois group G from a Belyĭ map $f : \mathbb{P}^1 \to \mathbb{P}^1$ of degree n and monodromy group G. Let us demonstrate this technique with an example in Figure 4.1, as the example will show us how to perform this construction in full generality. From the previous section, we know that the Belyĭ map is given by

$$f(x) = -\frac{7(343x^4 - 294x^2 - 224x + 159)^2}{221184(x-1)}.$$

Now, consider the polynomial

$$g(x,t) = -7(343x^4 - 294x^2 - 224x + 159)^2 + t(221184(x-1)).$$

The polynomial discriminant of $g(x,t)$ is

$$-2^{104}3^{24}7^{49}t^4(t+1)^4.$$

Hence, if t is chosen so that $g(x,t)$ is irreducible, and K_t is a root field of $g(x,t)$, then the only primes that can ramify (or, equivalently, divide the discriminant of K_t) are 2, 3, 7, and the primes dividing t and $t+1$. Choosing $t = -2$, for instance, then gives us a field ramified only at 2, 3, and 7, with Galois group $\mathrm{PGL}_2(\mathbb{F}_7)$.

Note that the monodromy group $\mathrm{PSL}_2(\mathbb{F}_7)$ and the Galois group $\mathrm{PGL}_2(\mathbb{F}_7)$ are quite closely related. The monodromy group is in fact the Galois group of a slightly different extension, of function fields of curves, and it coincides with the monodromy group of the corresponding cover of curves. If we delete the ramified points from the source and target $\mathbb{P}^1$'s for f, we obtain a covering space $f : X_1 \to Y_1$ of punctured genus-0 curves. However, this cover is not Galois; let X_2 be the Galois closure of f. Now, let X and Y be the obvious compactifications of X_2 and Y_1, respectively. Then f induces a map $f' : X \to Y = \mathbb{P}^1$ ramified above three points. Since the monodromy group of the dessin has order 168, we know that f' has degree 168. Now, $\overline{\mathbb{Q}}(X)/\overline{\mathbb{Q}}(Y)$ is a Galois field extension with Galois group equal to the monodromy group of the dessin. We have a natural map

$$\mathrm{Gal}(\overline{\mathbb{Q}}(X)/\overline{\mathbb{Q}}(Y)) \hookrightarrow \mathrm{Gal}(\mathbb{Q}(X)/\mathbb{Q}(Y)), \tag{4.5.1}$$

which is induced from taking the composita of $\mathbb{Q}(X)$ and $\mathbb{Q}(Y)$ with $\overline{\mathbb{Q}}$. Furthermore, the group on the left of (4.5.1) is *normal* in the group on the right.

Now, by Hilbert's Irreducibility Theorem (see [Völ96], Theorem 1.23), the Galois groups of the specializations of $\mathbb{Q}(X)/\mathbb{Q}(Y)$ are equal to $\mathrm{Gal}(\mathbb{Q}(X)/\mathbb{Q}(Y))$ for all but a thin set of specializations. Hence, even before computing any Galois groups, we knew that the Galois groups of $g(x,t)$ would contain $\mathrm{PSL}_2(\mathbb{F}_7)$ as a normal subgroup

for almost all values of t. In this case, the quotient is $C_2 \cong \mathrm{Gal}(\mathbb{Q}(\sqrt{-7})/\mathbb{Q})$. Indeed, the Galois group of $g(x,t)$ over $\mathbb{Q}(\sqrt{-7})$ is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_7)$ for almost all t; it is $\mathrm{PGL}_2(\mathbb{F}_7)$ over any number field not containing $\mathbb{Q}(\sqrt{-7})$.

Chapter 5

Origamis

5.1 Introduction

In addition to studying Belyĭ maps, it is also interesting to consider branched covers of other algebraic curves. Moving up a genus, then, we can attempt to construct branched covers of elliptic curves. This is a more difficult problem, but it is still possible to give concrete covers in at least a few cases.

By the Riemann-Hurwitz formula, an unramified cover of a genus-1 curve must again be a genus-1 curve, which means that such a map is simply a composition of an isogeny of elliptic curves and a translation. Since these maps are well-understood, we will not be concerned with them here.

However, if we allow one branched point on our elliptic curve, then there are covers by higher-genus curves. These one-point covers admit a pictorial interpretation analogous to that of dessins for Belyĭ maps. Such maps are called origamis.

Over $\mathbb{C}$, any elliptic curve E can be written as $\mathbb{C}/\Lambda$, for some lattice $\Lambda \subset \mathbb{C}$. We will find it most helpful to think of E as a fundamental parallelogram for Λ. The choice of lattice Λ or fundamental parallelogram determines the complex structure on E. Many of our arguments in this section do not depend on the choice of complex structure; when this happens, we choose to work with the square lattice $\Lambda = \mathbb{Z}[i]$, and our fundamental parallelogram of choice will be the square S with vertices 0, 1, $1+i$, and i. (The only reason we prefer this parallelogram is that it is easier to draw than

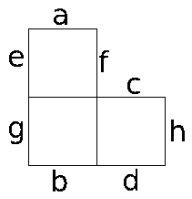


Figure 5.1: This diagram represents a genus-2 curve with a degree-3 map to the elliptic curve $y^2 = x^3 - x$. Here we identify opposite edges, meaning that edge a is identified with edge b, edge c with edge d, edge e with edge f, and edge g with edge h.

are other parallelograms. It should not generally be assumed that we are interested in the special properties of the elliptic curve $\mathbb{C}/\mathbb{Z}[i]$ not enjoyed by other elliptic curves.) Our elliptic curve will then be the square, with opposite edges identified.

Now, consider a disjoint union of n translates of S, and identify various edges to form an orientable surface X subject to the following requirements:

1. X is connected.

2. Every left edge is identified with a unique right edge, and vice versa.

3. Every top edge is identified with a bottom edge, and vice versa.

If we remove all the vertices of the n squares, the resulting figure carries the structure of a Riemann surface, obtaining its complex structure whose charts are (slightly enlarged versions of) the original n squares minus the vertices. The resulting Riemann surface $\widetilde{X}$ is then a compact Riemann surface with several punctures. There is a unique way of compactifying $\widetilde{X}$ so that its compactification is a compact Riemann surface; we call this Riemann surface X. Furthermore, X admits a map to the elliptic curve $\mathbb{C}/\mathbb{Z}[i]$ by mapping a point in any translate of S to the corresponding point in S. This map is branched only above the vertex of S. An example can be seen in Figure 5.1. In this diagram, we have explained the edge identification; in the future, if there are no markings on the edges, we take this to mean that opposite edges are identified.

Had we chosen to distinguish a different elliptic curve with a different fundamental parallelogram P, the corresponding origami would simply consist of of a disjoint union of n translates of P with similar edge identifications.

The origami diagram, though apparently extremely simple, turns out to carry a wealth of combinatorial information in readily available form. We will see later how to read off some of this information at various points throughout this chapter.

5.2 A first computation of an algebraic origami

In this section, we construct a family of examples of explicit origamis, one for each genus g.

Definition 5.2.1. We say that an origami is totally ramified if the preimage of the branch point is a single point.

The origamis we construct here will all be totally ramified. Later, we construct origamis which are not totally ramified.

Theorem 5.2.2. *For each $g \geq 1$ and $t \neq 0, -1$, the genus-g curve*

$$C_t : y^2 = x(x+1)(x^{2g-1} + tj(x)^2),$$

where

$$j(x) = \sum_{i=0}^{g-1} \binom{2g-1}{2i} (x+1)^i,$$

admits a degree $2g-1$ map to the elliptic curve

$$E_t : y^2 = x(x+1)(x+t),$$

totally ramified above $(0,0)$ and unramified everywhere else. The map is given by $(x,y) \mapsto (f_1(x), f_2(x)y)$, where

$$f_1(x) = \frac{x^{2g-1}}{j(x)^2}$$

and

$$f_2(x) = \frac{x^{g-1}\sum_{i=0}^{g-1}\binom{2g-1}{2i+1}(x+1)^i}{j(x)^3}.$$

Proof. We first check that $(f_1(x), f_2(x)y)$ actually gives a map from C_t to E_t. This amounts to checking that

$$f_2(x)^2(x(x+1)(x^{2g-1}+tj(x)^2)) = f_1(x)(f_1(x)+1)(f_1(x)+t)$$

is a formal identity. This does happen to be the case; hence $(f_1(x), f_2(x)y)$ does define a map from C_t to E_t.

Now, we check that the ramification type is as claimed. To do this, we check that if $f(x,y) = (f_1(x), f_2(x)y)$ is the map above, and $\omega = \frac{dx}{y} \in \Omega^1_{E_t}$ is an invariant differential on E_t, then

$$f^*\omega = (2g-1)\frac{x^{g-1}\,dx}{y}.$$

Hence, f is totally ramified at $(0,0)$ and unramified everywhere else. ■

Remark 5.2.3. It is worth noting that the map $(f_1(x), f_2(x)y)$ is independent of t and hence defines a map $F : \mathbb{P}^2_{\mathbb{C}} \to \mathbb{P}^2_{\mathbb{C}}$. If we fix an elliptic curve E_t in the target $\mathbb{P}^2$, then $F^{-1}(E_t)$ is a union of several irreducible components, one of which is C_t. It is also worth noting that if we take $t = 0$ or $t = -1$, then E_t is a nodal cubic, and C_t is a singular quintic of arithmetic genus 0. This will be relevant later in this section.

The proof given above thoroughly fails to capture the motivation that went into the discovery of this result. In fact, the story of finding these examples is much more interesting than is the given proof. Therefore, we now discuss how the reader could (and the author did) discover such an example. To do this, we carefully work with the lowest-degree example: that of a degree-3 origami from a genus-2 curve to an elliptic curve. Such an origami must necessarily be totally ramified.

In the remainder of this section, as well as in future sections, we perform some educated guesswork; it will not be clear whether our guesses will turn out to be successful until we present a proof in the style of that of Theorem 5.2.2.

We will construct a family of genus-2 curves mapping to a family of elliptic curves, parametrized (essentially) by their Legendre form. Hence, for any j-invariant other

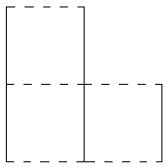


Figure 5.2: Here, we shrink the dotted edges to a point. The resulting surface has geometric genus 0.

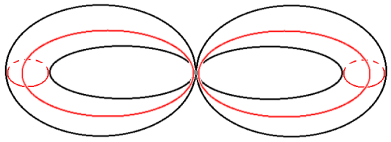


Figure 5.3: A three-dimensional version of Figure 5.2.

than 0 or 1728, we will actually construct six genus-2 curves mapping to an elliptic curve with this j-invariant. These six genus-2 curves are generically all distinct.

To do this, we start by constructing a cover C' of the nodal cubic

$$E' : y^2 = x^3 + x^2,$$

which we expect to arise as a degeneration of covers of elliptic curves which limit to E'. One possibility is that the degenerate origami diagram will look like Figure 5.2, with the dotted edges collapsed to a point. The curve represented by this origami has geometric genus 0, since it is a double torus with three pinched loops, as in Figure 5.3. Furthermore, since the origamis are totally ramified, the family of covers must degenerate to a curve with only one preimage of the branch point in E'. Finally, a map $C' \to E'$ can be described as a map from the normalization of C' to the normalization of E'.

The next thing to do is to construct explicit equations for C', as well as their normalization maps. While in general this is a notoriously difficult problem, it is easy in this case. By the picture, we can see that C' has one nodal point and has geometric

genus 0; hence it has a Weierstraß equation of the form $y^2 = (x-a)^4(x-b)$. We choose to take $a = 0$ and $b = -1$ so that we obtain the curve

$$C' : y^2 = x^5 + x^4.$$

To compute the normalization of E', we note that the map $E' \to \mathbb{P}^1$ given by $(x, y) \to x + 1$ has a square root y/x in $\mathbb{C}(E')$. Letting $u = y/x$, we have $x = u^2 - 1$ and $y = u^3 - u$, so $\mathbb{C}(E') = \mathbb{C}(u)$, and the normalization map is $\mathbb{P}^1 \to E'$, given by $u \mapsto (u^2 - 1, u^3 - u)$. A similar computation shows that the normalization of C' is $\mathbb{P}^1 \to C'$, given by $t \mapsto (t^2 - 1, t(t^2 - 1)^2)$. Note that, in the normalizations of both C' and E', the preimage of the nodal point is $\{\pm 1\} \subset \mathbb{P}^1$.

Earlier, we worked out that the map on normalizations must have degree 3 and exactly two branch points. Furthermore, the branch points must be $\{\pm 1\}$, and their preimages must be $\{\pm 1\}$. Fortunately, there are very few maps $\mathbb{P}^1 \to \mathbb{P}^1$ with only two branch points: they are simply conjugates of $z \mapsto z^n$, where n is the degree of the map. In this case, the map on normalizations is

$$z \mapsto \frac{z^3 + 3z}{3z^2 + 1}.$$

Now, in order to compute the map $f : C' \to E'$, note that we have the following commutative diagram:

$$\begin{array}{ccc} \mathbb{P}^1 & \longrightarrow & \mathbb{P}^1 \\ \downarrow & & \downarrow \\ C' & \xrightarrow{f} & E' \end{array}$$

Furthermore, the vertical maps have near-inverses; the inverse of the vertical arrow on the left is given by $(x, y) \mapsto y/x^2$. Hence, f is the composition of the other three arrows; putting this together, we have

$$f(x, y) = \left(\frac{x^3}{(3x+4)^2}, \frac{xy(x+4)}{(3x+4)^3} \right).$$

We now proceed to prolong f to a map from a family of genus-2 curves to the

Legendre family of elliptic curves by means of deformations.

In order to figure out the map from a family of nonsingular genus-2 curves to a family of elliptic curves, we deform the defining equation for the nodal quintic and for the map. We let the defining equation of the genus-2 curve be

$$C_t : y^2 = x^5 + (1 + at)x^4 + btx^3 + ctx^2 + dtx,$$

where $a, b, c, d \in \mathbb{C}[\![t]\!]$. The defining equation of the elliptic curve will be

$$E_t : y^2 = x(x + 1)(x + t).$$

The map will be

$$(x, y) \mapsto \left(\frac{x^3}{((3 + et)x + (4 + ft))^2}, \frac{(x^2 + (4 + gt)x)y}{((3 + et)x + (4 + ft))^2} \right).$$

A priori, a, b, c, d, e, f, g are power series in t; for now, we are only interested in their constant terms. Expanding everything out and equating the tx^i terms for various values of i gives us a system of linear equations; we then find that

$$\begin{aligned} a &= 9 \\ b &= 33 \\ c &= 40 \\ d &= 16 \\ e = f &= g = 0 \end{aligned}$$

is a solution. Miraculously, these values of a, b, c, d, e, f, g are not merely the constant terms of power series; they are in fact the entire power series. Hence, if we let

$$C_t : y^2 = x^5 + (1 + 9t)x^4 + 33tx^3 + 40tx^2 + 16tx$$

and

$$E_t : y^2 = x(x + 1)(x + t),$$

then

$$f(x,y) = \left(\frac{x^3}{(3x+4)^2}, \frac{xy(x+4)}{(3x+4)^3} \right)$$

is a map $f : C_t \to E_t$. Indeed, this map is only branched over $(0,0)$, with its preimage being $(0,0)$; we can check this directly, or we can verify that the pullback of the invariant differential $\omega = \frac{dx}{y} \in \Omega^1_{E_t}$ (which has no zeros or poles) is $3x\frac{dx}{y} \in \Omega^1_{C_t}$, which has a double zero at $(0,0)$ and no other zeros or poles.

The same method allows us to construct totally ramified origamis in every genus. For instance, in genus 3, we let

$$C_t : y^2 = x^7 + (1+25t)x^6 + 225tx^5 + 760tx^4 + 1200tx^3 + 896tx^2 + 256tx$$

and

$$E_t : y^2 = x(x+1)(x+t).$$

Then

$$f(x,y) = \left(\frac{x^5}{(5x^2+20x+16)^2}, \frac{x^3(x^2+12x+16)y}{(5x^2+20x+16)^2} \right)$$

is a totally ramified origami $f : C_t \to E_t$.

It is worth noticing that, in these cases, we need only change the equation of the genus-g curve as t varies; in particular, the map does not change. Hence, we have a map $f : \mathbb{P}^2 \to \mathbb{P}^2$ so that the inverse images of elliptic curves in a certain family are all genus-g curves, so that the map is an origami. The proof above explains this phenomenon.

It would be interesting to see this method generalize to cases where the base need not be an elliptic curve. In particular, we would like to know to what extent is it possible to construct branched covers of a curve C in $\mathbb{P}^2$ by constructing a suitable map $f : \mathbb{P}^2 \to \mathbb{P}^2$, chosen so that its branch locus is consistent with the desired branching properties of the cover of C, and restricting to the map $f\,|_D \colon D \to C$, where D is some irreducible component inside $f^{-1}(C)$ for which $f\,|_D \colon D \to C$ is flat. The author has used this method to construct several examples of branched covers of higher-genus curves, but a detailed study of this method may be the topic of future work.

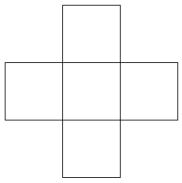


Figure 5.4: This is an origami diagram for a genus-2 curve with a degree-5 map to an elliptic curve. Above the branch point, we have one triple point and two unramified points. We call this origami a Swiss cross.

5.3 A non-totally ramified example

The method described in the last section works well for totally ramified origamis, mainly because we can work out an equation for the degenerate cover. In other cases, it is not clear how the degenerate cover ought to look, in which case we won't even be able to get started with the previous method. Fortunately, there are other approaches. Here we outline one which relies on some numerical magic that looks daunting in general, but which is possible to make work in at least a few instances.

Here, we work out an equation for origami $f : C \to E$ of degree 5 and genus 2, with one triple point (so that the monodromy type is a 3-cycle). An origami diagram for such a curve can be found in Figure 5.4.

Theorem 5.3.1. *The genus-2 curve*

$$C : -\sqrt{5}y^2 = x(x-1)(x-\alpha)(x-2\alpha+1)(x-2\alpha), \qquad \alpha = 81+36\sqrt{5},$$

admits a degree-5 map f to the elliptic curve

$$E : y^2 = x^3 - x$$

branched only above ∞ with a triple point above ∞. The map is given by

$$f(x,y) = (g(x), h(x)y),$$

where

$$g(x) = \frac{x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0}{b_2x^2 + b_1x},$$
$$h(x) = \frac{x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0}{dx^2(x - 2\alpha)^2},$$

and

$$\begin{aligned}
a_4 &= -45(9 + 4\sqrt{5}) \\
a_3 &= 660(161 + 72\sqrt{5}) \\
a_2 &= -3240(2889 + 1292\sqrt{5}) \\
a_1 &= 1980(51841 + 23184\sqrt{5}) \\
a_0 &= -324(930249 + 416020\sqrt{5}) \\
b_2 &= -100\sqrt{5}(2889 + 1292\sqrt{5}) \\
b_1 &= 1800\sqrt{5}(51841 + 23184\sqrt{5}) \\
c_5 &= -54(9 + 4\sqrt{5}) \\
c_4 &= 1030(161 + 72\sqrt{5}) \\
c_3 &= -7920(2889 + 1292\sqrt{5}) \\
c_2 &= 18780(51841 + 23184\sqrt{5}) \\
c_1 &= 216(930249 + 416020\sqrt{5}) \\
c_0 &= -1944(16692641 + 7465176\sqrt{5}) \\
d &= 1000\sqrt{5}(219602 + 98209\sqrt{5}).
\end{aligned}$$

Proof. In order to show that $f(x, y)$ gives a map $E \to C$, we need only check that whenever (x, y) is a point on C, then $(g(x), h(x)y)$ is a point on E. This amounts to checking that if

$$-\sqrt{5}y^2 = x(x - 1)(x - \alpha)(x - 2\alpha + 1)(x - 2\alpha),$$

then

$$-\frac{1}{\sqrt{5}}h(x)^2y^2 = g(x)^3 - g(x),$$

or

$$h(x)^2x(x-1)(x-\alpha)(x-2\alpha+1)(x-2\alpha) = g(x)^3 - g(x).$$

This now amounts to verifying a formal identity of rational functions.

To show that the map is only branched above ∞, pick a differential $\omega = \frac{dx}{y}$ on E. This differential has no zeros or poles. The pullback $f^*\omega \in \Omega^1_C$ will therefore have zeros or poles exactly at the branch points of f, and the order of each zero or pole is one less than the ramification index at that zero or pole. We compute $f^*\omega$ to be a constant multiple of $\frac{dx}{y}$, which has a double zero at ∞ and no other zeros or poles. Hence f is branched only above ∞, with a triple point above ∞. ■

As in the previous section, the proof sheds no light on how one could actually come up with the equations of E and f without first being told the answer. We now describe how to compute it from scratch, once again using some educated guesswork.

All genus-2 curves are hyperelliptic and hence can be written in the form $y^2 =$ a quintic in x (or a sextic in x, if we prefer, but that will be less convenient here). Let us decide that f will be branched above the point $O = (0:1:0)$ of E. Let us also decide that, if $\omega = \frac{dx}{y}$ is the invariant differential on E, then $f^*\omega = a\frac{dx}{y} \in \Omega^1_C$, for some $a \in \mathbb{C}^\times$. Now, $f^*\omega$ has a double zero at $P = (0:1:0) \in C$, and no other zeros or poles. Hence, such a map will be a cover of the desired form.

Now, suppose we had such a map f. Let γ be a loop in C (or an element of $H_1(C,\mathbb{Z})$, if we prefer). Then we have

$$\int_\gamma f^*\omega = \int_{f_*\gamma} \omega.$$

These integrals are known as periods. Now, since $H_1(E,\mathbb{Z})$ is $\mathbb{Z}^2$, the periods of E form a lattice in $\mathbb{C}$. But since $H_1(C,\mathbb{Z})$ is 4-dimensional, the periods of $\frac{dx}{y} \in \Omega^1_C$ are typically dense in $\mathbb{C}$. In order to find a curve C that admits such a map, it is necessary that its periods form a lattice, and in fact a lattice homothetic to that formed by E.

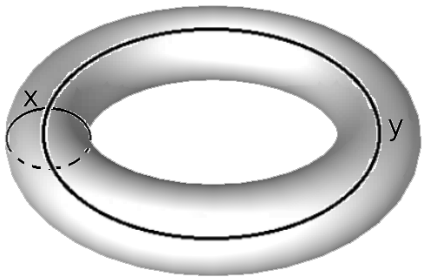


Figure 5.5: An elliptic curve with a typical basis of H_1 shown.

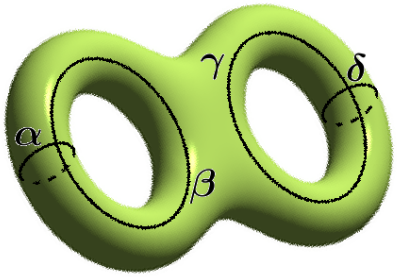


Figure 5.6: A genus 2 curve with a typical basis of H_1 shown.

It is now important to be able to determine the degree of the map from understanding its action on loops. That is, suppose we have a map $f : C \to E$, and that we know what its induced map $f_* : H_1(C, \mathbb{Z}) \to H_1(E, \mathbb{Z})$ (or equivalently $f^* : H^1(E, \mathbb{Z}) \to H^1(C, \mathbb{Z})$) is. We need to be able to use this information to determine the degree of f; in other words, the induced map $f^* : H^2(E, \mathbb{Z}) \to H^2(C, \mathbb{Z})$. Let x and y be the duals (in H^1) of the loops in E shown in Figure 5.5, oriented in such a way that x and y intersect positively. Then the fundamental class $[E]$ is $x \smile y$. Also, let $\alpha, \beta, \gamma, \delta$ be the duals of the loops in C shown in 5.6, oriented in such a way that α and β intersect positively, as do γ and δ. Suppose now that

$$\begin{aligned} f_*(\alpha^\vee) &= m_1 x^\vee \\ f_*(\beta^\vee) &= n_1 y^\vee \\ f_*(\gamma^\vee) &= n_2 y^\vee \\ f_*(\delta^\vee) &= m_2 x^\vee. \end{aligned}$$

The induced map on H^2 is then given by

$$f^*([E]) = f^*x \smile f^*y = (m_1\alpha + m_2\delta) \smile (n_1\beta + n_2\gamma) = (m_1n_1 - m_2n_2)[C].$$

Hence (the absolute value of) the degree is $|m_1n_1 - m_2n_2|$.

Since we are interested in degree-5 maps, we choose $m_1 = 1$, $n_1 = 3$, $n_2 = -1$, and $m_2 = 2$. Then we have the following map on H_1:

$$\begin{aligned} \alpha^\vee &\mapsto x^\vee, \\ \beta^\vee &\mapsto 3y^\vee, \\ \gamma^\vee &\mapsto -y^\vee, \\ \delta^\vee &\mapsto 2x^\vee. \end{aligned} \tag{5.3.1}$$

Now, we specialize to the elliptic curve $E : y^2 = x^3 - x$, which has j-invariant 1728. Computations with this elliptic curve are somewhat nicer than they are with arbitrary elliptic curves because its period lattice is a square lattice. Hence, we can take its fundamental periods to be ϖ and ϖi, where $\varpi \approx 5.2441151$.

If we write C as $y^2 =$ a quintic in x, let the roots of the quintic be r_1, r_2, r_3, r_4, r_5. We identify $\alpha^\vee, \beta^\vee, \gamma^\vee, \delta^\vee$ with representatives of their respective homology classes which pass through two of the Weierstraß points of C, i.e., the preimages of r_1, r_2, r_3, r_4, r_5, and ∞ under the natural hyperelliptic map $C \to \mathbb{P}^1$. We can therefore draw the images of $\alpha^\vee, \beta^\vee, \gamma^\vee, \delta^\vee$ under the hyperelliptic map in $\mathbb{P}^1$; this picture is given in Figure 5.7.

Figure 5.7 shows us how the loops in Figure 5.6 are related to periods of $\frac{dx}{y} \in \Omega^1_C$. The period $\int_{r_1}^{r_2} \frac{dx}{y}$ is $\frac{1}{2}\int_{\alpha^\vee} \frac{dx}{y}$, for example. Note that the sum of the three green loops

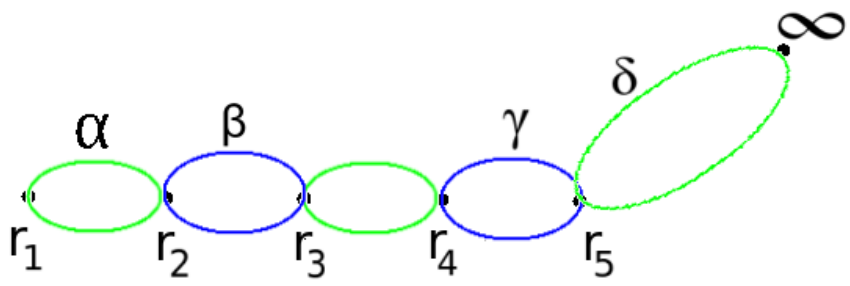


Figure 5.7: The data of Figure 5.6 has been rearranged. For example, the integral of a form over the dual of α is twice the integral from r_1 to r_2. This figure and Figure 5.6 have the same symplectic intersection matrix.

is $0 \in H_1(C, \mathbb{Z})$, so we have

$$\int_{r_1}^{r_2} \frac{dx}{y} + \int_{r_3}^{r_4} \frac{dx}{y} + \int_{r_5}^{\infty} \frac{dx}{y} = 0,$$

or

$$\int_{r_3}^{r_4} \frac{dx}{y} = -\int_{r_1}^{r_2} \frac{dx}{y} - \int_{r_5}^{\infty} \frac{dx}{y} = -3\int_{r_1}^{r_2} \frac{dx}{y}$$

since

$$\int_{r_5}^{\infty} \frac{dx}{y} = 2\int_{r_1}^{r_2} \frac{dx}{y}$$

by (5.3.1).

Now, we wish to find a genus-2 curve whose periods with respect to the differential $\frac{dx}{y}$ are proportional to ϖi, 3ϖ, $3\varpi i$, and ϖ. That is, if we let C be the curve

$$C : y^2 = (x - r_1)(x - r_2)(x - r_3)(x - r_4)(x - r_5),$$

then we have

$$2\int_{r_j}^{r_{j+1}} \frac{dx}{\sqrt{(x - r_1)(x - r_2)(x - r_3)(x - r_4)(x - r_5)}} = Km_j\varpi$$

for some constant K and for $j = 1, 2, 3, 4$, where $m_1 = i$, $m_2 = 3$, $m_3 = 3i$, and $m_4 = 1$. Notice now that this holds if we let $r_1 + r_5 = r_2 + r_4 = 2r_3$. Let us also

normalize C, by setting $r_1 = 0$ and $r_2 = 1$, which we can do because $\mathrm{PGL}_2(\mathbb{C})$ acts 3-transitively on $\mathbb{P}^1_{\mathbb{C}}$.

Now, it is not *a priori* clear that we can find a curve C whose underlying quintic has five real roots. Still, it is reasonable to begin the search by looking for such a C.

After this simplification, we see that C has the form

$$C : y^2 = x(x-1)(x-\alpha)(x-2\alpha+1)(x-2\alpha).$$

The task of finding α remains. Furthermore, α is an algebraic number.

Using a Newton's method algorithm, we can compute α to high precision, assuming that we can compute periods accurately. Fortunately, this can be done quite rapidly by using tanh-sinh quadrature, as described in [BB11]. Using this method, we can compute α to hundreds of digits. The task remaining is to determine which algebraic number α is, i.e. to find a nonzero polynomial in $\mathbb{Z}[x]$ having α as a root. This can be done by using continued fractions if α is rational or quadratic, and it can be done using LLL (see [KZ01]) in higher degrees.

This computation yields a number α, whose first few digits of α are

$$\alpha \approx 161.49844718999242907073,$$

and the continued fraction of this number is roughly

$$[161; 2, 160, 2, 160, 2, 160, 2, 160, 2, 7, \ldots].$$

A good guess, then, is that $\alpha = [161; \overline{2, 160}] = 81 + 36\sqrt{5}$. Indeed, computation of more digits helps to increase confidence in this guess.

It's worth mentioning here that this method does not *prove* that $\alpha = 81 + 36\sqrt{5}$ works, since this number might merely be exceptionally close to the true value of α. However, once we have the equation for the map as well, we will be able to check that this number is actually correct if we desire to do so. In the opinion of the author, this should not be seen as a defect of the method any more than having to verify that a clever approach to solving any other problem works by justifying our approach *a*

posteriori by presenting a complete solution as we eventually do in the above proof.

Now, working on the assumption that $\alpha = 81 + 36\sqrt{5}$, we compute the defining equation of the map $f : C \to E$. Analytically, $E = \mathbb{C}/\Lambda'$, where Λ' is the period lattice for C (not for E; they are only homothetic lattices), and the map $f : C \to \mathbb{C}/\Lambda'$ is given by

$$f(P) = \int_{(-\infty,0)}^{P} \frac{dx}{\sqrt{x(x-1)(x-\alpha)(x-2\alpha+1)(x-2\alpha)}}.$$

We can then convert this to a point on E by using the elliptic exponential function, which is given in terms of the Weierstraß $\wp$-function and its derivative for the lattice Λ': the map $\mathbb{C}/\Lambda \to E$ is given by $z \mapsto (\wp(z), \wp'(z))$. If we know the form of the map f and values of $f(P)$ at enough points, then we can compose with the map $\mathbb{C}/\Lambda \to E$ and solve a system of linear equations to determine the map, with coefficients being decimal expansions. Then, just as before, we can convert the decimal expansions into concrete algebraic numbers.

Before we compute the map from C to E, we change variables slightly, letting our genus-2 curve be

$$-\sqrt{5}y^2 = x(x-1)(x-\alpha)(x-2\alpha+1)(x-2\alpha).$$

This does not change the isomorphism class of the curve, but it does make the coefficients (slightly) cleaner. But since this change of variables also makes the equation of the curve slightly less pleasant, we will revert to the old form once we have computed it.

The map $f : C \to E$ can be written as $f(x, y) = (g(x, y), h(x, y))$, where $g, h : C \to \mathbb{P}^1$. Furthermore, the map $x : E \to \mathbb{P}^1$ which remembers the x-coordinate has degree 2, and the map $y : E \to \mathbb{P}^1$ which remembers the y-coordinate has degree 3. Hence, g has degree 10, and h has degree 15. Also, from the origami diagram of Figure 5.4, we can see that f respects the hyperelliptic involution: the elliptic involution on the elliptic curve corresponds to a rotation by π of the fundamental parallelogram; similarly, the hyperelliptic involution on the genus-2 curve corresponds to a rotation

by π of the origami diagram. Hence, $f(x,-y) = (g(x,y), -h(x,y))$, so $g(x,y)$ only depends on x, and $h(x,y)/y$ only depends on x. Finally, g has two simple poles. This allows us to determine that we can write

$$g(x,y) = \frac{x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0}{b_2x^2 + b_1x + b_0}.$$

Using the method as outlined above, we find that

$$\begin{aligned}
a_4 &= -45(9 + 4\sqrt{5}) \\
a_3 &= 660(161 + 72\sqrt{5}) \\
a_2 &= -3240(2889 + 1292\sqrt{5}) \\
a_1 &= 1980(51841 + 23184\sqrt{5}) \\
a_0 &= -324(930249 + 416020\sqrt{5}) \\
b_2 &= -100\sqrt{5}(2889 + 1292\sqrt{5}) \\
b_1 &= 1800\sqrt{5}(51841 + 23184\sqrt{5}) \\
b_0 &= 0.
\end{aligned}$$

Remark 5.3.2. The coefficients in the map are surprisingly nice. Let $\varepsilon = \frac{1+\sqrt{5}}{2}$; this is a fundamental unit in $\mathbb{Q}(\sqrt{5})$. Then the coefficients in the map are (essentially) integral multiples of powers of ε. We have

$$\begin{aligned}
\varepsilon^6 &= 9 + 4\sqrt{5}, \\
\varepsilon^{12} &= 161 + 72\sqrt{5} \\
\varepsilon^{18} &= 2889 + 1292\sqrt{5} \\
\varepsilon^{24} &= 51841 + 23184\sqrt{5} \\
\varepsilon^{30} &= 930249 + 416020\sqrt{5} \\
\varepsilon^{36} &= 16692641 + 7465176\sqrt{5}.
\end{aligned}$$

Hence, there is some homogeneity in the map: if we replace x by $\varepsilon^6 x$, then all the coefficients are either integers or integral multiples of $\sqrt{5}$. This seems unlikely to be

a coincidence, but at the moment, we lack an explanation for this phenomenon.

To compute $h(x,y)$, we recall that g and h satisfy the relation $-\sqrt{5}h^2 = g^3 - g$. Hence, we compute $g^3 - g$. Also, we know that $h(x,y)$ can be written as $h_1(x)y$, so

$$h_1(x)^2 = \frac{g(x)^3 - g(x)}{x(x-1)(x-\alpha)(x-2\alpha+1)(x-2\alpha)}.$$

We therefore have

$$h(x,y) = \frac{(x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0)y}{dx^2(x-2\alpha)^2},$$

where

$$\begin{aligned}
c_5 &= -54(9 + 4\sqrt{5}) \\
c_4 &= 1030(161 + 72\sqrt{5}) \\
c_3 &= -7920(2889 + 1292\sqrt{5}) \\
c_2 &= 18780(51841 + 23184\sqrt{5}) \\
c_1 &= 216(930249 + 416020\sqrt{5}) \\
c_0 &= -1944(16692641 + 7465176\sqrt{5}) \\
d &= 1000\sqrt{5}(219602 + 98209\sqrt{5})
\end{aligned}$$

With everything now so concrete, we can verify that all our numerics were correct: that f does in fact define a map $C \to E$, branched only above ∞, and with a triple point in C. This completes the construction of a curve C which admits a map to E.

5.4 Thickening to a family

Our goal ought to be larger than simply constructing one curve that admits a map of the desired type to one elliptic curve; we would like to find, for each elliptic curve E, a curve C which admits such a map to E. We would like to perform a degeneration similar to the one we did in the totally ramified case. Unfortunately, the process here

is much more complicated, and we have only the following partial result so far:

Theorem 5.4.1. *Let R be the ring $\mathbb{C}[t]/(t^2)$. Let C_t be the genus-2 curve given by*

$$y^2 = x(x-1)(x-(a_0+a_1t))(x-(b_0+b_1t))(x-(c_0+c_1t)),$$

where

$$\begin{aligned} a_0 &= 81+36\sqrt{5} & a_1 &= \frac{7}{2}+\frac{47}{30}\sqrt{5} \\ b_0 &= 161+72\sqrt{5} & b_1 &= \frac{161}{27}+\frac{8}{3}\sqrt{5} \\ c_0 &= 162+72\sqrt{5} & c_1 &= 6+\frac{161}{12\sqrt{5}}, \end{aligned}$$

and let E_t be the elliptic curve over R with j-invariant 1728 given by

$$y^2 = x^3 - x + \frac{t}{108}.$$

Then there is a degree-5 map $f_t : C_t \to E_t$ ramified only above ∞ so that there is one triple point above ∞, and the other two points are unramified.

Proof. The proof is as in the proof of Theorem 5.3.1. The equation for the map involves coefficients that take much space to write. Therefore, we have relegated them to Appendix A. ■

In fact, we know how to extend the genus-2 curve C_t in Theorem 5.4.1 to $\mathbb{C}[t]/(t^3)$:

Conjecture 5.4.2. *Let R be the ring $\mathbb{C}[t]/(t^3)$. Let C_t be the genus-2 curve given by*

$$y^2 = x(x-1)(x-(a_0+a_1t+a_2t^2))(x-(b_0+b_1t+b_2t^2))(x-(c_0+c_1t+c_2t^2)),$$

where

$$\begin{array}{lll} a_0 = 81 + 36\sqrt{5} & a_1 = \frac{7}{2} + \frac{47}{30}\sqrt{5} & a_2 = \frac{37}{432} + \frac{1241}{32400}\sqrt{5} \\ b_0 = 161 + 72\sqrt{5} & b_1 = \frac{161}{27} + \frac{8}{3}\sqrt{5} & b_2 = \frac{967}{7290} + \frac{961}{16200}\sqrt{5} \\ c_0 = 162 + 72\sqrt{5} & c_1 = 6 + \frac{161}{12\sqrt{5}} & c_2 = \frac{193}{1440} + \frac{971}{16200}\sqrt{5}, \end{array}$$

and let E_t be the elliptic curve over R with j-invariant $t^2 + 1728$ given by

$$y^2 = x^3 - x + \frac{t}{108}.$$

Then there is a degree-5 map $f_t : C_t \to E_t$ ramified only above ∞ so that there is one triple point above ∞, and the other two points are unramified.

This is only a conjecture, as we have not yet performed the computation analogous to that of Theorem 5.4.1. The computation is significantly more tedious, but we expect to encounter no new difficulties in performing it.

The choice of elliptic curve in Theorem 5.4.1 may be surprising, since the elliptic curve $y^2 = x^3 - x$ also has j-invariant 1728. However, we would like to extend this elliptic curve to a family parametrized by t with j-invariant $1728 + t^2$ over $\mathbb{C}[\![t]\!]$. One such elliptic curve over $\mathbb{C}[\![t]\!]$ is $y^2 = x^3 - x + h(t)$, for some $h(t) \in \mathbb{C}[\![t]\!]$. The image of one such $h(t)$ in $\mathbb{C}[\![t]\!]/(t^2) \cong \mathbb{C}[t]/(t^2)$ (or even $\mathbb{C}[t]/(t^3)$, as in Conjecture 5.4.2) is $t/108$.

We now explain the process by which we found these coefficients. We now revert to a different parametrization of the family of elliptic curves and use the elliptic curve

$$E_t : y^2 = x^3 - 3\frac{t^2 + 1728}{t^2}x + 2\frac{t^2 + 1728}{t^2}$$

over $\mathbb{C}(t)$, which has j-invariant $t^2 + 1728$.

We look for curves of the form

$$y^2 = x(x-1)(x-a(t))(x-b(t))(x-c(t))$$

mapping to the elliptic curve

$$y^2 = x^3 - 3\frac{t^2+1728}{t^2}x + 2\frac{t^2+1728}{t^2}.$$

We let $a(t)$, $b(t)$, and $c(t)$ be power series in t, with $a(0) = 81 + 36\sqrt{5}$, $b(0) = 161 + 72\sqrt{5}$, and $c(0) = 162 + 72\sqrt{5}$. To do this, we let t_0 be some 10^{-n}, for a decently-sized n, so that some consecutive string of digits in $a(t_0) - a(0)$, $b(t_0) - b(0)$, and $c(t_0) - c(0)$ hand us the coefficient of t^1 in these power series. Letting $t = 10^{-30}$ is sufficient for recognizing the next terms of the power series; the coefficients of the linear terms of $a(t)$, $b(t)$, and $c(t)$ are then seen to be

$$\begin{aligned} a_1 &= \frac{7}{2} + \frac{47}{30}\sqrt{5}, \\ b_1 &= \frac{161}{27} + \frac{8}{3}\sqrt{5}, \\ c_1 &= 6 + \frac{161}{12\sqrt{5}}. \end{aligned}$$

From here, it is now possible to compute as many terms as desired from the series expansions of $a(t)$, $b(t)$, and $c(t)$. To demonstrate the algorithm, we compute the quadratic terms. First, it is necessary to compute the power series expansions in t up to the quadratic term of the roots of the cubic polynomial

$$x^3 - 3\frac{t^2+1728}{t^2}x + 2\frac{t^2+1728}{t^2};$$

we find the roots to be

$$\begin{aligned} r_1(t) &= -\frac{72}{t} - \frac{1}{3} - \frac{t}{54} - \frac{t^2}{34992} + O(t^3), \\ r_2(t) &= \frac{2}{3} + \frac{t^2}{17496} + O(t^3), \\ r_3(t) &= \frac{72}{t} - \frac{1}{3} + \frac{t}{54} - \frac{t^2}{34992} + O(t^3). \end{aligned}$$

Now, we compute the power series expansions of the periods. Let

$$\omega_t = \frac{dx}{\sqrt{x^3 - 3\frac{t^2+1728}{t^2}x + 2\frac{t^2+1728}{t^2}}}.$$

Then the power series expansion for

$$\int_{r_1(t)}^{r_2(t)} \omega_t$$

is

$$\alpha t^{1/2} + \beta t^{3/2} + O(t^{5/2}),$$

and the power series expansion for

$$\int_{r_2(t)}^{r_3(t)} \omega_t$$

is

$$-\alpha i t^{1/2} + \beta i t^{3/2} + O(t^{5/2}),$$

where

$$\alpha = 0.309012446216895319738975057865876 67\ldots,$$
$$\beta = 0.000980570699993031350239003617039 41\ldots.$$

Call these periods I_1 and I_2.

Similarly, we compute power series for the four periods Q_1, Q_2, Q_3, Q_4 of the genus-2 curve

$$y^2 = x(x-1)(x-a(t))(x-b(t))(x-c(t))$$

with respect to the differential $\frac{dx}{y}$ up to the quadratic term, leaving a_2, b_2, and c_2

terms in the expansion. Now, by the hypotheses we made in (5.3.1), we know that

$$\begin{aligned} 3Q_1 &= Q_3, \\ 3Q_4 &= Q_2, \\ I_1 Q_1 &= -I_2 Q_4. \end{aligned}$$

Substituting in the appropriate power series and truncating as appropriate, we obtain a system of three linear equations in the three variables a_2, b_2, c_2. Solving these equations gives us

$$\begin{aligned} a_2 &= 0.171295072841890093001351373518451826667\ldots, \\ b_2 &= 0.265293223164579431304821281930288591407\ldots, \\ c_2 &= 0.268053827540265172544031334191681165555\ldots. \end{aligned}$$

Using a similar method as before, we find that

$$\begin{aligned} a_2 &= \frac{37}{432} + \frac{1241}{32400}\sqrt{5}, \\ b_2 &= \frac{967}{7290} + \frac{961}{16200}\sqrt{5}, \\ c_2 &= \frac{193}{1440} + \frac{971}{16200}\sqrt{5}. \end{aligned}$$

While this process is tedious to perform, it is clear how one could carry it out in general to obtain further coefficients of the power series expansions of $a(t)$, $b(t)$, and $c(t)$.

The eventual goal of this process is to write $a(t)$, $b(t)$, and $c(t)$ as explicit algebraic functions of t, not just elements of $\mathbb{C}[\![t]\!]$. Once we have enough terms of the power series expansions for $a(t)$, $b(t)$, and $c(t)$, we can hope to algebraize the expressions. However, before we can do that, we need a bound on the degree of $a(t)$, $b(t)$, and $c(t)$ are, as algebraic functions over $\mathbb{C}(t)$. We can derive such a bound by looking at the global structure of the family of genus-2 curves that admit covers of the desired type to elliptic curves.

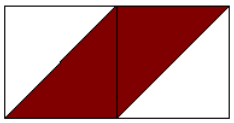


Figure 5.8: The red part of the figure is a fundamental parallelogram for the same elliptic curve as that of the square. However, by sliding the top edge of the parallelogram one unit over, we have performed a Dehn twist on the elliptic curve.

5.5 Global structure of the family

What we want to do is to find an irreducible closed substack Z of the moduli stack of genus-2 curves with a differential, so that Z maps to the j-line (or $\mathbb{A}^1$) of elliptic curves by a map of the given type. In this section, we show how to compute its degree, which in this case is 9. We can do this directly with the origami diagram.

To do this, consider starting with an elliptic curve represented by a square as its fundamental parallelogram, and transforming the parallelogram through various other ones until we reach another parallelogram which represents the same elliptic curve (see Figure 5.8). This amounts to performing a Dehn twist, or equivalently an element of the mapping class group, on the elliptic curve. As we perform such an action on the elliptic curve, we drag the genus-2 curve above it as well, possibly sending it to a genuinely different genus-2 curve, as we see in Figure 5.9. The orientation-preserving part of the mapping class group of an elliptic curve is $\mathrm{PSL}_2(\mathbb{Z})$. Hence, we must see what $\mathrm{PSL}_2(\mathbb{Z})$ does to the genus-2 curves in the fiber.

At this point, it is easier to work not with the origami diagram directly, but with an equivalent description. We instead describe the origami as a pair of permutations $(g, h) \in S_5 \times S_5$, as follows. Number the squares in the origami diagram from 1 to 5. (There are many ways of doing this; choose one at random, since the choice won't be relevant at the end.) Let g be the permutation given by moving one square to the right in the numbered diagram, and let h be the permutation given by moving one square up. Now, g and h generate a transitive permutation group, and their commutator $[g, h]$ is a 3-cycle. We can easily convert between the origami diagram and the pair

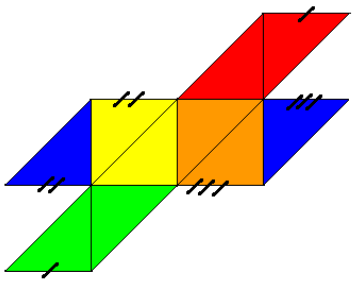


Figure 5.9: This is the genus-2 curve we obtain by applying the Dehn twist as shown in Figure 5.8 to the genus-2 curve in Figure 5.4. To turn the figure back into an origami diagram with squares, we can cut and paste some of the identified edges. We have labeled the resulting squares by color. This is shown in Figure 5.10.

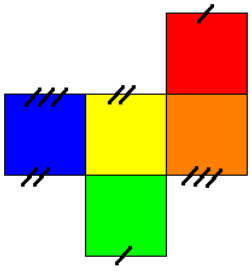


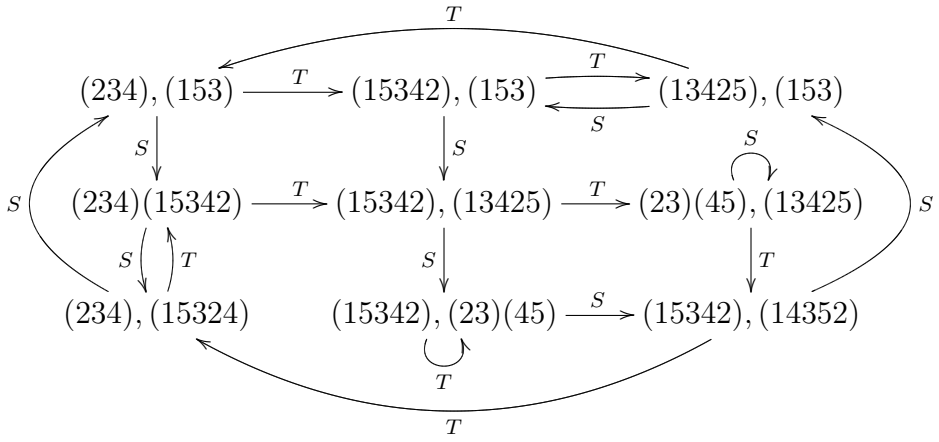
Figure 5.10: This is a rearrangement of Figure 5.9 back into squares.

of permutations, with an ambiguity of drawing an origami diagram with a different choice of edge cuts, and of choosing pairs of permutations which are simultaneously conjugate: (g, h) and (g', h') are simultaneously conjugate if there is some $\sigma \in S_5$ so that $\sigma^{-1} g \sigma = g'$ and $\sigma^{-1} h \sigma = h'$. In this case, we get isomorphic origamis.

Now, we pick two generators of $\mathrm{PSL}_2(\mathbb{Z})$ and observe their actions on permutations. We pick the generators

$$S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

which act on (equivalence classes of) permutations by $S(g, h) = (g, gh)$ and $T(g, h) = (hg, h)$. A computation shows that S and T have action on equivalence classes as given in the following diagram:



Each equivalence class of pairs of permutations in the diagram above corresponds to one preimage of an (arbitrary) elliptic curve with differential. Hence, the map $Z \to \mathbb{A}^1$ has degree 9.

In fact, it is perhaps worth pausing here to note that we can get a Belyĭ map out of this: if we compactify Z and $\mathbb{A}^1$, we get a map $\overline{Z} \to \mathbb{P}^1$ which is ramified only above three points: 0, 1728, and ∞. A change of variables then gives us a Belyĭ map.

An unfortunate consequence of the fact that $Z \to \mathbb{A}^1$ has degree 9 is that we cannot hope to get a reasonable parametrization for a family of curves C over the

Legendre family of elliptic curves $y^2 = x(x-1)(x+1-t)$, since the map from the Legendre family to $\mathbb{A}^1$ has degree 6. Instead, we parametrize our family of elliptic curves directly by j-invariant. If $j \neq 0, 1728$ and we let $t = \sqrt{j - 1728}$, then the elliptic curve

$$y^2 = x^3 - 3\frac{t^2+1728}{t^2}x + 2\frac{t^2+1728}{t^2}$$

has j-invariant j. We use $\sqrt{j-1728}$ rather than $j - 1728$ because $j - 1728$ has a double zero on the j-stack at $j = 1728$; hence $\sqrt{j-1728}$ is a local parameter on the j-stack at $j = 1728$.

5.6 Extracting number fields from origamis

Just as in the case of Belyĭ maps, we can extract number fields with limited ramification from origamis. Although the examples coming from the origami families in the previous section are solvable and thus not so exciting from the perspective of constructing fields, the techniques are worth presenting here.

Let us start with the degree-3 origami, where the equation of the genus-2 curve is

$$y^2 = x^5 + (1+9t)x^4 + 33tx^3 + 40tx^2 + 16tx =: f_t(x).$$

We can factor f_t as

$$f_t(x) = x(x+1)g_t(x), \qquad g_t(x) = x^3 + 9tx^2 + 24tx + 16t.$$

The polynomial discriminant of g_t is $2^8 3^3 t^2(t-1)$; hence if $t = 4$ (for example), then the polynomial discriminant is $2^{12}3^4$, and the field discriminant of the field $\mathbb{Q}[x]/(g_4(x))$ is 3^4. If $t = 9$, then the polynomial discriminant of $\mathbb{Q}[x]/(g_9(x))$ is $2^{11}3^7$, and the field discriminant is $2^3 3^5$. Hence, we have constructed some fields ramified only at 2 and 3. (In this case, of course, there are much quicker ways to construct cubic fields of small discriminant.)

We can do the same thing with the degree-5 origami, where the equation of the

genus-3 curve is

$$y^2 = x(x+1)g_t(x), \qquad g_t(x) = x^5 + 25tx^4 + 200tx^3 + 560tx^2 + 640tx + 256t.$$

The polynomial discriminant of g_t is $2^{32}5^5t^4(t-1)^2$. Letting $t = 5$, we have a field $\mathbb{Q}[x]/(g_5(x))$ with polynomial discriminant $2^{36}5^9$ and field discriminant 2^45^9. Its Galois group is $F_5 = (\mathbb{Z}/5\mathbb{Z}) \rtimes (\mathbb{Z}/5\mathbb{Z})^\times$.

There are other number fields that can be extracted from origamis. Let us return to the degree-3 origami, and consider the elliptic curve E_4 corresponding to $t = 4$, namely $y^2 = x(x+1)(x+4)$. This elliptic curve has conductor 24, and $E_4(\mathbb{Q}) \cong C_2 \times C_4$. One of its torsion points is $P = (2, 6)$. The x-coordinates of the preimages of P under the origami map satisfy

$$\frac{x^3}{(3x+4)^2} = 2,$$

or $x^3 - 2(3x+4)^2 = 0$. The number field corresponding to this cubic polynomial has discriminant -2^23^4. We can also look at the preimage under the map for the degree-5 origami; the x-coordinates of these preimages are roots of the quintic polynomial $x^5 - 2(5x^2+20x+16)^2 = 0$; this polynomial generates a field of discriminant $(-1)^22^43^25^5$ and Galois group F_5.

We can do something similar with points of infinite order. Let $t = 10$ so that E_{10} is the elliptic curve $y^2 = x(x+1)(x+10)$, which has rank 1 and conductor $2^5 \times 3 \times 5$. A generator of $E_{10}(\mathbb{Q})$ modulo torsion is $(-5, 10)$. The x-coordinates of the preimages under the degree-3 origami satisfy $x^3+5(3x+4)^2 = 0$, and the corresponding field has discriminant $2^23^35^2$. Under the degree-5 origami, the preimages satisfy $x^5 + 5(5x^2 + 20x + 16)^2 = 0$, and the corresponding field has discriminant 2^45^9 and Galois group F_5.

5.7 Computations

The computations described in this work were done using [J+10], [S+10], [Sym12], [The08], and [Wol07].

Chapter 6

Future possibilities

6.1 The Cohen-Lenstra heuristics

My work brings up many questions that would be interesting to investigate in the future. Regarding the Cohen-Lenstra heuristics and roots of unity, it would be interesting to gather numerical evidence for equidistribution of the invariant in a wider class of number fields. This is a tractable problem in theory; we can write down algorithms to compute the invariants associated to more general number fields. Unfortunately, actually running them takes far longer, as their complexity grows rapidly. However, it may be possible to do a limited amount of verification, perhaps for non-Galois cubic fields or for A_5 fields.

Another possibility to investigate is the dependence on the number of primes dividing the conductor. My numerical work here is only for the prime conductor case. While we do not suspect that the behavior of prime-conductor C_3 fields differs from that of arbitrary C_3 fields, it would still be nice to have numerical evidence to suggest that the behaviors are identical. Doing these numerics is well within our computational ability.

Finally, we noted that we expect the invariant to be asymptotically equidistributed, but that there is a small but definite bias in favor of invariant 1 for relatively small fields. At the moment, we have no explanation for the origin of this bias; any explanation for this behavior would be very exciting and would be expected to change

the way we think about the Cohen-Lenstra heuristics.

Finally, a proof of any nontrivial case of the Cohen-Lenstra heuristics in the number field case would be most welcome. At the moment, this seems to be outside of the realm of possibility, but we can hope that someone will have a new idea that will open up the Cohen-Lenstra heuristics to attack.

6.2 Belyĭ maps and origamis

We would like to be able to construct many more explicit examples of origamis. At the moment, we can construct many examples of totally ramified origamis, but the non-totally ramified case is much more difficult. We would like to complete the family of 3-1-1 origamis which was started in this work; I am confident that I can compute the entire family, but it is quite a time-consuming process that I hope to finish eventually. Explicit examples of higher-degree families would also be interesting.

Continuing on with branched covers of curves, perhaps the next place to go after origamis is to unramified covers of higher-genus curves. We expect that some of the techniques used here will be applicable in this case as well, and indeed, we have some explicit examples written down.

Motivating this desire for explicit covers of curves is the connection to number fields with limited ramification. Our totally ramified origamis do provide us with examples of number fields with limited ramification, but these fields are all solvable and can thus probably be constructed in a less involved manner through class field theory. By contrast, the non-totally ramified origamis generally give us non-solvable fields, and we would be more excited to find these and to understand how many of them exist.

Appendix A

Numbers involved in the Proof of Theorem 5.4.1

In this appendix, we write down the map needed to prove Theorem 5.4.1. The reader is strongly advised not to look at the numbers in this appendix, but only to be appeased by their presence.

The map from C_t to E_t in Theorem 5.4.1 is of the form $(x, y) \mapsto (f_1(x), f_2(x)y)$, where

$$f_1(x) = \frac{x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0}{b_2x^2 + b_1x}(1 + bt)$$

and

$$f_2(x) = \frac{x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0}{(b_2x^2 + b_1x)^2}(1 + dt).$$

Now, the a_i's, b_i's, and c_i's are elements of $\mathbb{C}[t]/(t^2)$, and the constant terms of the a_i, b_i, c_i are the same as in Theorem 5.3.1. We denote the linear term of a_i by a_i^1, and similarly for the b_i and c_i. Then we have

a_0^1 = {−(75(75187816195014802213989615534838491836479213548661307610090888458352406563154378504991079435680906152844387492794494948541844923274433894105592885991345869370692155550737110776556158844573452190002128412188207096298392968726717811943898394784541424492719320877425622971080739744263251926155914311700258019130836430863396875963100370456560288503552959787545959172905309042899060560905411008281739575836795460157192149864055430087593490378570977327795652261169537772546330645266538511849556494596179733873228992695754791162688625689782700136554798575950561627292634956889135585628312235591410894404665150364435281761998909107593685013432826829744617503931731012027646887992198528459190201200807070185233159750780123185160819091646400936985950392407039244338175991662534595625395488583292423822619883881864503470495480945984699833473345430298114732966866465352840639026519704974220565107852682402357736387125098466588331017948556 1

74998945388837896081252172740473427258660029805940187474668512205711692317279764377860575428862533882111757777184532974
00978077257446604823218821735881713546275537779576988450856073421838936882516929539699415209508820525223438962684896 45
18435281014465176757072674150424555990198832833395585416880654271839971155708346904035600665539967436204239898105686 50
93478267549010607624458865335641803809983523615425661564050572655797463969035632765319003568724422092246113150247680847
60245352529184009447393680250033091706757429330465364555778033829392148128609475937153205500890051474399885698688503094 1
91475036691348461406451701323929971265805322391678938406092585700594422238173587726371003619257477202060605163720647257
76321389183300261634559215968402380498297428286927199648829558956696920465788418722155161944161599165876481822800747683
04020711819357463997330754842644323228422117483437665868762375270 + 33625013618362536420293216003686229894425026311118 8
95354530161837124127114695299966803425052759985435188112893955932090805913477655432817350795967789172625645184301764 5
44786974635366237556039880986259234296216540298959003914463639472675931963841765539919351072818271291720579899402868720
07433971272862866865900471687318469643201220648321523457304086088001872019027740855289211437855748375833807999314921617
17193374593913064478308254572417837581007087268308950138415961877016302751381909072882344823695322999477252363206261850
26247949135607176493794676658613872571174090306361814691030399638992375793380108144503305416893643627431950240834063620
68358807581122398650274649312831942350751639085398081039387709655922856255684350864345977353244903063755118911122913299
93006519172805971020006171852575134596426734391094280961922529068355495108552724847030102611838698112721849097818998934
49999874502906926513589141996822031461363635368353885826431702138645244705915921870748815699420531951961614615186632437
11249856028291720168364919788551870919506160681506116765339286901921118998758934774152278639468018988352289177955027606
28671673866488792263640321463650331414478557384782644255774128699054673355535700945915666816481930947948208850471650231
01355757873533048945333213963234952446045866962999944553952343159900675939115882624753622737884652084804723067314073844
67276229998054568549950770518453645310850127809054945639149223381700113829153303352673757938385083444450728607282642 10
75076406161903002304686491289129138556094627141785903356455082815542637128033625018254825936090736721896773663169299213
99237242462906806407927113647134132673254750143923471187924868354593280681537541951832304171107774810606839838236872448
89530132839767264078796425606790985356877648532105742203249035093048837282955768103584709587683588735455587 5))/((416025
69376551409155240 + 1860523463292399924496 1 5)^3 (1049731083682069301329499561297510448410878058514029929216766295603382 1
87555234921518045136244421277628550762685750603461854551141154906673056247017354107460803130647044304502544457845114369
99320007281074743648277467422899735784265461035898555946700599296069538956196144323687371229526654578599054481306129 73
50699365526128580111643566434485718185315959280297906534195845982401673200988879962387708013654959149628633875996423439
58500824910838397266997839823195885349546914173061608021767612846559523482247375982185915850074744122859274171757200299
60336573771596001975648582679639715479890134643845547598029396616372451182829332557531040688481398628319093680219344 40
71077227309648027493874169437701143663661065333394079622406485315484538012203141119133726506831195322506483169987122191
50538559358571234022823841068396007696220355980685645060402484958013540767035442135643165451359452806673511478782425566
45495704685887963521562034940979061568226990398168928131292454776343034489725886771545015781428650009096593702835653669
37557012071325098717356566660126384833428063579639995984741821773408987330302813296015516850247978948785473283276514842
78856911438444183913769176984005871116960101342734788835321265706242494334614007411340269806078005105712530351831742 70
14683850670616637857428551257352799682941658762549657415946660867279947555858652939707513482402744764880615243745746461
75123127672032033378375637402635002460292633896853706930343106212245060487779365174609239844237702728727555636779461329
98980055949228635963637119543291454056609571653036319918612082230778215346750322776520111957990800214577816949729660059
79109766594446184722153117505676139070412561509889056309474505045978791514418542595692723139785524321271357575754443800
518049326120 + 4694540122415254386844783579813530604085408107148567390955631652669719589716512953536243120619713195084 5
13683890518097100758928431424868592510252777257469241250517129974974499736854444301202713579827885279758060334701446982
46042723333923035779242550170127117825105738101551007400289534853597023526853059491159266772240249315086024225910599055
34213172971172804160043337323380136550812119309762188647156744677038015026948386885919011114822401373817100224042621627
12518171332772858823022806189665619403541838963663703211927303789550874611361109362547212763689196269724590981824827591
59039077309697427580475026602341942967884515382762123512745543341543793588701275223679638618863641292868865467439802767
95059385756342909945488610612470281578188530139145034017292797620742389423243581402615293383023051670818104904596739550
50544363322447020878672436848990647320261063698385619078315973483999801918330785929589459713818554496015894758635814910
03490808357478507144246343120346284360425934114029238278050539816221934550826391012498389121405445909000505640081462997
90437989136646775991759534261071330341226023368866583284973433170489742620499975744326305185923469168613651853945418694
55117638665748310836297438762985501230301297331585283973540443672949347905441590812476600467599269885565617528796212051
48187178025010733511210239371002298034000243891739510095915279357520279315768360773673701859337353209232222301618360827
89646984388911649148203281252242744494199408876857954767022660594428505619307545536979380718406532772378480980384867962
01564682508920496331888776592634426730580736683247551288766792730779535339509469158186963948033999595152697528698562709
65473863335378467949838801990109427280096615651701455986796365889911642389128216355663544624206 41 5))}

$$a_1^1 = \{(100(225208401581761492694498913218691156073311728330384347171411473194627149232103455205124317623659911132$$
$$57405146501581579263926965505415559260220500897007646521111994128864654796018999440945401674545889697863944597541780 62$$
$$55568497712448609963138891825784910644849858107619878640022943458439521457624964821249749509547449317059732008431019 27$$
$$58827754622463743895549404131567707320723824035717535208237161629374921679270859907669958641511447757393124739609699 76$$
$$76598179674115557014121972627017514189524874836494529075874626103683218159986727789046179335387745791412426479180555 8$$
$$84619786844850983716214593345674592175262885748934802323127046233091164940440332931660086672071610904745462295723933 01$$
$$45144746003055177366956571675963480179113482246235037333699732720591657737149070279763393649107671660686076201427208 86$$
$$94839672815849843366799807393415807074898021974785344683138686238126336016554153483226989488775052053024641114913202 47$$
$$71797370378599396238897340189503335374502196329262907421537247100040033888074659221681281747277829085122359382235015 89$$

$$
\begin{aligned}
&146099989964786708076004560481342181251493330074353815063212600158781110189806069968824714005129045514247970195008486749812233994604461999147537034623057651930973675212051555948085384394011730128957900957912568783168788034114929065796594209714847797981216825552844050863571506640072969773947639381409822698783988634635219474587101950101587859784820424458\\
&588015638088819977439011541338413127661288795727641618962211604785325938896632388218098477462802178152077896081191259382352844167177194806124950459675296511780578618691074990119096116257436638351028281484875689490 + 1007162590081779719442\\
&464614784446057247628647469746676633946239662847538503021185349622474751922074873006551220766611572093959194836120307482993267730796126519471747550483683189041858501098697489830925445117158087950431176681206719973660998886522788076228399\\
&418341855367805686617721288999908264987256223370685643533893986358277618628946519626678223723732803302272764243563212585555859299228785730905343460153465221862571226308624080041196018926191348846951662816532950040438574338886066419844882170555939101518172319292105563832587204751944124694910788567254544513324119998496142049911616004847627423062389341285792\\
&260646452578799151125427439302250024376490900097920611815173093211279623181831474140185499399544011935133192710028884059808184352173274963570109338111215989407098891837281525745059286377328911350893935968155415648816064813677637289154805173681987233245534122244017785409093830093856551103853043054180390036397586030424011681739084001891657459099475743880812462385503086638294392222309547951193832806375677264956403909151076636991987308923235206081214045274638934302548066367716843553542545870346972025655984992268259913385124733652812253560209644765873642304373759722948280053151888856252033595\\
&987329902106190309092519104264946605080887674365834541682655674019532190112648488281988652528688875643107741621728577936061806411706256468719552164082137370498235185962711121035860469818727862271519829829568293679512741774711899415737380\\
&958899121818486764763966918563813185642615439271433554335751576001327547588545844253885551138700987236591066895336596628742781846205007081887121896533010680216445972)/(3(41602569376551409155240 + 18605234632923999244961\sqrt{5})^3(412536639806\\
&517932878408874048711350603019195210442966261398635376933015303716442476044439830006476200495368832291114612723278986260207398166248438537106766655167672639018762556899144383295197360815988987172394026019131290357971969998889186050196347967936859066692717586192014593914597732439056494059866937428642091336928695209418258667300882431417847551578085950069012731629934781858725706053057552435222378631974268638576678735799355931578583523070534219443195630063441142660009690638506746971180185568969392183897730426529445424364122872723676592380501115640325591151580276873071112334111046762489398649551094284022621418723012307622477443181245888179628990857773956576121500902564521561259415059290735978308372387591575459314912250851608165903909425805221036915220748872651580583338011864175442189181086881459528876354917381945615338937139704203218955820684322608236107605652914916721945535794634658007383146311027017616400226002514132131025967007759832281096\\
&522648325036849221290385753636439399459737180137358467959656297776031031199442223713270220631309675818846654906770363453639279919433979604868480010565962679723119545750744202458531582495716699977209484910810004319352137613634832131643480\\
&910297549140234646350867777337271745201820751977752461835245161790230562276841741241423198474824689079263993562848917015267699584680974958073239649138900539148360385156201402989230775593978352124862106759472999156351034384543567828255111982715229391820938009530007980512032182295372539858502182121094486743531055242602339246397962779414 + 18449199396334395\\
&751044114897210083183340154679215624756754377355434379879030385795503746103588095266824674616212402530454577285147674798179871297987940377821728855344736891243142312753450210638086243618821026503126374847582058247465252164975033110030490961622220077300275087051327593390218664685526776565555620553242967440125054905494092089168858241502004629769409889022763\\
&242719996400820715864725281053671869966975940513125636356120963486509598126533646677057948566783830740921952229034431304960480129093959692501834885126974531823966266451259053717487893184233446492582606508168980032898509754335356988488649975893023547304879349064015582174890613747427980692574426905289800983391122782963968773545248770866185040805261653074031\\
&594008904353106857690736048246648016192609536509191903344286841393249509670848072450526590874353954366425704261955203128368716331587477007927729260591230512760378404135850627027695318829494630675742150785126324541051059039220636988034990396695694859349746354531972254184188969228460488917420781947698923277145224800033707216589444959634754216253183653044651\\
&365672631593998532378710842437568482421459357121584386351529065263450577012595817495132010705653453823866559027235977137052764718129388265524580905512341421375819440738335443795461747897327558584990287975273218179662936950327097761133102566974525824430480225849175062786770369358015677368164372212364931994449492772218192140753703733802050615205029383834526\\
&462069981528932658276246276967658442963327689785886766129968858945043282910007875709157047008912\sqrt{5}))\}
\end{aligned}
$$

$$
\begin{aligned}
a_2^1 = \{&-(25(80368479059433684260013857840191311869495152438314166606185969175458023584706733184414751959489429315370085668277130416226175066041828041730753931615270430827946803044005292167576355357587963637929058794012795233832078100046796711697399282512993023988227338059978657157087359274888176908373845586053265334850574960865798697875585311777502\\
&956965624026840636711249817865028410128971391434454898512207656140097754370138718715367633826911511381504343215496543672511770784498955221964995455369130176202904174577379981552447732943501683154745646666730730398131772779401476264647277853084241349324786969769833613786529203679008355016491056334686343381924940200277602602622592381098420406801820507562\\
&491773083610223814335020860183495160390063215191120068057571790854557632367332178579423453249653892529419201937323411275277179997941065119369113494377372771553251451924775896307140280895488306038167523930588183973699646029302547850172268805493612341527240454295340028493419470369785257530087161688350849856455139570334097290408801666487802542023371272555\\
&785540293668856700381825379836583881319123577000174720944119263704326773537547370086221228878158844668060300848374275553752508030269682867773375255188206647761878742159151768420230624710873759567865847917745870555957754679499556320164665\\
&105281791399190980819653176909603680631292551337581612114776089008331560763067797504204505818503380905787454125285946793403584467093955465180370550607625914871 + 3594187648503241577578546430165114327936582301478564148523914533039346602\\
&335610571867000629948798526465259047070806286228229836433495400955550790168587141796399837588671905801770067055681175952887818461965228903510466040295409856703998635651191980420123599596049367652649921031084258845468472963302627692822120465861352139577696260784626558966642532675924377631220213150970724054080071116687017889285728553856707114228669539551084\\
&502545927279104594682795631804966855411554889831810812146009761548686052389834147016709480460744709718946995083591393265
\end{aligned}
$$

$$0413816425587575003663633025641822535447439559827805540151300481260750745162932896609497207222934263838332611059213219099045039242507387095029159741876614285348895647805453209935000329346999151352001056447731573268690163384868191938071612180088585737671057618527383863541570443772762802308752974209234883169672790082142290191659798490687672058079282364432850507944281561972334075765856066274284436465992087696632282964569660873915342081765775170946406211254071745847844641521635868540259264543102330452691049626076347236289804336035869219366371424014757044499376623749007340233786123281970522839432483373648455772079938222920145191058137554924932473280797737716926931465556249383735542463604935069046768212578344658183432311149882044176419669346114522796764429299989020029242381254429264589912011397079886418921338581673585842305025732483574050220965478434171540149764724645596721736580555645(\sqrt{5}))/(54(41602569376551409155240+18605234632923999244961\sqrt{5})^2(2502000478198922358596073807402526897175303480040797294364421724660902916117238128260382337487721528993257700931002598085231603400354282541843901146484582561525687125288593533417143371840357562527354160284919147803239515944014327726927810477743329455381138169536794719047133303323532344644435214358317729652643901711678287116184954988700746240769360414491266482673474940570931497911598653372931635697504469712392160498034515979093368403949818589944879599352949963304666084161646770067810800502743495364549500070145192517129023396465156755597193179584050244375246260565969103115181802129317478349961840122541465595512618862593820773763255565890513546852325262552137516739229301729109195121465692268397908758230468872116272587543717852111947915786920109228642099406124771366893688544779885873592334742039829843309199176283626278908772268785186157206565026383912652841718597838668309758064427348086773338411175458127992643258976877362671640393034138646902983801554415929619476003522882310715199034094620400067283057749713488578331732735563100886514156796367287291290983202590290210022926655874796628597645119469074057159407782316944941248277201692989467021983982314450932725328966930265765688622786095430198592320417757151008022913261319936719985102325218857845049602218280125561474830021444915914576272590136561284281005288393753387662235099535758536426538240013889169328186193127470874375440+11189286297979541962761276133247302489064082109246579981777819461120296435501962253146580413478673500950468014634215347961845005475820742411941493897313891877064094240829359883055014522710596989913546130842293537453003794630264365651752193426492935732641055450298045060512981238648296407698299751892329535033341227659374575836985263024096229879759065321481566016670992508187622185495240681432692337010248379064885968941794749137323582909701326137457177922421896548727499100041512485236944121687784631774410019730351115696070025882570557035488449163793303099024074080156372731416918509936223347372353098191071975990133041257599926250011025062285877580671264673334442403322389043997907074415136508245653888009479826434231489455998971902764278966067665328990162240051742461610231486405618646190673705872870074510065653752543163300593490811197305697695432649619221893833588920458473423579368801651407391655658863139224740498634717558116390344156337552091161937861052961665287134662694263113216358365461164363033187910445351704557871211865162874132079512273838516484667044482782995416097926412629923974287129780502071321090386713862969924239609844977517404245188932604713618019724547071449071428530577448745315133038436677768391267539775097973819592253369710378914666057100289905572662960401067978349894124513668385290934263242930836959578588895056270417804081103813090517088090743031738425612\sqrt{5}))\}$$

$$a_3^1 = \{(5(4742289407149488276684073702255570358613493810345989396622477130376865764690623403342234642639813203274305079959509323198854773019259893526062746026636181700661344602510875378707324579931792384733225367056557399691322762960268928296621208295018975468153548999628374953084290597358262714209983248406922905772665952668399585831708603846769019723854443207595502754631622405078022050686276487807067928912218812016717493107199370517601211134993179444900207856160596178910190290323674868726291657336523334708867080072283701289057418499603108836634360496666477520159983924830664453247386092634860487714878054091504660370159535931295617237640900401249174805390665959551036416773858771427427599320160081641041260976728455559904836133306706432951779094840676908941570324657455689543854072045955968708049453965865844361746298228157811922449452195629405246824751735674906743138397089183846779866571898143900209799258955911274798671495188451529724919185978634570896354039428165764078116055292450490677896331875820428230106559467706486096129100332668054698469351305536609651237992747133728861724812633031437154365979645104660546343212767071008648002231804696821403456164741689229378656302994581173295559233930567408199906377351024053421444247622127+212081629667268659410277117575796714399639332314123377764505383387894167371649337543153100428224747505291842094085080220589211331215438366002688755789641591441585818451380471931289721253733696072860806039468637561336417697729667127529794501765506017259743554590419261630136821823357530895689568949705728264499044789994990958536908078753233245733324483750412516329222806626826098847780007207513217134820448165091062969538126255699996523683566825578912433385364303213341702128080988424224122414107778197522829474621190223597561751158201621325865913192497418446613673425498165800609020559161071538583241353989521407895945200746458170248834037204231543766979395557713616972215815175911881328574778775174483051034661277356673478069033085762676767666770078921275989034845442855638967326978477820527040356187968993609814386296662609761718838148950821964106882359444335915223588495776750002095630363169804685580249384570889981644562339546335277548037596679218623331559393926136460832434592851905005795852735056418456811552907746886106748348749661621747880007022754941311980474591813263825346088781237509116943479081917457693807779652593776252674960308609406651955802296762804063438426476712840983929132645629823538148299275918304850783252073400005)/(18(81561093986731750369521099816740327014656168055757766238126243787687336257295606793974995655322323166027511544023929913597562722685877539025175357416637216266307208445602560146412736250420344267753704456885047020692640090126124874962714835119677744630679822878144631324190252623494609209359952942669266104953567850585028645318142220143669127965876016236870292253988220616396736400135457784249814365991439496663835250224455309191129153031583851735016375539448559588061415988875328459622809844831768975595853298193007867485528589492764247103777657572578095156466898954434413871516265120806973515602321926560300787939629739384850608938002407238002940843959011386251861380097685414480878088458577435915120520665217962361598980002942227712665646235257986797208045837136671081469228229044679091773449517757220194432266588790708627641205451046906195254584395544193764022507239335746263788089168885169364977922794089665272594611137073687987700347851186825116962568018977696301172876975142299126822198412134653994817642352266838260150824903606055975982159320475491

$$90325357536759278740565821733256461099010349609564417565766933200771794339018758252351139489459470546968039187482588833$$
$$92861790793692566010550217517121180424708301438658453437232 0+ 3647523009471630485857455794581038306095358488515082401 1$$
$$99364639163812397154961039007789267230117716848267516346925150754144060709363701926750731514790260355603644897596132339$$
$$79542743344497075112078648620301707924646012007956408683942523514147661648168724166461297126652119244556436604561888826$$
$$81213438576914114297170945175981349288888154673121825275178937800824890809533098529851578114035463216663807215883977209$$
$$75760570408984873481929729065650252760143488774551755623458644171418198772785324085738371275117085509235646474210157892$$
$$56021267595503649065251729983441197153033556403772928400088345919513865677319968535918340018148745109963512072061878839$$
$$06476558661759585423704837793603620246947333661741390912525326499103105490826415440575899950859674953846925620313688670$$
$$07871047331021701743574817370194061889477768231343815982649117798449998620469088702434009627118923097164936545884390656$$
$$29242552515618448107447541381840912094275816059008709660413242523941390253714672400048182260253893182162496278999509367$$
$$98363546764577275531606307625344150193842463529844150761753246111278477593535400925432800816914597335307379861296533475$$
$$17145158338177111348920203604453518950739698125991511910434737686228356505158378795103698888270596025981441\sqrt{5}))\}$$

$$a_4^1 = \{-(51089719477157124899631545315937734662242191246658151338813004630926770791190882158827597373283318567195 4$$
$$45121140115878918120250098013934400083665160492521304155434751738963352223882730615673921697040243635479697455025577 7$$
$$56644928941729556229625157490137792043647006307922122639075014767008448849324589236558573094236658941672014980417963 4$$
$$29455538779960705627352694215735914466452202643449261791389807560992236557408996441267827826340788600884344877138399 4$$
$$41114545537875996339981938972435145515521250207547293415764400141616011426623425425504345638852509694175993042620833262$$
$$86988125698138206692103474796348111876307662325430682820675646402708184241371951154208793822601628565366503717536683 3$$
$$49678185384510751044235488999511577691287869258249959156838331899178219134076209828088692223581616650783963719076666 78$$
$$63834209804236231375604553374087974833636025485369438201992306684823684807517517809127482848333379070692939981972706 43$$
$$35747118314010827276019996888714221 5+ 22848017140463669074514728786146743497222897932245689415602190731561561831067470$$
$$13784824107664279257010616352724362324918800932750421503115965449208349233898568375621939228768943251856640149583525 79$$
$$56865395461518238091650661959723190121086767498395926042461904069093357515739208260932866859547942647620678419554303 08$$
$$53707099813280025148310396661975712138969529977357507942561482425640018623600088188954427887363758640242635926661189 5$$
$$83128949762295315707215461523201210848311119646341923208109407007016076772728479363953725955441510813014290062857379 84$$
$$59006412841919308607494342703948346474911370808996995876180656866354791844144657658250299532746946408730558596205954846$$
$$64422495212887088400651718106364317189780372865123906007225020067091223186741954995429410437764448612791432191738188048$$
$$35844106821957935861669707471367283183032724225618553694147863199171750879728694191364106848964199270692423187790284237 3$$
$$28313768673934811454814243719211614783302638354374095580 7\sqrt{5})/(167191665025242008509491743763319680793167195009663517959$$
$$39237649487026761013869891710860341643421728888844847166788393328400874324570982848054240991110605797488966378237806425 4$$
$$88050675848649195261664696606725224664898151817744794424215009127139497183592310821979767263889116455319726323300677234$$
$$67423915039862267539537916828267862661438573737897186489217056548819880674389747730415960544703554436089044900770292448$$
$$64767977161958141491669497455510015218989801050686814210929530969726492791870526923245585690658429262593522663740481457$$
$$05616737466014135494511865217453244862486265707429948465728744716982512130830418938095174164006989661904187434787486327$$
$$65731163323488982272715181823630245964443551836382290043460189801080818384426266965857786521275891509872821121026546856$$
$$07331986138337202651864409493324602440455318870913639358458237610268601973129031578487822570282303969088202281785690471$$
$$67864392187270024802170593456753569181658648680091110280719537991610513409 62+ 74770385653563044681669190298821154754 33$$
$$32774249222845057406582106973395631795864775362753372204287260301917414073622203603128556922326074774942602168209413276$$
$$96271791203995663547309478488390551803078507087674434364791650302787382997721250609750172031603666607175384355244356997$$
$$95289230454129567371845698637141395705637639305252108061727746233825539770052625398341752412606243546292802049225848008$$
$$54760997180566417158536564998959541008830517288872616849906291457194193302773711304384308499826225837607962996332482540$$
$$54850292069100099215781277386070607782273498679529322693701503589903135891654062790347638127213283540844375078547837 71$$
$$14017624730315826686024530373791655582542955300609638361678624260521489307636845681557225283117890661911439861527586646$$
$$33306941880390698400226727089962880918253463491126612500000455391303079503354839999307608654469328520396123523779312088$$
$$36547004426023958399651454177563118735993377611779509554418854924863397120524209479920080968\sqrt{5})\}$$

$$b = \{-(38080438331802890585707318022866282925027104716761625478233452891364303237545284228722362537340089151571866$$
$$20384687514343548066312456927813720080701732681783487093454338528542280222760316376381301071978040004382164476677967 50$$
$$52655456831693835817636200147703810344284600918059501992084845353135869236156119136664911235308090563979394339645744 8$$
$$19587365511122036936148503593837655240211971062773256274778721860380704058410254027341233587496538451628754478028141 16$$
$$39685627147904722402913373062991075957627701379917944728073740479920028369251188323861074530246935360486395093412938 82$$
$$15691301177897332722325306115413736278308253319971923221166852856448716138630173306849953072850264652 89+ 1703008974457$$
$$99910055429868404714161604929263712928330637807820450681055274098545809763822386426731771158531111904213463470881156 16$$
$$15303855225474676143662555827053298546222566606585882638730562631295315438180262673441361651693219252167764122362267 51$$
$$46856684996883850347265865847543368164742775428813898242092344993997314462952209962939990556397454841940111288140064 77$$
$$49501505441061235184346402285507160495916527247463024259966361870896654155995032290207636986604097928901025804260159 20$$
$$72877193956587059480769354259466733537734026316677274981000757651248864312823338282069060353048280819203245133568748$$
$$00488712548578043484129544060639901296007332176198617438684548970893670570517052\sqrt{5})/(72(4745271870041783535288047363888 0$$
$$68721639592372944978305466134200778683982537771569489893270902462655840149234193931898522832577813031107411302200799284$$
$$58314798707566874307041251812655467599058193893586717235387409525680825141757210915508789949314157901006279091634544335$$
$$20450996098705063621769119022985114222265051729890215698604455066601414937205770825672275799448008800213799713189083033$$

45159286647794416758532415404089301803747285012932945070216373803616439069425758806674364889686668755128548921363586373
52730388260923819112751197499749731194524570502335607743250628183812057900345083513655659430479890931743035030612183509
80845621877490402047012117500794347130756451236961560 + 212215009462619516050612539636822311538541502499796802848543512
09166185897104664389736435877545600991508961224103359822514973688881742613029776963306810939729734491954311747308833077
56992630644705717148367891413340737840416095140681299620751133755076159642993308607137308046167061400313322714246847440
23038308432117148355603161529025700057542718945079787256962404103334152801503943737087215473545868750491037184159964376
63133473604941605340745942098869792972675212066310626416423036211812531770444530350880552983619196596772474991987805698
71459814052244955567970989942690437933315655467604269677871781540612985293486873116206591877106990836933740928504366823
9255163586831119846561$\sqrt{5}$))}

c_0^1 = {−(27(374704540874767682763464451275160249390934814845776297798137195613318121944441123060003034593096301762
8967731149800976336947863377075065461271311004266235033134029552277396121099228425744619206873830987095482259624018773
7673846363002863980733425122382752249026847418561696641712988362430595816578958812821066232801104702470581156471245152
5125967659620613280937342240995223869336055906458276648761421442519324784525021331944911895294593432712149696504783510
2554598221323918722833362301164409544154756935556345307353685592315826554241131864413169829455945031650344170857825165
9829970951045917005066629043109651260204910322566830127334749795854258051871764873674244867806107819270589872654655561
6821800717702616832245280353922604709038309643248037863847803008399181412298807317114549175413747947427609788432947695
7532500578251590601564249782662360726185929401435545343486229708439195539071236109024858418389610014504137772812035038
8407949668874015832266005062102895000570737397055359966638513624997020774842417209178676160807104413653503926500114897
1837157009263129814723520128983341917746493562447831582015320152514274110413411163608633524335466815183533414096670363
5104920335929875610525273053595814398391793449286471167774779515856591262829997987899960389252320697753956204815464350
19792226397652032870101145235890729171960593791267059971343460100478247716799694208915289338915109344664366455209346176
02901654269296813804894423048275449728673595745147877591737372643153559984248211664438501169123811866618459221261051305
38933110521067557687136672365867535195945468749447827985594274846018896002974408278413488438228991464098258349628541163
58583324440737983375188608058236606830798077757555015620656389026927158012789159268766608921497263614613471061750950133
136696963440 + 16757296497476581029376333419864722693472295811429587442540946732697759565264169237432231290074324267858
06282550840349659167477199080615399404108813360311528310357205447237558387257013597134651250581939491246652277019209195
90368146014428609587738731952004012530744093036803437422824733975475286966374101653836482199123749642711496962863539532
33564868441311583043699700462068060345267160631896798806213044836125979160800647928030004282742125161586399172195135179
87940468487311256561981285224553853282203069678898562945700544121122317933499352808541030137279448381642884874389501018
53524474468825447365889376836684772836285698888059449867945434028477559557505088709433240097707090539868643352339305382
68077908832393225627016025997836566657641601707605611779351681636461472944632772646430078414021071002887782434242321701
67925209396028653109514650776662431736497259195044052687503465984502331732574574077957158046059395359841495107482550818
30399000268248085948275461061411925874275731822991350748375600800325100794147478363274444376001521793031599195328644567
79790188182809756609672015201085553845566742357760022081564166388793556662052073085808023889804372120071460166483886523
86650973429088941323184752472919032054914644593345778244157819007799128750068064214924048234025646250845073924565401768
41047598175123693677393793692713911360536584046046459371338956573196985194805942905487564590114000716460650348756070264
45930564713685225002846999386787286544842265713244748208327694592282967061705827820512542395736745820938700474870641025
07013439895769701973239178939256224260686942170139471316384322176896958895029265320909553638853904756053120418881973665
10295862918353814902320009438126303129189706922924508737132193269004395475020241560517080464684834987034166390320706413
$\sqrt{5}$))/(81249645445061675598115117675187441238605615172687071576849556637382447731797110743976785493570490639356697637461
96688728941694206080099649263385819249527838663297814802315466789371664844237718117238271317761902403105943733313819616
12629076464665453995892725461936188363231636813622031801030640437839718807226464248662857384956083489540678379051824085
61025096441892061623198489958333674335038068516573785433155038538423667349344862154191225437039912314271799808216478989
91430978023979581249330848163952083183015825051325978084880041939092370743641943611705341913888451548922344411644367432
96195582716912471984112421381805821511218745959531092006565661073488553016253120144002084332177199860368675874089597408
68307845076372278205835615722649741277328512435867874452763861587709635480491676436665314353591326013426588196325322811
11658986436986447831210500888231560724938432399311516570930298879099190863358966644721885324060508098171216103999592902
12313795162409935421335679261169877125945183187812011400185396882198259255987416373712147716320464061436119233392493257
44451921539838614527249893178149962603697929171299642332080511673547507911050641144537989749262767241333277011331582191
85428134815711197533452801653191871528745434000993796827388307894650176497389369729803858149250759279418254641585482501
92708807179301305485178210145372026067065053125244870269935899663583425510407974288059372463120051708736042869927879342
50321942815352921620787367446284023473050608698158860807873238962157856136817653228601798663368625435162701345506670445
14803068739166451180898590827986956875539599456995453299279520742496412358342374696090731731841887281126994250328490675
95256407425681701445642944201112963155524081558367564600851406979463811874537968674323057977738499205 + 363359460725828
12245049582250275442160951586754860334473710994008690159721838066799527548341288105286648883022765893409773491259932675
64550065716454645821204701697206019287795034665784831133941503890201851194057900929932982170034880309183230462240731464
40693809683386578851125062253490615415271772062174798108202835679550271247874881601161910322431780033224313875655589732
68041068804310224725385611709602461238492276505944914820913109435948730214896499236445342598119075634911694750784768917
76499698879483762348074669163552062128464166199714377456755781155347970784405839332083724630290398989750523705792525005
86694178428319305948844223115823265547868863257516653978522403790292988497342956201603518342034143390218769260122154309
20827222432707322062467203602282422657490656549666533746919938532042077176228214810330223859438993234931708304117874981
79301485368199422387187886871675816240513461456949845685412095246555927701144381716967574864653327344629942822855077989

896997199020033892828891419018515983771353282180732818621657497618678072424826353193640475576175628668846977179947649288219742326039133796622833867792488475642136309224405643598028441839528927593628756802710239402053852532786756092560896812221289966528288526730699304339808937248879521340929900812821524759451223210371048016501436799304844596926569434998518437185673239719674392444193461429952286901753982527899173751536200439844085923365794439244911192389801914627591994173504437695098900325966061382050956121590377320367544556715432395948847042308009142020928076994555551819844046952454803217313854804930193804779799433030762083780486284852224848005273371041534536027506034620072438849784782528634048277334941861734487013457914026727123949460385946775960630918160098829644124488297426916792010√5)}

$$c_1^1 = \{(731895558097527340543181593949679297074909024752156901652833782811133196585273181440953153858973470927660$$
$$085683503799303693368274036327779450260056823317169035416727813522226814392555349878007444382423362550583506642206503 7$$
$$996455120902928212564279244137092994954061988708430076768012616141233340172604650149142622149206343023169858428582758 27736$$
$$450637118037585159978797364238939745708270234778815091117654181124808531602695803516731918408677644617009112646137129 63$$
$$932751587169571844674546560201840956892383892637671081262007053485821483241500739350341584948730683920691402016430754 2$$
$$015746031584220335352170291134399163108156432814186087162088053643033951345426067901009428241184717557599631983640142 1$$
$$680570891745236362457665949113533982670844179326741377900980883232798172253540078647801519072690625401554254702589124$$
$$150164488908995486101279117420491326519407982101438010138938039349601193762568691081242479736809714210800181831590123 1$$
$$955863190159656509563715940286956565797083318857716225110840443450793725252436331019202498246045039806944014237813213 5$$
$$241269300931375226763547939893169256021274210912469946908979712809082850420773950553404709081198391234999878478634833 1$$
$$166691076106009220000545424330844095926711899239631499495526890039796189074813394464645162117606169069498679336807846 0$$
$$940843357204979590706349652816029192678748635453466605036651613460223444876421690670697302990842278576213064890850915 41$$
$$222605599557352132126924370922015558330143253422025213444980622786316702826545379574500141412100000747072444331459606 61$$
$$906392438312286840760423370552763972592542126674253241181425590258276242563463071368321603217345356823270493026508133 01$$
$$2868468960346093774928079725612982020375017377630 + 32731364406724355757107361328867004428871767948470261530612264424 66$$
$$080453134913531411237348771388595618567903211323008733556153108061260874974100287757490182358285166975316463023080263 24$$
$$240491789210268917709645549230746291066044972532212074154886599222986084425669767128375556099287151217561669169767975418 42$$
$$188981620528351581005677882059830289236676860254076009872913594262835188193751781620127565779343850200881817747146300 30$$
$$322007295182118990360120024037862357100509819884424563222045461858913365587473967175542160413188309351778951456238313 76$$
$$188957087525482136051138190557989737146255643580110146627466243771121614335307270750571403698553738130445975757634050 58$$
$$975464388083464647717689677642837737957461776699851845761681496213270159966175409558390269633192402041731046940344170 22$$
$$627282976509601764201121092336243616309443906739526681346086931863078025760716803346856841129629989172061822506106270 $$
$$111349488787981183521553811713870743168582377723665029403635598907608714051181445683761325283626073185116790533921435 33$$
$$341237661588282050675711380974929244350309505883867456706889250894720646229777026132683240719182260535367121335449698 43$$
$$062426885192765378091480274231299899118952564383741413202542071607951160379987038045831376923011644178093147340644856 53$$
$$866033171097575547654589502194249875705557894823420652477225817285858972181729569352821002063720980350244873138494855 5$$
$$459484843739380475300896646850672751278581809308549504673777830895425701135411494189557829044432198583463352434149301 74$$
$$330928677368745247611481721284097297123755212704085770220958472499085261333248136580205826086566771393513274123770672 94$$
$$041136635010336603053263303404742600852961813729427809547720287519218081699060\sqrt{5})/(1177226801136682986299990991162545 92$$
$$890983697219273895355970255930386232496296577698555013220339523141144080382023078053760087014261092219614275534073715 72$$
$$940781743821835484224097010263350118979874730678875462584417715531335260317056243880761167303714913611967014240186657 80$$
$$571868039438506749578197421043464033378124781432132147281715484094762685744328995836268888315188479329603433874100840 32$$
$$157401761427763415932135709612425077204252780990530502834613171505673815468605395052766381584236217642291039876405492 2$$
$$027083686428853259023427770992802193526155067031577643294830922614435094947589597906341339315112926229915213660900461 28$$
$$037337606407956985352533589663867677216248404002635591432227452082379116051186001517625246896590771609726738680713791 58$$
$$150090508656163222776024990992933557406190947107259410633261050852263523495339623589249138039047549287311432675939572 300$$
$$377409633135431462844743553396854878454707704615541970996647208660182922659947564095056206472243522759778602197414923 75$$
$$438826512810787294246903037689671265407855775986993846669659347927102950795968732963850459375587392459519371563115057 33$$
$$523660654898810745937785152215300452771527151984927433045316907875610555936690765229276020604467581285056870 27951687771$$
$$350609070672076749150138931237720673060052769815238130484633792596186280661932570656944622658924540407262133094507515 31$$
$$787828370719723066366598495257754556178165095235238881622358347391980355628298363457756806522073887237824390801143864 24$$
$$199645287765003198186939502588730470488946698896273266341003487867799024057233043506774730712433886265965116067321719 40$$
$$376722837051201285906397639909119904421737484995997951347879235105258083507427015945111207088069761260 + 52647183045524$$
$$997024219700480963694911909370980904512730836473933218542807052115986999811546499370476595124138361216746686313139565 90$$
$$382143977113910280284060963714910618359354409315956988257991120115170488532802015906193556291295913086312227872197549 87$$
$$524220886682196577701065013419368717450856511356179379075339285151550601158877500855131065911090842804759236323489498 15$$
$$334077265896366935730664608599300319714684694729883875658549207325967114112543716047061998866731708823592098129779373 53$$
$$964452911860148722709366932715846769510063746194935979257897695057087568064946383749495073493748620870659323333818028 76$$
$$520676900279710272139470595688654221855620686144833469132173232189154389333477435795471683131619851181302195306229318 52$$
$$652784138772075590725235029389783304977258373472551836260377729098550500719753862345188332734348466991882547326471945 96$$
$$872588415259785611242679994633700386635137335470972833541977616556314372976809995181706547652350348122294058091533895 66$$
$$201180809848904192422179981616615916877821207223829674856031545982732746783662108816452080147918459592672535616565678 5$$
$$567255274576215379756023009424616805895082077451634233311854030585254054796738106171742802155168133842521739070234059 77$$
$$014741675938886795183467057620558988752604398662605419761660602386546103193659138630721560899937475414267069271813727 18$$
$$383111214809127575621711694512692547755928889457006195572572165071779748195132736043441775615181778860177016648098009 28$$

87169210913858487594050495244392254463208946366066752089983104396204097538273420942299705187130063522641821868436199995
99937923113183339927637564220223892488022028037293906970988071911556297483654633541408480962048159728206468407220123043
3289$\sqrt{5}$)}

c_2^1 = {(18265261813102329749041403674816116274868352801833962565016378290143509246122163330554939038716065919457207795350515042438961590891130117371078852246146736830148448022762089138739998783276914957732936894470433382071085730972
58062003699649984036676429855215720100697494721850296987659376608095371846473381841809873200493847507441264755655511440396321012725480674721339780794427962714549655001230456367492494649289563745639658429438797600864669025164555705418433495745792026539532466691234600942071071463937517684176442877428833224909668876748462405469304514895073958937991619795933504159300208362068582354461702596668320550803140131860882083736116999577848488075422124057802552340876020539999071468095694477733409281376520798959018971381580242954308159800764076407621065877945688692349681071905284443199983899083618934145425379666932135708629434349080344209180501992382131109229846095588808753637997966647054362108195231457733941845369031040946972361407022802864044448358464317709821591110057877528216181209656427984786873019585910514389889855634191791225179604878245485714508379194713859551435084855701589138084484766923026722225708147982023075866931579366070773231535308272652166305146075379974491573506234295412630000652712704134655881110703384945376786915984991825475199972332456283492473159121107332283138828002859823637025966051465921330521821096964999607035080626099769689886957230555712871987515276031141233532674821557178067995018935725120684196701107647658654538520619043392716541126699969557813619101703040242586079692193563798962240925433891413015594128500920140 + 8168473408185573646466083118591192204114965778380225960398158287159998626844127126645955129186375324114153935531418571083846055256748898947824928831469904678718774826070937977072673955717597612796962375638378117419828355460896134907364282632076381911128362907388048666873350732120375286044412358106716878753412663250653699296849538789733786821252833332715160988157224091633944893364673234644788466877946454685150972958110067373821545742780890326515524446143080052476518374752264272594975118449693691527657947804720698689153808383984597249313240290554120320880709940869719732315042951118559374583007530711058456056591244426792594955758935370646381412638489868633878007156164433730577960749884250826748217685204517898533454622789546173289320149064932889716517324760731259235132919597929874794073154912132910043317478385342983026287858379021717526079780281089327197325966845642055107486278130092608564124442371308330300413065912217217630197981636292156307570981934887853561917637771291549785131607170926733626064112101574241052738037099388121998222414844171962432308272012228980138034880594226799312992201127303658940689138092604114357080308674957139340309368428821292640560226013594420546131182139715934468066766985262159105054543884754300345450493740438147368763601548505090137709102337108027265611368547897507326019822300034276529121043145191377944868056068959912774366448848846203005959854568204892022093995818861296625597415163749105206540843691691904224700155854652653362048949680239257206696850355033250857923565906667845615264422814203636311596588353049521380180281 3$\sqrt{5}$)/(617853030405122231986441563558718359326470260023181041366660238937324981494092528179569569925602945483591504562898177040622030747716658105714377303112441135548064422370442155925430417938411308994134838065635487728664689696991554918827225298961002113669661484104396828801660323926640897954836912967063126184887809878796647021441645858359232038372856144311632663470043003679951714241244248596531911360468995333309054029993911178278260997680481236065887935076353732159390214775333948243555312079577644427309304568742217948932051515023424402020177025044440958299573079429412224933935556411471838376494336061403757962514113050965711075723157409353589630826322954703300035604655145992999116116863510781173666326153442691665163209070606575300072699682407158935534239521310873841009836628566484115983480488457725068411768537462424871288692343922090593180394243951251563419424151444375693680024227111929673890498383122189133959336503980337148593629734525504609146977197859128194570729956529748589785071637454813448749744282597077157885010095513008556144215730627873372887728951311334856429284451304482599587498530947104261605354135086171961190595147323750388311615247806630033634782772145383091065729637656411502836756064275542567817671497477211704270626209132251083114609817169965031716523450741018668220546912081688462649353580067172927617846663970972103545651497518941345840535195241047322395312043819728286622660442720162436722132427190337388653352144319420678401764609014096421070914269263546532758738238616959285937682764389467353279899309851576197153449090150372241 + 2763122752180195476414622136208120308103017678540526147171750515739253856012060539844618099901506980506898854041327315761073316753513234582658905547155158355012209782574875118431743318417387969394525116542791402076099843699667734681733997351076563616328007049504911967361199558196177415621960344207646592937252578579194542212389654972146956372859081013056838661151124747946557466799710677856142070488219351949379141409269133562155805641065488417121175282840744002716518309289197385054185876327447270319266469907744982595985064499882917063557727824355480932685643071221702913673430680978715564693582496776139447762017209837579575226355444900661238910137024973572104781299499282274069888541706171470402539283132401716234527699086730417503118939930607660015259677295854325808489451042165680582922094306411210075956811181135863595368504063323755866336718993899512419952713394083139811273629713633900726824545018158792655125447691668281321650887740392633522987999579146413630695066203056843352980542930587795678659249885428659513169117289539933230983739710843852155505121328435293841174174669956603636051364271717098617947560643431216098822919242318138974412409827545754996029423720378277801056829198832719628492756935777448060771861850584004004047480030332410908703055336569335750711208201816805493319785398357798219838547702344687266378747676366110240616133595369729328550564390174905255326324622604968572005086683889794227406182721724371012366087632484309914078552177310036703378749150664891064923199566773635881355984995242903295639370764243997653375212300820$\sqrt{5}$)}

c_3^1 = {−(4(53897620009170799154595849410771580281084488400741441730855433551774257870179930263935588570283245433976566468097222559847861738280151001786532420682089525740962931399011448410375714886824019401723080000422506624884640445827264836712599348540612168724334073739492301027790815505883850717717685710641384057787828847462478148232020441143724996443704235884335982391931252215402961161234610482268136475142549269909867589022027699151507017387328113985834027617 1

$$0758050272133513752158166475753887537920841805582811992080715178341659695123035986422520553886010540297879345920280766$$
$$3855968028228960411736744628977536342461945309767770786673676125423873299953806720158115376106775321160390632897682621$$
$$9325312172181388405301861369718421125368525150642212025565565000064802350231751252339327836948419622415676048921628294$$
$$1442582733268000983242736804908360365465913229150751227834584646050148888653681044645112116868784056399933167701629353$$
$$7434777267549002503293795778172854019360715030048058969329673753005383286216514471348098617325298503394618284745332863$$
$$9726047810987461702517915248983956940968293253521071459643851125999299935159984853687590011511503970440381175417251990$$
$$6825421153487178686589308813850936776732842196710381405174002462806197734813709939372611329991726357391186127656894421$$
$$9956647845777210261800089747668128076083063736616740219459868436603271997341261802975806178088963735428470134905553227 8$$
$$548263311520570 + 2410374843319174909093018581622596485923632834650999148472111735831034539706597338764796067137706790$$
$$3012545397841622401350792403355329157507590561433433430755763450160908184439508051060417758095629405684604216323273 7 24$$
$$6204031299730145685850756029527754268784386065873638668215738041308181192014155481319263629319594530555533838660562662 2$$
$$4671982956406913807665357956616101204698802166466728925646122314258436278757622410843521132961884632034550115890970888 1$$
$$2791705079724766603026060662419513797468505069369504595298244781162630433287821216683678153771832966100367056094691804 5$$
$$3614579987665882219757836586073867775108456469003146448617876487327701962800970497246058807483101185053890566794152750 5$$
$$7558858549707711711566002956641186652847434374026104605296925556238493432449036262025175710428438349313305288661863575 0$$
$$8387523550305010142559354328664065906210452472712035160177193597065658986768301610237587650184063479584367897673215652 4$$
$$2733796668952466481016580245496261640523565788392073518012221254842209726508255796424717779451448910102855624677891 6 4$$
$$8564583487503776297464071817376543689037867977725246584491857124880525342481228518559600703666622149977640535089590781 4$$
$$4740494000564718087533513858070820534717000773986271253099335215691510705877233999424768985014122025609739333389172055 4$$
$$0649454433958881046469753606512333899271786411561977418975691077562140476245584162547808600232783325386408921985056006 1$$
$$501959619\sqrt{5}))/(41635859389774187568809781739244758803184839740975989149955671751350981315738834848358942412761557176898$$
$$6338027640514710633407481863151075395785542870987903343883434417261030928071520941974554364925876802606972230794890981 9$$
$$5781299105843371654017585828833061044907356703627140965964814644917469366294173192125582437092986430207022058860705560 9$$
$$1361135916365373676284789922003010108616490515702307178437402239957266235863451018274194169308648036998191825549476764 8$$
$$4412205991483038505486326938289344858144656109726865979336743391294647383729779673863762037882119377516565779708340390 8$$
$$2284445064513710327894861775165611425551631017025733932889262994658558987103977073499043225880402630856736861747827652 9$$
$$1249595888851868587833118840189580540748176707394958252577166477658886019142909812890827787490732613044247667408484975 1$$
$$4400557061256863730527269795792747735168079709825979074859029389756159557920164117830737935352661144468200427122695108$$
$$1297309941627432131178771211786394579133899577717665849343162682439853263542031674643683623019104584017708404940629291 5$$
$$0082258273738500740117410444497054935196765060906661498969011344913806687538323963504429616689244170081353552552341231 2$$
$$0648998530960446274783134601335257701232929948630381330241030987098989106451748963450738494163133733094761300842167488$$
$$4173074681326927788073599019980811614785747408929724834329099978915193888948401064589723391674115766550785395687246241+$$
$$1862012237943159912159146420048808995106256905357562401137751806695410072830208727891360302745696457959775010572011251 6$$
$$9382292062202650796358311204141276199372139585270136552558782319387925173091957937004810377099792449156533076592287144$$
$$3788273493860354575244284001811218962627289615758221327734656883915978083011644351944746376526760272150829169966825682302$$
$$5067000150104254890204699334011749065009903175850733097333112877198783622477856173647523676017114183521507135179815795 1$$
$$5516179308591591624892633448717158013260617964033995481716747977662672239509627409209384307968929237327571740494011481 2$$
$$4373215514784241156225470746186028944395959335805096571933343904767663368525132074273898042095423470546622567482368627$$
$$6756220903307074689348164254584009603319309120669722149095631568513290904849508247449383872897760306197500419192023284 2$$
$$8080291376829414737949556909904403373804413056575450659704194808173802147041686938971737836461047622175433378933973922 4 0$$
$$2917796182350597029362818492011134708649109667540074730046263705644197904107552604262758505709823801069710022628661334 9$$
$$0853587529170464607731467990474624740962133916956919303580250335851456172999311313786292425458384807004411897523080843 4$$
$$9968151609655677782635869536025819898715924168909404978732445851594404577562670204048119671503044074328377697729851344 2$$
$$0250178554228836410921065813766755968383299665771507067358733889925578873054619785227376123693642065496\sqrt{5})\}$$

$$c_4^1 = \{(1525791444949213642009794781366452101038073926277289015747515086976216539271189199000940655931668603604665$$
$$8481811936098100939898711812588618578219265138733018110692533599925063284437026519491682790680143308052465957746236827$$
$$5122391942401446835888959903016903228509651231080651602528202971420644289645559653201551707845704650957221208229297776$$
$$1577274372256117670908539053490612016443725412336309224658255415600470876315077033437090630554387064006577206185533502$$
$$1628952989955505985202992196196638008885396274068427455724067478367424052232299192780314976867599162028918293317700119$$
$$2208209005147078243279870871374183352574624843866949566576378368001409593964426212005730806555518590006930455054277142$$
$$8548714541533805254933173247760611693109001275123987079136397504400704444314578127860577451315102970345744002797794909014178978 4 8$$
$$1450208276777565520865092612992810686025004722876211443712035188982202598432876551798630602453172113746425887913365543$$
$$9331790211937663219884779179641263660789328243953775337900430795571772387994502380538147022211801266431028270866659650$$
$$1713806028523041154216877312820133922828562688279645030348345487440246703466125013753223544383290440874612176009139780$$
$$0260637457575568522327217387429771958218482404878766 0 + 68235467807881397185690518715660657031677603780500738668731168$$
$$1936465298862454849693950244248084644497936199789305177073297812045500998045769894626046616273480899335672154146705 9 0$$
$$7856742727363848109270988427321217559966763720769377535913594023485843885379140251039308694641506986392674887735941315$$
$$0806750587093158122813173245222249828567207585271548162775305853865056248000669687887970345774400279779490901417897848$$
$$6584830453775962904375349584095625027720248964118035830277906838310271245845499549574858360270658146762458117462652048 2$$
$$7393018615494024234034352279154201072631709219616664487741367095063171387010472423941444102986301482258013510830804133 8$$
$$1270657769026042614583935055090946059076639628420899392981236153396500604589338247493984345008270181770290102527275962 2$$
$$9976800238023850392083149875911392187821625128027027892401070277978067277505523527379500032293268565731846701321671 4325$$

88134424977758930231314947060928861258445829738427153194911211329400400373181294952726242484029389117606046675554190390
61655446109076300726353563715675860220799499106493897333975807609975760732652213553633542680586292481648227165891278065
28732384710343943939191607508423005607215985382043462118004381903746228706283889055316771$\sqrt{5}$)/(6116939332376492591759064
42352645692834444239759510254364165936336953792043114754808641577242840108183063803666802529045437992204918863523579011
23794706031912405497322674862222407606605134410795620563530871607518962466781355924136372689563507241427576556716358292
60699033515350043056577067440822069711572095802733013540252738084001383225258154542024612996940029817256456221477328517
77967195996965341644090026768140366814877776076104181881726090965217318313599425195452790537245921936822863292278417800
55205390095529844878405244417904047430252935611151940201919561967326726788687777840424483191571138428883957319202637485
02646793726632403545472567590535073294379017791890522093119750574342684130210175159450587478910018952393071499815206450
95401191538665575463236045579891271759318971102998066191687066024358373723016075152432923895708474270123303388601719089
90275313231918908394249482856781074179175785373863445348342377275494058709312789902924023252528435137229108105122897074
29690482184517980339807783458081392343249600397409105042508744093888122690820055025598275086301295883914741199611468012
85026810130341976365418408671192545554625442846904458147848302491090799385476297288868260287007198022375594193572384137
72 + 273557843228720352877839175098882473227266165385248225714694351670921656526037755228508314374566902157870541651901
13336349984016060926664411822547053260847357182694180616873517960543144285794892873181599685296522156972637466431136732
60044859500286809690889649898971027139567128727611830381427471271973871398440229552297780458910507831652519792752615130
22323570484680575565434009989456005149214660602157420941318648914320794165398996880671676586207976560039608437268117190
15855387884077441786540952522653213504047600245052151432954543260340957614143571722353060893268210685713146273567235045
36671566626405354402040827983976869215319646092106177148471112384630373853378734364368336933809289248169474841780432253
37741210737524397199068841600805948519815779210689214709292843673823010809583510061263894811661189688501200370499825168
50875941674570924246090243151395889248357337983957040170601666137459321322502715118714981150104656659862107536265789522
51564209925032925958586741472072403534854298767760245269472112721349003333996563747622839931441466484216376109987489269
00018024581688924964526313635728714620065788381716594522717314349833982639314082080284258050352509399991662289695340444
64870346819395181664493129788208$\sqrt{5}$)}

c_5^1 = {−(758964876433740262031460718319859215532806936026666243479301424618139779789053771319823857971460849033722
7303469247803183379533688098212646853730125551322679328395246062099625244708457568617129719141086784343588262217852289
7297869762035152779032553880613832119815815230431431218782712005722015761262575275212200940875742021510280033018127667
3923853537522494631331655073577197857792405969483804590299739868358277726893297291904519201337402057425703184280722763
2042754581975260952073722548795190712235290862725467187735902744707923360115685703167815327175306351737822078028988660
5093297074173437070632883064709413805982566015840695201221740850325200430469586353881976542555314869945854491581862852
4247315864784444071075891715766590453923895064773212000408573964674040264595461852587731671951709864964841467429827075
1697545991949790118605540823467372097879311163129115156059291557417351001388877589645013976741732200460042856317483234
41893046596823697908474527906538970416125925463722993946862 + 339419411248114277488436666280138353898217645764557330409
3521166181747521702683802540814082637670199525324829508360942576678735243080765424853565615113202643918754864888493640
3754872211849907202021726862518732022020118872643630622861933678488880582056385815154136363599420052251008588147704345
7912436316802351796598762547909781066389614831634312439891966269973801990459707460746822365655081654847004590244840847
46622740637967752747398966025161559547876415018596363418195179445725861516452053181968475114350725563551779669186184123
24458007441454552040801656552085571429710189967358176561025579558147228549535458777461407390355983732071619489985932631
65013640184091092948456102977712371713800228131172720845517973341162889361725874092723092082522596587777542106686390462
84425987882108097864171069522977879462834546906318213393442911048390486077419004007476025281111606801873045523974694163
7881991669394864920343485299296611762251585586991009385279355878748208928367234642912430901494139027963$\sqrt{5}$)/(20866808530
18132339494135112080450623464259875759365604406691205350859739423504084403377537639693147527018470615672569385755505842
80571001731305306837206576856053955754465595542566262891397045903469073441959871573425679255265291280366362034470273488
23191871137782100145071699999545519343284517625815168031152845100939083963609804253972707653720268600410259190202458745
58968089301322294231010403754851667653457684304641540557207140119418955033659420684559651454319620146469939006962774969
60301297439021030389125572641823687651049895187016142359849478464166787450837104472087937897447159110704932028253784998
51844295969164053980132501431042328745194036213918679168625712852677601483464279246352532658687607499060850802048789135
01771858570363734741085016452877238642898841433637623637984292305504882208069936462915381057339427760425051452343821464
16557221016552281153290321672957124524938546357899116868457786077143987069769754518201698328015552769147920247596328619
95407048558621093338428180 + 933192046939158222944739161595736453385817056715983921339188037014303527662572565684395305
59367482418514144158870826529244674018849627850286866855858667835250950983031178581484705913729213764083618847252436229
45403267167348583445327651289032648780761000479001547594663921932358191696032779823407345763042815343633401967322108708
30620609746103760670556618405524275723397272406529226092577577562978303396017048840500029969284657100223111364875703663
97216681475098416233626282368364406427877925512010740917461317812296661150701683453721583413558146557293103259434025662
85153690011485004278407300406633531497308093058555950158262971444560317164092817708966989293329998580582213399414389573
42180680930716021226515583986816313375264502953585125756948815717691062823721534957435182995246471062611670071257659037
57490132136537682950462170469981348451483166709674202399307690041584198635816696002948967626623829325193890450610109445
44955400312574402981124481461434675538535934767356743682779297203$\sqrt{5}$)}

d = {−(3764319823697395338782061174654769962354702143320794389501549491665992010269267493962197924404400906079826
5927219231767307032288562417212254002545543245931439906078865795054438368087130519338651804695358877773497228165749151

$$35681473992960789223064599722909153277912368550663805097440692099303502248279149504368335735128363409788067614634499783323305095771724891683455002967479943446477707920474542068087490868750178960577566091014424952212016145058296678712704576101413461063222638007055953868019438416180535030430317866104154370416131743258826117910820426018495763728977537541724118741790334499226344658546378106443648676306206500773460569396276749840467492050819410568828332262915716166293909048144400918165077139774685(46907865958869067945027336332595514596989422267787026319500064077580891746419084728366486245405358432803175130938148409625294079922645022072303298987750142416252921507861705171047291426730961556144159161225699473304608704066693557260596972517329502033178112487553192152152962367401861175675099217670388338823056024926393903172187361447650237485132655585536280+209778353926959180108996413483438819830569472512145926302394103173639593379167122758615386065354063196411065276044137816187940628815102260278680288312731938593387891807226359666101895109188378103855907715416596754514691861385326575952120209836653835377309405975087186940505034489040693896922170393495957327938454970896956364766730350747610031546444319150030415))}

Bibliography

[BB11] D. H. Bailey and J. M. Borwein. High-precision numerical integration: progress and challenges. *J. Symbolic Comput.*, 46(7):741–754, 2011.

[Bec89] Sybilla Beckmann. Ramified primes in the field of moduli of branched coverings of curves. *J. Algebra*, 125(1):236–255, 1989.

[Bel79] G. V. Belyĭ. Galois extensions of a maximal cyclotomic field. *Izv. Akad. Nauk SSSR Ser. Mat.*, 43(2):267–276, 479, 1979.

[Bil95] Patrick Billingsley. *Probability and measure*. Wiley Series in Probability and Mathematical Statistics. John Wiley & Sons Inc., New York, third edition, 1995. A Wiley-Interscience Publication.

[BST10] Manjul Bhargava, Arul Shankar, and Jacob Tsimerman. On the Davenport-Heilbronn theorem and second order terms. 2010.

[CF86] J. W. S. Cassels and A. Fröhlich, editors. *Algebraic number theory*, London, 1986. Academic Press Inc. [Harcourt Brace Jovanovich Publishers]. Reprint of the 1967 original.

[Chi09] Nancy Childress. *Class field theory*. Universitext. Springer, New York, 2009.

[CL84] H. Cohen and H. W. Lenstra, Jr. Heuristics on class groups of number fields. In *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, volume 1068 of *Lecture Notes in Math.*, pages 33–62. Springer, Berlin, 1984.

[CM87] H. Cohen and J. Martinet. Class groups of number fields: numerical heuristics. *Math. Comp.*, 48(177):123–137, 1987.

[CM90] Henri Cohen and Jacques Martinet. Étude heuristique des groupes de classes des corps de nombres. *J. Reine Angew. Math.*, 404:39–76, 1990.

[Dem09] Lassina Dembélé. A non-solvable Galois extension of $\mathbb{Q}$ ramified at 2 only. *C. R. Math. Acad. Sci. Paris*, 347(3-4):111–116, 2009.

[DGV11] Lassina Dembélé, Matthew Greenberg, and John Voight. Nonsolvable number fields ramified only at 3 and 5. *Compos. Math.*, 147(3):716–734, 2011.

[Die12] Luis V. Dieulefait. A nonsolvable extension of $\mathbb{Q}$ unramified outside 7. *Compos. Math.*, 148(3):669–674, 2012.

[Don11] Simon Donaldson. *Riemann surfaces*, volume 22 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2011.

[EV10] Jordan S. Ellenberg and Akshay Venkatesh. Statistics of number fields and function fields. *Proceedings of the ICM*, 2010. To appear.

[EVW09] Jordan S. Ellenberg, Akshay Venkatesh, and Craig Westerland. Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields. 2009.

[EVW12] Jordan S. Ellenberg, Akshay Venkatesh, and Craig Westerland. Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields, II. 2012.

[Frö83] Albrecht Fröhlich. *Central extensions, Galois groups, and ideal class groups of number fields*, volume 24 of *Contemporary Mathematics*. American Mathematical Society, Providence, RI, 1983.

[FT93] A. Fröhlich and M. J. Taylor. *Algebraic number theory*, volume 27 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1993.

[FW89] Eduardo Friedman and Lawrence C. Washington. On the distribution of divisor class groups of curves over a finite field. In *Théorie des nombres (Quebec, PQ, 1987)*, pages 227–239. de Gruyter, Berlin, 1989.

[Ger89] Frank Gerth, III. The 4-class ranks of quadratic extensions of certain imaginary quadratic fields. *Illinois J. Math.*, 33(1):132–142, 1989.

[Gro97] Alexandre Grothendieck. Esquisse d'un programme. In *Geometric Galois actions, 1*, volume 242 of *London Math. Soc. Lecture Note Ser.*, pages 5–48. Cambridge Univ. Press, Cambridge, 1997. With an English translation on pp. 243–283.

[Gro98] Benedict H. Gross. Modular forms (mod p) and Galois representations. *Internat. Math. Res. Notices*, (16):865–875, 1998.

[Har77] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[Har94] David Harbater. Galois groups with prescribed ramification. In *Arithmetic geometry (Tempe, AZ, 1993)*, volume 174 of *Contemp. Math.*, pages 35–60. Amer. Math. Soc., Providence, RI, 1994.

[J+10] Fredrik Johansson et al. *mpmath: a Python library for arbitrary-precision floating-point arithmetic (version 0.14)*, February 2010. `http://code.google.com/p/mpmath/`.

[Jon] John Jones. Number fields. `http://hobbes.la.asu.edu/NFDB/`.

[Kar87] Gregory Karpilovsky. *The Schur multiplier*, volume 2 of *London Mathematical Society Monographs. New Series*. The Clarendon Press Oxford University Press, New York, 1987.

[KZ01] Maxim Kontsevich and Don Zagier. Periods. In *Mathematics unlimited—2001 and beyond*, pages 771–808. Springer, Berlin, 2001.

[LZ04] Sergei K. Lando and Alexander K. Zvonkin. *Graphs on surfaces and their applications*, volume 141 of *Encyclopaedia of Mathematical Sciences*. Springer-Verlag, Berlin, 2004. With an appendix by Don B. Zagier, Low-Dimensional Topology, II.

[MZM86] B. Heinrich Matzat and Andreas Zeh-Marschke. Realisierung der Mathieugruppen M_{11} und M_{12} als Galoisgruppen über $\mathbf{Q}$. *J. Number Theory*, 23(2):195–202, 1986.

[Rob04] David P. Roberts. An *ABC* construction of number fields. In *Number theory*, volume 36 of *CRM Proc. Lecture Notes*, pages 237–267. Amer. Math. Soc., Providence, RI, 2004.

[Rob11] David P. Roberts. Nonsolvable polynomials with field discriminant 5^A. *Int. J. Number Theory*, 7(2):289–322, 2011.

[S+10] W. A. Stein et al. *Sage Mathematics Software (Version 4.5.1)*. The Sage Development Team, 2010. `http://www.sagemath.org`.

[Šaf54] I. R. Šafarevič. On the problem of imbedding fields. *Izv. Akad. Nauk SSSR. Ser. Mat.*, 18:389–418, 1954.

[Ser73] Jean-Pierre Serre. Congruences et formes modulaires [d'après H. P. F. Swinnerton-Dyer]. In *Séminaire Bourbaki, 24e année (1971/1972), Exp. No. 416*, pages 319–338. Lecture Notes in Math., Vol. 317. Springer, Berlin, 1973.

[Shi74] Kuang-yen Shih. On the construction of Galois extensions of function fields and number fields. *Math. Ann.*, 207:99–120, 1974.

[Sym12] SymPy Development Team. *SymPy: Python library for symbolic mathematics*, 2012.

[The08] The PARI Group, Bordeaux. *PARI/GP, version* `2.3.3`, 2008. available from `http://pari.math.u-bordeaux.fr/`.

[Tho84] John G. Thompson. Some finite groups which appear as $\mathrm{Gal}\, L/K$, where $K \subseteq \mathbf{Q}(\mu_n)$. *J. Algebra*, 89(2):437–499, 1984.

[TT11] Takashi Taniguchi and Frank Thorne. Secondary terms in counting functions for cubic fields. 2011.

[Völ96] Helmut Völklein. *Groups as Galois groups*, volume 53 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1996. An introduction.

[Was97] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[Wol07] Wolfram Research, Inc., Champaign, Illinois. *Mathematica, Version 6.0.1.0*, 2007.

I certify that I have read this dissertation and that, in my opinion, it is fully adequate in scope and quality as a dissertation for the degree of Doctor of Philosophy.

(Akshay Venkatesh) Principal Adviser

I certify that I have read this dissertation and that, in my opinion, it is fully adequate in scope and quality as a dissertation for the degree of Doctor of Philosophy.

(Brian Conrad)

I certify that I have read this dissertation and that, in my opinion, it is fully adequate in scope and quality as a dissertation for the degree of Doctor of Philosophy.

(Persi Diaconis)

Approved for the University Committee on Graduate Studies