Combinatorial Arithmetic on Elliptic Curves

by

Gabriel Gauthier-Shalom

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Combinatorics and Optimization

Waterloo, Ontario, Canada, 2017

Examining Committee Membership

The following served on the Examining Committee for this thesis. The decision of the Examining Committee is by majority vote.

External Examiner:	Paulo Barreto Professor
Supervisor:	David Jao Associate Professor
Internal Member:	Alfred Menezes Professor
Internal Member:	Kevin Purbhoo Associate Professor
Internal-external Member:	David McKinnon Professor

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

We propose a scalar multiplication technique on an elliptic curve, which operates on triples of collinear points. The computation of this operation requires a new approach to operation chains, with similarities to Montgomery ladders for x-only scalar multiplication. We develop a diagrammatic calculus with a combinatorial flavor for the purpose of developing these operation chains. Some interesting algebra arises when studying this diagrammatic calculus, which leads us to improvements to our algorithms. We propose some cryptographic applications for our scalar multiplication technique.

Acknowledgements

Thank you Professor David Jao for your infinite patience.

Dedication

This is dedicated to Cécile.

Table of Contents

Chapter 1

Introduction

In this thesis, we explore an operation associated to an elliptic curve, which we call *line multiplication*. This will be defined for an elliptic curve E with the following equation:

$$E: \ y^2 = x^3 + a\ x + b$$

for constants a, b in a field $\mathbb{F}$. A *line* ℓ in this context is a collection of three points $P_0, P_1, P_2 \in E$ satisfying $P_0 + P_1 + P_2 = \mathcal{O}$, without regard to their ordering and with repetitions allowed. Such a line ℓ is typically encoded by an equation of the form $y = m_\ell x + b_\ell$; geometrically, this corresponds to a line in the (x, y)-plane.

For a line ℓ, we observe that we can multiply the equation $P_0 + P_1 + P_2 = \mathcal{O}$ through by $k \in \mathbb{Z}$ to obtain $kP_0 + kP_1 + kP_2 = \mathcal{O}$; thus the three points kP_0, kP_1, kP_2 correspond to another line which we denote $k \boxdot \ell$. We refer to the operation $\ell \mapsto k \boxdot \ell$ as *line multiplication*, and our goal is to develop algorithms for line multiplication and other related operations.

The algorithms that we develop are similar to double-and-add operation chains for elliptic curve point multiplication, but they face additional obstacles. Namely, the addition operation is ambiguous, with six possible outcomes when two typical lines would be added. To deal with this, we develop a *diagrammatic algebra* that allows us to study the various possible combinations. The diagrammatic algebra also endows additional structure to the objects of our operation chains, and this assists in overcoming the obstacles. In conjunction with the diagrammatic algebra, we develop a *diagrammatic calculus* which encompasses formulas to express relations between the various objects in our diagrams. Together, these give a powerful framework for developing line multiplication algorithms.

Our secondary goal is to explore potential applications of line multiplication in elliptic curve cryptography. In fact, the inspiration for line multiplication came from Montgomery's x-only scalar multiplication, which has many such applications. In principle, the line multiplication algorithms could be applied to perform point multiplication as well, but our

algorithms fall short of being competitive with existing implementations. On the other hand, there is much more structure to our operation, and we hope to use this to develop new cryptographic capabilities.

1.1 Elliptic Curve Point Multiplication

The study of elliptic curves has a long history in theoretical mathematics, and is particularly notable for connecting seemingly disparate topics. More recently, elliptic curves have risen to prominence in applied cryptography. This is largely due to the intractability of its discrete logarithm problem; that is to say that in a suitable context, no efficient algorithm is known that recovers $k \in \mathbb{Z}$ given $P \in E$ and $k \cdot P \in E$. Because of the the wide deployment of elliptic curve point multiplication, there is a lot of research devoted to developing more efficient implementations.

In a point multiplication algorithm on E, we start with a point $P \in E$ and an integer $k \in \mathbb{Z}$, and the goal is to compute the coordinates of $k \cdot P$. The prototypical example is the double-and-add operation chain, where we use a point doubling operation and a point addition operation to iteratively compute a list of points, terminating with $k \cdot P$. For example, to compute $5 \cdot P$, we could iteratively compute:

$$P,\ 2 \cdot P = \text{DOUBLE}(P),\ 4 \cdot P = \text{DOUBLE}(2 \cdot P),\ 5 \cdot P = \text{ADD}(P, 4 \cdot P)$$

There are many ways to improve the efficiency of these algorithms. For example, by choosing a different equation to define an elliptic curve, we can obtain much more efficient implementations of elliptic curve addition/doubling. There are also many methods to improve on the double-and-add operation chain, often by using different representations of the scalar k, or by using different arithmetic operations. We discuss elliptic curve point multiplication in more detail in chapter 2.

1.2 Montgomery's x-only Point Multiplication

Here we focus on a particular development in the theory of elliptic curve operation chains, since it serves as a template for our line multiplication operation. That development is Montgomery's x-only point multiplication operation from his paper "Speeding the Pollard and Elliptic Curve Methods of Factorization" [7]. In that paper, Montgomery considers various ways to improve the efficiency of factorization algorithms for large composite integers. In particular, he develops a specialized operation chain to improve on the elliptic curve factorization algorithm from Hendrik Lenstra's "Factoring integer with elliptic curves" [6].

The essential idea is that for $k \in \mathbb{Z}$ and a point P on an elliptic curve in reduced Weierstrass form[1]:

$$E: \ y^2 = x^3 + ax + b,$$

it is possible to compute $x(k \cdot P)$ from $x(P)$, without knowing $y(P)$. Note that P can only be determined up to sign if we are given $x(P)$, since $x(P) = x(-P)$. But this problem resolves itself by noting that $x(k \cdot P) = x(-k \cdot P)$, and hence the resulting x-coordinate will be the same in any case.

The next challenge is to adapt an operation chain on E to the case where only the x-coordinate is known. The doubling operation runs into no problems; given $x(P)$, we can compute:

$$x(2 \cdot P) = \frac{a^2 - 2ax(P)^2 - 8bx(P) + x(P)^4}{4\left(b + ax(P) + x(P)^3\right)}.$$

The addition operation requires modification; if we are only given $x(P)$ and $x(Q)$, we cannot distinguish between $x(P+Q)$ and $x(P-Q)$. This problem is resolved by noting that symmetric combinations of those quantities can be computed. For example, $x(P+Q) + x(P-Q)$ can be expressed as a function of $x(P)$ and $x(Q)$:

$$x(P+Q) + x(P-Q) = \frac{2\left(2b + a(x(P) + x(Q)) + x(P)^2 x(Q) + x(P)x(Q)^2\right)}{(x(P) - x(Q))^2}$$

So then if $x(P-Q)$ is known, we can compute $x(P+Q)$. This allows for an operation chain called a *Montgomery ladder* to compute $x(k \cdot P)$, which is explained in section 2.7.

1.3 Line Multiplication

For the line multiplication operation, we start with a line, defined as the zero set of the following function:

$$\ell(x, y) = y - m_\ell x - b_\ell$$

which intersects E at P_0, P_1, P_2. The goal is to compute the coefficients of $k \boxdot \ell$:

$$(k \boxdot \ell)(x, y) = y - m_{k \boxdot \ell} x - b_{k \boxdot \ell}$$

which intersects E at points $k \cdot P_0, k \cdot P_1, k \cdot P_2$ for some $k \in \mathbb{Z}$.

We note that in the precise definition of line multiplication, we must include the possibility of vertical lines:

$$\ell(x) = x - x_\ell$$

[1] Montgomery in fact uses the form $By^2 = x^3 + Ax^2 + x$, but this does not affect our discussion significantly.

which correspond to x-coordinates. This allows us to consider line multiplication as a generalization of the x-only point multiplication operation.

Now we consider operation chains for computing line multiplication. We face similar obstacles to those faced in the x-only operation. Namely, line doubling can be achieved with an explicit formula, but line addition faces a problem of ambiguity. In fact, the ambiguity in line addition is much more daunting since it is 6-fold! This corresponds to the six possible ways of matching the points between the lines that we are adding. Furthermore, the method of resolving the x-only addition ambiguity will not work for line multiplication; if we add $k_0 \boxdot \ell$ and $k_1 \boxdot \ell$, we have 6 possible sum lines; one of those will be the "good" sum line $(k_0 + k_1) \boxdot \ell$, but the other 5 "bad" sum lines will not be multiples of ℓ, and thus will not have appeared earlier in our operation chain. Fortunately, there are ways to overcome those obstacles, which are summarized here:

- **Obstacle: Reduce the 6-fold ambiguity in line addition.** To deal with this first obstacle, we attach additional structure to our lines. This consists of a cyclic orientation on the set of three points that form each line. By imposing that the line addition respect this structure, we reduce the 6-fold ambiguity down to a 3-fold ambiguity (see the figure in the next section.) After that comes a magical vanishing act: it turns out that with a little care, we can get the benefits of this reduction in ambiguity without ever using cyclic orientations.

- **Obstacle: Deal with "bad" sum lines in line addition.** To deal with the second obstacle, we will note that when summing lines $k_0 \boxdot \ell$ and $k_1 \boxdot \ell$, the two "bad" lines that appear will be the same as the two "bad" lines that appear when adding $(k_0 - k_1) \boxdot \ell$ and $-k_1 \boxdot \ell$. This will allow for a trick where we eliminate the "bad" lines together. In essence, the trick to overcoming the second obstacle boils down to the observation that if $P_0 + P_1 + P_2 = \mathcal{O}$, then adding P_0 is equivalent to subtracting both P_1 and P_2.

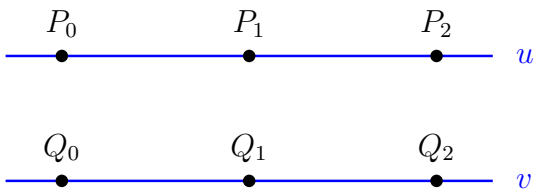
In chapter 3, we elaborate on these obstacles and solutions, and present a conceptually simple line multiplication algorithm. In fact, this *generic line multiplication* algorithm applies to arbitrary abelian groups, which we describe in chapter 4 along with potential applications. While generic line multiplication is conceptually simple, it is quite inefficient, and we devote our efforts to finding more efficient algorithms in later chapters.

1.4 Diagrammatic Algebra

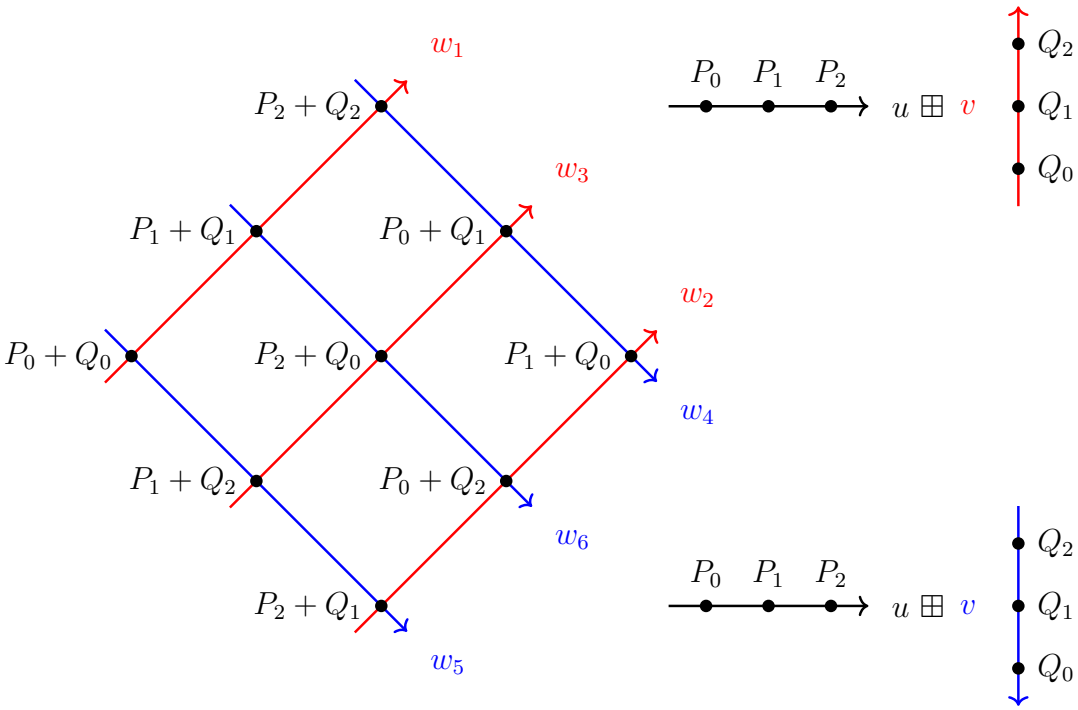
To improve our line multiplication algorithms from chapters 3 and 4, we take a closer look at the line addition step in chapter 5. By studying the structures that emerge, we find

simple relations between the objects in our operation chains. These relations are then used to develop more efficient line multiplication algorithms.

We start by considering the addition of two lines u, v, represented as follows:



and organize the results into the *nine point diagram* shown on the left:



We note that the six possible sum lines between u, v are included, with the labels $w_1, \ldots, w_6$. As mentioned earlier, by specifying cyclic orientations on u and v, we reduce the ambiguity down from 6-fold to 3-fold. This is indicated in the diagram; if u, v are given the orientations indicated in the northeast corner, then the possible sum lines are w_1, w_2, w_3, while the orientations in the southeast corner correspond to the possible sum lines w_4, w_5, w_6.

To make our notion of diagram more precise, and to develop symbolic methods to work with them, we develop a *diagrammatic algebra* in chapter 5. This has a combinatorial flavor, with some inspiration coming from the theory of combinatorial species. And just as that theory attaches a calculus to its algebra, in chapter 6 we attach a *diagrammatic calculus* to our diagrammatic algebra.

The starting point of the diagrammatic calculus is the *linear sum* function $u \boxplus v$ on E which vanishes exactly at the points in the nine point diagram:

$$\mathrm{Div}(u \boxplus v) = \sum_{i,j \in \{0,1,2\}} (P_i + Q_j) - 9(\mathcal{O})$$

We note that by partitioning the nine point diagram into three lines, we can factor $u \boxplus v$ as a product of three line functions. Since there are two ways to partition the points, we can compare the corresponding expressions of $u \boxplus v$ to obtain relations among the six possible sum lines. For example, if the lines w_i are defined by $y = m_i x + b_i$, then

$$m_1 + m_2 + m_3 = m_4 + m_5 + m_6.$$

The benefits of studying nine point diagrams are amplified by the fact that they appear in line addition under many guises. In fact we can already describe a second appearance: we can form a nine point diagram between the lines $u, v, -w_i$ for any sum line w_i. In this way, we can apply the results from our diagrammatic calculus in multiple ways to obtain relations between the lines that appear in our operation chains.

1.4.1 Improved Line Multiplication

Using the diagrammatic tools that we develop, we gain a better understanding of the generic line multiplication algorithm. Then we develop the diagrammatic tools further, and this allows us to find simple relations which are used to improve our algorithms. The main tools that we develop come from comparing structural elements of the input lines u, v to structural elements of the nine point diagram.

For example, the cyclic orientation structure on u can be encoded via a forward difference line Δu with points $P_2 - P_1, P_0 - P_2, P_1 - P_0$; this same line can be found in the nine point diagram by starting at $P_1 + Q_0$ and taking the forward difference while traveling west. Then by algebraically encoding these structures, we obtain explicit relations between the lines u, v and the lines w_1, w_2, w_3. This leads to a cyclic line multiplication algorithm which improves on the generic line multiplication algorithm.

1.4.2 Three Torsion

To further improve our line multiplication algorithms, we study the symmetries of $u \boxplus v$ that arise from three torsion points in chapter 7. Three torsion points $T \in E$ satisfy $3 \cdot T = \mathcal{O}$, and so their tangent lines have a triple intersection with E:

$$\ell_T(x, y) = y - m_T x - b_T$$
$$\mathrm{Div}(y - m_T x - b_T) = 3(T) - 3(\mathcal{O})$$

This has an important consequence: there is in fact no ambiguity in the line addition between ℓ_T and any line u, and we denote the line sum by $u^{\boxplus T}$. And since the mapping $u \mapsto u^{\boxplus T}$ takes lines to lines, it is in fact a projective linear map; stated otherwise, the map $\boxplus T$ is given by a matrix multiplication. In fact, the map on points $P \mapsto P + T$ can also be realized as a projective linear map as a consequence.

The aforementioned symmetries of $u \boxplus v$ come from the following transformations for three torsion points $T \in E[3]$:

$$(u, v) \mapsto (u^{\boxplus T}, v^{\boxminus T})$$
$$(u^{\boxplus T}) \boxplus (v^{\boxminus T}) = u \boxplus v$$

Since there are 9 three-torsion points in $E(\overline{\mathbb{F}})$, this imposes a group of 9 simple symmetries on the coefficients of $u \boxplus v$. This tells us a lot about their structure, and we can exploit this to simplify calculations involving the line sum function.

1.4.3 Trilinear Forms

Lastly, we combine the previous two approaches; by incorporating the action of $E[3]$, we can expand our diagrammatic calculus. Specifically, there are certain trilinear forms that give simple relations between the lines that appear in a cyclic line addition. These can be used to further improve on our cyclic line multiplication algorithms.

The aforementioned trilinear forms have analogues $d_{\mathcal{O}}, e_0, e_1$ in point arithmetic. These have a simple arithmetic interpretation; for collinear points R_0, R_1, R_2, we have

$$0 = d_{\mathcal{O}}(R_0, R_1, R_2) = e_0(R_0, R_1, R_2) = e_1(R_0, R_1, R_2)$$

Since each of these is linear in the third point when we fix the first two, this allows us to use linear algebra to derive point addition formulas.

In fact, this property has a simple explanation in terms of three torsion. First note that if $R_0 + R_1 + R_2 = \mathcal{O}$, then those points are collinear. Hence the determinant $d_{\mathcal{O}}(R_0, R_1, R_2)$ of the (projective) coordinate vectors must vanish. This gives the first of the trilinear

forms. To get another, we note that for any three torsion point T, we also have that $d_{\mathcal{O}}(R_0, R_1 + T, R_2 - T)$ vanishes, since its arguments also add up to $\mathcal{O}$. But because $\boxplus T$ is given by a matrix multiplication, it turns out that from $\det(R_0, R_1 + T, R_2 - T)$ we get a trilinear form that also vanishes when $R_0 + R_1 + R_2 = \mathcal{O}$. By taking all of these together for various T, we find that we get a three dimensional space of trilinear forms; the aforementioned $d_{\mathcal{O}}, e_0, e_1$ give a basis for that space, with simpler coefficients.

In line arithmetic, the determinant form first appears when considering the *nine point diagram orientation*, which corresponds to a choice between the two ways to partition the nine points into three lines. Specifically, the nine point diagram orientation is related to the cyclic line orientations for u and v by a determinant formula. Then using three torsion algebra, we can bootstrap this to replace the determinant form with other trilinear forms. These provide simple relations between line coefficients in a nine point diagram.

1.5 Applications and Future Work

The most natural application for line multiplication is in implementations of point multiplication. As a simple illustration: given a point $P \in E$, we can choose two lines ℓ, ℓ' that contain it; then we could calculate $k \cdot P = k \boxdot \ell \cap k \boxdot \ell'$. Of course, this would be very inefficient. In chapter 8, we explain how to make better use of line multiplication to perform point multiplication. In particular, line multiplication is well suited to point multiplication in quadratic or cubic extensions of the base field. This is because we can choose lines with coefficients in the base field, but whose points lie in an algebraic extension.

We also consider other uses of line multiplication in cryptography. For example, in a Weierstrass form elliptic curve over a composite modulus $N = pq$, suppose that we choose a random x-coordinate. Then determining the corresponding y coordinate involves taking a square root; this problem is considered intractable for large N with unknown factorization. Montgomery's x-only point multiplication can be used in these cases, since the y coordinate is not needed. In some applications, we can similarly work with partial information about a point, by specifying a more general line that contains it.

The main work that we are doing at present is to look for improvements to line multiplication algorithms. In particular, we can make many savings by working with the Hessian form of elliptic curves, as we briefly mention in section B.6. This form arises naturally when studying the invariance of the line sum function. There are also many mysteries about the line addition algebra that we are trying to understand better. In fact, only a small proportion of our experimentally discovered results are presented here, but most of these are too fragmentary to be presented.

Chapter 2

Elliptic Curve Cryptography

Elliptic curves are mathematical objects with connections to a surprising number of mathematical fields. They arise naturally in geometry when trying to solve degree 3 or 4 polynomial equations in two variables. They also arise in analysis in connection to ellipse circumference functions, and this is the source of their name. Today they play an important role in a practical field of mathematics: cryptography.

In this chapter, we present the basic theory of elliptic curve cryptography. We start with an overview of the history of cryptography leading up to the computer era. Then we discuss elliptic curves, and how they fill an important niche in *public key cryptography*.

We then focus on algorithms for elliptic curve arithmetic. We present various methods that cryptographic researchers have found to improve these algorithms. In particular, we highlight Peter Montgomery's x-only point multiplication algorithm, which serves as a template for our own line multiplication operation.

2.1 Cryptography

At its core, cryptography is about rendering messages unreadable for everyone except for the intended recipient. This need to obfuscate communications has a long history in military applications. Historical cryptographic systems relied on prior secret agreements between the communicating parties. The parties would agree on a suitable method to transform a message into a *ciphertext*, and then a recipient who was privy to the method could reverse it to recover the *plaintext*. The secret part of the method would often be encapsulated in a secret key; this might be a password or a configuration of a physical device. This type of system is called a *private key* cryptographic system today, or alternatively a *symmetric key* system, since communicating parties have knowledge of the same secret. A famous example of such a system is the Enigma machine used by the Germans during

the Second World War. Its continued fame comes in part from the team at Bletchley Park (including Alan Turing) that developed a computer to assist in cracking the Enigma code.

In the aftermath of the war, cryptographic researchers pondered systems that did not rely on prior secret communications. This type of system would face significant challenges; if an eavesdropper intercepted all communications, then surely they should be able to decode all future communications. In fact, such *public key* cryptographic systems are indeed possible. The essential idea is that each communicating party has a *private key* known only to them, and a corresponding *public key* that can be broadcast to the world. Then other parties use this public key to encode messages in such a way that the private key is required to decode it. Because communicating parties do not have access to the same secret keys, these system are also called *asymmetric key* systems.

Any public key system will have an inherent weakness; the private key can be calculated from the public key. But this weakness can be overcome by carefully designing the system to make sure that this calculation is impractical. For example, the widely deployed RSA cryptosystem relies on the difficulty of factoring a large number into two prime factors. This is considered to be infeasible if the prime factors are properly chosen to be large enough. But modern advances in number theory have weakened this; the world record for factorization is uncomfortably close to the size of some keys that are in use today.

With this in mind, cryptography has been slowly shifting towards using elliptic curve systems. These systems use elliptic curves because they have a group structure that has a difficult *discrete logarithm problem*. That is, we can multiply a point P on the curve by an integer $k \in \mathbb{Z}$, but given P and $k \cdot P$, it is considered infeasible to recover k. Because of the growing use of elliptic curve cryptography, there is much research dedicated to improving the efficiency of the underlying algorithms. This is the context for the system that we are developing.

In fact, theoretical weaknesses in elliptic curve cryptography have now been found; these rely on quantum computers, which have capabilities that allow for effective attacks on any discrete logarithm problem. Although no quantum computer has yet been created of the necessary size to implement such an attack, there is a lot of optimism (or pessimism) that this will be achieved soon. Thus much attention has been shifted to newer *post quantum* cryptographic systems. We will not discuss these systems further in this thesis.

2.2 The Discrete Logarithm Problem

In this section, we discuss an important early example of public key cryptography, called the *Diffie Hellman* system. This will be used to illustrate the utility of finding an abelian group G which has a difficult discrete logarithm problem.

Definition 2.2.1. *The* discrete logarithm problem *in a finite abelian group G is to find an efficient algorithm which takes as input g, g^k for some $g \in G$ and $k \in \mathbb{Z}$, and outputs k.*

Given an abelian group G with a difficult discrete logarithm problem, the Diffie Hellman system works as follows, for communicating parties Alice and Bob:

- A fixed element $g \in G$ is agreed upon.
- Alice secretly chooses a random integer $a \in \{0, 1, \ldots, |G| - 1\}$, and sends g^a to Bob.
- Bob secretly chooses a random integer $b \in \{0, 1, \ldots, |G| - 1\}$, and sends g^b to Alice.
- Alice computes $(g^b)^a = g^{ab}$.
- Bob computes $(g^a)^b = g^{ab}$.

Now the quantity is g^{ab} a shared secret between Alice and Bob.

An eavesdropper Eve who could solve the discrete logarithm problem would be able to get in on the secret. By intercepting the values g^a, g^b, Eve finds a from g^a, then computes $(g^b)^a = g^{ab}$.

2.3 Introduction to Elliptic Curves

Thankfully, there exists a convenient class of groups with discrete logarithm problems which are considered difficult. These come from elliptic curves over finite fields. We define elliptic curves in a more general context in this section.

A typical presentation of an elliptic curve E is as the solution set in (x, y) of a Weierstrass equation:

$$y^2 = x^3 + ax + b$$

where a, b are fixed elements of a field $\mathbb{F}$, with $4a^3 + 27b^2 \neq 0$. Additionally, E includes a distinguished *base point* $\mathcal{O}$ in the vertical direction at infinity.

An important focus of the study of elliptic curves is to find and characterize points with some desired property, such as being rational. In contrast with simpler curves, such as conic sections, there is no simple parametrization of rational points on an elliptic curve. But there is a saving grace; the points of an elliptic curve can be endowed with a group structure. The problem of finding rational or integral points on an elliptic curve go at least as far back as the third century AD, when Diophantus published a solutions from old for certain cubic equations (See [5], book VI, problem 19 for example.)

The group structure is now well understood, but there are still many challenges remaining. In fact, the Clay Institute has offered a million dollar prize for the solution to an outstanding problem in the field, known as the Birch and Swinnerton-Dyer conjecture (which is normally shortened to "BSD conjecture" for obvious reasons.) This conjecture posits a connection between the algebraic structure of an elliptic curve, and analytic properties of an associated function. There is extensive numerical support for the BSD conjecture, in addition to having parallels in well established results of algebraic number theory and geometry.

The BSD conjecture and other mysterious connections involving elliptic curves are an important focus in modern mathematics. One prominent success in this vein came from Princeton's Andrew Wiles, who used deep results about elliptic curves to prove Fermat's Last Theorem. As a conjecture, Fermat's Last Theorem had stymied mathematicians for centuries, and attracted much attention due to its simplicity:

Theorem 2.3.1 (Fermat's Last Theorem)**.** *For $n \in \mathbb{Z}$ greater than 2, there is no solution in positive integers to the equation*

$$x^n + y^n = z^n.$$

In recent decades, elliptic curves have risen to prominence in another field: cryptography. This stems from the fact that in a suitable setting, the group of points on an elliptic curve has a difficult *discrete logarithm problem.* Namely, if we use the group structure to multiply a point $P \in E$ by a scalar $k \in \mathbb{Z}$, then it is intractable to recover the scalar k by an adversary who is given only P and $k \cdot P$. It turns out that the difficulty of this problem can be used as a basis for the security of public key cryptography protocols. Such protocols are indispensable to the security of modern communications. For this reason, there is a large amount of research devoted to improving the efficiency of point multiplication algorithms.

For completeness, we include a precise technical definition of an elliptic curve:

Definition 2.3.2. *An* elliptic curve *over a field $\mathbb{F}$ is a non-singular curve E of genus 1, along with a distinguished point $\mathcal{O}$ of E.*

If the field $\mathbb{F}$ has characteristic other than 2 or 3, then E can be modeled by a *reduced Weierstrass equation*:

$$E \ : \ y^2 = x^3 + ax + b$$

for suitable coefficients $a, b \in \mathbb{F}$; by default, the distinguished point is then $\mathcal{O} := (0 : 1 : 0)$ in the projective completion of E.

2.4 Elliptic Curve Point Addition

In this section, we define an abelian group structure on an elliptic curve E. Given points $P, Q \in E$, this allows us to form a new point denoted $P + Q$ on E. Furthermore, this operation is given by rational functions in the input, and the $+$ operation satisfies the group axioms with identity element $\mathcal{O}$.

The addition on E is characterized by the following property: for any rational function $f \in \mathbb{F}(E)$ with divisor

$$\mathrm{Div}(f) = c_0(P_0) + \ldots + c_k(P_k),$$

the following equation holds in the additive group structure on E:

$$c_0 P_0 + \ldots + c_k P_k = \mathcal{O}.$$

In other words, given a rational function f on E, the sum of all zeroes of f is equal to the sum of all poles of f. We note that any rational function $f \in \mathbb{F}(E)$ has the same number of zeroes and poles; that is, $c_0 + \ldots + c_k = 0$.

Now suppose that our curve is in reduced Weierstrass form:

$$E \ : \ y^2 = x^3 + ax + b$$

for $a, b \in \mathbb{F}$. We will more explicitly describe the addition on this curve.

We start by noting that for a fixed $x_0 \in \mathbb{F}$, the function $x - x_0 \in \mathbb{F}[E]$ vanishes at two points $(x_0, \pm y_0) \in E(\overline{\mathbb{F}})$. Hence we have:

$$\mathrm{Div}(x - x_0) = ((x_0, y_0)) + ((x_0, -y_0)) - 2(\mathcal{O})$$

and so $(x_0, y_0) + (x_0, -y_0) = \mathcal{O}$. In other words, negation in the group structure of E corresponds to reflection across the x-axis: $(x_0, y_0) \mapsto (x_0, -y_0)$.

Now we consider points $P, Q \in E$, and outline a method to obtain $P + Q$. Let ℓ be the line through P and Q (or the tangent line at P if $P = Q$.) Then ℓ intersects E at a third point R, which will satisfy $P + Q + R = \mathcal{O}$. Thus $R = -P - Q$, and we can reflect R across the x-axis to obtain $P + Q$. (For more details, see for example §13.1.2 of [3].)

Now we obtain a formula for R. Let our line be given by the equation $\ell : \ y = m_\ell x + b_\ell$; note that if ℓ is a vertical line, then $P + Q = \mathcal{O}$. Then the intersection points between ℓ and E satisfy the following:

$$\begin{aligned} 0 =& b + ax + x^3 - (m_\ell x + b_\ell)^2 \\ =& (b - b_\ell^2) + (a - 2m_\ell b_\ell)x - m_\ell^2 x^2 + x^3 \end{aligned}$$

Now since $P, Q \in \ell \cap E$, we know that x_P, x_Q are two roots of the above cubic. So by Vieta's formulas, the third root x_R satisfies:

$$x_P + x_Q + x_R = m_\ell^2$$

which allows us to solve for x_R. Then we get $y_R = m_\ell x_R + b_\ell$. Finally, we calculate $(x(P+Q), y(P+Q)) = (x_R, -y_R)$, since $P + Q = -R$.

This leads to addition formulas. First we note some special cases:

- If $P = \mathcal{O}$, then $P + Q = Q$.
- If $Q = \mathcal{O}$, then $P + Q = P$.
- If $P = Q$, we use a doubling formula:

$$\begin{aligned} m &:= \frac{a + 3x_P^2}{2y_P} \\ x(2P) &:= m^2 - 2x_P \\ y(2P) &:= -\left(m\left(x(2P) - x_P\right) + y_P\right) \end{aligned}$$

- If $P \neq Q$ but $x(P) = x(Q)$, then $P + Q = \mathcal{O}$.
- Otherwise:

$$\begin{aligned} m &:= \frac{y_P - y_Q}{x_P - x_Q} \\ x(P+Q) &:= m^2 - x_P - x_Q \\ y(P+Q) &:= -\left(m\left(x(P+Q) - x_P\right) + y_P\right) \end{aligned}$$

2.4.1 Elliptic Curve Point Multiplication

Using the group structure on E, we define *scalar multiplication* of a point $P \in E$ by a scalar $k \in \mathbb{Z}$:

$$k \cdot P = \underbrace{P + P + \cdots + P}_{k}$$

Of course, this can be calculated by simply adding P to itself k times. But for large k, this will be very inefficient, so we consider better algorithms. The simplest of these is the double-and-add operation chain. Here it is, where ADD and $DOUBLE$ represent the formulas from the previous section:

Algorithm 1: Double-and-add point multiplication

Input : Parameters a, b of the elliptic curve $E: \ y^2 = b + ax + x^3$, a point $P = (x_P, y_P) \in E$ and a positive integer $k \in \mathbb{Z}_{>0}$ with binary expansion $k_{b-1} \dots k_1 k_0$ and $k_{b-1} = 1$.

Output: $k \cdot P$

```
if P = O then
    return O;
else
    x, y ← x_P, y_P;
end
for i ← b − 2 to 0 do
    x, y ← DOUBLE(x_P, y_P);
    if k_i = 1 then
        x, y ← ADD((x, y), (x_P, y_P))
    end
    return (x, y);
end
```

2.5 Elliptic Curves for Cryptography

As mentioned earlier, elliptic curves found a new niche in recent decades, since scalar multiplication is hard to reverse in an appropriately setting. These elliptic curves found in cryptography are defined over finite fields. We will now give a brief overview of the qualities that make an elliptic curve secure for cryptographic applications.

An elliptic curve over a finite field $\mathbb{F}$ can be modeled by a *Weierstrass equation* of the form

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

for constants a_i in the base field. The set of points $E(\mathbb{F})$ that lie in the base field form a finite group, which gives the setting for cryptographic algorithms. The cryptographic applications of elliptic curves normally hinge on the difficulty of the discrete logarithm problem. So suppose an adversary knows the curve, and is given the points $P, kP \in E(\mathbb{F})$, but is not given $k \in \mathbb{Z}$. Then it should be computationally infeasible for him to discover k.

A simple example of elliptic curve point multiplication in cryptography is Elliptic Curve Diffie Hellman (ECDH). This is an implementation of the prototypical public key cryptography scheme; in fact the Diffie Hellman scheme is also one of the oldest. Alice and Bob would like to communicate securely, but have no private communication channel. So they first agree on a suitable elliptic curve E and a point P on that curve; this information is assumed to be public. Alice chooses a secret k_a, and sends $k_a \cdot P$ to Bob. Bob simultaneous chooses a secret k_b, and sends $k_b \cdot P$ to Alice. Then Alice computes $k_a \cdot (k_bP) = k_ak_bP$, and Bob computes $k_b \cdot (k_aP) = k_ak_bP$. These are the same, and Alice and Bob have now established a shared secret, over public channels! Of course, if an eavesdropper could solve the discrete logarithm problem, then they could discover k_a, k_b from $k_a \cdot P, k_b \cdot P$, and thus the secret would be out.

Now we discuss the group structure of $E(\mathbb{F})$ as it pertains to the cryptographic applications. We first note that if the group order n of $E(\mathbb{F})$ is small enough, then an adversary could run an exhaustive search to solve the discrete logarithm problem. In fact, the points of $E(\mathbb{F})$ form a group whose order is approximately the same as the order q of $\mathbb{F}$:

Theorem 2.5.1. *For an elliptic curve E defined over a finite field $\mathbb{F}_q$, the number of points on E with coordinates in $\mathbb{F}_q$ is $q + 1 - t$ for some integer $-2\sqrt{q} \leq t \leq \sqrt{q}$.*

Hence we need q to be large enough that an exhaustive search would be infeasible. But this is not enough; it turns out that a variety of attacks exist on the elliptic curve discrete logarithm problem, and curves must be selected carefully.

A simple example of an attack on the discrete logarithm occurs when the order n is composite; in this case, the discrete logarithm problem can be broken down into smaller subproblems. Hence n is normally chosen to be prime, or to at least have a large prime

factor. Thankfully, by choosing a curve with random parameters, a curve of prime order is likely to be found after a reasonable number of iterations. But this is still not enough! Once elliptic curves started being seriously considered for cryptographic applications, more attacks emerged. For example, there are bilinear pairings on some curves which allow the discrete logarithm problem to be transposed to a much simpler setting. Fortunately, cryptographers have overcome all known practical attacks, through careful selection of elliptic curve parameters.

That said, there is a thorn in the side of elliptic curve cryptography; a theoretical attack exists that can solve the discrete logarithm problem on any elliptic curve. These attacks are quantum algorithms, which can in fact solve large discrete logarithm problems in any group. In fact there are quantum algorithms that break the most widely deployed public key cryptography systems; for example, Shor's algorithm can break RSA by factoring large composite numbers. At the moment, quantum computers have not been sufficiently developed for this to be an immediate threat, but this is an important consideration in cryptography today.

2.6 Efficient Elliptic Curve Arithmetic

Because of the widespread deployment of elliptic curve cryptography in the twenty-first century, there has been a lot of focus on improving the efficiency of algorithms that compute elliptic curve arithmetic. Namely, a straightforward implementation of the algorithms outlined in this chapter would be considered woefully inadequate today. We will now outline in broad strokes some modern advances in this area.

A first improvement is in the base field arithmetic itself. For example, divisions use many more resources than do the other basic arithmetic operation. Hence algorithms have been adapted to minimize the number of divisions. Most notably, this can be achieved by using projective coordinates; in essence, rather than dividing, we keep track of numerators and denominators separately at each step. Other examples of ways to improve base field arithmetic efficiency come from careful selection of the field, or from hardware considerations.

Similarly, considerations of the arithmetic of E can lead to improved efficiency. There are usually some operations that are more expensive than others, and algorithms are adapted to replace expensive operations with cheaper ones. For example, in Weierstrass form, point addition is normally more expensive than point doubling. But point subtraction has around the same cost as point addition. Hence the double-and-add operation chain can be adapted to one which uses subtractions as well as additions. This extra freedom allows for better chains which have fewer total numbers of additions/subtractions.

An important consideration is the equation that defines the elliptic curve itself. In fact,

although any elliptic curve can be transformed into one with a Weierstrass equation, it is often beneficial to use a different form. For example, more efficient arithmetic can be achieved using the Edwards form af an elliptic curve, for a fixed parameter d, with origin $(0, 1)$:

$$E: \ x^2 + y^2 = 1 + dx^2y^2 \qquad (x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right)$$

Compared to Weierstrass form arithmetic, many fewer multiplications are necessary. See [1] for much more detail.

2.7 x-only point multiplication

One common trick for point multiplication is to use the x-only point multiplication operation (see §13.2.3 of [3].) For any integer k, this operation allows one to compute $x(kP)$, given only the x-coordinate $x(P)$ of a point P. This operation has applications which come from the fact that x-only multiplication is often computationally quicker than full point multiplication. Furthermore, this operation can be slightly tweaked to allow for the computation of $y(kP)$ at little additional cost; see formula 13.7 in [3].

There is another type of application which comes from elliptic curves E in composite moduli. On a curve

$$E: \ y^2 = x^3 + ax + b$$

in modulus $N = p \cdot q$ for large primes p and q, there is no known efficient general method for finding points on E without knowing the factorization of N. One approach to this problem is to choose an x-coordinate, and then to attempt to find the square root of $x^3 + ax + b$. Unfortunately, finding such square roots is provably as hard as factoring N. This is where x-only formulas come in; for certain applications, we can choose a point P via its x-coordinate, and then manipulate it without ever knowing its y-coordinate. An example of such an application is Demytko's elliptic curve analog of the RSA cryptosystem, found in [4].

We will outline the idea behind this operation here. In analogy with square-and-multiply exponentiation algorithms, we would like a formula to compute $x(2P)$ and $x(P + Q)$ given $x(P)$ and $x(Q)$ for points $P, Q \in E$. The following formula gives us $x(2P)$ (assuming $2P \neq \mathcal{O}$):

$$x(2P) = \frac{x(P)^4 - 2ax(P)^2 - 8bx(P) + a^2}{4(x(P)^3 + ax(P) + b)}.$$

Unfortunately, if we only know $x(P)$ and $x(Q)$, we are dead in the water when trying to compute $x(P + Q)$. This is because $x(P)$ is invariant under the negation of P, and so

P (or Q) can only be known up to sign. Hence there are two possibilities for $x(P+Q)$, which correspond to $x(P+Q) = x(-P-Q)$ and $x(P-Q) = x(-P+Q)$. These cannot be distinguished in general without using more than just the knowledge of $x(P)$ and $x(Q)$. Fortunately, there is a workaround, which involves tweaking the double-and-add operation chain.

To this end, we make the following note: any function $f(x,y) \in \mathbb{F}(E)$ can be expressed uniquely as $f(x,y) = f_0(x) + yf_1(x)$. Then f is an even function if and only if $f_1 = 0$; stated otherwise, the functions on E which are even are exactly the functions of x. Now the workaround comes from the observation that $x(P+Q)+x(P-Q)$ is an even function of both P and Q, and hence this quantity can be expressed as a function of $x(P)$ and $x(Q)$. Explicitly,

$$x(P+Q) + x(P-Q) = \frac{2(x(P)x(Q)+a)(x(P)+x(Q))+4b}{(x(P)-x(Q))^2}. \tag{2.1}$$

This formula allows us to compute $x(P+Q)$ given $x(P)$, $x(Q)$ and $x(P-Q)$. In particular, we can compute $x((2\ell+1)P)$ from $x(\ell P)$ and $x((\ell+1)P$, which allows for a relatively efficient recursive point multiplication algorithm to compute $x(kP)$ from $x(P)$. Using the Montgomery ladder algorithm (§13.2.3.d of [3]), we can compute $x(kP)$ from $x(P)$ with around $\log_2(k)$ point doublings and the same number of point additions.

Algorithm 2: Montgomery's x-only point multiplication

Input : Parameters a, b of the elliptic curve $E: y^2 = b + ax + x^3$, an x-coordinate $x(P)$ and a positive integer $k \in \mathbb{Z}_{>0}$ with bits $k_0, k_1, \ldots, k_b = 1$.

Output: $x(k \cdot P)$

if $k = 1$ **then**
  return $x(P)$;
else
  $r, s \leftarrow x(P), x(2P) = \frac{x(P)^4 - 2ax(P)^2 - 8bx(P) + a^2}{4(x(P)^3 + ax(P) + b)}$;
end
for $i \leftarrow b-1$ **to** 0 **do**
  if $k_i = 0$ **then**
    $r, s \leftarrow \frac{2(rs+a)(r+s)+4b}{(r-s)^2} - x(P), \frac{s^4 - 2as^2 - 8bs + a^2}{4(s^3+as+b)}$;
  else
    $r, s \leftarrow \frac{r^4 - 2ar^2 - 8br + a^2}{4(r^3+ar+b)}, \frac{2(rs+a)(r+s)+4b}{(r-s)^2} - x(P)$;
  end
  return r;
end

In the next chapter, we will consider a more general version of x-only point multiplication. Then we revisit this operation for comparison in section 4.2.

Chapter 3

Line Multiplication

In this chapter, we introduce the theory of *line multiplication* on an elliptic curve E in reduced Weierstrass form:

$$E: \ b + ax + x^3 - y^2 = 0$$

This operation takes as input a line $\ell: \ y - m_\ell x - b_\ell = 0$ which intersects E at points P_0, P_1, P_2. The collinearity of P_0, P_1, P_2 can be equivalently stated as $P_0 + P_1 + P_2 = \mathcal{O}$. Then we note that for $k \in \mathbb{Z}$, we also have collinearity of kP_0, kP_1, kP_2, since these sum to $\mathcal{O}$ once again. So the line multiplication operation aims to compute the coefficients of the line through kP_0, kP_1, kP_2.

The line multiplication is a generalization of Montgomery's x-only point multiplication; x-coordinates correspond to lines where one of the three points is $\mathcal{O}$. As such, we will face similar obstacles, and we will consider similar solutions. So we start by highlighting the obstacles that appear when trying to adapt double-and-add type algorithms to the line multiplication operation. In particular, the two way ambiguity that shows up in x-only point addition is amplified to a six way ambiguity in the line addition step. To compound this, we can no longer use the trick from x-only point addition, where we used knowledge of one possible x-sum to determine the other. This is because five out of six possible sum lines will not be part of a typical operation chain.

Next we outline the various methods for overcoming these obstacles. One important method is to attach additional structure to the lines that we consider, which allows for a reduction in the ambiguity in the line addition step. This leads us to cyclic line addition, where the points on our lines are endowed with a cyclic orientation. The ambiguity in line addition is thus reduced from six fold to three fold. Unfortunately, there still remains the problem that two out of three possible sum lines are not part of a typical operation chain. But we have a fortunate trick where we can eliminate these undesirable lines in pairs.

An interesting phenomenon then emerges: with a bit of care, it turns out that we do not need to concern ourselves with cyclic orientations at all. The resulting algorithm

is referred to as *generic line multiplication*, and will serve as the template and point of comparison for most line multiplication algorithms presented in this thesis. Because of this, generalizations of generic line multiplication are the focus of chapter 4.

A natural question then arises: why bother with cyclic line multiplication at all if it is simpler to circumvent it entirely? This is because while generic line multiplication is conceptually simple to present, it is quite inefficient. In later chapters, we develop the algebra that allows us to improve line multiplication algorithms. This algebra relies on some additional structure that we introduce in this chapter. In chapter 5, we study those structures in much greater depth.

In chapter 6, we develop a diagrammatic calculus that allows us to find algebraic relations between the various quantities that appear in our operation chains. Then in chapter 7, we incorporate the three torsion of E into our algorithms to obtain further refinements.

3.1 Lines

Suppose that E is an elliptic curve in reduced Weierstrass form over a field $\mathbb{F}$. The objects of study in this thesis are appropriately scaled functions on E that have a pole of order at most 3 at $\mathcal{O}$, and no other poles:

$$\mathcal{L}_3(E) = \{\ell \in \overline{\mathbb{F}}[E]^\times \ : \ \mathrm{Div}(\ell) \geq -3(\mathcal{O}),\ \ell \text{ normalized at } \mathcal{O}\}$$

Elements $\ell \in \mathcal{L}_3(E)$ are typically of the form $\ell(x, y) = y - m_\ell x - b_\ell$ for constants m_ℓ, b_ℓ. We will refer to elements of $\mathcal{L}_3(E)$ as *lines* (or *linear 3-sets*.)

For any non-zero function $f \in \mathbb{F}(E)$, there is $v \in \mathbb{Z}$ such that $(x/y)^{-v} f(x, y)$ has neither a pole nor zero at $\mathcal{O}$. Hence by scaling f appropriately, we can assure that this latter function has value 1 at $\mathcal{O}$; we then say that f is *normalized*:

Definition 3.1.1. *For $f \in \mathbb{F}(E)^*$, we say that f is* normalized *at $\mathcal{O}$ with respect to the uniformizer $u(x, y) = x/y$ (or simply* normalized*) if*

$$u(P)^{-\operatorname{ord}_\mathcal{O}(f)} f(P)\big|_{P=\mathcal{O}} = 1.$$

where $\operatorname{ord}_\mathcal{O}(f)$ is the order of vanishing of the function f at $\mathcal{O}$. Note that $\operatorname{ord}_\mathcal{O}(u) = 1$.

The following lemma makes the normalization constraint more explicit, and gives us a more precise form for $\mathrm{Div}(\ell)$ when $\ell \in \mathcal{L}_3(E)$:

Lemma 3.1.2. *A line $\ell \in \mathcal{L}_3(E)$ has*

$$\mathrm{Div}(\ell) = (P_0) + (P_1) + (P_2) - 3(\mathcal{O})$$

for points $P_0, P_1, P_2 \in E$ which satisfy $P_0 + P_1 + P_2 = \mathcal{O}$.

Furthermore, there are $\zeta_\ell, m_\ell, b_\ell \in \overline{\mathbb{F}}$ such that

$$\ell(x, y) = \zeta_\ell y - m_\ell x - b_\ell$$

where one of the following conditions holds:

- $\zeta_\ell = 1$ *(when $\mathcal{O} \notin \{P_0, P_1, P_2\}$)*
- $\zeta_\ell = 0$ *and* $m_\ell = -1$ *(when one of P_0, P_1, P_2 is $\mathcal{O}$)*
- $\zeta_\ell = m_\ell = 0$ *and* $b_\ell = -1$ *(when all of P_0, P_1, P_2 are $\mathcal{O}$)*

Conversely, given $P_0, P_1, P_2 \in E$ which satisfy $P_0 + P_1 + P_2 = \mathcal{O}$, there is $\ell \in \mathcal{L}_3(E)$ with $\mathrm{Div}(\ell) = (P_0) + (P_1) + (P_2) - 3(\mathcal{O})$.

Proof. The first and last claims follow from corollary III.3.5 of Silverman's book [8], which characterizes principal divisors. Using the notation and results from section II.5 of [8], we see that by the Riemann-Roch theorem,

$$\mathcal{L}(3(\mathcal{O})) = \{f \in \overline{\mathbb{F}}(E) \ : \ \mathrm{Div}(f) \geq -3(\mathcal{O})\} \cup \{\mathcal{O}\}$$

is a vector space of dimension 3. In Weierstrass form, the functions $1, x, y$ form a basis, and hence $\ell(x, y) = \zeta_\ell y - m_\ell x - b_\ell$ for appropriate constants $\zeta_\ell, m_\ell, b_\ell$.

Recall that $\mathrm{ord}_{\mathcal{O}}(x) = -2$ and $\mathrm{ord}_{\mathcal{O}}(y) = -3$ so $\mathrm{ord}_{\mathcal{O}}(x/y) = 1$. The following calculation shows that y is normalized at $\mathcal{O}$ (in projective coordinates):

$$\left(\frac{x}{y}\right)^3 \frac{y}{z}\bigg|_{(x:y:z)=(0:1:0)} = \frac{y^2 - axz - bz^2}{y^2}\bigg|_{(x:y:z)=(0:1:0)} = 1$$

using the elliptic curve equation:

$$\begin{aligned} bz^3 + axz^2 + x^3 - y^2 z &= 0 \\ x^3 &= z(y^2 - axz - bz^2). \end{aligned}$$

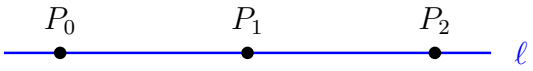
Then $x = y(x/y)$ is normalized at $\mathcal{O}$, since it is a product of normalized functions. Note that the sum of two functions with different orders at $\mathcal{O}$ is normalized if and only if the lower order function is normalized. Hence if ζ_ℓ is non-zero, then it must be 1. Similarly, if $\zeta_\ell = 0$, then the coefficient of x must be 1 or 0, and in the latter case the constant coefficient must be 0. □

Because such a function ℓ traces out a line in the plane, we use the following terminology:

Definition 3.1.3. *A* line ℓ *is a normalized function in* $\mathbb{F}(E)$ *such that there are points* $P_0, P_1, P_2 \in E$ *with*

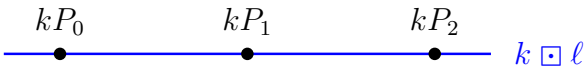
$$\mathrm{Div}(\ell) = (P_0) + (P_1) + (P_2) - 3(\mathcal{O})$$

We refer to P_0, P_1, P_2 *as the points of* ℓ*, and we represent this line diagrammatically as follows:*



3.2 Line Multiplication

We begin with the observation that for a line ℓ with points P_0, P_1, P_2, we can multiply the equation $P_0 + P_1 + P_2 = \mathcal{O}$ through by any $k \in \mathbb{Z}$ to obtain $kP_0 + kP_1 + kP_2 = \mathcal{O}$. Hence these latter three points form a line denoted $k \boxdot \ell$:



Definition 3.2.1. *For a line* ℓ *with:*

$$\mathrm{Div}(\ell) = (P_0) + (P_1) + (P_2) - 3(\mathcal{O})$$

and for $k \in \mathbb{Z}$*, the* line multiplication by k *map is:*

$$\begin{aligned} k\boxdot : \quad & \ell \mapsto k \boxdot \ell \\ & \mathrm{Div}(k \boxdot \ell) = (kP_0) + (kP_1) + (kP_2) - 3(\mathcal{O}). \end{aligned}$$

Line multiplication by -1 *is called* line negation*, and is denoted* $\boxminus \ell := -1 \boxdot \ell$*. If there is no chance of confusion with negation in* $\mathbb{F}(E)$*, we sometimes notate the line negation of* ℓ *as* $-\ell$*.*

Our aim is to develop *line multiplication algorithms* to compute this function for an arbitrary ℓ and k. Typically that means that we start with coefficients m_ℓ, b_ℓ such that:

$$\begin{aligned} \ell(x, y) &= y - m_\ell x - b_\ell \\ \mathrm{Div}(\ell) &= (P_0) + (P_1) + (P_2) - 3(\mathcal{O}). \end{aligned}$$

and we want to compute $m_{k\boxdot\ell}, b_{k\boxdot\ell}$ which satisfy:

$$\begin{aligned}(k \boxdot \ell)(x, y) =& y - m_{k\boxdot\ell}x - b_{k\boxdot\ell} \\ \mathrm{Div}(k \boxdot \ell) =& (kP_0) + (kP_1) + (kP_2) - 3(\mathcal{O}).\end{aligned}$$

In fact we will often assume that our lines ℓ have $\zeta_\ell = 1$ when not otherwise specified, and the line coordinates will be denoted m_ℓ and b_ℓ as above.

We are primarily interested in adapting double-and-add type operation chains to perform line multiplication. The doubling step runs into no obstacles, as we will see in section 3.8.1:

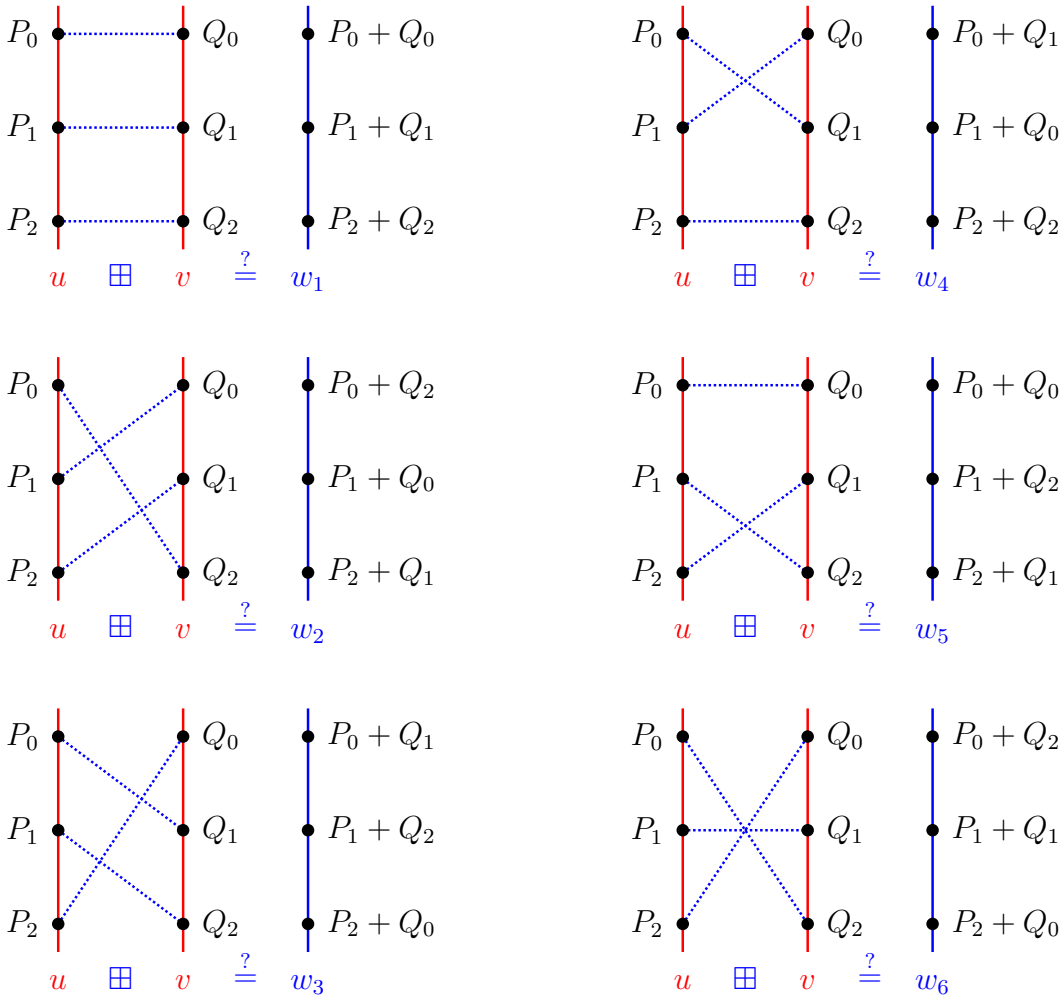
Theorem 3.2.2. *If ℓ has no 2-torsion point, then*

$$\begin{aligned}m_{2\boxdot\ell} =& \frac{a^2m_\ell^2 + 9bm_\ell b_\ell - 3ab_\ell^2 + m_\ell(bm_\ell^3 - am_\ell^2 b_\ell - b_\ell^3)}{2(bm_\ell^3 - am_\ell^2 b_\ell - b_\ell^3)} \\ b_{2\boxdot\ell} =& \frac{4a^3 + 27b^2 + 6abm_\ell^2 - 8a^2 m_\ell b_\ell - 18bb_\ell^2 - a^2 m_\ell^4 - 8bm_\ell^3 b_\ell + 2am_\ell^2 b_\ell^2 - b_\ell^4}{8(bm_\ell^3 - am_\ell^2 b_\ell - b_\ell^3)}\end{aligned}$$

On the other hand, the "addition" step is much trickier to adapt to line multiplication operation chains. This will be the topic of the next section.

3.3 Obstacles to Line Addition

In this section, we explain the obstacles that appear when trying to adapt the "addition" step to a line multiplication operation chain. The first obstacle that we discuss is similar to that encountered in x-only point multiplication, where it was necessary to disambiguate between $x(P \pm Q)$. Line addition faces a more daunting obstacle; there is generally a six way ambiguity in adding lines $u, v \in \mathcal{L}_3(E)$, corresponding to each possible bijective pairing between the points of u and those of v. These *sum lines* are indicated as $w_1, \ldots, w_6$ in the following diagram, with $w_i(x, y) = y - m_{w_i}x - b_{w_i}$:



Now we consider the possibility of adapting the methods from the x-only operation to our situation. Recall that the trick to overcome the two way ambiguity in x-only addition was:

- Compute a symmetric combination of the possible output x-coordinates as a function of the input x-coordinates.
- Since one x-coordinate is known, deduce the value of the other.

In our operation, we could consider the six possible sums $w_1, \ldots, w_6$, and compute, say, the sum of the six slopes $m_{w_1} + \ldots + m_{w_6}$. But we now face a new problem; if we add $u = m \boxdot \ell$ to $v = n \boxdot \ell$, then five of the six sum lines will not normally be multiples of ℓ. So our obstacles are:

- Six way ambiguity in line addition.
- Unwanted sum lines appearing in our line additions.

To deal with this, we will introduce cyclic line addition in the next section. This will reduce the ambiguity, and will allow for a trick to eliminate unwanted sum lines. Then we will explain how to circumvent cyclic orientations entirely. The resulting *generic line multiplication* algorithm will be presented in various contexts in chapter 5. In later chapters, we will focus on improving the results of that chapter.

3.4 Cyclically Oriented Lines

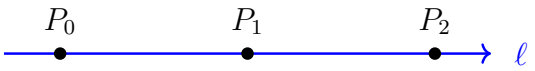
In this section, we reduce the ambiguity problem in line addition by attaching additional structure to our lines. Specifically, for a line ℓ with points P_0, P_1, P_2, we will choose a cyclic orientation on the points, which will be either $P_0 \to P_1 \to P_2 \to P_0$ or $P_0 \to P_2 \to P_1 \to P_0$. By endowing all of our lines with cyclic orientations, we will reduce the ambiguity in line addition from 6-fold down to 3-fold.

We will define cyclic orientations in terms of forward differences between the points of a line:

Definition 3.4.1. *A line $\Delta\ell$ is a* forward difference *of the line ℓ if for points P_0, P_1, P_2 we have:*

$$\begin{aligned}\mathrm{Div}(\ell) =& (P_0) + (P_1) + (P_2) - 3(\mathcal{O}) \\ \mathrm{Div}(\Delta\ell) =& (P_1 - P_0) + (P_2 - P_1) + (P_0 - P_2) - 3(\mathcal{O})\end{aligned}$$

A cyclically oriented line *consists of a pair $(\ell, \Delta\ell)$ where $\Delta\ell$ is a forward difference of ℓ. This will be represented diagrammatically with an added arrowhead:*



We interpret the points of ℓ as having the cyclic orientation $P_0 \to P_1 \to P_2 \to P_0$ when the forward difference $\Delta\ell$ has the points indicated in the above diagram. Note that the only other possible orientation for ℓ is then $-\Delta\ell = -1 \boxdot \Delta\ell$.

Now we will compare a second approach to cyclic orientation. Suppose $u(x, y) = y - m_u x - b_u$ is a line with:

$$\mathrm{Div}(u(x, y)) = (P_0) + (P_1) + (P_2) - 3(\mathcal{O})$$

and $P_i \neq \mathcal{O}$. The x-coordinates of the P_i are then the roots of the following polynomial:

$$\begin{aligned}(x - x_{P_0})(x - x_{P_1})(x - x_{P_2}) =& b + ax + x^3 - (m_u x + b_u)^2 \\ =& (b - b_u^2) + (a - 2m_u b_u)x - m_u^2 x^2 + x^3 \\ =& \frac{1}{27}\left(27b + 9am_u^2 - 2m_u^6 - 18b_u m_u^3 - 27b_u^2\right) \\ &+ \frac{1}{3}\left(3a - m_u^4 - 6b_u m_u\right)\left(x - \frac{m_u^2}{3}\right) + \left(x - \frac{m_u^2}{3}\right)^3\end{aligned}$$

whose discriminant Δ_u satisfies:

$$\begin{aligned}\Delta_u =& \left((x_{P_0} - x_{P_1})(x_{P_1} - x_{P_2})(x_{P_2} - x_{P_0})\right)^2 \\ =& \frac{-1}{27}\left(4\left(3a - m_u^4 - 6m_u b_u\right)^3 + \left(27b + 9am_u^2 - 2m_u^6 - 18m_u^3 b_u - 27b_u^2\right)^2\right) \\ =& -4a^3 - 27b^2 - 18ab\, m_u^2 + a^2 m_u^4 + 4b\, m_u^6 - 4a\, m_u^5 b_u \\ &+ 24a^2\, m_u b_u + 36b\, m_u^3 b_u + 54b\, b_u^2 - 30a\, m_u^2 b_u^2 - 4m_u^3 b_u^3 - 27b_u^4\end{aligned}$$

We will interpret a choice of square root δ_u of Δ_u as indicating a cyclic orientation on the points. The cyclic orientation P_0, P_1, P_2, corresponds to

$$\delta_u = (x_{P_1} - x_{P_0})(x_{P_2} - x_{P_1})(x_{P_0} - x_{P_2})$$

while the cyclic ordering P_0, P_2, P_1 corresponds to

$$\delta_u = -(x_{P_1} - x_{P_0})(x_{P_2} - x_{P_1})(x_{P_0} - x_{P_2}).$$

The relation between the two points of view on cyclic orientation are given by the following formulas, which can be checked by a direct calculation on a computer algebra system:

Theorem 3.4.2. *If u is a line with points P_0, P_1, P_2 which are distinct from each other and from $\mathcal{O}$, and δ_u satisfies:*

$$\delta_u^2 = \frac{-1}{27}\left(4\left(3a - m_u^4 - 6m_u b_u\right)^3 + \left(27b + 9am_u^2 - 2m_u^6 - 18m_u^3 b_u - 27b_u^2\right)^2\right)$$

then the following give coordinates of a forward difference of u:

$$\begin{aligned}m_{\Delta u} =& \frac{-6ab_u + am_u^3 + 3b_u^2 m_u + 9bm_u}{\delta_u} \\ b_{\Delta u} =& \frac{-2a^2 m_u - ab_u m_u^2 + 2bm_u^3 + b_u^3 - 9bb_u}{\delta_u}\end{aligned}$$

If

$$\delta_u = (x_{P_1} - x_{P_0})(x_{P_2} - x_{P_1})(x_{P_0} - x_{P_2})$$

then

$$\mathrm{Div}(\Delta u) = (P_1 - P_0) + (P_2 - P_1) + (P_0 - P_2) - 3(\mathcal{O})$$

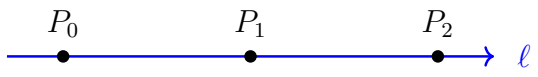
In fact, this can be proven by hand using the theory we develop in chapter 7, where we study cubic forms such as the numerators of $m_{\Delta u}, b_{\Delta_u}$ above; see theorem 7.2.7.

We make a final note that will come into play often in this thesis: the double forward difference is essentially the same as multiplying by -3:

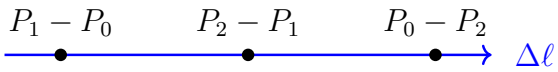
$$\begin{aligned}
&\mathrm{Div}(\Delta(\Delta\ell)) \\
=&\big((P_2 - P_1) - (P_1 - P_0)\big) + \big((P_0 - P_1) - (P_2 - P_0)\big) + \big((P_1 - P_2) - (P_0 - P_1)\big) - 3\big(\mathcal{O}\big) \\
=&(-3P_1) + (-3P_2) + (-3P_0) - 3(\mathcal{O})
\end{aligned}$$

Hence while there are two possible forward difference lines for a typical line ℓ, when it is cyclically oriented, we single the following one out:

Definition 3.4.3. *For a cyclically oriented line* $(\ell, \Delta\ell)$*:*



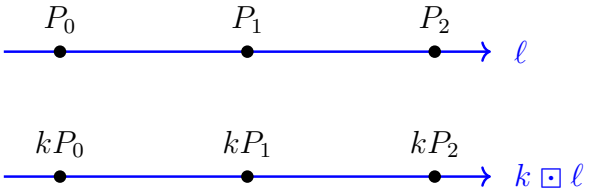
the forward difference *of* ℓ *is* $(\Delta\ell, -3 \boxdot \ell)$*:*



3.5 Cyclic Line Addition

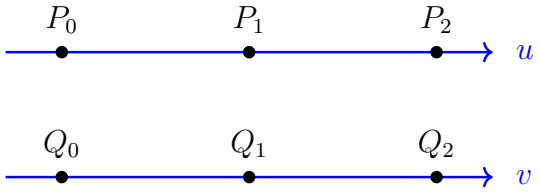
We will consider cyclic line multiplication algorithms in this section. As noted earlier, the additional structure helps us with the first obstacle to a recursive algorithm, by reducing the ambiguity in line addition. In fact, it also allows us to tackle the second obstacle of "bad" sum lines as well. We will present these methods in abbreviated form here, and we will present a full algorithm in chapter 6. This is because in section 3.6 we will first present a simpler version of cyclic line multiplication; we call this *generic line multiplication*, which is essentially cyclic line multiplication without cyclic orientations.

Cyclic line multiplication by $k \in \mathbb{Z}$ is represented diagrammatically as:

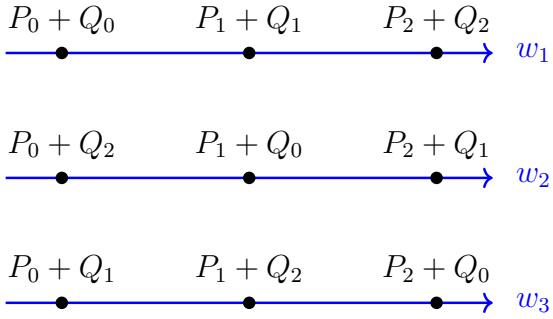


Definition 3.5.1. *For a cyclically oriented line ℓ with forward difference $\Delta\ell$, the multiplication by k map results in the line $k \boxdot \ell$ with forward difference $k \boxdot \Delta\ell$.*

Now we consider line addition with this additional structure. Let u, v be cyclically oriented lines u, v with respective points P_0, P_1, P_2 and Q_0, Q_1, Q_2 in cyclic order:



When we consider sum lines between u and v, we impose that the pairing must respect the cyclic orientations. That is, if P_i and Q_j are added together, then the sum consists of the points $P_i + Q_j, P_{i+1} + Q_{j+1}, P_{i+2} + Q_{j+2}$ (with indices in modulus 3.) So we have the following three possibilities for the cyclic sum of u and v:



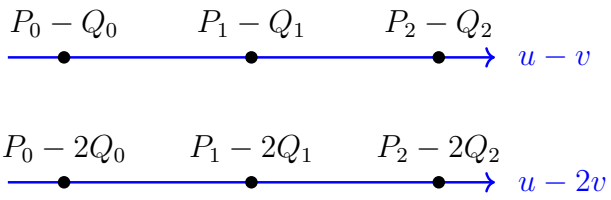
Any symmetric polynomial in the coefficients of w_1, w_2, w_3 can be expressed as a function of u and v along with their orientations specified by δ_u and δ_v. In particular, we can define functions m_Σ, b_Σ with:

$$\begin{aligned} m_\Sigma(u, \delta_u, v, \delta_v) =& m_{w_1} + m_{w_2} + m_{w_3} \\ b_\Sigma(u, \delta_u, v, \delta_v) =& b_{w_1} + b_{w_2} + b_{w_3} \end{aligned}$$

as we will see in chapter 6. Thus we have reduced the ambiguity in line addition from six-fold to three-fold, which was the first obstacle mentioned in section 3.3.

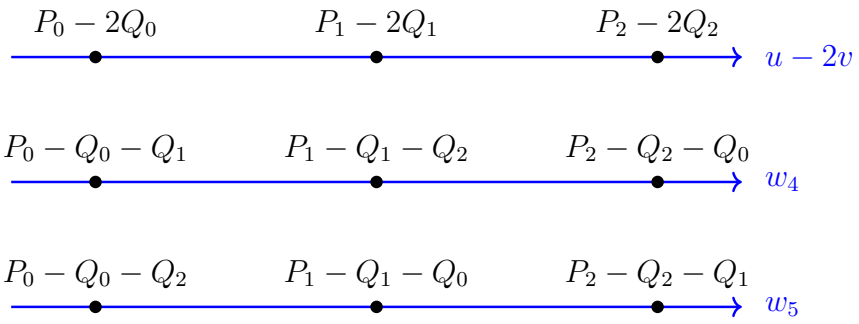
Recall the second obstacle mentioned in section 3.3: when we consider the possible sum lines of $u = m \boxdot \ell$ and $v = n \boxdot \ell$, we have $w_1 = (m+n) \boxdot \ell$, but normally w_2, w_3 will not be multiples of ℓ. Thus given, say, $m_{w_1} + m_{w_2} + m_{w_3}$, we have trouble separating "good" slope m_{w_1} from the "bad" ones m_{w_2}, m_{w_3}. In particular, it is unlikely that we can use the trick like the one for x-only point multiplication. But as mentioned earlier, there is a trick that lets us use the cyclic orientation structure to overcome this obstacle.

To overcome this second obstacle for the cyclically oriented lines u, v, we additionally suppose that we know the lines $u - v, u - 2v$ indicated below:

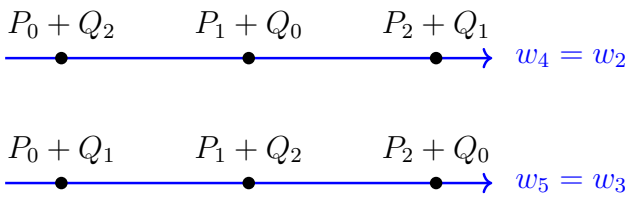


The trick that we will use boils down to the following observation: since $Q_0 + Q_1 + Q_2 = \mathcal{O}$, addition of one of the Q_i is equivalent to subtraction of the other two.

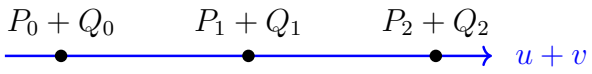
So when we take the cyclic linear sum between $u - v$ and $-v = -1 \boxdot v$ (with forward difference $-\Delta v = -1 \boxdot \Delta v$), we get three possible sum lines:



then by adding $Q_0 + Q_1 + Q_2 = \mathcal{O}$ to each point in the two "bad" sum lines, we see that they are in fact the same as the two "bad" sum lines between u and v!



Now we can use this method to eliminate the "bad" sum lines together. Let $u+v := w_1$ denote the "good" sum line:



Then since we assume knowledge of the cyclically oriented lines $u - v, u - 2v$, we calculate:

$$\begin{aligned} m_\Sigma(u, \Delta u, v, \Delta v) =& m_{u+v} + m_{w_2} + m_{w_3} \\ m_\Sigma(u - v, \Delta(u - v), -v, -\Delta v) =& m_{u-2v} + m_{w_3} + m_{w_2} \end{aligned}$$

Then by taking the difference between these, we can isolate m_{u+v}:

$$m_{u+v} = m_\Sigma(u, \Delta u, v, \Delta v) - m_\Sigma(u - v, \Delta(u - v), -v, -\Delta v) + m_{u-2v} \tag{3.1}$$

and similarly

$$b_{u+v} = b_\Sigma(u, \Delta u, v, \Delta v) - b_\Sigma(u - v, \Delta(u - v), -v, -\Delta v) + b_{u-2v}$$

So we have successfully calculated the "good" line $u + v$!

We then need to calculate the forward difference of this line. This can be done similarly: recall that if $(\ell, \Delta\ell)$ is a cyclically oriented line, then its forward difference is $(\Delta\ell, -3 \boxdot \ell)$. So by applying the same formulas again, we get:

$$\begin{aligned} m_{\Delta(u+v)} =& m_\Sigma(\Delta u, -3 \boxdot u, \Delta v, -3 \boxdot v) \\ & - m_\Sigma(\Delta(u - v), -3 \boxdot (u - v), -\Delta v, 3 \boxdot v) + m_{\Delta(u-2v)} \\ b_{\Delta(u+v)} =& b_\Sigma(\Delta u, -3 \boxdot u, \Delta v, -3 \boxdot v) \\ & - b_\Sigma(\Delta(u - v), -3 \boxdot (u - v), -\Delta v, 3 \boxdot v) + b_{\Delta(u-2v)} \end{aligned}$$

Note that the above algorithm is quite inefficient; it involves multiple calls to the functions m_Σ, b_Σ, as well as a line tripling function. As we will later see, there are simple ways to improve the calculation of $\Delta(u + v)$.

We have now overcome enough obstacles to perform the line addition step in a modified Montgomery ladder, provided that we have the functions m_Σ, b_Σ. That said, we will not present an explicit algorithm for cyclic line multiplication here. This is because of the next section's simple method to circumvent cyclic orientations entirely. We will return to cyclic line multiplication in the conclusion to chapter 6.

3.6 Generic Line Addition

When we first implemented cyclic line addition, an interesting phenomenon emerged. Certain combinations of the coefficients of w_1, w_2, w_3, such as $m_{w_1} + m_{w_2} + m_{w_3}$, only depended on the lines u, v that we were adding. Namely, they did not depend on the cyclic orientations of u or v at all. Note that other combinations such as $b_{w_1} + b_{w_2} + b_{w_3}$ do indeed depend on the cyclic orientations of u and v. Yet the independence of orientation applied to enough coefficient combinations to allow a modified version of cyclic line addition to run without having ever keeping track of cyclic orientations.

There turns out to be a simple explanation for a general version of this phenomenon. In this section, we give this explanation in the context of one step of cyclic line addition. This then leads to a simple formalism for line multiplication, which applies in the more general context of an arbitrary abelian group. Because of this generality, we term this *generic line addition*. Chapter 5 is devoted to *generic line multiplication*, which uses generic line addition as part of its operation chain.

The formalism of generic line addition is built around the following operation:

Definition 3.6.1. *For lines $u, v \in \mathcal{L}_3(E)$ with*

$$\begin{aligned}\mathrm{Div}(u) =&(P_0) + (P_1) + (P_2) - 3(\mathcal{O})\\ \mathrm{Div}(v) =&(Q_0) + (Q_1) + (Q_2) - 3(\mathcal{O}),\end{aligned}$$

the linear sum function *$u \boxplus v \in \mathbb{F}(E)$ is the normalized function satisfying:*

$$\begin{aligned}\mathrm{Div}(u \boxplus v) = &\sum_{i,j\in\{0,1,2\}} (P_i + Q_j) - 9(\mathcal{O})\\ =&(P_0 + Q_0) + (P_0 + Q_1) + (P_0 + Q_2)\\ &+(P_1 + Q_0) + (P_1 + Q_1) + (P_1 + Q_2)\\ &+(P_2 + Q_0) + (P_2 + Q_1) + (P_2 + Q_2) - 9(\mathcal{O})\end{aligned}$$

The line difference function *is $u \boxminus v := u \boxplus (-v) = u \boxplus (-1 \boxdot v)$.*

Recall that normalization is with respect to the uniformizer x/y at $\mathcal{O}$. In effect, normalization means that if we represent $(u \boxplus v)(x, y)$ as a polynomial reduced modulo $b + ax + x^3 - y^2$ (with respect to either x or y), then the leading non-zero term will be $x^i y^j$ with coefficient 1 (where the leading term is the monomial that minimizes $\mathrm{ord}_{\mathcal{O}}$.)

So if we are in the typical situation where $P_i + Q_j \neq \mathcal{O}$ for $i, j \in \{0, 1, 2\}$, with

$$\begin{aligned}u(x, y) =&y - m_u x - b_u\\ \mathrm{Div}(u) =&(P_0) + (P_1) + (P_2) - 3(\mathcal{O})\\ v(x, y) =&y - m_v x - b_v\\ \mathrm{Div}(v) =&(Q_0) + (Q_1) + (Q_2) - 3(\mathcal{O})\end{aligned}$$

then for the proper choice of coefficients γ_i, we have:

$$(u \boxplus v)(x,y) = -\gamma_9 - \gamma_7 x + \gamma_6 y - \gamma_5 x^2 + \gamma_4 xy - \gamma_3 y^2 + \gamma_2 x^2 y - \gamma_1 x y^2 + y^3 \tag{3.2}$$

Note that these γ_i are indexed by weight, with x and y having respective weights 2 and 3 (corresponding to poles of those orders at $\mathcal{O}$). In section 3.7, we will find an explicit expression for $(u \boxplus v)(x,y)$ in terms of the coefficients of u, v. Note also that the signs correspond to the index parity. These make certain formulas nicer in chapter 6.

Now we make a fundamental observation: if the three possible cyclic sum lines of u and v are w_1, w_2, w_3, then we can decompose the divisor of $u \boxplus v$:

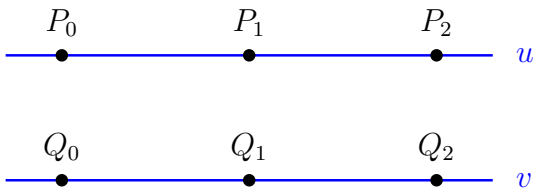
$$\begin{aligned}\mathrm{Div}(u \boxplus v) =&(P_0 + Q_0) + (P_1 + Q_1) + (P_2 + Q_2) - 3(\mathcal{O}) \\ &+(P_1 + Q_0) + (P_2 + Q_1) + (P_0 + Q_2) - 3(\mathcal{O}) \\ &+(P_2 + Q_0) + (P_0 + Q_1) + (P_1 + Q_2) - 3(\mathcal{O}) \\ &= \mathrm{Div}(w_1) + \mathrm{Div}(w_2) + \mathrm{Div}(w_3) = \mathrm{Div}(w_1 w_2 w_3)\end{aligned}$$

and since both functions are normalized, we in fact have:

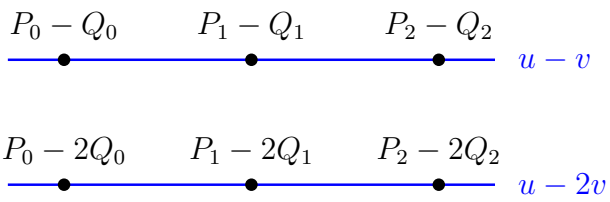
$$(u \boxplus v)(P) = w_1(P) w_2(P) w_3(P).$$

Furthermore, we observe that $u \boxplus v$ is defined in terms of the lines u, v, with no dependence on their cyclic orientations. These two observations will allow us to perform what is essentially a step of cyclic line addition as presented in section 3.6, all while ignoring cyclic orientations.

Namely, suppose that we are given lines $u, v \in \mathcal{L}_3(E)$:



without cyclic orientations. Then suppose that we also know the lines $u - v, u - 2v \in \mathcal{L}_3(E)$ that correspond to the "good" pairing between u and v:



where again we assume no knowledge of their cyclic orientations. Then we will be able to calculate the "good" sum line $u+v$ by comparing the following:

$$\begin{aligned}(u \boxplus v)(P) =& (u+v)(P) w_2(P) w_3(P) \\ ((u-v) \boxminus v)(P) =& (u-2v)(P) w_2(P) w_3(P)\end{aligned}$$

Explicitly, we have:

$$(u+v)(P) = \frac{(u \boxplus v)(P)(u-2v)(P)}{((u-v) \boxminus v)(P)}.$$

This is the addition step in a generic line multiplication. Note that this allows us to dispense of the need to compute the cyclic orientation of $u+v$ as well.

3.7 Formula for Linear Sum Function

Now that we have explained how to perform a generic line addition, the next step towards an explicit algorithm is to compute the linear sum function $u \boxplus v$ as a function of u and v. The following lemma allows us to use a computer algebra system to compute this:

Lemma 3.7.1. *For lines $u, v \in \mathcal{L}_3(E)$ with v having points Q_0, Q_1, Q_2, we have the following formula for $u \boxplus v \in \mathbb{F}(E)$ as a function of $R \in E$:*

$$(u \boxplus v)(R) = c^{-1} \cdot v(R)^3 u(R-Q_0) u(R-Q_1) u(R-Q_2)$$

for a non-zero constant c.

Proof. We only need to check that both sides have the same divisor. Since

$$\mathrm{Div}(u(R-Q_i)) = (P_0+Q_i) + (P_1+Q_i) + (P_2+Q_i) - 3(Q_i)$$

we have

$$\begin{aligned}&\mathrm{Div}\left(v(R)^3 u(R-Q_0) u(R-Q_1) u(R-Q_2)\right) \\ =&3\left((Q_0)+(Q_1)+(Q_2)-3(\mathcal{O})\right) \\ &+ ((P_0+Q_0)+(P_1+Q_0)+(P_2+Q_0)-3(Q_0)) \\ &+ ((P_0+Q_1)+(P_1+Q_1)+(P_2+Q_1)-3(Q_1)) \\ &+ ((P_0+Q_2)+(P_1+Q_2)+(P_2+Q_2)-3(Q_2)) \\ =&\sum_{i,j\in\{0,1,2\}} (P_i+Q_j) - 9(\mathcal{O}) = \mathrm{Div}(u \boxplus v)\end{aligned}$$

□

Since $u \boxplus v$ is normalized, the constant c must be chosen to normalize the right hand side. If $\mathcal{O}$ is not a point of u, v or $u \boxplus v$, then we can make this constant explicit:

Corollary 3.7.2. *Suppose that $u, v \in \mathcal{L}_3(E)$ and v has points Q_0, Q_1, Q_2. Suppose further that for $i \in \{0, 1, 2\}$, the point $-Q_i$ is not $\mathcal{O}$ and is not a point of u. Then as a function of $R \in E$:*

$$(u \boxplus v)(R) = v(R)^3 \prod_{i \in \{0,1,2\}} \frac{u(R - Q_i)}{u(-Q_i)}$$

To turn lemma 3.7.1 into an explicit formula, we first expand the terms in the product as a rational function of x_{Q_i}. Recall the addition algorithm 2.4:

$$\begin{aligned} m &= \frac{-y_R - y_{Q_i}}{x_R - x_{Q_i}} \\ x(R - Q_i) &= m^2 - x_R - x_{Q_i} \\ y(R - Q_i) &= m(x(R - Q_i) - x_R) - y_R \\ &= m^3 - m(2x_R + x_{Q_i}) - y_R \end{aligned}$$

Now by substituting in the above expressions as well as $y_{Q_i} = m_v x_{Q_i} + b_v$, we get an expression for $u(R - Q_i)$ as a rational function of Q_i:

$$\begin{aligned} u(R - Q_i) &= y(R - Q_i) - m_u x(R - Q_i) - b_u \\ &= m^3 - m(2x_R + x_{Q_i}) - y_R - m_u \left(m^2 - x_R - x_{Q_i}\right) - b_u \\ m &= \frac{-y_R - m_v x_{Q_i} - b_v}{x_R - x_{Q_i}} \end{aligned}$$

Now we can use a computer algebra system to take the product of the $u(-R - Q_i)$ over the three points $Q_i \in v$. This is done via a resultant calculation, and gives a formula for $(u \boxplus v)(x, y)$ in terms of the line coordinates of u and v:

Theorem 3.7.3. *Given lines $u, v \in \mathcal{L}_3(E)$:*

$$\begin{aligned} u(x, y) &= y - m_u x - b_u \\ v(x, y) &= y - m_v x - b_v \end{aligned}$$

suppose that $\mathcal{O}$ is not the sum of a point from u and one from v. Then the linear sum function is:

$$(u \boxplus v)(x, y) := -\gamma_9 - \gamma_7 x + \gamma_6 y - \gamma_5 x^2 + \gamma_4 xy - \gamma_3 y^2 + \gamma_2 x^2 y - \gamma_1 x y^2 + y^3$$

with γ_i being the coefficient found in section A.5 of the appendix.

These coefficients are indicated in figure 3.7. For instance, we have the following expression for γ_2:

$$\frac{-a^2(m_u+m_v)^3-9b(b_u+b_v)(m_u+m_v)^2+3a(b_u+b_v)^2(m_u+m_v)-3(b_u+b_v)(b_vm_u-b_um_v)^2}{b(m_u+m_v)^3-a(b_u+b_v)(m_u+m_v)^2-(b_u+b_v)^3-(m_u+m_v)(b_vm_u-b_um_v)^2}$$

Formulas for the linear sum function in other cases can be found in section A.5.

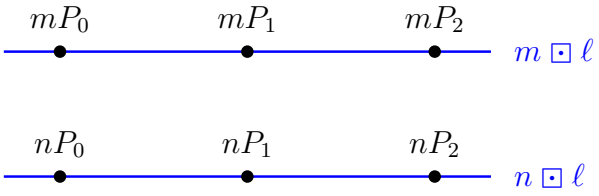
In[1]:=
```
γ0 = b (mu + mv)^3 - a (mu + mv)^2 (bu + bv) - (bu + bv)^3 - (mu + mv) (mu bv - bu mv)^2;
γ1 = γ0^-1 ((a^2 - 3 b mu mv + 2 a (mu bv + mv bu)) (mu + mv)^2 +
      (9 b - a mu mv + 9 bu bv) (mu + mv) (bu + bv) - 3 (a + mu bv + mv bu) (bu + bv)^2 - mu mv (bv mu - bu mv)^2);
γ2 = γ0^-1 (-a^2 (mu + mv)^3 - 9 b (mu + mv)^2 (bu + bv) + 3 a (mu + mv) (bu + bv)^2 - 3 (bu + bv) (mu bv - bu mv)^2);
γ3 = γ0^-1 (
    4 a^3 + 27 b^2 - 18 b bu^2 + 18 b bu bv - 3 bu^3 bv - 18 b bv^2 + 21 bu^2 bv^2 - 3 bu bv^3 - 8 a^2 bu mu +
     4 a^2 bv mu + 6 a b mu^2 - 7 a bu bv mu^2 + 3 a bv^2 mu^2 + 9 b bv mu^3 - bv^3 mu^3 + 4 a^2 bu mv - 8 a^2 bv mv -
     6 a b mu mv + a bu^2 mu mv + 12 a bu bv mu mv + a bv^2 mu mv + 3 b bu mu^2 mv - 6 b bv mu^2 mv - bu bv^2 mu^2 mv +
     a^2 mu^3 mv + 6 a b mv^2 + 3 a bu^2 mv^2 - 7 a bu bv mv^2 - 6 b bu mu mv^2 + 3 b bv mu mv^2 - bu^2 bv mu mv^2 +
     a^2 mu^2 mv^2 - 2 a bv mu^3 mv^2 + 9 b bu mv^3 - bu^3 mv^3 + a^2 mu mv^3 - 2 a bu mu^2 mv^3 + 4 b mu^3 mv^3);
γ4 = γ0^-1 (
    12 a bu^2 bv + 12 a bu bv^2 - 4 a^3 mu - 27 b^2 mu + 9 b bu^2 mu - 18 b bu bv mu - 9 b bv^2 mu + 3 bu^2 bv^2 mu - 6 bu bv^3 mu +
     4 a^2 bu mu^2 - 3 a b mu^3 + 3 a bv^2 mu^3 - 4 a^3 mv - 27 b^2 mv - 9 b bu^2 mv - 18 b bu bv mv - 6 bu^3 bv mv + 9 b bv^2 mv +
     3 bu^2 bv^2 mv - 3 a b mu^2 mv - 6 a bu bv mu^2 mv - 3 a bv^2 mu^2 mv + 4 a^2 bv mv^2 - 3 a b mu mv^2 - 3 a bu^2 mu mv^2 -
     6 a bu bv mu mv^2 + 12 b bu mu^2 mv^2 + 12 b bv mu^2 mv^2 + a^2 mu^3 mv^2 - 3 a b mv^3 + 3 a bu^2 mv^3 + a^2 mu^2 mv^3);
γ5 = γ0^-1 (
    9 a^2 bu^2 - 18 a^2 bu bv + 9 a^2 bv^2 - 27 a b bu mu + 27 a b bv mu + 3 a bu^2 bv mu - 15 a bu bv^2 mu + a^3 mu^2 + 27 b^2 mu^2 -
     9 b bu bv mu^2 + 9 b bv^2 mu^2 - 3 bu bv^3 mu^2 - a^2 bv mu^3 + 27 a b bu mv - 27 a b bv mv - 15 a bu^2 bv mv + 3 a bu bv^2 mv +
     2 a^3 mu mv - 27 b^2 mu mv + 9 b bu^2 mu mv + 36 b bu bv mu mv + 9 b bv^2 mu mv - 3 bu^2 bv^2 mu mv + 4 a^2 bu mu^2 mv -
     3 a^2 bv mu^2 mv - 3 a b mu^3 mv - a bv^2 mu^3 mv + a^3 mv^2 + 27 b^2 mv^2 + 9 b bu^2 mv^2 - 9 b bu bv mv^2 - 3 bu^3 bv mv^2 -
     3 a^2 bu mu mv^2 + 4 a^2 bv mu mv^2 + 12 a b mu^2 mv^2 - 4 a bu bv mu^2 mv^2 - a^2 bu mv^3 - 3 a b mu mv^3 - a bu^2 mu mv^3 - a^2 mu^3 mv^3);
γ6 = γ0^-1 (
    -4 a^3 bu - 27 b^2 bu - 4 a^3 bv - 27 b^2 bv + 18 b bu^2 bv + 18 b bu bv^2 - 3 bu^3 bv^2 - 3 bu^2 bv^3 - a^2 bu^2 mu + 6 a^2 bu bv mu +
     3 a^2 bv^2 mu + 3 a b bu mu^2 - 3 a b bv mu^2 - 6 a bu bv^2 mu^2 - a^3 mu^3 - 9 b^2 mu^3 + 9 b bv^2 mu^3 + 3 a^2 bu^2 mv +
     6 a^2 bu bv mv - a^2 bv^2 mv - 6 a b bu mu mv - 6 a b bv mu mv + a^3 mu^2 mv + 9 b^2 mu^2 mv + 6 b bu bv mu^2 mv -
     3 b bv^2 mu^2 mv + 2 a^2 bv mu^3 mv - 3 a b bu mv^2 + 3 a b bv mv^2 - 6 a bu^2 bv mv^2 + a^3 mu mv^2 + 9 b^2 mu mv^2 -
     3 b bu^2 mu mv^2 + 6 b bu bv mu mv^2 - a^2 bu mu^2 mv^2 - a^2 bv mu^2 mv^2 - a^3 mv^3 - 9 b^2 mv^3 + 9 b bu^2 mv^3 + 2 a^2 bu mu mv^3);
γ7 = γ0^-1 (
    27 a b bu^2 - 54 a b bu bv + 27 a b bv^2 - 12 a bu^2 bv^2 + 8 a^3 bu mu - 27 b^2 bu mu - 4 a^3 bv mu + 54 b^2 bv mu + 9 b bu^2 bv mu -
     9 b bu bv^2 mu - 3 bu^2 bv^3 mu - 9 a^2 b mu^2 + 4 a^2 bu bv mu^2 - 3 a b bv mu^3 + a bv^3 mu^3 - 4 a^3 bu mv + 54 b^2 bu mv +
     8 a^3 bv mv - 27 b^2 bv mv - 9 b bu^2 bv mv + 9 b bu bv^2 mv - 3 bu^3 bv^2 mv + 18 a^2 b mu mv - 4 a^2 bu^2 mu mv - 4 a^2 bv^2 mu mv +
     12 a b bu mu^2 mv - 21 a b bv mu^2 mv + a bu bv^2 mu^2 mv - 9 b^2 mu^3 mv - 3 b bv^2 mu^3 mv - 9 a^2 b mv^2 + 4 a^2 bu bv mv^2 -
     21 a b bu mu mv^2 + 12 a b bv mu mv^2 + a bu^2 bv mu mv^2 - 4 a^3 mu^2 mv^2 + 18 b^2 mu^2 mv^2 - 6 b bu bv mu^2 mv^2 +
     a^2 bv mu^3 mv^2 - 3 a b bu mv^3 + a bu^3 mv^3 - 9 b^2 mu mv^3 - 3 b bu^2 mu mv^3 + a^2 bu mu^2 mv^3 - 4 a b mu^3 mv^3);
γ9 = γ0^-1 (
    a^3 bu^2 + 27 b^2 bu^2 + 2 a^3 bu bv - 27 b^2 bu bv + a^3 bv^2 + 27 b^2 bv^2 - 18 b bu^2 bv^2 - bu^3 bv^3 + 9 a^2 b bu mu - 9 a^2 b bv mu -
     a^2 bu^2 bv mu - 3 a^2 bu bv^2 mu + a^4 mu^2 + 3 a b bu bv mu^2 + 3 a b bv^2 mu^2 - a^3 bv mu^3 - 9 b^2 bv mu^3 + b bv^3 mu^3 - 9 a^2 b bu mv +
     9 a^2 b bv mv - 3 a^2 bu^2 bv mv - a^2 bu bv^2 mv - 2 a^4 mu mv - 3 a b bu^2 mu mv + 12 a b bu bv mu mv - 3 a b bv^2 mu mv +
     2 a bu^2 bv^2 mu mv + 9 b^2 bu mu^2 mv + a^3 bv mu^2 mv - 18 b^2 bv mu^2 mv - 3 b bu bv^2 mu^2 mv + a^2 b mu^3 mv + a^4 mv^2 +
     3 a b bu^2 mv^2 + 3 a b bu bv mv^2 + a^3 bu mu mv^2 - 18 b^2 bu mu mv^2 + 9 b^2 bv mu mv^2 - 3 b bu^2 bv mu mv^2 - 6 a^2 b mu^2 mv^2 -
     a^2 bu bv mu^2 mv^2 + 2 a b bv mu^3 mv^2 - a^3 bu mv^3 - 9 b^2 bu mv^3 + b bu^3 mv^3 + a^2 b mu mv^3 + 2 a b bu mu^2 mv^3 - 4 b^2 mu^3 mv^3);
LineSumFunction = -γ9 - γ7 x + γ6 y - γ5 x^2 + γ4 x y - γ3 y^2 + γ2 x^2 y - γ1 x y^2 + y^3;
```

In[11]:=
```
m = (-y - (mv xq + bv))/(x - xq); xs = m^2 - x - xq; ys = m (xs - x) - y;
Together@PolynomialRemainder[
  -(y - mv x - bv)^3 Resultant[ys - mu xs - bu, b + a xq + xq^3 - (bv + mv xq)^2, xq] - γ0 LineSumFunction, b + a x + x^3 - y^2, y]
```

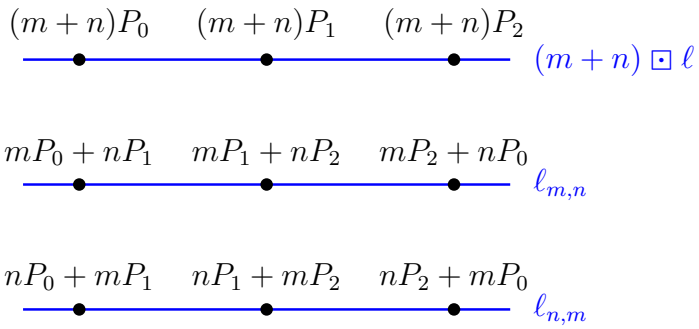
Out[12]= 0

3.8 Generic Line Multiplication Operation Chain

Now that we have the $\boxplus$ operation, we will present an operation chain to compute the $k\boxdot$ operation on lines. We will perform a line addition step using the idea presented in section 3.6. So suppose that we have a line ℓ with points P_0, P_1, P_2 in cyclic order, and we aim to calculate $k \boxdot \ell$. Then consider the cyclic linear sum of $m \boxdot \ell$ and $n \boxdot \ell$:

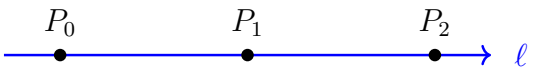


The "good" sum line is $(m+n) \boxdot \ell$, while the "bad" sum lines are the lines $\ell_{m,n}$ and $\ell_{n,m}$ indicated below:

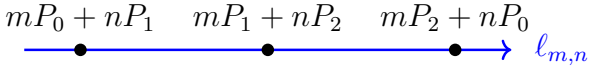


This uses the following notatation:

Definition 3.8.1. *For a cyclically oriented line ℓ:*



we define $\ell_{m,n}$ to be the following cyclically oriented line:



Furthermore, we define $\ell_m := \ell_{m,0} = m \boxdot \ell$.

With this new notation, we have the following in $\mathbb{F}(E)$:

$$\ell_m \boxplus \ell_n = \ell_{m+n}\ell_{m,n}\ell_{n,m} \tag{3.3}$$

with the three lines on the right corresponding to the three cyclic sum lines. Note also that we have $\Delta(\ell_{m,n}) = (\Delta\ell)_{m,n} = \ell_{-m-n,m-2n}$, and that $\ell_{m,n}$ has symmetries coming from the fact that $P_0 + P_1 + P_2 = \mathcal{O}$:

Lemma 3.8.2. *For $m, n \in \mathbb{Z}$ and a cyclically oriented line ℓ, we have:*

$$\ell_{m,n} = \ell_{-n,m-n} = \ell_{n-m,-m}$$

Proof. This follows from the fact that $P_0 + P_1 + P_2 = \mathcal{O}$, and so we can eliminate P_0 or P_1 from the expression $mP_0 + nP_1$. Then by cycling around, we get the desired result. More explicitly, for indices i in modulus 3, we get:

$$mP_i + nP_{i+1} = (n-m)P_{i+1} + (-m)P_{i+2} = (-n)P_{i-1} + (m-n)P_i.$$

□

3.8.1 Line Doubling

For the doubling step, consider equation (3.3) with $m = n = 1$, noting that $\ell_{1,1} = \ell_{-1}$ by lemma 3.8.2:

$$\begin{aligned} \ell \boxplus \ell =& (2 \boxdot \ell)\ell_{1,1}\ell_{1,1} = (2 \boxdot \ell)(\ell_{-1})^2 \\ 2 \boxdot \ell =& \frac{\ell \boxplus \ell}{(\ell_{-1})^2}. \end{aligned}$$

By a direct calculation, we get the following explicit formulas:

Theorem 3.8.3. *For a line ℓ, we have*

$$2 \boxdot \ell = \frac{\ell \boxplus \ell}{(\boxminus \ell)^2}.$$

If ℓ contains no 2-torsion, then

$$\begin{aligned} m_{2\boxdot\ell} =& \frac{a^2m_\ell^2 + 9bm_\ell b_\ell - 3ab_\ell^2 + m_\ell(bm_\ell^3 - am_\ell^2 b_\ell - b_\ell^3)}{2(bm_\ell^3 - am_\ell^2 b_\ell - b_\ell^3)} \\ b_{2\boxdot\ell} =& \frac{4a^3 + 27b^2 + 6abm_\ell^2 - 8a^2 m_\ell b_\ell - 18bb_\ell^2 - a^2 m_\ell^4 - 8bm_\ell^3 b_\ell + 2am_\ell^2 b_\ell^2 - b_\ell^4}{8(bm_\ell^3 - am_\ell^2 b_\ell - b_\ell^3)} \end{aligned}$$

Note that we can save a few operations in the computation of $b_{2\boxdot\ell}$ by rewriting the above formula:

$$b_{2\boxdot\ell} = \frac{4a(a - m_\ell b_\ell)^2 + (9b - am_\ell^2 - 9b_\ell^2)(3b + am_\ell^2 + b_\ell^2) - 8b_\ell(bm_\ell^3 - am_\ell^2 b_\ell - b_\ell^3)}{8(bm_\ell^3 - am_\ell^2 b_\ell - b_\ell^3)}$$

3.8.2 Line Addition

For the line addition step, we simply translate section 3.6 into our context. So consider the linear sum of ℓ_m and ℓ_n. We get the "good" sum line $\ell_{m+n} = (m+n) \boxdot \ell$, and two "bad" sum lines $\ell_{m,n}, \ell_{n,m}$. We then take advantage of the fact that we get the same "bad" sum lines $\ell_{m,n}, \ell_{n,m}$ when we sum the lines ℓ_{m-n} and ℓ_{-n}, to eliminate them together.

Theorem 3.8.4.

$$(m+n) \boxdot \ell = \frac{(m \boxdot \ell) \boxplus (n \boxdot \ell)}{((m-n) \boxdot \ell) \boxplus ((-n) \boxdot \ell)} ((m-2n) \boxdot \ell)$$

Proof. Using lemma 3.8.2, we get the following decomposition of the linear sum function between ℓ_{m-n} and ℓ_{-n}:

$$\begin{aligned} \ell_{m-n} \boxplus \ell_{-n} =& \ell_{m-2n} \ell_{m-n,-n} \ell_{-n,m-n} \\ =& \ell_{m-2n} \ell_{n,m} \ell_{m,n} \end{aligned}$$

Subsequently, we can divide this by the linear sum function between ℓ_m and ℓ_n to eliminate the "bad" sum lines:

$$\begin{aligned} \frac{\ell_m \boxplus \ell_n}{\ell_{m-n} \boxplus \ell_{-n}} =& \frac{\ell_{m+n} \ell_{m,n} \ell_{n,m}}{\ell_{m-2n} \ell_{n,m} \ell_{m,n}} \\ \ell_{m+n} =& \frac{(\ell_m \boxplus \ell_n) \ell_{m-2n}}{\ell_{m-n} \boxplus \ell_{-n}} \end{aligned}$$

□

3.8.3 Line Multiplication Ladder

Now we have all of the tools needed to perform our modified Montgomery ladder. In this modified ladder, at each step we will keep track of three consecutive multiples of ℓ. Then if we are given $\ell_m, \ell_{m+1}, \ell_{m+2}$, we note that we can then calculate five consecutive multiples of ℓ:

$$\ell_{2m} = 2 \boxdot \ell_m \tag{3.4}$$

$$\ell_{2m+1} = \ell_{m+(m+1)} = \frac{(\ell_m \boxplus \ell_{m+1}) (\ell_{-m-2})}{\ell_{-1} \boxplus \ell_{-m-1}} \tag{3.5}$$

$$\ell_{2m+2} = 2 \boxdot \ell_{m+1} \tag{3.6}$$

$$\ell_{2m+3} = \ell_{(m+2)+(m+1)} = \frac{(\ell_{m+2} \boxplus \ell_{m+1}) (\ell_{-m})}{\ell \boxplus \ell_{-m-1}} \tag{3.7}$$

$$\ell_{2m+4} = 2 \boxdot \ell_{m+2} \tag{3.8}$$

Then just as in the Montgomery ladder, we choose to either calculate the first three or the last three, according to a bit in the binary expansion of k.

Suppose that the binary expansion of $k \in \mathbb{Z}_{>0}$ is $k = \sum_{i=0}^{b} k_i 2^i$. Then our ladder will consist of triples $(\ell_{K_i}, \ell_{K_i+1}, \ell_{K_i+2})$ where K_i is obtained from k by truncating the last $i+1$ bits, and then doubling the result. Precisely, we have:

$$K_i = \sum_{j=i+1}^{b} k_j 2^{j-i} = 2 \left\lfloor \frac{k}{2^{i+1}} \right\rfloor$$

for i decreasing from b to 0. Note that K_{i-1}

$$K_{i-1} - 2K_i = \left(\sum_{j=i}^{b} k_j 2^{j-i+1} \right) - 2 \left(\sum_{j=i+1}^{b} k_j 2^{j-i} \right) = 2k_i$$

so $K_{i-1} = 2K_i + 2k_i$. Thus

$$(\ell_{K_{i-1}}, \ell_{K_{i-1}+1}, \ell_{K_{i-1}+2})$$

can be computed from

$$(\ell_{K_i}, \ell_{K_i+1}, \ell_{K_i+2})$$

using formulas (3.4), (3.5) and (3.6) when $k_i = 0$, or using formulas (3.6), (3.7) and (3.8) when $k_i = 1$. In both cases, there are four $2\boxdot$ operations, and two line additions.

Finally we get $K_0 = k - k_0$, and so the last triple in the iteration will contain ℓ_k among the first two entries.

For example, to calculate $25 \boxdot \ell$, we write $25 = 11001_2$ in binary and iteratively compute:

$$\begin{aligned}
0: \quad & (\ell_0, \ell_1, \ell_2) = (1, \ell, 2 \boxdot \ell) \\
10: \quad & (\ell_2, \ell_3, \ell_4) = \left(\ell_2, \frac{\ell_1 \boxplus \ell_2}{\ell_1 \boxplus \ell_{-1}} \ell_0, 2 \boxdot \ell_2 \right) \\
110: \quad & (\ell_6, \ell_7, \ell_8) = \left(2 \boxdot \ell_3, \frac{\ell_3 \boxplus \ell_4}{\ell_1 \boxplus \ell_{-3}} \ell_{-2}, 2 \boxdot \ell_4 \right) \\
1100: \quad & (\ell_{12}, \ell_{13}, \ell_{14}) = \left(2 \boxdot \ell_6, \frac{\ell_6 \boxplus \ell_7}{\ell_{-1} \boxplus \ell_{-7}} \ell_{-8}, 2 \boxdot \ell_7 \right) \\
11000: \quad & (\ell_{24}, \ell_{25}, \ell_{26}) = \left(2 \boxdot \ell_{12}, \frac{\ell_{12} \boxplus \ell_{13}}{\ell_{-1} \boxplus \ell_{-13}} \ell_{-14}, 2 \boxdot \ell_{13} \right)
\end{aligned}$$

And the result is $\ell_{25} = 25 \boxdot \ell$.

We remark that this algorithm is quite inefficient because of the size of the formula for $\boxplus$. In chapter 5, we will see that there are simple ways to improve this situation. With careful study of the algebra involved, we will in fact do much better by the end of the thesis.

Algorithm 3: Recursive Algorithm to Compute $k\boxdot : \mathcal{L}_3^\bullet(E) \to \mathcal{L}_3^\bullet(E)$

Input : ℓ with $\mathrm{Div}(\ell) \in \mathcal{L}_3^\bullet(E)$ and a positive integer k with binary representation $k = k_b \ldots k_1 k_0$.

Output: $k \boxdot \ell$

$r, s, t \leftarrow 1, \ell, 2 \boxdot \ell$;
for $i \leftarrow b - 1$ **to** 0 **do**
  if $k_i = 0$ **then**
    $r, s, t \leftarrow 2 \boxdot r, \frac{r \boxplus s}{(\boxminus \ell) \boxplus (\boxminus s)}(\boxminus t), 2 \boxdot s$;
  else
    $r, s, t \leftarrow 2 \boxdot s, \frac{t \boxplus s}{\ell \boxplus (\boxminus s)}(\boxminus r), 2 \boxdot t$;
  end
end
if $k_0 = 0$ **then**
  return r;
else
  return s;
end

3.9 Improving on Generic Algorithm

We now consider some simple improvements to the efficiency of the generic line multiplication algorithm. As a first refinement, we will show that $u \boxplus v$ carries more information than we need, and we can implement essentially the same algorithm without keeping track of all of the coefficients. To achieve this, we reconsider equation (3.2), holding off on evaluating the coefficients in the linear sum functions.

So for a line $u \in \mathcal{L}_3(E)$, let $u_n := n \boxdot u$, and suppose that we are given $u_k, u_l, u_{k-l}, u_{k-2l}$. Suppose further that the coefficients γ_i, γ_i^* satisfy the following:

$$\begin{aligned}(u_k \boxplus u_l)(x,y) =& -\gamma_9 - \gamma_7 x + \gamma_6 y - \gamma_5 x^2 + \gamma_4 xy - \gamma_3 y^2 + \gamma_2 x^2 y - \gamma_1 x y^2 + y^3 \\ (u_{k-l} \boxplus u_{-l})(x,y) =& -\gamma_9^* - \gamma_7^* x + \gamma_6^* y - \gamma_5^* x^2 + \gamma_4^* xy - \gamma_3^* y^2 + \gamma_2^* x^2 y - \gamma_1^* x y^2 + y^3.\end{aligned}$$

Then if $u_n(x,y) = y - m_n x - b_n$, then:

$$u_{k+l}(x,y) \cdot (u_{k-l} \boxplus u_{-l})(x,y) = u_{k-2l}(x,y) \cdot (u_k \boxplus u_l)(x,y)$$

or equivalently,

$$\begin{aligned}&(y - m_{k+l}x - b_{k+l})(-\gamma_9^* - \gamma_7^* x + \gamma_6^* y - \gamma_5^* x^2 + \gamma_4^* xy - \gamma_3^* y^2 + \gamma_2^* x^2 y - \gamma_1^* x y^2 + y^3) \\ =&(y - m_{k-2l}x - b_{k-2l})(-\gamma_9 - \gamma_7 x + \gamma_6 y - \gamma_5 x^2 + \gamma_4 xy - \gamma_3 y^2 + \gamma_2 x^2 y - \gamma_1 x y^2 + y^3).\end{aligned}$$

Now we reduce both sides of this equation modulo $b + ax + x^3 - y^2$ with respect to x and compare coefficients. The coefficients of $x^1 y^3$ and $x^0 y^3$ give us respectively:

$$\begin{aligned}m_{k+l} + \gamma_1^* =& m_{k-2l} + \gamma_1 \\ b_{k+l} + \gamma_3^* + m_{k+l}\gamma_2^* =& b_{k-2l} + \gamma_3 + m_{k-2l}\gamma_2.\end{aligned}$$

Note that we could get alternative algorithms by comparing other coefficients.

Lemma 3.9.1. *Given multiples $u_k, u_l, u_{k-l}, u_{k-2l}$ of u, we can calculate the coefficients of*

$$u_{k+l}(x,y) = y - m_{k+l}x - b_{k+l}$$

as follows:

$$\begin{aligned}m_{k+l} =& \gamma_1(u_k, u_l) - \gamma_1(u_{k-l}, u_{-l}) + m_{k-2l} \\ b_{k+l} =& \gamma_3(u_k, u_l) - \gamma_3(u_{k-l}, u_{-l}) + m_{k-2l}\gamma_2(u_k, u_l) - m_{k+l}\gamma_2(u_{k-l}, u_{-l}) + b_{k-2l}\end{aligned}$$

with γ_i as found in theorem 3.7.3 or in section 6.2.1 of the appendix. (Note that we are assuming that $\mathcal{O}$ does not lie on any of these lines.)

The formulas above in fact have simple interpretations. The formula for m_{k+l} actually has an interpretation that we have already seen! To see this, we start with equation 3.1 from the section on cyclic line addition, and translate it into this section's notation. For comparison, we juxtapose this with the above formula from lemma 3.9.1 for m_{k+l}:

$$\begin{aligned} m_{k+l} =& m_\Sigma(u_k, \Delta u_k, u_l, \Delta u_l) - m_\Sigma(u_{k-l}, \Delta u_{k-l}, u_{-l}, \Delta u_{-l}) + m_{k-2l} \\ m_{k+l} =& \gamma_1(u_k, u_l) - \gamma_1(u_{k-l}, u_{-l}) + m_{k-2l} \end{aligned}$$

These formulas are in fact the same! More precisely, we have the following, as we will prove in the next section 3.10:

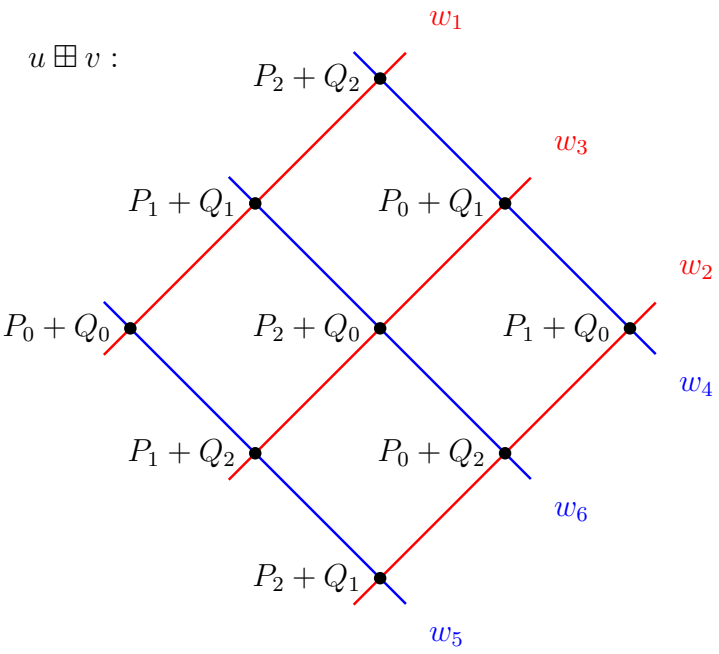
$$\begin{aligned} \gamma_1(u, v) =& m_\Sigma(u, \Delta u, v, \Delta v) \\ =& m_{w_1} + m_{w_2} + m_{w_3} \end{aligned}$$

So $\gamma_1(u, v)$ gives the sum of the slopes of the three cyclic sums of u and v. This is interesting because a priori, we expect that m_Σ should depend on the cyclic orientations of u, v, but it in fact does not. Note that b_Σ does depend on the cyclic orientations of u, v. We will study these combinations that do not depend on the cyclic orientation in the next section 3.10. This will set the stage for further improvements to the generic algorithm.

3.10 Nine Point Diagrams

In this section, we introduce nine point diagrams. These diagrams represent all of the possible sum lines and sum points between $u, v \in \mathcal{L}_3(E)$. These will also reappear in other guises in later chapters; for example, for lines u, v and any sum line w, the lines $u, v, -w$ can also be arranged into a nine point diagram. This phenomenon means that the results that we obtain about nine point diagrams can be applied in multiple ways in the algebra line addition. Because of this central role in the algebra of line addition, we will be studying nine point diagrams in greater depth in chapter 6.

Let w_1, w_2, w_3 denoted the three cyclic sum lines of u and v with respective cyclic orders P_0, P_1, P_2 and Q_0, Q_1, Q_2. Then let w_4, w_5, w_6 be the three cyclic sum lines of u with the same cyclic order P_0, P_1, P_2 and v with the opposite cyclic order Q_0, Q_2, Q_1. These six lines represent all possible sum lines of u and v, and can be overlaid to form this diagram:



The above configuration of points and lines will be referred to as a *nine point diagram*; these will be studied in detail in chapter 6.

The normalized function with divisor $\sum_{i,j\in\{0,1,2\}}(P_i+Q_j)-9(\mathcal{O})$ will be called the *nine point diagram function*. For the diagram associated to the line addition of $u, v \in \mathcal{L}_3(E)$, this function is the same as the linear sum function $u \boxplus v$. This function can be written as a product of three line functions, as we saw in section 3.6. In fact, we get two factorizations this way:

$$\begin{aligned}(u \boxplus v)(x,y) =& (y - m_{w_1}x - b_{w_1})(y - m_{w_2}x - b_{w_2})(y - m_{w_3}x - b_{w_3}) \\ =& (y - m_{w_4}x - b_{w_4})(y - m_{w_5}x - b_{w_5})(y - m_{w_6}x - b_{w_6})\end{aligned}$$

which correspond to two different ways of partitioning the divisor (and noting that the factors are all normalized.)

Reducing modulo $b + ax + x^3 - y^2$ with respect to x, we get:

$$\begin{aligned}(u \boxplus v)(x,y) =& (y - m_{w_1}x - b_{w_1})(y - m_{w_2}x - b_{w_2})(y - m_{w_3}x - b_{w_3}) \\ =& -(b_{w_1}b_{w_2}b_{w_3} - b \cdot m_{w_1}m_{w_2}m_{w_3}) \\ & - x\,(b_{w_2}b_{w_3}m_{w_1} + b_{w_1}b_{w_3}m_{w_2} + b_{w_1}b_{w_2}m_{w_3} - a \cdot m_{w_2}m_{w_3}m_{w_1}) \\ & + y\,(b_{w_1}b_{w_2} + b_{w_1}b_{w_3} + b_{w_2}b_{w_3}) \\ & - x^2\,(b_{w_3}m_{w_1}m_{w_2} + b_{w_1}m_{w_3}m_{w_2} + b_{w_2}m_{w_1}m_{w_3}) \\ & + xy\,(b_{w_2}m_{w_1} + b_{w_3}m_{w_1} + b_{w_1}m_{w_2} + b_{w_3}m_{w_2} + b_{w_1}m_{w_3} + b_{w_2}m_{w_3}) \\ & - y^2\,(b_{w_1} + b_{w_2} + b_{w_3} + m_{w_1}m_{w_2}m_{w_3}) \\ & + x^2y\,(m_{w_1}m_{w_2} + m_{w_3}m_{w_2} + m_{w_1}m_{w_3}) \\ & - xy^2\,(m_{w_1} + m_{w_2} + m_{w_3}) + y^3\end{aligned} \tag{3.9}$$

Hence we can now explain the interesting result mentioned in the last section 3.9:

Theorem 3.10.1. *Consider the cyclic sum of oriented lines u and v. If the three possible sum lines are w_1, w_2, w_3, then the following combinations of coefficients of w_1, w_2, w_3 are also coefficients of $(u \boxplus v)(x, y)$:*

$$\begin{aligned}\gamma_1 =& m_{w_1} + m_{w_2} + m_{w_3} \\ \gamma_2 =& m_{w_1}m_{w_2} + m_{w_3}m_{w_2} + m_{w_1}m_{w_3} \\ \gamma_3 =& b_{w_1} + b_{w_2} + b_{w_3} + m_{w_1}m_{w_2}m_{w_3} \\ \gamma_4 =& b_{w_2}m_{w_1} + b_{w_3}m_{w_1} + b_{w_1}m_{w_2} + b_{w_3}m_{w_2} + b_{w_1}m_{w_3} + b_{w_2}m_{w_3} \\ \gamma_5 =& b_{w_3}m_{w_1}m_{w_2} + b_{w_1}m_{w_3}m_{w_2} + b_{w_2}m_{w_1}m_{w_3} \\ \gamma_6 =& b_{w_1}b_{w_2} + b_{w_1}b_{w_3} + b_{w_2}b_{w_3} \\ \gamma_7 =& b_{w_2}b_{w_3}m_{w_1} + b_{w_1}b_{w_3}m_{w_2} + b_{w_1}b_{w_2}m_{w_3} - a \cdot m_{w_2}m_{w_3}m_{w_1} \\ \gamma_9 =& b_{w_1}b_{w_2}b_{w_3} - b \cdot m_{w_1}m_{w_2}m_{w_3}\end{aligned} \tag{3.10}$$

Consequently, these are functions of u, v that do not depend on the orientations of u and v.

Explicit equations for these combinations as functions of u, v can be found in section A.5 of the appendix.

Note that as a consequence of the independence from orientation, the above combinations will be equal if we substitute w_1, w_2, w_3 for w_4, w_5, w_6. For example,

$$m_{w_1} + m_{w_2} + m_{w_3} = m_{w_4} + m_{w_5} + m_{w_6}, \tag{3.11}$$

and similar equations hold for the other quantities. Relations between the nine point diagram line coordinates will be visited in much greater detail in chapter 6.

3.11 Recursion

Now we will present the algorithm alluded to in section 3.9 in more detail. Suppose we are given multiples $u_k, u_l, u_{k-l}, u_{k-2l}$ of u. Then by theorem 3.10.1:

$$\begin{aligned}
\gamma_1(u_k, u_l) =& m_{k+l} + m_{k,l} + m_{l,k} \\
\gamma_1(u_{k-l}, u_{-l}) =& m_{k-2l} + m_{k,l} + m_{l,k} \\
\gamma_2(u_k, u_l) =& m_{k+l}(m_{k,l} + m_{l,k}) + m_{k,l}m_{l,k} \\
\gamma_2(u_{k-l}, u_{-l}) =& m_{k-2l}(m_{k,l} + m_{l,k}) + m_{k,l}m_{l,k} \\
\gamma_3(u_k, u_l) =& b_{k+l} + b_{k,l} + b_{l,k} + m_{k+l}m_{k,l}m_{l,k} \\
\gamma_3(u_{k-l}, u_{-l}) =& b_{k-2l} + b_{k,l} + b_{l,k} + m_{k-2l}m_{k,l}m_{l,k}
\end{aligned}$$

So we isolate m_{k+l}:

$$m_{k+l} = \gamma_1(u_k, u_l) - \gamma_1(u_{k-l}, u_{-l}) + m_{k-2l}$$

and similarly, we isolate b_{k+l}:

$$b_{k+l} = \gamma_3(u_k, u_l) - \gamma_3(u_{k-l}, u_{-l}) + m_{k-2l}\gamma_2(u_k, u_l) - m_{k+l}\gamma_2(u_{k-l}, u_{-l}) + b_{k-2l}$$

Thus if we take the following formulas:

$$\gamma_1(u, v) = \frac{3\left(m_u m_v + 3X\right)\left(b + aX + X^3 - Y^2\right) - \left(a + 3X^2 - 2m_u Y\right)\left(a + 3X^2 + 2m_v Y\right)}{\left(m_u + m_v\right)\left(b + aX + X^3 - Y^2\right)}$$

$$\gamma_2(u, v) = \frac{-a^2 + 3aX^2 + 9bX + 3XY^2}{b + aX + X^3 - Y^2}$$

$$\begin{aligned}
\gamma_3(u, v) = &-\big(4a^3 + 4a^2 b_v m_u + 4a^2 b_u m_v - 8a^2 b_u m_u - 8a^2 b_v m_v + a^2 m_u m_v^3 \\
&+ a^2 m_u^2 m_v^2 + a^2 m_u^3 m_v - 2ab_u m_u^2 m_v^3 + 3ab_v^2 m_u^2 - 7ab_u b_v m_u^2 \\
&- 2ab_v m_u^3 m_v^2 + 3ab_u^2 m_v^2 - 7ab_u b_v m_v^2 + ab_u^2 m_u m_v + ab_v^2 m_u m_v \\
&- 6abm_u m_v + 12ab_u b_v m_u m_v + 6abm_u^2 + 6abm_v^2 + 27b^2 - b_v^3 m_u^3 + 9bb_v m_u^3 \\
&- b_u^3 m_v^3 + 4bm_u^3 m_v^3 + 9bb_u m_v^3 - 6bb_u m_u m_v^2 - b_u^2 b_v m_u m_v^2 + 3bb_v m_u m_v^2 \\
&- b_u b_v^2 m_u^2 m_v + 3bb_u m_u^2 m_v - 6bb_v m_u^2 m_v - 3b_u b_v^3 + 21b_u^2 b_v^2 - 3b_u^3 b_v + 18bb_u b_v \\
&- 18bb_u^2 - 18bb_v^2\big) / \left((m_u + m_v)^3 (b + aX + X^3 - Y^2)\right)
\end{aligned}$$

where

$$(X, Y) := u \cap (-v) = \left(\frac{-b_u - b_v}{m_u + m_v}, \frac{b_u m_v - b_v m_u}{m_u + m_v}\right),$$

we get algorithm 4. Note that we assume that no line in the algorithm has $\mathcal{O}$ as a point for simplicity. Those cases can be found in section A.5 of the appendix.

Algorithm 4: Recursive Algorithm to Compute $k\boxdot : \mathcal{L}_3(E) \to \mathcal{L}_3(E)$

Input : $u = (m_1, b_1) \in \mathcal{L}_3^{\bullet}(E)$; and a positive integer k with binary representation $k = k_{b-1} \dots k_1 k_0$ and $k_{b-1} = 1$.

Output: $k \boxdot u = (m_k, b_k)$

$m_r, b_r \leftarrow \text{LineDouble}(m_1, b_1)$;
$m_s, b_s \leftarrow \text{LineTriple}(m_1, b_1)$;
$m_t, b_t \leftarrow \text{LineDouble}(m_r, b_r)$;
for $i \leftarrow b-2$ **to** 0 **do**
  if $k_i = 0$ **then**
    $m'_s \leftarrow \gamma_1(m_r, b_r, m_s, b_s) - \gamma_1(-m_1, -b_1, -m_s, -b_s) - m_t$;
    $m_s, b_s \leftarrow m'_s, \gamma_3(m_r, b_r, m_s, b_s) - \gamma_3(-m_1, -b_1, -m_s, -b_s) - m_t\gamma_2(m_r, b_r, m_s, b_s) - m'_s\gamma_2(-m_1, -b_1, -m_s, -b_s)b_t$;
    $m_r, b_r \leftarrow \text{LineDouble}(m_r, b_r)$;
    $m_t, b_t \leftarrow \text{LineDouble}(m_s, b_s)$;
  else
    $m'_s \leftarrow \gamma_1(m_r, b_r, m_s, b_s) - \gamma_1(-m_1, -b_1, -m_s, -b_s) - m_t$;
    $m_s, b_s \leftarrow m'_s, \gamma_3(m_r, b_r, m_s, b_s) - \gamma_3(-m_1, -b_1, -m_s, -b_s) - m_t\gamma_2(m_r, b_r, m_s, b_s) - m'_s\gamma_2(-m_1, -b_1, -m_s, -b_s)b_t$;
    $m_r, b_r \leftarrow \text{LineDouble}(m_s, b_s)$;
    $m_t, b_t \leftarrow \text{LineDouble}(m_t, b_t)$;
  end
end
return m_r, b_r;

Chapter 4

Generalized Line Multiplication

In this chapter, we generalize line multiplication to other settings. We focus mostly on generic line multiplication, since the formalism can be translated to other settings with little work. This chapter should be considered as an optional addendum to chapter 3; the definitions and results that are necessary for future chapters will be repeated in place. That said, the generic algorithm is the basis for the main algorithms proposed in this thesis, so it does not hurt to be familiar with it.

The main motivation for studying this generalization was to work with "toy" models, where we could more easily make discoveries and test theories through computational means. Many of these discoveries in fact had analogues for elliptic curve multiplication. The notation and results from this chapter also set the stage for future generalizations.

Our first generalization of line multiplication is to *linear n-set multiplication* operation $\boxdot k : \mathcal{L}_n(E) \to \mathcal{L}_n(E)$, which is an analogue with n points for $n \in \mathbb{Z}_{>0}$. For $n = 2$ this corresponds to x-only point multiplication, and for $n = 3$ this corresponds to line multiplication.

Next we explain how the discussions and algorithms from chapter 3 generalize to replace E with an arbitrary abelian group. To achieve this, we focus on algorithms for $\boxdot k : \mathcal{L}_3(E) \to \mathcal{L}_3(E)$, whose only connection to the specifics of the group E is via the operation $\boxplus$ which computes the linear sum function. This then allows us to replace E with an arbitrary abelian group. In particular, we translate the generic line multiplication algorithm to work in the multiplicative group of a field. Then as an illustration, we propose a variant of Cipolla's square root finding algorithm.

4.1 Generalized Elliptic Curve Line Multiplication

We start by generalizing line multiplication in $\mathcal{L}_3(E)$ to arbitrary number of points:

Definition 4.1.1. *For a positive integer n,*

$$\mathcal{L}_n(E) = \{f \in \overline{\mathbb{F}}(E)^\times \ : \ \mathrm{Div}(f) \geq -n(\mathcal{O}),\ f \text{ normalized at } \mathcal{O}\}$$

and an element of $\mathcal{L}_n(E)$ is called a linear n-set *over E.*

By the characterization of principal divisors, for $\ell \in \mathcal{L}_n(E)$, the *points* of ℓ are P_i for $i = 0, \ldots, n-1$ with

$$\mathrm{Div}(\ell) = (P_0) + \ldots + (P_{n-1}) - n(\mathcal{O})$$

and $P_0 + \ldots + P_{n-1} = \mathcal{O}$. Conversely, given such a collection of points, there is a corresponding linear n-set.

Definition 4.1.2. *The* linear n-set sum *operation is:*

$$\boxplus : \ \mathcal{L}_n(E) \times \mathcal{L}_n(E) \to \mathcal{L}_{n^2}(E)$$

with $u \boxplus v$ being a normalized function satisfying:

$$\begin{aligned}
\mathrm{Div}(u) =& (P_0) + \ldots + (P_{n-1}) - n(\mathcal{O}) \\
\mathrm{Div}(v) =& (Q_0) + \ldots + (Q_{n-1}) - n(\mathcal{O}) \\
\mathrm{Div}(u \boxplus v) =& \sum_{i,j \in \{0,\ldots,n-1\}} (P_i + Q_j) - n^2(\mathcal{O})
\end{aligned}$$

We then define a *generic linear n-set multiplication algorithm* to be an operation chain in $\mathbb{F}(E)$ that starts with an element of $\mathcal{L}_n(E)$ and where we allow the following operations:

- Multiplication between elements in the operation chain:

$$\cdot : \ \mathcal{L}_m(E) \times \mathcal{L}_n(E) \to \mathcal{L}_{m+n}(E)$$

- Division between elements in the operation chain, provided the result has no poles away from $\mathcal{O}$. That is, the partial function:

$$\div : \ \mathcal{L}_{m+n}(E) \times \mathcal{L}_m(E) \to \mathcal{L}_n(E)$$

- The linear n-set sum operation:

$$\boxplus : \ \mathcal{L}_m(E) \times \mathcal{L}_n(E) \to \mathcal{L}_{mn}(E)$$

- The negation map $\boxminus = -1\boxdot : \ \mathcal{L}_n(E) \to \mathcal{L}_n(E)$:

$$\begin{aligned}
\mathrm{Div}(u) =& (P_0) + \ldots + (P_{n-1}) - n(\mathcal{O}) \\
\mathrm{Div}(\boxminus u) =& (-P_0) + \ldots + (-P_{n-1}) - n(\mathcal{O})
\end{aligned}$$

4.1.1 Generalizing to Abelian Groups

In section 4.3, we will generalize generic linear set multiplication to an arbitrary abelian group G instead of E. Since we do not have an algebraic structure on G a priori, we work with the collection of points in a linear n-set directly, rather than a function that encapsulates them. So rather than working with $\mathcal{L}_n(E)$, we work with $\mathcal{L}_n^\bullet(E)$:

$$\mathcal{L}_n^\bullet(E) = \{(P_0) + (P_1) + \ldots + (P_{n-1}) \in \mathbb{Z}[E] \ : \ P_0 + P_1 + \ldots + P_{n-1} = \mathcal{O}\}$$

We remark that there is a bijection between $\mathcal{L}_n(E)$ and $\mathcal{L}_n^\bullet(E)$, with $\ell \mapsto \mathrm{Div}(\ell) + n(\mathcal{O})$. This is because the condition that $P_0 + \ldots + P_{n-1} = \mathcal{O}$ means that $(P_0) + \ldots + (P_{n-1}) - n(\mathcal{O})$ is a principal divisor, and ℓ can be recovered as the normalized function with that divisor. Furthermore, under this bijection, the $\boxplus$ operation translates to multiplication in the group ring $\mathbb{Z}[E]$.

The map $k\boxdot$ on $\mathcal{L}_n(E)$ then corresponds to the k-power map on $\mathcal{L}_n^\bullet(E)$:

$$\pi_k : \ (P_0) + \ldots + (P_{n-1}) \mapsto (kP_0) + \ldots + (kP_{n-1})$$

In these terms, it is now simple to generalize line multiplication to n points in an arbitrary abelian group. This will be done in section 4.3. A very convenient observation is that in this setting a "generic" algorithm to compute π_k is simply an operation chain in $\mathbb{Z}[E]$ using the ring operations.

4.2 Generic Linear 2-Set Multiplication

Here we present the simplest non-trivial case of generic linear n-set multiplication on E. So we develop the linear 2-set multiplication algorithm, which computes the map $k\boxdot$ on $\mathcal{L}_2(E)$. This is essentially equivalent to Montgomery's x-only point multiplication operation from section 2.7.

Non-trivial linear 2-sets correspond to x-coordinates for E in Weierstrass form:

$$\mathcal{L}_2(E) = \{\chi(x, y) = x - x_P \in \mathbb{F}(E) \ : \ P \in E \backslash \{\mathcal{O}\}\} \cup \{1\}$$

and we have $\mathrm{Div}(\chi) = (P) + (-P) - 2(\mathcal{O})$. Our goal is to compute the function

$$(k \boxdot \chi)(x, y) = x - x_{kP}.$$

Note that $k \boxdot \chi = (-k) \boxdot \chi$, which simply states that x-coordinates are invariant under negation.

The doubling formula for $\chi(x,y) = x - x_P$ is:

$$\begin{aligned}(2 \boxdot \chi)(x,y) =& (x - x_{2P}) \\ =& x + 2x_P - \left(\frac{a + 3x_P^2}{2y_P}\right)^2 \\ =& x - \frac{(a+3x_P^2)^2 - 8x_P(b + ax_P + x_P^3)}{4(b + ax_P + x_P^3)} \\ =& x - \frac{a^2 - 8bx_P - 2ax_P^2 + x_P^4}{4(b + ax_P + x_P^3)}\end{aligned}$$

The linear 2-set addition operation between $\chi_0(x,y) = x - x_{P_0}$ and $\chi_1(x,y) = x - x_{P_1}$ gives a function with the following divisor (when $P_0 \neq \pm P_1$):

$$\begin{aligned}\mathrm{Div}(\chi_0 \boxplus \chi_1) =& (P_0 + P_1) + (P_0 - P_1) + (-P_0 + P_1) + (-P_0 - P_1) - 4(\mathcal{O}) \\ =& ((P_0 + P_1) + (-P_0 - P_1) - 2(\mathcal{O})) + ((P_0 - P_1) + (-P_0 + P_1) - 2(\mathcal{O}))\end{aligned}$$

and so we have

$$(\chi_0 \boxplus \chi_1)(x,y) = (x - x(P_0 + P_1))(x - x(P_0 - P_1)). \tag{4.1}$$

Note that this corresponds to the fact that although we cannot distinguish $x(P_0+P_1)$ from $x(P_0 - P_1)$ given only $x(P_0)$ and $x(P_1)$, we can determine symmetric polynomials in those quantities.

We will now explicitly compute a formula for $\chi_0 \boxplus \chi_1$ in the case $P_0 \neq \pm P_1$:

$$\begin{aligned}&(x - x_{P_0}) \boxplus (x - x_{P_1}) = (x - x_{P_0+P_1})(x - x_{P_0-P_1}) \\ =& \left(x + x_{P_0} + x_{P_1} - \left(\frac{y_{P_0} - y_{P_1}}{x_{P_0} - x_{P_1}}\right)^2\right)\left(x + x_{P_0} + x_{P_1} - \left(\frac{y_{P_0} + y_{P_1}}{x_{P_0} - x_{P_1}}\right)^2\right) \\ =& (x + x_{P_0} + x_{P_1})^2 - (x + x_{P_0} + x_{P_1})\frac{2y_{P_0}^2 + 2y_{P_1}^2}{(x_{P_0} - x_{P_1})^2} + \frac{(y_{P_0}^2 - y_{P_1}^2)^2}{(x_{P_0} - x_{P_1})^4} \\ =& (x + x_{P_0} + x_{P_1})^2 - 2(x + x_{P_0} + x_{P_1})\frac{2b + a(x_{P_0} + x_{P_1}) + x_{P_0}^3 + x_{P_1}^3}{(x_{P_0} - x_{P_1})^2} + \frac{(a + x_{P_0}^2 + x_{P_0}x_{P_1} + x_{P_1}^2)^2}{(x_{P_0} - x_{P_1})^2}\end{aligned}$$

It turns out to be quite simple to perform an operation chain to compute $\boxdot k$. The following formula will give us all of the needed ingredients. Given $m, n \in \mathbb{Z}$, we use equation (4.1) to obtain:

$$\begin{aligned}\mathrm{Div}(\chi) =& (P) + (-P) - 2(\mathcal{O}) \\ (m \boxdot \chi) \boxplus (n \boxdot \chi) =& ((m+n) \boxdot \chi) \cdot ((m-n) \boxdot \chi)\end{aligned} \tag{4.2}$$

Just as for x-only point multiplication, this is interpreted as follows: given $m \boxdot \chi, n \boxdot \chi$, we cannot determine $(m+n) \boxdot \chi$, since we cannot distinguish it from $(m-n) \boxdot \chi$ in general. That said, we can determine symmetric combinations of the two possible outcomes.

In our generic linear 2-set multiplication algorithm, we will use (4.2) to perform the "addition" step. Again, the key will be to assume knowledge of $m \boxdot \chi, n \boxdot \chi, (m-n) \boxdot \chi$ to determine $(m+n) \boxdot \chi$, just as is the x-only algorithm:

$$((m+n) \boxdot \chi) = \frac{(m \boxdot \chi) \boxplus (n \boxdot \chi)}{((m-n) \boxdot \chi)}$$

Specifically, if we take $m = n+1$, we get:

$$(2n+1) \boxdot \chi = \frac{(n \boxdot \chi) \boxplus ((n+1) \boxdot \chi)}{\chi}$$

With this formula and the doubling formula, we can now perform a Montgomery ladder operation chain. Suppose we want to compute $k \boxdot \chi$. The idea is that at each step of our operation chain, we will keep track of two consecutive values $(i \boxdot \chi, (i+1) \boxdot \chi)$, where i will be a truncated binary expansion of k. From that pair, we can compute either $(2i \boxdot \chi, (2i+1) \boxdot \chi)$ or $((2i+1) \boxdot \chi, (2i+2) \boxdot \chi)$:

$$\begin{aligned}
(2i) \boxdot \chi &= 2 \boxdot (i \boxdot \chi) \\
(2i+1) \boxdot \chi &= \frac{(i \boxdot \chi) \boxplus ((i+1) \boxdot \chi)}{\chi} \\
(2i+2) \boxdot \chi &= 2 \boxdot ((i+1) \boxdot \chi)
\end{aligned}$$

Hence by choosing the next bit of k, we can progressively compute these pairs until we get $(k \boxdot \chi, (k+1) \boxdot \chi)$, and we are done. Specifically, we progressively compute $(i \boxdot \chi, (i+1) \boxdot \chi)$ with i being a binary truncation of k to its most significant bits. This operation chain is called the Montgomery ladder, since it is essentially the same as that in algorithm 5.

Algorithm 5: Algorithm to compute $k\boxdot : \mathcal{L}_2^\bullet(E) \to \mathcal{L}_2^\bullet(E)$

Input : $\chi = x - x_P$ and a positive integer k with binary representation $k = k_{b-1} \dots k_1 k_0$.

Output: $k \boxdot \chi = x - x_{kP}$

```
r, s ← χ, 2 ⊡ χ;
for i ← b − 2 to 0 do
    if k_i = 0 then
        r, s ← 2 ⊡ r, (r ⊞ s)/χ;
    else
        r, s ← (r ⊞ s)/χ, 2 ⊡ s;
    end
end
return r;
```

For example, to compute $13 \cdot \chi$, we write $13 = 1101_2$ in binary and iteratively compute:

$$\begin{aligned}
1 : \quad & (1 \boxdot \chi, 2 \boxdot \chi) = (\chi, 2 \boxdot \chi) \\
11 : \quad & (3 \boxdot \chi, 4 \boxdot \chi) = \left(\frac{\chi \boxplus (2 \boxdot \chi)}{\chi}, 2 \boxdot (2 \boxdot \chi) \right) \\
110 : \quad & (6 \boxdot \chi, 7 \boxdot \chi) = \left(2 \boxdot (3 \boxdot \chi), \frac{(3 \boxdot \chi) \boxplus (4 \boxdot \chi)}{\chi} \right) \\
1101 : \quad & (13 \boxdot \chi, 14 \boxdot \chi) = \left(\frac{(6 \boxdot \chi) \boxplus (7 \boxdot \chi)}{\chi}, 2 \boxdot (7 \boxdot \chi) \right)
\end{aligned}$$

An important note is that the above algorithm calculates more than is necessary. In particular, consider the operation $\boxplus$ between χ_0 and χ_1:

$$(x - x_{P_0}) \boxplus (x - x_{P_1}) = x^2 - (x_{P_0+P_1} + x_{P_0-P_1})x + x_{P_0+P_1} x_{P_0-P_1}.$$

This computes both the sum $x_{P_0+P_1} + x_{P_0-P_1}$ and the product $x_{P_0+P_1} x_{P_0-P_1}$. The x-only multiplication algorithm from section 2.7 improves on this, since we only keep track of $x_{P_0+P_1} + x_{P_0-P_1}$ in the addition step, and the other coefficient $x_{P_0+P_1} x_{P_0-P_1}$ is made superfluous. A similar situation arose for linear 3-set generic multiplication, as we saw in section 3.9.

4.3 Generic Linear Multiplication

In this section, we explain how the generic line multiplication algorithm can be used in a more general setting. Suppose that G is a multiplicative abelian group, with identity

element denoted 1_G. In this context we will use the same terminology of *linear sets* to denote elements of the following:

Definition 4.3.1. *For a positive integer n, elements of the set*

$$\mathcal{L}_n^\bullet(G) = \{(g_0) + (g_1) + \ldots + (g_{n-1}) \in \mathbb{Z}[G] \ : \ g_0 \cdot g_1 \cdot \ldots \cdot g_{n-1} = 1_G\}$$

are called linear n-sets *over G.*

For $k \in \mathbb{Z}$ and $(g_0)+(g_1)+\ldots+(g_{n-1}) \in \mathcal{L}_n^\bullet(G)$, the k-power map *on $\mathcal{L}_n^\bullet(G)$ is defined by:*

$$\pi_k((g_0) + (g_1) + \ldots + (g_{n-1})) = (g_0^k) + (g_1^k) + \ldots + (g_{n-1}^k)$$

An element $(g_0) + (g_1) + \ldots + (g_{n-1}) \in \mathcal{L}_n^\bullet(G)$ will be interpreted as an element g of G for which we only have partial information; it is only known to be one of $g_0, g_1, \ldots, g_{n-1}$. Note then that for $k \in \mathbb{Z}$, we have $g_0^k \cdot \ldots \cdot g_{n-1}^k = 1_G$, and so our goal is to compute the same partial information about g^k.

In this setting, a *generic linear n-set power algorithm* computes the map π_k, with restrictions on the operations that are allowed. In fact, the restrictions are simpler to state in this case: we are restricted to using multiplication in the group ring $\mathbb{Z}[G]$, element-wise group inversion π_{-1}. Explicitly, the following operations are allowed in the operation chain:

- Addition between elements in the operation chain.
- Subtraction between elements in the operation chain, provided the result has no negative coefficients.
- Multiplication between elements in the operation chain.
- The -1-power map: $(g_0) + \ldots + (g_{n-1}) \mapsto (g_0^{-1}) + \ldots + (g_{n-1}^{-1})$

4.3.1 Generic Line Multiplication

Note that for the case $n = 3$, algorithm 3 can be directly translated into this setting. The $\boxplus$ operation in $\mathcal{L}_3(E)$ corresponds to the ring multiplication in $\mathbb{Z}[G]$. Note that we identify $\mathbb{Z}$ with a subset of $\mathbb{Z}[G]$ via the embedding $n \mapsto n(1_G)$. Although we have not done so explicitly, we can also easily translate algorithm 5 into a generic linear 2-set power algorithm.

Algorithm 6: Recursive Algorithm to Compute $\pi_k : \mathcal{L}_3^\bullet(G) \to \mathcal{L}_3^\bullet(G)$

Input : $u = (g_0) + (g_1) + (g_2) \in \mathcal{L}_3^\bullet(G)$ and a positive integer k with binary representation $k = k_b \dots k_1 k_0$.

Output: $\pi_k(u) = (g_0^k) + (g_1^k) + (g_2^k)$

$r, s, t \leftarrow 3, u, u^2 - 2\pi_{-1}(u)$;
for $i \leftarrow b - 1$ **to** 0 **do**
  if $k_i = 0$ **then**
    $r, s, t \leftarrow r^2 - 2\pi_{-1}(r), rs - \pi_{-1}(u)\pi_{-1}(s) + \pi_{-1}(t), s^2 - 2\pi_{-1}(s)$;
  else
    $r, s, t \leftarrow s^2 - 2\pi_{-1}(s), st - u\pi_{-1}(s) + \pi_{-1}(r), t^2 - 2\pi_{-1}(t)$;
  end
end
if $k_i = 0$ **then**
  return r;
else
  return s;
end

4.3.2 Breakdown

We will now translate the concepts from section 3.8 to our new situation. The explanations will be terse, because the explanations from the elliptic curve case can be repeated here with little modification.

Definition 4.3.2. *For $u \in \mathcal{L}_3^\bullet(G)$ with points in cyclic order g_0, g_1, g_2, we define:*

$$u_{k,\ell} := (g_0^k g_1^\ell) + (g_1^k g_2^\ell) + (g_2^k g_0^\ell) \in \mathcal{L}_3^\bullet(G)$$

and $u_k = u_{k,0} = \pi_k(u)$.

In analogy with the decomposition of the line sum function, we now have

$$u_k \cdot u_\ell = u_{k+\ell} + u_{k,\ell} + u_{\ell,k}$$

As a consequence of the relation $g_0 g_1 g_2 = 1$, there are multiple representations of $u_{k,\ell}$:

$$u_{k,\ell} = u_{-\ell,k-\ell} = u_{\ell-k,-k} \tag{4.3}$$

and thus the "bad" lines $u_{k,\ell}, u_{\ell,k}$ can be eliminated as before:

$$\begin{aligned} u_k \cdot u_\ell &= u_{k+\ell} + u_{k,\ell} + u_{\ell,k} \\ u_{-\ell} \cdot u_{k-\ell} &= u_{k-2\ell} + u_{k,\ell} + u_{\ell,k} \\ u_{\ell-k} \cdot u_{-k} &= u_{\ell-2k} + u_{k,\ell} + u_{\ell,k} \end{aligned}$$

from which:

$$u_{k+\ell} = u_{k-2\ell} + u_k \cdot u_\ell - u_{-\ell} \cdot u_{k-\ell} \tag{4.4}$$
$$= u_{\ell-2k} + u_k \cdot u_\ell - u_{\ell-k} \cdot u_{-k} \tag{4.5}$$

This is the formula that forms the basis for algorithm 6.

In particular, the modified Montgomery ladder can be understood in terms of the following:

$$u_{2k} = u_k^2 - 2u_{-k} \tag{4.6}$$
$$u_{2k+1} = u_{k+(k+1)} = u_{-k-2} + u_k u_{k+1} - u_{-1} u_{-k-1} \tag{4.7}$$
$$u_{2k+2} = u_{k+1}^2 - 2u_{-k-1} \tag{4.8}$$
$$u_{2k+3} = u_{(k+2)+(k+1)} = u_{-k} + u_{k+1} u_{k+2} - u_1 u_{-k-1} \tag{4.9}$$
$$u_{2k+4} = u_{k+2}^2 - 2u_{-k-2} \tag{4.10}$$

4.4 Linear Sets over a Field

Now we consider implementing generic line multiplication for $G = \mathbb{F}^\times$ with $\mathbb{F}$ being an arbitrary field. Of course we could simply use algorithm 6 directly. But rather than working over $\mathbb{Z}[\mathbb{F}^\times]$, we would like to work in $\mathbb{F}$ using field operations.

Then to encode a linear n-set u:

$$u = (g_0) + (g_1) + \ldots + (g_{n-1}) \in \mathcal{L}_n^\bullet(\mathbb{F}^\times)$$

we note that there is a polynomial function in $\mathbb{F}[z]$ that vanishes exactly at $g_0, g_1, \ldots, g_{n-1}$. Moreover, it is unique up to a scalar factor. We choose the polynomial whose lowest degree non-zero coefficient is 1; equivalently, we normalize the polynomial at ∞ with respect to the uniformizer z^{-1}.

More precisely, we let $\rho_u(z) \in \mathbb{F}[z]$ denote the normalized function whose zeroes correspond to u:

$$\begin{aligned} u &= (g_0) + (g_1) + \ldots + (g_{n-1}) \in \mathcal{L}_n^\bullet(\mathbb{F}^\times) \\ \rho_u(z) &= (g_0 - z)(g_1 - z)\cdots(g_{n-1} - z) \\ &= 1 - (g_0^{-1} + \ldots + g_{n-1}^{-1})z + \ldots + (g_0 + \ldots + g_{n-1})(-z)^{n-1} + (-z)^n \end{aligned}$$

We note that since we are in a field, we can recover u by taking the roots of this polynomial, with multiplicities. The addition operation in $\mathbb{Z}[G]$ translates into multiplication of functions:

$$\rho_{u+v} = \rho_u \cdot \rho_v.$$

The multiplication in $\mathbb{Z}[G]$ can be expressed as a resultant:

$$\begin{aligned} \rho_{u\cdot v}(z) &= \prod_{i,j}(g_i h_j - z) \\ &= \prod_{i,j}(g_i - \frac{z}{h_j}) \\ &= \mathrm{Res}_x(\rho_u(x), x^n \rho_v(z/x)) \end{aligned}$$

4.4.1 Generic Line Multiplication Over a Field

Now we consider the $n = 3$ case of line multiplication in $\mathcal{L}_3^\bullet(\mathbb{F}^\times)$, while working with the arithmetic in $\mathbb{F}$ directly. So we will translate algorithm 6. Then we will see how to make simple improvements; these will be useful to us since there will be analogues for elliptic curve line multiplication.

An element $u = (g_0) + (g_1) + (g_2) \in \mathcal{L}_3^\bullet(\mathbb{F}^\times)$ is encoded as ρ_u:

$$\begin{aligned}\rho_u(z) =& (g_0 - z)(g_1 - z)(g_2 - z)\\ =& 1 - t(u)z + s(u)z^2 - z^3 \in \mathbb{F}[z]\end{aligned}$$

where $s(u) = g_0 + g_1 + g_2 \in \mathbb{F}$ and

$$t(u) = g_0g_1 + g_0g_2 + g_1g_2 = g_0^{-1} + g_1^{-1} + g_2^{-1} = s(\pi_{-1}(u)).$$

The addition operation in $\mathbb{Z}[G]$ simply translates into multiplication of functions, as noted earlier: $\rho_{u+v} = \rho_u \cdot \rho_v$. The multiplication in $\mathbb{Z}[G]$ is the following when $\rho_u(z) = 1 - cz + dz^2 - z^3$ and $\rho_v(z) = 1 - ez + fz^2 - z^3$:

$$\begin{aligned}\rho_{u\cdot v}(z) =& \prod_{i,j}(g_ih_j - z) = \mathrm{Res}_x(\rho_u(x), x^n\rho_v(z/x))\\ =& \mathrm{Res}_x(1 - cx + dx^2 - x^3, z^3 - fxz^2 + ex^2z - x^3)\\ =& 1 - cez + \left(c^2f + de^2 - 2df\right)z^2 - \left(c^3 + e^3 + cdef - 3cd - 3ef + 3\right)z^3\\ &+ \left(c^2de + ce^2f - ce - 2cf^2 - 2d^2e + d^2f^2\right)z^4\\ &+ \left(-c^2e^2 + 2c^2f - cd^2f + 2de^2 - def^2 + df\right)z^5\\ &+ \left(cdef - 3cd + d^3 - 3ef + f^3 + 3\right)z^6\\ &+ \left(2ce - cf^2 - ed^2\right)z^7 + dfz^8 - z^9\end{aligned} \tag{4.11}$$

The 2-power operation is simple to calculate:

$$\begin{aligned}\rho_{\pi_2(u)}(z) =& \prod_{i\in\{0,1,2\}}(g_i^2 - z)\\ =& \mathrm{Res}_x(1 - cx + dx^2 - x^3, x^2 - z)\\ =& 1 - (c^2 - 2d)z + (d^2 - 2c)z^2 - z^3\end{aligned}$$

Note that we can calculate $\rho_{\pi_k(u)}(z) = \mathrm{Res}_x(1 - cx + dx^2 - x^3, x^k - z)$ more generally, using general resultant algorithms, but we will not be exploring this idea, since our main motivation is to have a "toy" model of line multiplication.

So now we are ready to translate algorithm 6! Unfortunately, this is quite messy already. It involves calculating $\rho_{u\cdot v}$ twice for each "multiplication" step, and then we need to do multiplication and division with these polynomials of degree 9. It turns out that we can do much better, and we only need to calculate a small number of the coefficients of $\rho_{u\cdot v}$.

4.4.2 Improved Line Multiplication Over a Field

Suppose that we have a group homomorphism $\psi : G \to \mathbb{F}^\times$. Then we get a ring homomorphism $\mathbb{Z}[G] \to \mathbb{F}$ with $(g) \mapsto \psi(g)$. This allows us to interpret the formulas from $\mathbb{Z}[G]$ in terms of the arithmetic in $\mathbb{F}$. So in this vein, we define $s_{k,\ell}$ to be the image of $u_{k,\ell} \in \mathcal{L}_3^\bullet(\mathbb{F}^\times)$ under the identity homomorphism:

Definition 4.4.1. *For a line $u \in \mathcal{L}_3^\bullet(\mathbb{F}^\times)$ with points g_0, g_1, g_2 in cyclic order, we define:*

$$\begin{aligned} s_{k,\ell} =& g_0^k g_1^\ell + g_1^k g_2^\ell + g_2^k g_0^\ell \in \mathbb{F} \\ s_k =& s_{k,0} = g_0^k + g_1^k + g_2^k \in \mathbb{F} \end{aligned}$$

Recall the encoding of $u_{k,\ell}$, which can be expressed in terms of the above notation:

$$\begin{aligned} \rho_{u_{k,\ell}}(z) =& (g_0^k g_1^\ell - z)(g_1^k g_2^\ell - z)(g_2^k g_0^\ell - z) \\ =& 1 - \left(g_0^{-k} g_1^{-\ell} + g_1^{-k} g_2^{-\ell} + g_2^{-k} g_0^{-\ell}\right) z + \left(g_0^k g_1^\ell + g_1^k g_2^\ell + g_2^k g_0^\ell\right) z^2 - z^3 \\ =& 1 - s_{-k,-\ell} z + s_{k,\ell} z^2 - z^3 \end{aligned}$$

So we can encode $u_{k,\ell}$ as the pair of coefficients $(s_{k,\ell}, s_{-k,-\ell})$ of $\rho_{u_{k,\ell}}$.

By the aforementioned principle, we have that for any $k, \ell \in \mathbb{Z}$,

$$\begin{aligned} s_{k+\ell} &= s_{k-2\ell} + s_k \cdot s_\ell - s_{-\ell} \cdot s_{k-\ell} \\ &= s_{\ell-2k} + s_k \cdot s_\ell - s_{\ell-k} \cdot s_{-k} \end{aligned}$$

Alternatively, a simple calculation verifies this directly. This allows us to run an algorithm very similar to the generic algorithm directly. Namely, if we know $s_{\pm k}, s_{\pm(k+1)}, s_{\pm(k+2)}$, then we can obtain:

$$s_{\pm 2k} = s_{\pm k}^2 - 2 s_{\mp k} \tag{4.12}$$

$$s_{\pm(2k+1)} = s_{\mp(k+2)} + s_{\pm k} s_{\pm(k+1)} - s_{\mp 1} s_{\mp(k+1)} \tag{4.13}$$

$$s_{\pm(2k+2)} = s_{\pm(k+1)}^2 - 2 s_{\mp(k+1)} \tag{4.14}$$

$$s_{\pm(2k+3)} = s_{\mp k} + s_{\pm(k+1)} s_{\pm(k+2)} - s_{\pm 1} s_{\mp(k+1)} \tag{4.15}$$

$$s_{\pm(2k+4)} = s_{\pm(k+2)}^2 - 2 s_{\mp(k+2)} \tag{4.16}$$

Algorithm 7 is a vast improvement over the generic algorithm itself, since that involved computing $\rho_{u \cdot v}$ multiple times. Note that in there are approximately $\log_2(k)$ steps in the operation chain, and each step involves 4 squarings and 4 multiplications.

Algorithm 7: Algorithm to Compute $\pi_k : \mathcal{L}_3^\bullet(\mathbb{F}^\times) \to \mathcal{L}_3^\bullet(\mathbb{F}^\times)$ Using $\mathbb{F}$ Arithmetic.

Input : $c, d \in \mathbb{F}$ (representing $\rho_u(z) = 1 - cz + dz^2 - z^3$) and a positive integer k with binary representation $k = k_b \dots k_1 k_0$ and $k_b = 1$.

Output: $(g_0^{-k} + g_1^{-k} + g_2^{-k}, g_0^k + g_1^k + g_2^k)$, where $(g_0^{-1} + g_1^{-1} + g_2^{-1}, g_0 + g_1 + g_2) = (c, d)$

$r, s, t \leftarrow 3, c, c^2 - 2d$;
$\rho, \sigma, \tau \leftarrow 3, d, c^2 - 2c$;
for $i \leftarrow b - 1$ **to** 0 **do**
    if $k_i = 0$ **then**
        $r, s, t \leftarrow r^2 - 2\rho, rs - c\sigma + \tau, s^2 - 2\sigma$;
        $\rho, \sigma, \tau \leftarrow \rho^2 - 2r, \rho\sigma - ds + t, \sigma^2 - 2s$;
    else
        $r, s, t \leftarrow s^2 - 2\sigma, st - d\sigma + \rho, t^2 - 2\tau$;
        $\rho, \sigma, \tau \leftarrow \sigma^2 - 2s, \sigma\tau - cs + r, \tau^2 - 2t$;
    end
end
if $k_i = 0$ **then**
    return r, ρ;
else
    return s, σ;
end

For example, to calculate $s_{\pm 25}$ given $s_{\pm 1}$, we write $25 = 11001_2$ in binary and iteratively compute:

$$
\begin{aligned}
0: \qquad (s_0, s_1, s_2) &= \left(3, s_1, s_1^2 - 2s_{-1}\right) \\
(s_0, s_{-1}, s_{-2}) &= \left(3, s_{-1}, s_{-1}^2 - 2s_1\right) \\
10: \qquad (s_2, s_3, s_4) &= \left(s_2, s_1 s_2 - s_1 s_{-1} + 3, s_2^2 - 2s_{-2}\right) \\
(s_{-2}, s_{-3}, s_{-4}) &= \left(s_{-2}, s_{-1} s_{-2} - s_1 s_{-1} + 3, s_{-2}^2 - 2s_2\right) \\
110: \qquad (s_6, s_7, s_8) &= \left(s_3^2 - 2s_{-3}, s_3 s_4 - s_1 s_{-3} + s_{-2}, s_4^2 - 2s_{-4}\right) \\
(s_{-6}, s_{-7}, s_{-8} &= \left(s_{-3}^2 - 2s_3, s_{-3} s_{-4} - s_{-1} s_3 + s_2, s_{-4}^2 - 2s_4\right) \\
1100: \qquad (s_{12}, s_{13}, s_{14}) &= \left(s_6^2 - 2s_{-6}, s_6 s_7 - s_1 s_{-6} + s_{-5}, s_7^2 - 2s_{-7}\right) \\
(s_{-12}, s_{-13}, s_{-14}) &= \left(s_{-6}^2 - 2s_6, s_{-6} s_{-7} - s_{-1} s_6 + s_5, s_{-7}^2 - 2s_7\right) \\
11000: \qquad (s_{24}, s_{25}, s_{26}) &= \left(s_{12}^2 - 2s_{-12}, s_{12} s_{13} - s_1 s_{-12} + s_{-11}, s_{13}^2 - 2s_{-13}\right) \\
(s_{-24}, s_{-25}, s_{-26}) &= \left(s_{-12}^2 - 2s_{12}, s_{-12} s_{-13} - s_{-1} s_{12} + s_{11}, s_{-13}^2 - 2s_{13}\right)
\end{aligned}
$$

And we have obtained $s_{\pm 25}$.

4.5 Application: Cipolla's algorithm

In this section, we propose an application of line multiplication in a square root finding algorithm. This algorithm is a modification of Cipolla's square root finding algorithm over a finite field of odd order. In particular, we use our operation to implement an exponentiation in a quadratic extension of a finite field. For some context about the general problem of finding the square root of $n \in \mathbb{F}_p$, see for example section 11.1.5 of [3].

The idea for Cipolla's algorithm is to choose $\alpha \in \mathbb{F}_{p^2} \backslash \mathbb{F}_p$ with norm n. Then the conjugates of α over $\mathbb{F}_p$ are α, α^p, so their product gives the norm: $\alpha \cdot \alpha^p = n$. Equivalently, we have $\alpha^{p+1} = n$, so we can find a square root simply by raising α to the power of $\frac{p+1}{2}$:

$$\left(\alpha^{\frac{p+1}{2}}\right)^2 = \alpha \cdot \alpha^p = N(\alpha) = n$$

Note that such an α will be a root of an irreducible $x^2 - ax + n \in \mathbb{F}_p[x]$ for some $a \in \mathbb{F}_p$. So we approach this problem by choosing $a \in \mathbb{F}_p$ randomly, and checking if $x^2 - ax + n$ is irreducible in $\mathbb{F}_p[x]$; concretely, we want $a^2 - 4n$ to be a non-square, or equivalently

$$\left(\frac{a^2 - 4n}{p}\right) = -1$$

for the Legendre symbol. If this condition does not hold, we choose another a randomly, and check again; since half of $\mathbb{F}_p^\times$ consists of non-squares, it should not take long before an appropriate a is found.

Once we have this value for a, we simply define $\alpha \in \mathbb{F}_{p^2} \backslash \mathbb{F}_p$ to be a root of $x^2 - ax + n$. Then as mentioned earlier, the other conjugate root is α^p, so $\alpha^{p+1} = n$, and thus $\alpha^{\frac{p+1}{2}}$ is a square root of n. In the usual presentation of Cipolla's algorithm, this is calculated using a recursion.

We define $r_k, s_k \in \mathbb{F}_p$ to be the coefficients such that

$$\alpha^k = r_k + s_k \alpha.$$

Then since $\alpha^2 = a\alpha - n$, we can equivalently define r_k, s_k via the following recursion:

$$\begin{aligned}(r_0, s_0) &= (1, 0)\\ (r_{i+1}, s_{i+1}) &= (-ns_i, r_i + as_i)\end{aligned}$$

More efficiently, we can deduce a doubling formula:

$$\begin{aligned}\alpha^{2k} &= (r_k + s_k\alpha)^2 = r_k^2 + 2r_k s_k \alpha + s_k^2 \alpha^2\\ &= (r_k^2 - ns_k^2) + (2r_k s_k + as_k^2)\alpha\\ (r_{2k}, s_{2k}) &= \left(r_k^2 - ns_k^2, (2r_k + as_k)s_k\right)\end{aligned}$$

Combining this with the previous formula, we get a "double plus one" formula:

$$\begin{aligned}(r_{2k+1}, s_{2k+1}) =& (-ns_{2k}, r_{2k} + as_{2k}) \\ =& \left(-n(2r_k + as_k)s_k, (r_k^2 - ns_k^2) + a(2r_k s_k + as_k^2\right) \\ =& \left(-n(2r_k + as_k)s_k, r_k^2 + 2ar_k s_k + (a^2 - n)s_k^2+\right) \\ =& \left(-n(2r_k + as_k)s_k, (r_k + as_k)^2 - ns_k^2\right)\end{aligned}$$

These two formulas allow us to perform an operation chain to compute $\alpha^{\frac{p+1}{2}}$, which will give us a square root of n. This is presented in algorithm 8.

Algorithm 8: Cipolla's Algorithm to Compute Square Root

Input : An odd prime p and an integer n satisfying $\left(\frac{n}{p}\right) = 1$; that is, a square in $\mathbb{F}_p$.

Output: A square root of $n \in \mathbb{F}_p$

```
a ← Random(F_p);
while ((a^2 − 4n)/p) ≠ −1 do
    a ← Random(F_p);
end
r, s ← 1, 0;
for i ← b − 1 to 0 do
    if k_i = 0 then
        r, s ← r^2 − ns^2, (2r + as)s;
    else
        r, s ← −n(2r + as)s, (r + as)^2 − ns^2;
    end
end
return r;
```

Note that this calculation involves roughly $5\log_2 n$ multiplications for the main loop.

4.5.1 Cipolla Using Line Multiplication

Now we will explain how we use line multiplication to compute $\alpha^{\frac{p+1}{2}}$ in Cipolla's algorithm. The simplest approach is to take

$$\begin{aligned} u =&(\alpha) + (\alpha^p) + (\alpha^{-p-1}) \in \mathcal{L}_3^\bullet(\mathbb{F}_p^\times) \\ =&(\alpha) + (n/\alpha) + (1/n) \in \mathcal{L}_3^\bullet(\mathbb{F}_p^\times) \end{aligned}$$

Then we will calculate $\pi_{\frac{p+1}{2}}(u)$, noting that it contains $\sqrt{n} := \alpha^{\frac{p+1}{2}}$. In fact, we have:

Lemma 4.5.1.

$$\pi_{\frac{p+1}{2}}\left((\alpha) + (\alpha^p) + (\alpha^{-p-1})\right) = \left(\sqrt{n}\right) + \left(\sqrt{n}\right) + \left(\frac{1}{n}\right)$$

Proof. Recall that $\sqrt{n} = \alpha^{\frac{p+1}{2}}$ is in the base field $\mathbb{F}_p$. Hence it is fixed under the Frobenius automorphism, or equivalently

$$\alpha^{\frac{p+1}{2}} = \left(\alpha^{\frac{p+1}{2}}\right)^p = \alpha^{\frac{1}{2}p(p+1)}$$

From this, we get:

$$\begin{aligned} \pi_{\frac{p+1}{2}}(u) &= \left(\alpha^{\frac{1}{2}(p+1)}\right) + \left(\alpha^{\frac{1}{2}p(p+1)}\right) + \left(\alpha^{-\frac{1}{2}(p+1)^2}\right) \\ &= \left(\sqrt{n}\right) + \left(\sqrt{n}\right) + \left(\frac{1}{n}\right) \end{aligned}$$

□

So if we compute the coefficients of $u_{\frac{p+1}{2}}$, then we get:

$$\begin{aligned} 1 - s_{-\frac{p+1}{2}} z + s_{\frac{p+1}{2}} z^2 - z^3 &= \left(\sqrt{n} - z\right)^2 \left(\frac{1}{n} - z\right) \\ &= 1 - \left(n + \frac{2}{\sqrt{n}}\right) z + \left(\frac{1}{n} + 2\sqrt{n}\right) z^2 - z^3 \end{aligned}$$

and we can extract $\sqrt{n} = \frac{1}{2}\left(s_{\frac{p+1}{2}} - \frac{1}{n}\right)$.

Recall that the standard implementation of Cipolla's algorithm used roughly $5\log_2(n)$ multiplications. Our method requires roughly $8\log_2(n)$ multiplications, but there is room

for improvement. By adding a parameter to the above process, we can save one multiplication at each step of the operation chain. Note that while this does not make our algorithm competitive, it illustrates how extra degrees of freedom can be used to improve our operation chains.

We can achieve this improvement by adding a parameter $k \in \mathbb{F}_p^\times$:

$$\begin{aligned} u &= \left(\frac{\alpha}{k}\right) + \left(\frac{\alpha^p}{k}\right) + \left(\frac{k^2}{\alpha^{p+1}}\right) \in \mathcal{L}_3^\bullet(\mathbb{F}_p^\times) \\ \rho_u(z) &= \left(\frac{\alpha}{k} - z\right)\left(\frac{\alpha^p}{k} - z\right)\left(\frac{k^2}{\alpha^{p+1}} - z\right) \\ &= 1 - \left(\frac{n}{k^2} + \frac{ak}{n}\right) z + \left(\frac{a}{k} + \frac{k^2}{n}\right) z^2 - z^3 \\ &= 1 - \left(\frac{n^2 + ak^3}{k^2 n}\right) z + \left(\frac{an + k^3}{kn}\right) z^2 - z^3 \end{aligned}$$

Then we notice that this gives us some freedom in choosing the initial parameters c, d that appear in each step of algorithm 7. In particular, we can choose one of c, d to be 0, to save a multiplication at each step. To achieve this, notice that if we take $a = n^2b^3, k = -nb$, then

$$\left(\frac{\alpha}{k} - z\right)\left(\frac{\alpha^p}{k} - z\right)\left(\frac{k^2}{n} - z\right) = 1 - \left(\frac{1 - n^3b^6}{nb^2}\right) z - z^3$$

Then using the same process as earlier, we can recover $(\alpha/k)^{\frac{p+1}{2}} = \frac{\sqrt{n}}{k^{\frac{p+1}{2}}}$. Then we note that $k^{\frac{p+1}{2}} = k \cdot k^{\frac{p-1}{2}} = \pm k$, so $k\left((\alpha/k)^{\frac{p+1}{2}}\right) = \pm\sqrt{n}$ is a square root of n. Recall that we need the following condition:

$$\left(\frac{a^2 - 4n}{p}\right) = -1$$

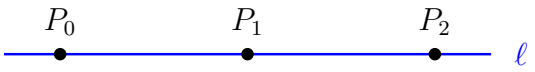
Experimentally, by choosing a random b, we get this approximately half of the time for $a = n^2b^3$.

Chapter 5

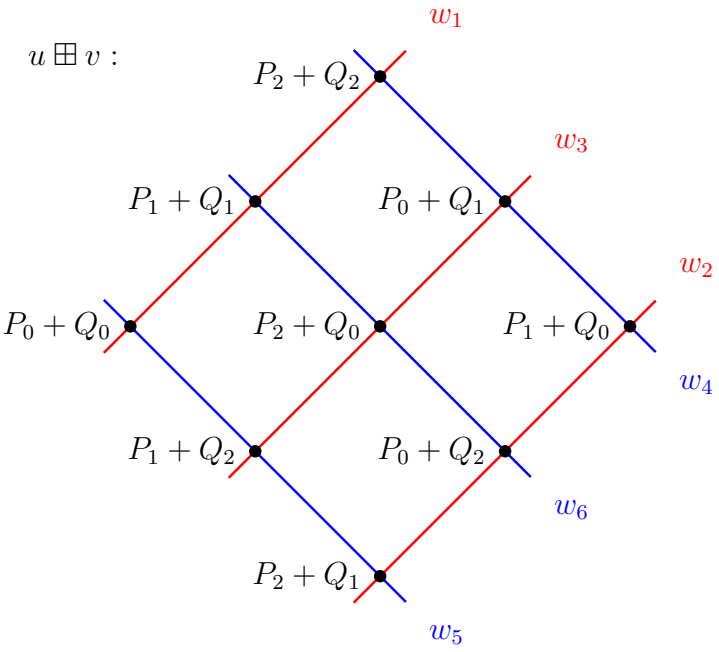
Diagrammatic Algebra

In this chapter, we introduce a diagrammatic algebra which gives a unified treatment of various forms of line multiplication, as well as other diagrams that emerge from the study of line addition. In chapter 6, we will supplement this algebra with a diagrammatic calculus that gives explicit tools for designing line multiplication algorithms. The diagrammatic algebra and calculus have a combinatorial flavor, with some inspiration coming from the theory of combinatorial species.

The diagrammatic calculus is based on *diagrams*, a term we use to refer to incidence structures on elliptic curve points, subject to certain constraints. We have already used *unlabeled line diagrams* to represent elements $\ell \in \mathcal{L}_3(E)$ in chapter 3:



This usage will be given a precise meaning in this chapter. We will generalize the scalar multiplication of lines to other diagrams. Then we will consider the structures that arise when we consider the addition of two diagrams with the same structure. This will generalize the linear sum diagram $u \boxplus v$ that we have previously considered:



This was introduced in section 3.10 as a natural structure on the possible sums between points/lines of $u, v \in \mathcal{L}_3(E)$ with respective points P_0, P_1, P_2 and Q_0, Q_1, Q_2. We will more generally define *nine point diagrams*, as well as other diagrams that combine multiple diagrams together. Nine point diagrams will be studied in greater depth in chapter 6.

Our diagrams will not be restricted to elliptic curves, but in fact will be defined over an arbitrary abelian group. Recall that this was also the case in chapter 4; but in contrast, the present chapter will take full advantage of this fact. For example, we use this to define homomorphisms between diagrams, and we will re-interpret nine point diagrams as lines of lines. In chapter 6, we will then revisit the diagrammatic algebra with elliptic curves in mind. We will develop a *diagrammatic calculus* of formulas that encode structural information about a diagram or between multiple related diagrams.

5.1 Label Structures

Recall that in chapter 3, we took a bottom-up approach: we first defined lines in $\mathcal{L}_3(E)$ with little structure, and then added structure to obtain cyclically oriented lines. In this chapter, we take a top-down approach, and start with *labeled lines*, where the points are all distinguished from one another. More generally, we define *labeled diagrams*, and then we will whittle down the structure to obtain more general diagrams suited to our needs.

To do this, we will borrow some concepts and terminology from discrete geometry. The underlying structure of a labeled diagram is a finite incidence structure; it is from this

structure that the *labels* will be taken. Since incidence structures normally have "points" and "lines", we will avoid a conflict of terminology by emphasizing their roles as labels:

Definition 5.1.1. *An* incidence structure $\mathfrak{D}$ *consists of a set* $\mathfrak{P}$ *of* point labels*, a set* $\mathfrak{L}$ *of* line labels*, and an* incidence relation $\mathfrak{I} \subseteq \mathfrak{P} \times \mathfrak{L}$*.*

A line structure *on a finite set* N *is the incidence structure* $\mathfrak{L}_N$ *with point labels from* N*, and a single line label which is incident to all point labels. In particular, for a positive integer* n*, the* n-line structure $\mathfrak{L}_n$ *is the line structure on the integers modulo* n*.*

We will normally represent our incidence structure with point labels drawn in a circle, line labels drawn in a rectangle, and incidence will be indicated by a line emanating from the rectangle and passing through the circle. For example an $(n+1)$-line with line label a is represented as follows:

$\mathfrak{L}_{n+1}$:

In practice we will sometimes omit line labels, especially when considering n-line structures individually. This will also be the case when there is little relevance to the label, or when the context makes it clear. So the 3-line structure $\mathfrak{L}_3$ will be represented as follows:

5.1.1 Isomorphisms of Incidence Structures

When we later generalize labeled diagrams, we will use isomorphisms to allow for symmetries of the underlying structure:

Definition 5.1.2. *An* isomorphism $\phi : \mathfrak{D} \to \mathfrak{D}'$ *between incidence structures* $\mathfrak{D}, \mathfrak{D}'$ *consists of a bijection* $\phi : \mathfrak{P} \to \mathfrak{P}'$ *and a bijection* $\phi : \mathfrak{L} \to \mathfrak{L}'$*, which preserves the incidence relation. That is,* $\phi(i) \in \phi(k) \Leftrightarrow i \in k$ *for all* $(i, k) \in \mathfrak{P} \times \mathfrak{L}$*.*

An isomorphism $\phi : \mathfrak{D} \to \mathfrak{D}$ *is called an* automorphism*, and these form a group* $\mathrm{Aut}(\mathfrak{D})$ *under composition. Any subgroup of* $\mathrm{Aut}(\mathfrak{D})$ *is called an* automorphism group*.*

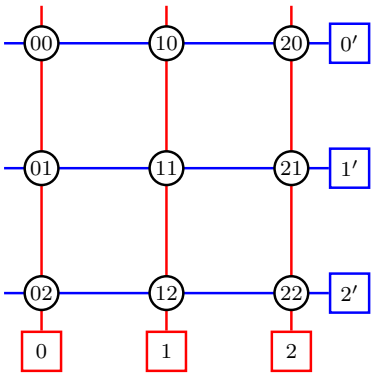
In the simplest case of an n-line structure, the automorphism group is the full permutation group S_n of its labels. We will notate permutations in cycle notation, and the group operation is functional composition; so for example, on labels $0, 1, 2$, the permutation $(012)(01) = (02)$ transposes $0, 2$ and fixes 1.

5.1.2 Nine Point Diagram Structure

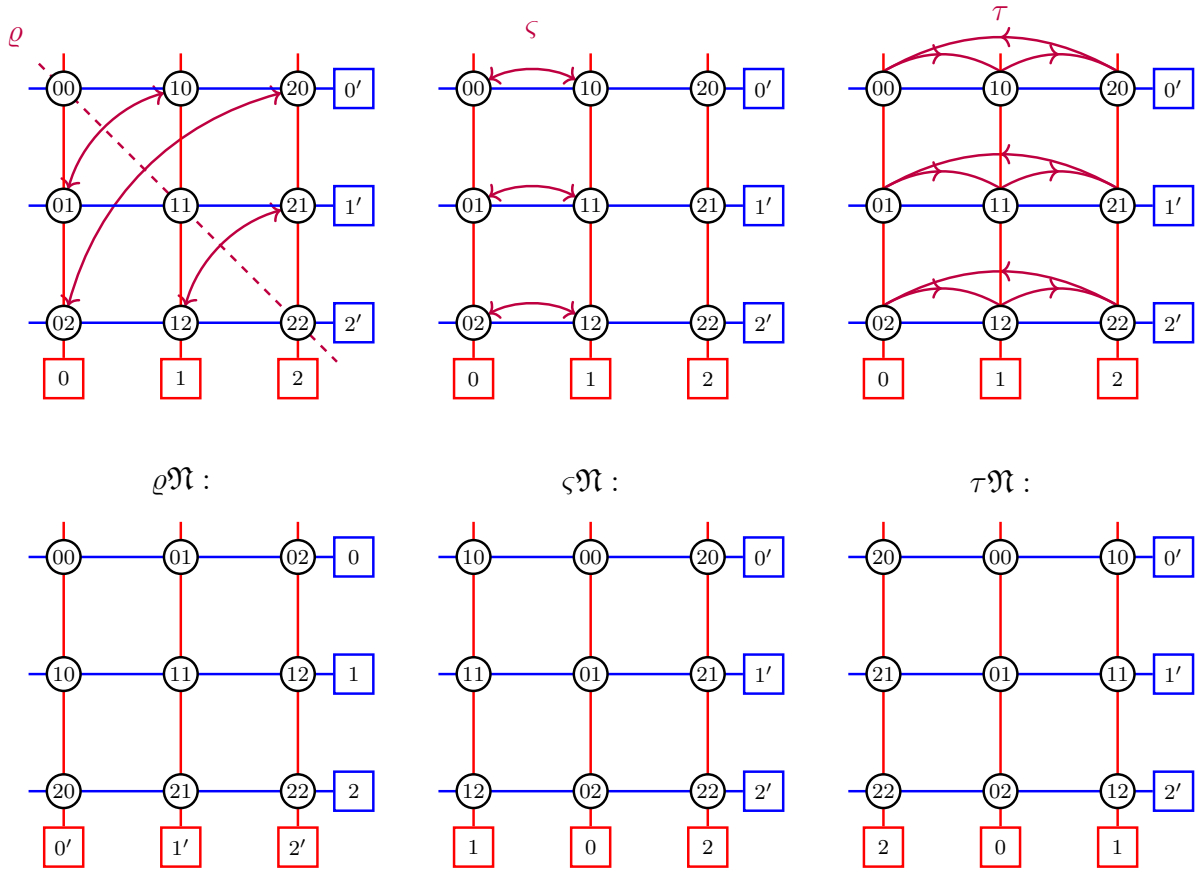
We will often combine incidence structures into larger ones. Notably, we will work with *nine point diagrams*, which will be defined on the following structure:

Definition 5.1.3. *The following incidence structure* $\mathfrak{N}$ *is the* nine point diagram structure*:*

$\mathfrak{N}$:



This in fact has 72 symmetries, generated by ϱ, ς, τ, with ϱ being a reflection across the northwest to southeast diagonal, ς transposing the lines (01) and τ cycling the lines (012):



Lemma 5.1.4. *The automorphism group* $\mathrm{Aut}(\mathfrak{N})$ *is generated by the automorphisms* ϱ, ς, τ*, which are defined on point/line labels as follows, working in modulus* 3*:*

$$\begin{aligned}
&\varrho(ij) = ji,\ \varsigma(ij) = (1-i)j,\ \tau(ij) = (i+1)j\\
&\varrho(l) = l',\ \varsigma(l) = (1-l),\ \tau(l) = (l+1)j\\
&\varrho(l') = l,\ \varsigma(l') = l',\ \tau(l') = l'
\end{aligned}$$

Furthermore, this automorphism group has order 72*.*

Note that by applying combinations of ς, τ, we can permute lines $0, 1, 2$ arbitrarily, while fixing lines $0', 1', 2'$. We can do similarly with $\varsigma' = \varrho\varsigma\varrho, \tau' = \varrho\tau\varrho$; these permute the lines $0', 1', 2'$ arbitrarily, while fixing lines $0, 1, 2$.

Proof. First note that $\mathrm{Aut}(\mathfrak{N})$ acts faithfully on the line labels; that is because if we are given lines labeled $\phi(i), \phi(j')$, we must have the point labeled $\phi(ij)$ at their intersection. So we will consider $\mathrm{Aut}(\mathfrak{N})$ as a permutation group on the line labels.

We will prove that the order of the group is 72 by the orbit-stabilizer theorem. First note that $\mathrm{Aut}(\mathfrak{N})$ acts transitively on the line labels: $id(0) = 0, \tau(0) = 1, \tau^2(0) = 2, \varrho(0) = 0', \varrho\tau(0) = 1', \varrho\tau^2(0) = 2'$. So the orbit of 0 has order 6. Next we consider the stabilizer of 2; so suppose that $\phi(2) = 2$. Then ϕ must induce a permutation on $\{0, 1\}$, since the lines labeled $\phi(0), \phi(1)$ cannot intersect the line labeled $\phi(2) = 2$. Hence the stabilizer of 2 is $\langle \varsigma, \varsigma', \tau' \rangle$, which has order 12. Hence $|\mathrm{Aut}(\mathfrak{N})| = 6 * 12 = 72$.

Lastly since $\langle \varsigma, \tau, \varsigma', \tau' \rangle \subsetneq \langle \varrho, \varsigma, \tau \rangle \subseteq \mathrm{Aut}(\mathfrak{N})$, the subgroup $\langle \varrho, \varsigma, \tau \rangle$ must have index 1, so we are done. □

5.2 Labeled Diagrams

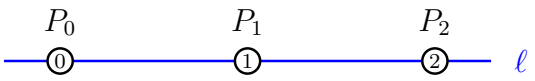
To form a *labeled diagram* $\mathcal{D}$ on an incidence structure $\mathfrak{D}$, we assign a point $P_i \in E$ to each line label $i \in \mathfrak{P}$. For each line label $j \in \mathfrak{L}$, we impose a condition on the collection ℓ_j of points assigned to labels $i \in \mathfrak{P}$ that are incident to j; namely, ℓ_j must be a *linear set*. Recall from chapter 4 that a linear n-set is an unordered n-tuple of points from E that sum to $\mathcal{O}$. More concisely, it is an element from $\mathcal{L}_n^\bullet(E)$:

$$\mathcal{L}_n^\bullet(E) = \{(P_0) + (P_1) + \ldots + (P_{n-1}) \in \mathbb{Z}[E] \ : \ P_0 + P_1 + \ldots + P_{n-1} = \mathcal{O}\}$$

Definition 5.2.1. *A* labeled diagram $\mathcal{D}$ *with incidence structure* $\mathfrak{D}$ *assigns a point* $\mathfrak{p}_i(\mathcal{D}) \in E$ *to each point label* $i \in \mathfrak{P}$ *of* $\mathfrak{D}$*, and a linear set* $\mathfrak{l}_j(\mathcal{D}) \in \mathcal{L}_n^\bullet(E)$ *to each line label* $j \in \mathfrak{L}$ *of* $\mathfrak{D}$*. Furthermore, for each line label* $j \in \mathfrak{L}$*, the linear set* $\mathfrak{l}_j$ *must correspond to the collection of points assigned to the point labels incident to* j*. The set of labeled diagrams on* $\mathfrak{D}$ *will be denoted* $\mathcal{L}_{\mathfrak{D}}^\circ(E)$*.*

We will normally indicate point assignments from E for each point label, and then linear set assignments will be implicit; we note that there is really no choice in the matter.

We will normally represent the point $\mathfrak{p}_i(\mathcal{D})$ near its label i; often this will be denoted P_i or similar. Similarly, the linear set $\mathfrak{l}_i(\mathcal{D})$ will be represented near the line label, or else near an endpoint of the line drawing; often we will denote that line by ℓ_i or similar. For example, if we assign a point $P_i \in E$ to each $i \in \{0, 1, 2\}$ such that $P_0 + P_1 + P_2 = \mathcal{O}$ then we get a *labeled line diagram*:



The symbol ℓ then represents the linear set with points P_0, P_1, P_2, and this is assigned to the (omitted) line label. We will use the symbol ℓ° to refer to the above labeled diagram.

In some cases, we simply use the symbol ℓ, and the context makes it clear that we are including the additional structure.

We will identify elements of $\mathcal{L}_n^\circ(E)$ with the n-tuple of points assigned to the labels:

Definition 5.2.2. *A* labeled n-line ℓ° *is an* n*-tuple of points* $(P_0, P_1, \ldots, P_{n-1})$ *from* E *satisfying* $P_0 + P_1 + \ldots + P_{n-1} = \mathcal{O}$*. The set of labeled* n*-lines is denoted* $\mathcal{L}_n^\circ(E)$*.*

Again, the indices will be in modulus n, and if n is not otherwise specified, it should be taken to be 3.

5.2.1 Automorphisms on Labeled Diagrams

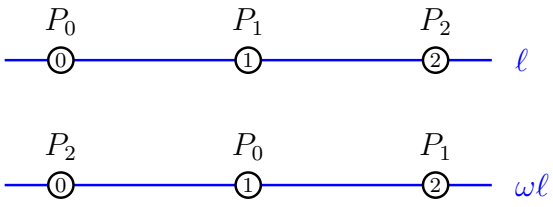
To define new classes of diagrams, we will take equivalence classes of labeled diagrams under the action of a *symmetry group*. These symmetries will be automorphisms of the underlying incidence structure, which will be applied to the labels of a diagram. So if $\mathcal{D} \in \mathcal{L}_{\mathfrak{D}}^\circ(E)$ assigns the point $P_i \in E$ to each label i of $\mathfrak{D}$, then $\sigma\mathcal{D} \in \mathcal{L}_{\mathfrak{D}}^\circ(E)$ assigns the point P_i to the label $\sigma(i)$ of $\mathfrak{D}$. Equivalently, $\sigma\mathcal{D}$ assigns the point $P_{\sigma^{-1}i}$ to the label i of $\mathcal{D}$. More generally:

Definition 5.2.3. *Given an isomorphism* $\phi : \mathfrak{D} \to \mathfrak{D}'$ *and a labeled diagram* $\mathcal{D} \in \mathcal{L}_{\mathfrak{D}}^\circ(E)$*, we define the labeled diagram* $\phi(\mathcal{D})$ *on structure* $\mathfrak{D}'$ *as follows:*

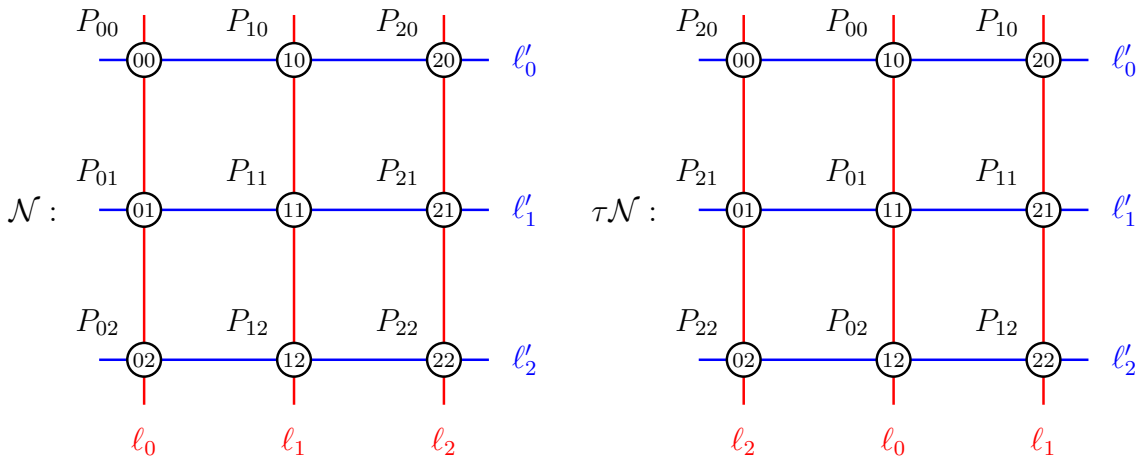
- $\mathfrak{p}_i(\phi(\mathcal{D})) = \mathfrak{p}_{\phi^{-1}i}(\mathcal{D})$ *for each point label* i *of* $\mathfrak{D}'$
- $\mathfrak{l}_j(\phi(\mathcal{D})) = \mathfrak{l}_{\phi^{-1}j}(\mathcal{D})$ *for each line label* j *of* $\mathfrak{D}'$

The induced map $\phi : \mathcal{L}_{\mathfrak{D}}^\circ(E) \to \mathcal{L}_{\mathfrak{D}'}^\circ(E)$ *is called a* structural isomorphism*.*

This gives an action of $\mathrm{Aut}(\mathfrak{D})$ on $\mathcal{L}_{\mathfrak{D}}^\circ(E)$. For example, consider the automorphism $\omega = (012)$ of a 3-line structure. We can apply this to a labeled line diagram ℓ to obtain the labeled line diagram $\omega\ell$:



As another example, recall the automorphism $\tau \in \mathrm{Aut}(\mathfrak{N})$ from section 5.1.2. Here we have a labeled nine point diagram $\mathcal{N}$ on the left hand side, and $\tau\mathcal{N}$ on the right:



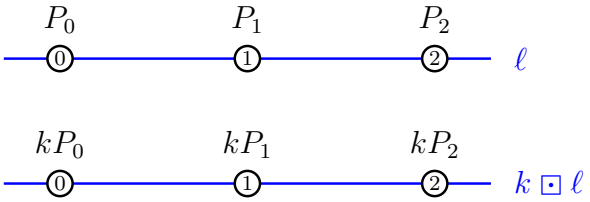
5.2.2 Labeled Diagram Arithmetic

We will now discuss arithmetic in $\mathcal{L}^\circ_{\mathfrak{D}}(E)$, with the goal of developing a more general context to understand line arithmetic. We first define *labeled diagram multiplication* by $k \in \mathbb{Z}$ to be the map $k\boxdot : \mathcal{L}^\circ_{\mathfrak{D}}(E) \to \mathcal{L}^\circ_{\mathfrak{D}}(E)$ that multiplies each point by k:

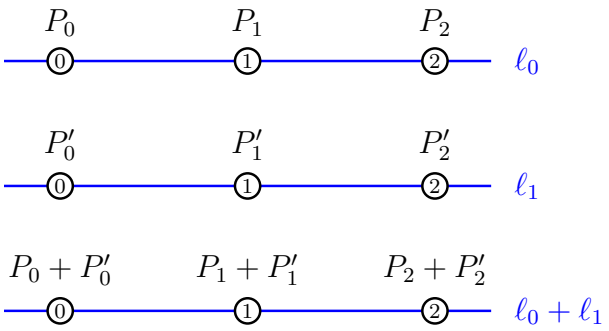
Definition 5.2.4. *For a labeled diagram $\mathcal{D}$ on an incidence structure $\mathfrak{D}$, the* multiplication by k map $k\boxdot : \mathcal{L}^\circ_{\mathfrak{D}}(E) \to \mathcal{L}^\circ_{\mathfrak{D}}(E)$ *results in the labeled diagram $k \boxdot \mathcal{D}$ with:*

$$\begin{aligned}\mathfrak{p}_i(k \boxdot \mathcal{D}) &= k\mathfrak{p}_i(\mathcal{D})\\ \mathfrak{l}_j(k \boxdot \mathcal{D}) &= k \boxdot \mathfrak{l}_j(\mathcal{D})\end{aligned}$$

So for a labeled line $\ell \in \mathcal{L}^\circ_3(E)$, and $k \in \mathbb{Z}$, we get:



Recall that the (unlabeled) line addition in $\mathcal{L}_3(E)$ that we have considered has an inherent six way ambiguity. In contrast to this, *labeled line addition* has no ambiguity, since we simply pair the points according to their labels:



or equivalently,

$$(P_0, P_1, P_2) + (Q_0, Q_1, Q_2) = (P_0 + Q_0, P_1 + Q_1, P_2 + Q_2)$$

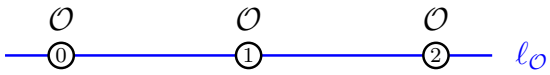
More generally, we can take the sum of two labeled diagrams in this same way:

Definition 5.2.5. *For labeled diagrams $\mathcal{D}_0, \mathcal{D}_1 \in \mathcal{L}^\circ_{\mathfrak{D}}(E)$, the* labeled diagram sum $\mathcal{D}_0 + \mathcal{D}_1 \in \mathcal{L}^\circ_{\mathfrak{D}}(E)$ *satisfies the following for each label:*

$$\mathfrak{p}_i(\mathcal{D}_0 + \mathcal{D}_1) = \mathfrak{p}_i(\mathcal{D}_0) + \mathfrak{p}_i(\mathcal{D}_1)$$

This operation is termed labeled diagram addition*, and gives $\mathcal{L}^\circ_{\mathfrak{D}}(E)$ an abelian group structure. The identity element of this group is $\mathcal{D}_{\mathcal{O}}$, which has the point $\mathcal{O}$ assigned to each label.*

For labeled lines, we denote the additive identity as follows:



We will extend our diagram multiplication $k\boxdot$ to include the possibility that k is a structural automorphism:

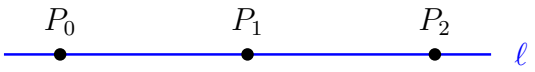
Definition 5.2.6. *For $k = k_0\sigma_0 + \ldots + k_m\sigma_m \in \mathbb{Z}[\mathrm{Aut}(\mathfrak{D})]$ with $k_i \in \mathbb{Z}$ and $\sigma_i \in \mathrm{Aut}(\mathfrak{D})$, we define*

$$k \boxdot \mathcal{D} = k_0 \boxdot \sigma_0\mathcal{D} + \ldots + k_m \boxdot \sigma_m\mathcal{D}$$

This notation will make it simpler to discuss addition of diagrams in certain contexts. We will make good use of this notation in section 5.6.1, when we discuss cyclic line arithmetic.

5.3 Diagrams With Symmetry

In this section, we define more general diagrams in terms of labeled diagrams. In particular, this will give a precise meaning to the line diagrams that we have used to represent a line $\ell \in \mathcal{L}_3(E)$:



First we note that the points of a line $\ell \in \mathcal{L}_3(E)$ are unordered. Hence if we want a diagram that represents such a line, the diagram resulting from a permutation of the points should be considered to be equivalent to the original diagram. Thus we define an *unlabeled line diagram* to be an equivalence class of labeled line diagrams under arbitrary permutations of its points.

More generally, a *diagram* will correspond to an equivalence class of labeled diagrams on an incidence structure $\mathfrak{D}$ under the action of a *symmetry group*:

Definition 5.3.1. *Given an incidence structure $\mathfrak{D}$ and an automorphism group $S \subseteq \mathrm{Aut}(\mathfrak{D})$, a* diagram $\mathcal{D}$ with symmetry group S *is an orbit of $\mathcal{L}^\circ_{\mathfrak{D}}(E)$ under the action of S. The collection of such diagrams is denoted $\mathcal{L}^S_{\mathfrak{D}}(E)$.*

If S is the full automorphism group, then we say that $\mathcal{D}$ is an unlabeled diagram*, and the set of unlabeled diagrams is denoted $\mathcal{L}^\bullet_{\mathfrak{D}}(E)$.*

Generally speaking, unlabeled diagrams will be drawn with filled circles, while labeled diagrams will be drawn with unfilled circles. Furthermore, the labels will often be omitted. Note that we will identify $\mathcal{L}^\circ_{\mathfrak{D}}$ and $\mathcal{L}^{\{id\}}_{\mathfrak{D}}$ by a slight abuse of notation. Accordingly, a diagram with only trivial symmetry group will also be termed a labeled diagram.

For a diagram $\mathcal{D}$ with symmetry group S, the notation $\mathcal{D}^\circ$ will be used to refer to some labeled diagram in its equivalence class. Normally $\mathcal{D}$ is defined in terms of a drawing, and $\mathcal{D}^\circ$ is understood to refer to the specific representative that is drawn. On the other hand, we use the notation $\mathcal{D}^\bullet$ to denote the same diagram, but with full symmetry group.

Recall that the n-line structure has points labeled by integers modulo n, and a single line that passes through all of them. We will refer to any diagram on this structure as an n-line diagram:

Definition 5.3.2. *An* n-line diagram *is a diagram on an n-line incidence structure. An* unlabeled n-line diagram *has full symmetry group S_n. When n is not specified, it should be assumed to be* 3.

Later in this section, we will redefine the lines from previous chapters in diagrammatic terms. Note that the line structure has automorphism group S_3, and we will use the generators $\rho = (01)$ and $\omega = (012)$.

5.3.1 Automorphisms on Diagrams with Symmetry

Definition 5.3.3. *Given an isomorphism $\phi : \mathfrak{D} \to \mathfrak{D}'$ and a symmetry group $S \subseteq \mathrm{Aut}(\mathfrak{D})$, we define the symmetry group $S' \subseteq \mathrm{Aut}(\mathfrak{D}')$ by element-wise conjugation: $S' = \phi \circ S \circ \phi^{-1}$. Then we can apply ϕ to $\mathcal{D} \in \mathcal{L}^S_{\mathfrak{D}}(E)$ to obtain $\phi(\mathcal{D}) \in \mathcal{L}^{S'}_{\mathfrak{D}'}(E)$.*

In light of this, we consider automorphisms of diagrams with symmetry. To preserve their symmetry group, we simply define the automorphism group of $\mathfrak{D}$ to be:

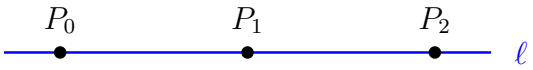
Definition 5.3.4. *For a symmetry group $S \subseteq \mathrm{Aut}(\mathfrak{D})$ of an incidence diagram $\mathfrak{D}$, we define the* S-automorphism group *of $\mathfrak{D}$ to be the quotient of the normalizer of S by S:*

$$\mathrm{Aut}_S(\mathfrak{D}) = N_{\mathrm{Aut}(\mathfrak{D})}(S)/S$$

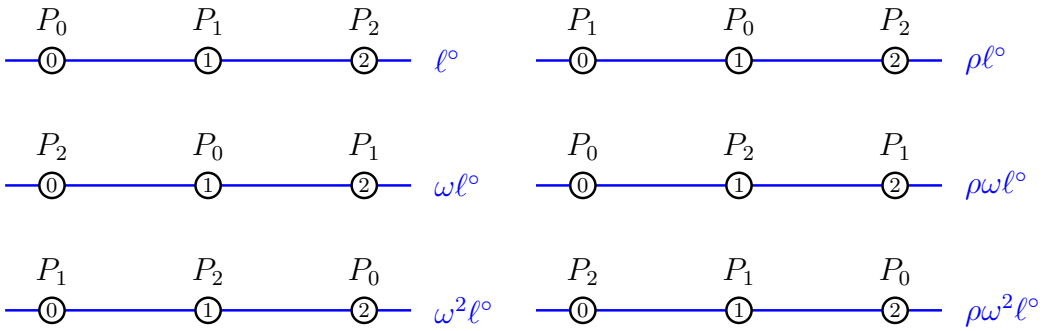
Note that for $\mathcal{D} \in \mathcal{L}^S_{\mathfrak{D}}(E)$ and $\nu \in N_{\mathrm{Aut}(\mathfrak{D})}(S)$, we have $\mathcal{D} = S\mathcal{D}^\circ$ for some labeled diagram $\mathcal{D}^\circ \in \mathcal{L}^\circ_{\mathfrak{D}}(E)$. Thus we can unambiguously define $\nu\mathcal{D} = \nu S\mathcal{D}^\circ = S\nu\mathcal{D}^\circ$. Furthermore, every element $\sigma \in S$ acts trivially on $\mathcal{D}$ by definition.

5.3.2 Unlabeled Line Diagrams

An *unlabeled line diagram* $\ell \in \mathcal{L}^\bullet_3(E)$ will be represented as follows:



This represents the equivalence class consisting of the following six labeled line diagrams:



Such an unlabeled line diagram corresponds to an unordered triplet of points of E, with repetitions allowed. Note that this gives an alternate but equivalent definition to the one from section 4.1.1:

$$\mathcal{L}^\bullet_3(E) = \{(P_0) + (P_1) + (P_2) \in \mathbb{Z}[E] \ : \ P_0 + P_1 + P_2 = \mathcal{O}\}$$

More generally, unlabeled n-line diagrams correspond to elements of $\mathcal{L}_n^\bullet(E)$ as defined in section 4.1.1:

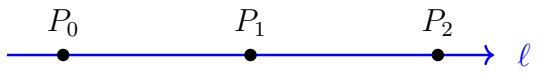
$$\mathcal{L}_n^\bullet(E) = \{(P_0) + \ldots + (P_{n-1}) \in \mathbb{Z}[E] \ : \ P_0 + \ldots + P_{n-1} = \mathcal{O}\}$$

5.3.3 Cyclic Line Diagrams

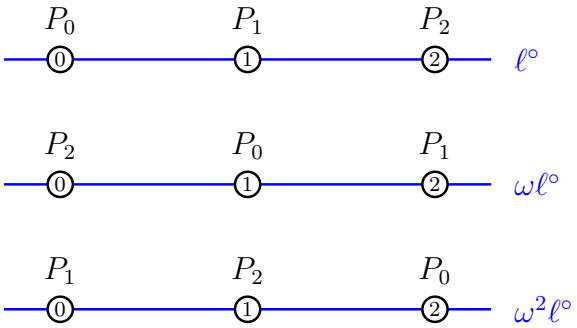
Now we can redefine cyclically oriented lines in diagrammatic terms:

Definition 5.3.5. *A* cyclic n-line diagram *has symmetry group generated by the permutation* $i \mapsto i+1$ *in modulus* n*. We denote the set of cyclic* n*-line diagrams by* $\mathcal{L}_n^\triangleright(E)$*.*

For $n = 3$, we simply refer to this as a *cyclic line diagram*. We use the notation $\omega = (012)$, and thus a cyclic line diagram has symmetry group $\{1, \omega, \omega^2\}$. It is drawn as follows:



and represents the following three diagrams:

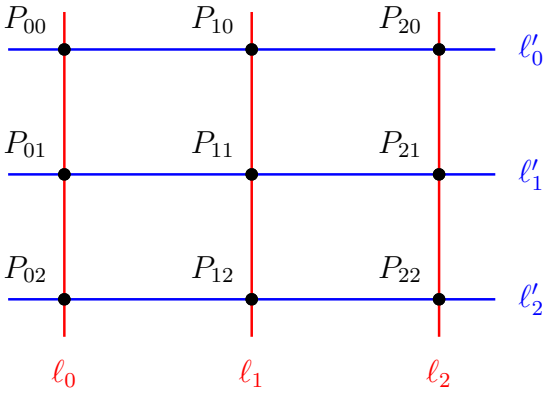


We note that since $S = \{1, \omega, \omega^2\}$ is a normal subgroup of $\mathrm{Aut}(\mathfrak{L}_3)$, cyclic line diagrams have an automorphism group of order 2. We will use the symbol ρ for the non-trivial automorphism.

5.3.4 Nine Point Diagrams with Symmetry

Any diagram on a structure isomorphic to $\mathfrak{N}$ will be referred to as a *nine point diagram*. An unlabeled nine point diagram will be represented as follows:

$\mathcal{N}^\bullet$:



The prototypical nine point diagram is the $u \boxplus v$ line sum diagram that we have referred to countless times. As we will see in the next section, the line sum diagram has $6*6*2 = 72$ symmetries corresponding to an arbitrary permutation of each line, and to swapping the order of summation. Thus the symmetry group must be the full $\mathrm{Aut}(\mathfrak{N})$, since the latter has order 72. Thus the line sum diagram is in fact an unlabeled nine point diagram.

In the following chapters, we will consider nine point diagrams with other symmetry groups. The goal will be to track additional information in our operation chains, that impose additional structure on the nine point diagrams that we consider. For example, if u, v are cyclically oriented lines, then $\mathcal{N}$ can be determined up to a symmetry group of order 18, and we will benefit from this in chapter 6 when we develop a diagrammatic calculus.

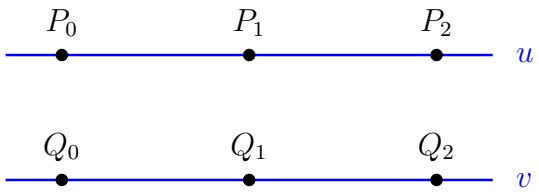
5.4 Diagrammatic Arithmetic

In this section, we develop the arithmetic of diagrams in $\mathcal{L}^S_{\mathfrak{D}}(E)$ for a symmetry group S. The first step is easy; for a diagram $\mathcal{D} \in \mathcal{L}^S_{\mathfrak{D}}(E)$, the scalar multiplication by $k \in \mathbb{Z}$ map simply applies to each labeled diagram in the orbit of $\mathcal{D}$:

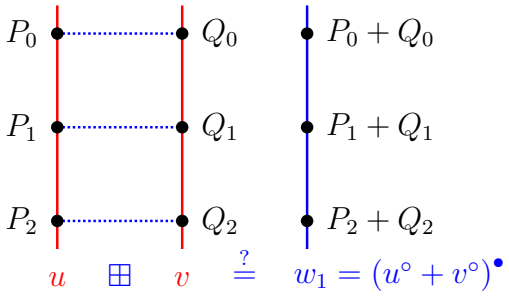
Definition 5.4.1. *Given a diagram $\mathcal{D}$ with symmetry group S, let $\mathcal{D}^\circ$ denote a labeled diagram in its equivalence class. Then we define $k \boxdot \mathcal{D}$ to be the equivalence class of $k \boxdot \mathcal{D}^\circ$ with symmetry group S.*

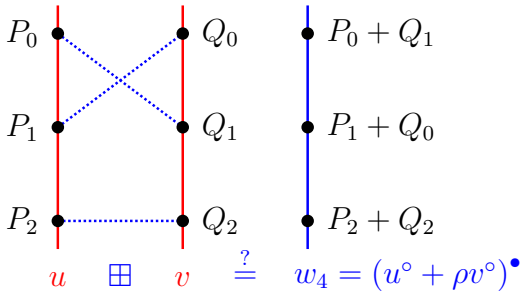
Next we consider operation chains to compute scalar multiplication. Of course, the addition step will be our point of focus, as it has been for line multiplication in previous chapters. First we consider unlabeled line addition; a typical 3-line ℓ represents six possible labeled lines. Hence for ℓ, ℓ' there are 36 possible labeled sum lines! Of course, we will consider such diagrams to be equivalent under the action of S, which reduces the number of possibilities to 6.

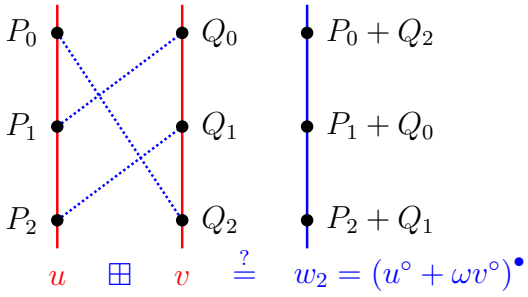
This is a reinterpretation of the discussion from section 3.3 about the ambiguity inherent to line addition. Explicitly, suppose that $u, v \in \mathcal{L}_3^\bullet(E)$ are represented by $u^\circ, v^\circ \in \mathcal{L}_3^\circ(E)$ with respective points P_i, Q_i on label i:

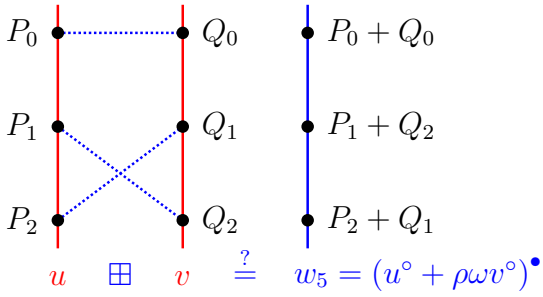


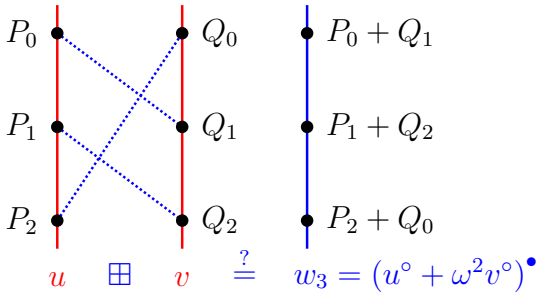
Then there are six possible sum lines between u and v. Recall that for any line diagram ℓ, the notation $\ell^\bullet$ indicates the unlabeled line that is represented by ℓ:

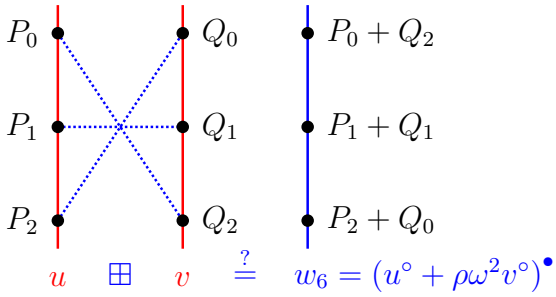








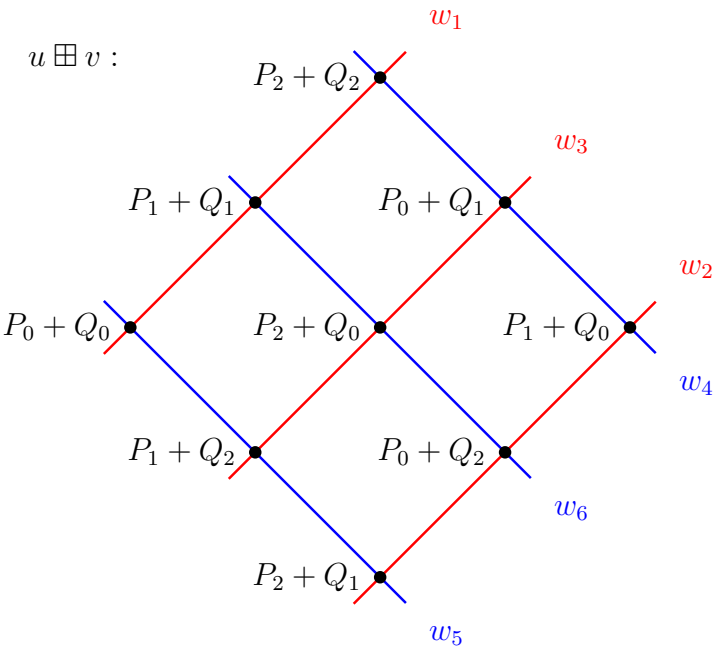




More generally, we define the following, which matches our definition of "sum line" between elements of $\mathcal{L}_3(E)$:

Definition 5.4.2. *Suppose we have diagrams $\mathcal{D}_1, \mathcal{D}_2 \in \mathcal{L}^S_{\mathfrak{D}}(E)$ with the same structure and symmetry group. Let $\mathcal{D}_1^\circ, \mathcal{D}_2^\circ$ represent labeled diagram in their respective orbits. For any $\sigma \in S$, the equivalence class of $\mathcal{D}_1^\circ + \sigma\mathcal{D}_2^\circ$ under S is termed a* sum diagram *between $\mathcal{D}_1$ and $\mathcal{D}_2$.*

Next we recall that in section 3.10, we organized the six sum lines between $u, v \in \mathcal{L}_3(E)$ into the following diagram:



In the remainder of this section, we will precisely define this *unlabeled line sum diagram*. In fact, we will generalize this to a *diagrammatic sum* between any two diagrams. We will use this definition as the centerpiece of our renewed discussion of line addition, where we reconsider cyclic line addition.

5.4.1 Isomorphic Diagrammatic Sum

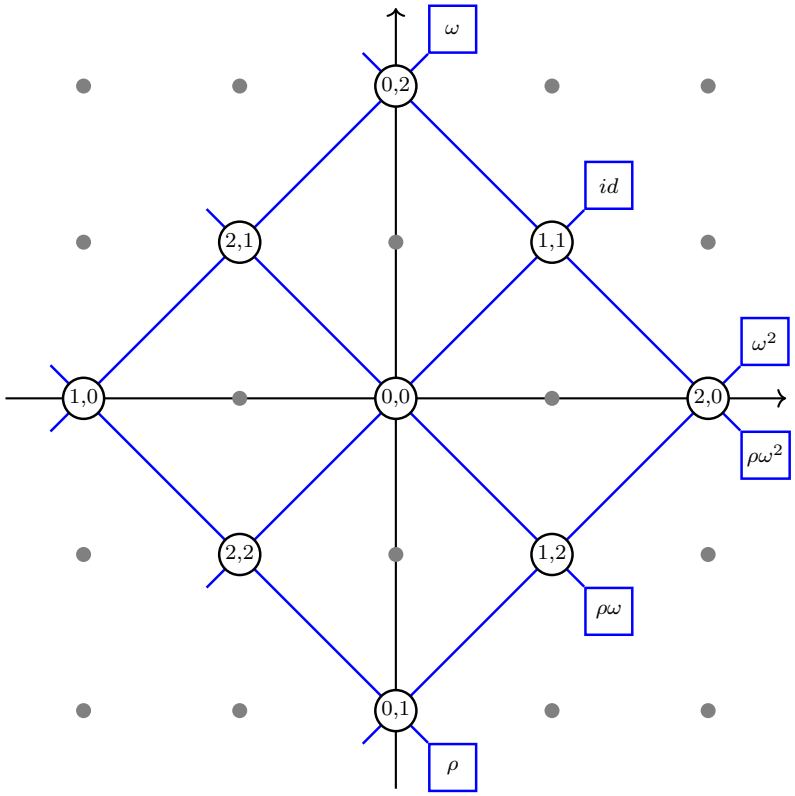
Suppose that $\mathfrak{D}, \mathfrak{D}'$ are two incidence structures, with respective labeled diagrams $\mathcal{D}, \mathcal{D}'$, and suppose that $I \subseteq \mathrm{Iso}(\mathfrak{D}, \mathfrak{D}')$ is a set of isomorphisms between the structures. We will consider sums between $\mathcal{D} + \phi^{-1}\mathcal{D}'$ as ϕ varies over I. In fact, we will put all of these into a single diagram $\mathcal{D} \boxplus_I \mathcal{D}'$, called an *$I$-diagrammatic sum*. When $I = \mathrm{Iso}(\mathfrak{D}, \mathfrak{D}')$ contains all isomorphisms, we call this a *full diagrammatic sum*.

Definition 5.4.3. *Given incidence structures $\mathfrak{D}, \mathfrak{D}'$ and a set I of isomorphisms between them, we define $\mathfrak{D} \boxplus_I \mathfrak{D}'$ to have points and lines being respectively:*

$$\{(i, \phi(i)) \ : \ i \in \mathfrak{P}, \ \phi \in I\}$$
$$\{(k, \phi^{-1}) \ : \ k \in \mathfrak{L}, \ \phi \in I\}$$

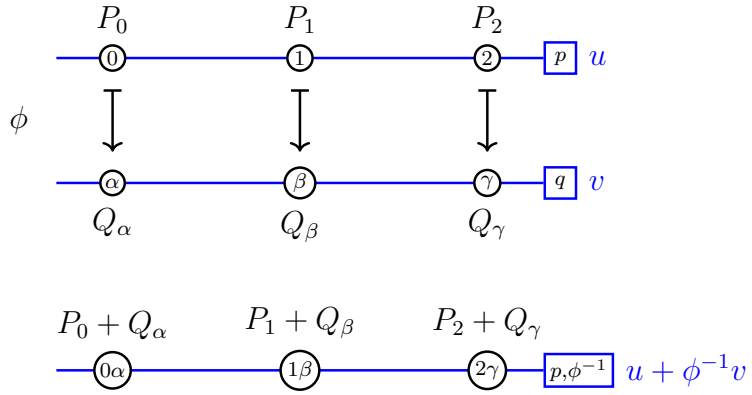
where $\mathfrak{P}$ and $\mathfrak{L}$ denote the point and line labels of $\mathfrak{D}$. The incidences of $\mathfrak{D} \boxplus_I \mathfrak{D}'$ are exactly those of the form $(i, \phi(i)) \in (k, \phi^{-1})$ for each incidence $i \in k$ of $\mathfrak{D}$ and for each $\phi \in I$.

The full diagrammatic sum structure between $\mathfrak{L}_3$ and itself is denoted $\mathfrak{L}_{\boxplus}$, and can be represented as follows:



We embedded $\mathfrak{L}_{\boxplus}$ in the Cartesian plane in modulus 3, which convenient choices of representatives. Note that we simplified the line labels by ignoring the first components; these would would have all been the same. We will next consider an example in more detail.

The idea behind this structure is that for each isomorphism $\phi \in I$, we will consider $\mathcal{D} + \phi^{-1}\mathcal{D}'$ as a diagram on $\mathfrak{D}$, embedded into $\mathfrak{D} \boxplus_I \mathfrak{D}'$ by identifying the point labels $i \leftrightarrow (i, \phi(i))$ and the line labels $k \leftrightarrow (k, \phi^{-1})$. For example, consider a labeled line diagram u on $\mathfrak{L}_3$, and v on $\mathfrak{L}_{\{\alpha,\beta,\gamma\}}$, with a structural isomorphism ϕ which maps $0 \mapsto \alpha$, $1 \mapsto \beta$ and $2 \mapsto \gamma$. Then we consider $u + \phi^{-1}v$ as if it were a diagram on point labels $0, 1, 2$:

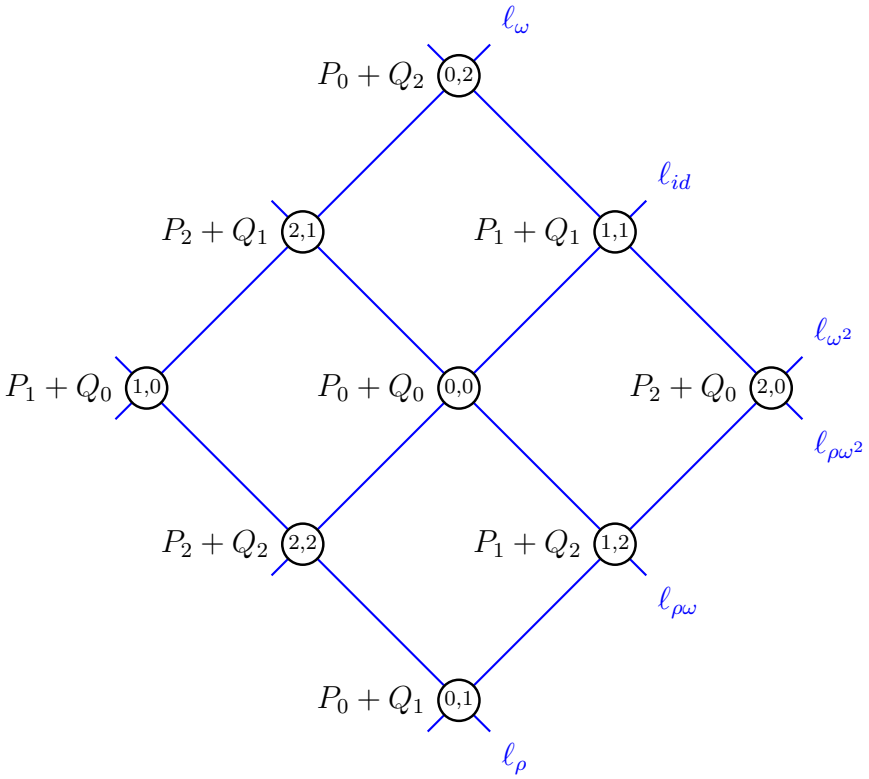


Definition 5.4.4. *The* I-diagrammatic sum $\mathcal{D} \boxplus_I \mathcal{D}'$ *of two labeled diagrams on structures* $\mathfrak{D}, \mathfrak{D}'$ *with a set* $I \subseteq \mathrm{Iso}(\mathfrak{D}, \mathfrak{D}')$ *of isomorphisms, is the labeled diagram on structure* $\mathfrak{D} \boxplus_I \mathfrak{D}'$ *with*

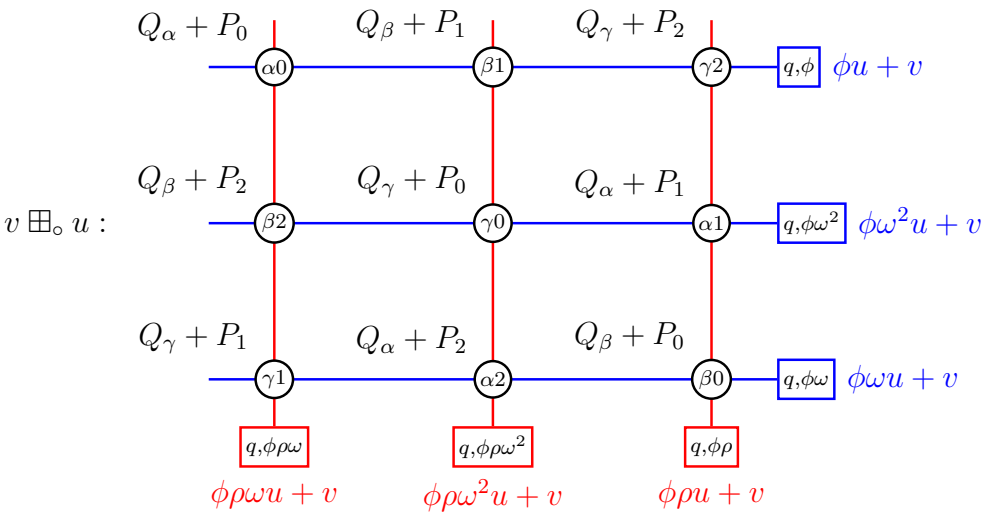
$$\begin{aligned} \mathfrak{p}_{i,j}(\mathcal{D} \boxplus_I \mathcal{D}') =& \mathfrak{p}_i(\mathcal{D}) + \mathfrak{p}_j(\mathcal{D}') \\ \mathfrak{l}_{k,\phi^{-1}}(\mathcal{D} \boxplus_I \mathcal{D}') =& \mathfrak{l}_k(\mathcal{D} + \phi^{-1}\mathcal{D}') \\ =& \mathfrak{l}_k(\mathcal{D}) + \mathfrak{l}_{\phi(k)}(\mathcal{D}') \end{aligned}$$

when $I = \mathrm{Iso}(\mathfrak{D}, \mathfrak{D}')$ *contains all isomorphisms, we call this a* full diagrammatic sum*, and denote it* $\mathcal{D} \boxplus_\circ \mathcal{D}'$*.*

For example, for labeled lines ℓ_0, ℓ_1 with respective points P_0, P_1, P_2 and Q_0, Q_1, Q_2, we get the following full diagrammatic sum, with $\ell_\sigma = (\ell_0 + \sigma\ell_1)^\bullet$:



With more detail, we get the following full diagrammatic sum for the ϕ-related line diagrams u, v from earlier, noting that we have changed the order of summation:



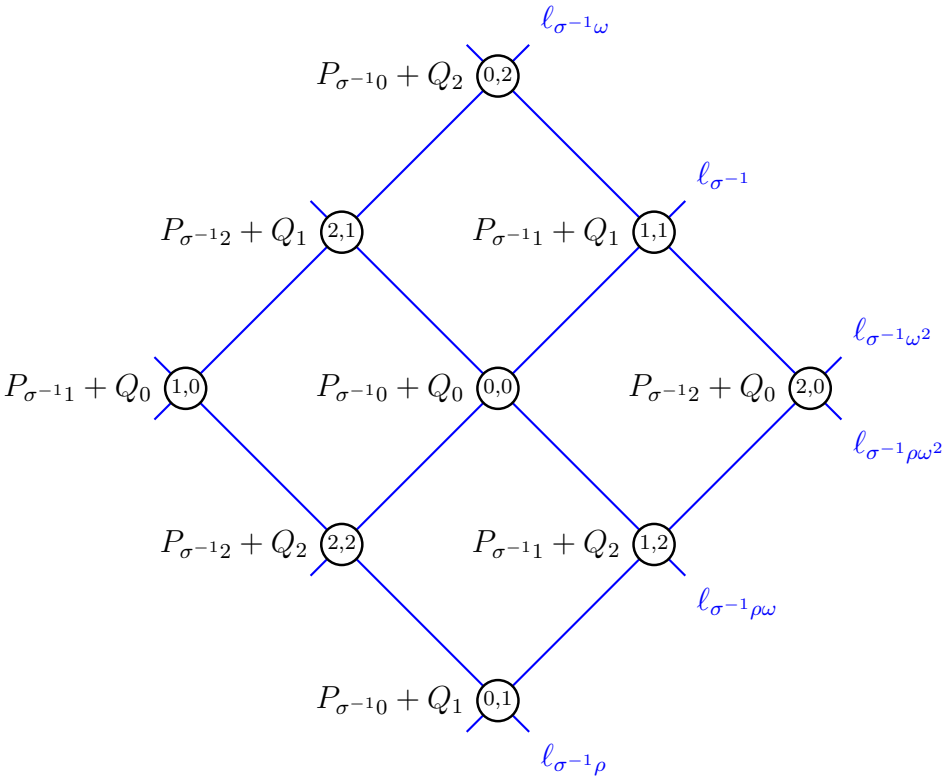
5.4.2 Diagrammatic Sum Symmetries

We will next define diagrammatic sums for diagrams with symmetry. We accomplish this by defining an appropriate group of symmetries for an I-diagrammatic sum. First we note that the full diagrammatic sum inherits the automorphisms of both of its summands:

Definition 5.4.5. *The automorphism group* $\mathrm{Aut}(\mathfrak{D}) \times \mathrm{Aut}(\mathfrak{D}')$ *acts on the respective point and line labels of* $\mathfrak{D} \boxplus_\circ \mathfrak{D}'$ *as follows:*

$$\begin{aligned}(\sigma_0, \sigma_1)(i, j) :=& (\sigma_0(i), \sigma_1(j)) \\ (\sigma_0, \sigma_1)(l, \phi^{-1}) :=& (\sigma_0(l), \sigma_0 \circ \phi^{-1} \circ \sigma_1^{-1})\end{aligned}$$

For example, for the linear sum structure $\mathfrak{L}_\boxplus = \mathfrak{L}_3 \boxplus_\circ \mathfrak{L}_3$, we can apply $\sigma \in S$ in the first coordinate. We illustrate this with the $(\sigma, id)\ell_0 \boxplus_\circ \ell_1$ diagram:



The action of $\mathrm{Aut}(\mathfrak{D}) \times \mathrm{Aut}(\mathfrak{D}')$ allows us to extend I-diagrammatic sums to include diagrams with symmetry $\mathcal{D} \in \mathcal{L}^S_{\mathfrak{D}}(E)$, $\mathcal{D}' \in \mathcal{L}^{S'}_{\mathfrak{D}'}(E)$. The symmetry group of $\mathcal{D} \boxplus_I \mathcal{D}'$ will be $S \times S'$. For the symmetries to be well defined, we need that $I \subseteq \mathrm{Iso}(\mathfrak{D}, \mathfrak{D}')$ be closed under composition on the right by S, and on the left by S':

Definition 5.4.6. *Suppose diagrams $\mathcal{D} \in \mathcal{L}^S_{\mathfrak{D}}(E)$, $\mathcal{D}' \in \mathcal{L}^{S'}_{\mathfrak{D}'}(E)$ are represented by $\mathcal{D}^\circ \in \mathcal{L}^\circ_{\mathfrak{D}}(E)$, $\mathcal{D}'^\circ \in \mathcal{L}^\circ_{\mathfrak{D}'}(E)$ respectively, and that $I \subseteq \mathrm{Iso}(\mathfrak{D}, \mathfrak{D}')$ satisfies $S' \circ I \circ S = I$.*

Then the I-diagrammatic sum $\mathcal{D} \boxplus_I \mathcal{D}'$ has underlying structure $\mathfrak{D} \boxplus_I \mathfrak{D}'$, symmetry group $S \times S'$, and is represented by the labeled diagram $\mathcal{D}^\circ \boxplus_I \mathcal{D}'^\circ$.

For diagrams $\mathcal{D}_1, \mathcal{D}_2 \in \mathcal{L}^S_{\mathfrak{D}}(E)$ with the same underlying structure, we can take $I = S$ to get the *ordered diagrammatic sum* $\mathcal{D}_1^\circ \boxplus_S \mathcal{D}_2^\circ$. In this case, there is also another canonical automorphism, and we will use this *commutation* automorphism to get a commutative diagrammatic sum.

We note that generally, the I-diagrammatic sum operation is almost commutative; in fact, $\mathcal{D} \boxplus_I \mathcal{D}'$ and $\mathcal{D}' \boxplus_{I^{-1}} \mathcal{D}$ are related by an isomorphism ς of their underlying structures. For point labels, the map is $\varsigma(i,j) = (j,i)$; then we note that $(i,j) \in (l, \phi^{-1})$ if and only if $i = \phi^{-1}(j) \in l$, which is equivalent to $j = \phi(i) \in \phi(l)$. Hence:

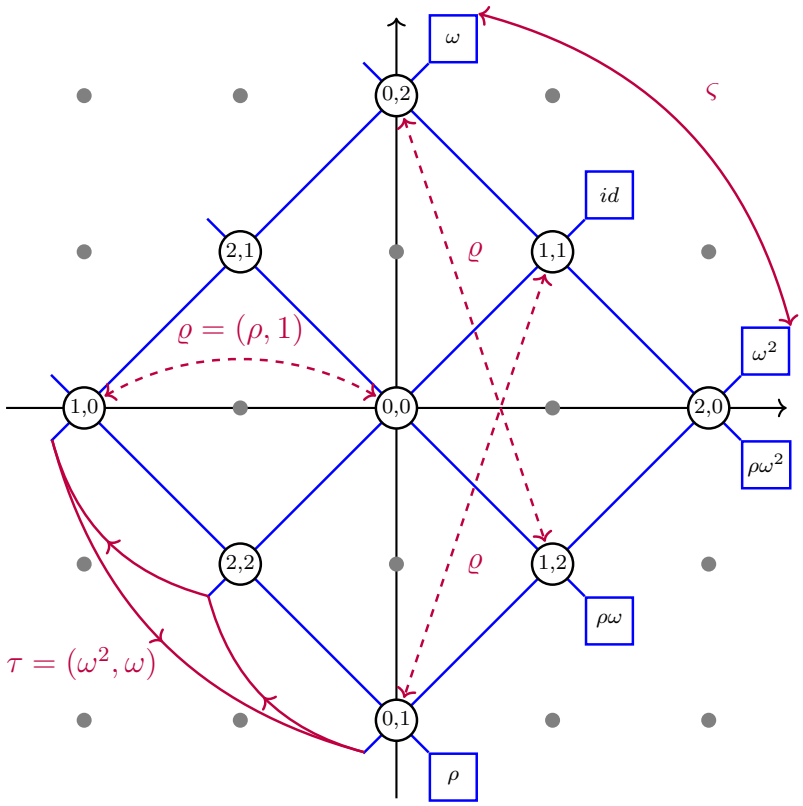
Definition 5.4.7. *The* commutation isomorphism $\varsigma : \mathfrak{D} \boxplus_I \mathfrak{D}' \to \mathfrak{D}' \boxplus_{I^{-1}} \mathfrak{D}$ *is defined as follows on point and line labels respectively:*

$$\varsigma(i,j) := (j,i), \qquad \varsigma(k, \phi^{-1}) := (\phi(k), \phi)$$

For the linear sum structure $\mathfrak{L}_\boxplus$, the symmetry group has generators ϱ, ς, τ:

- $\varrho = (\rho, id)$ transposes (01) in the first coordinate. This can also be thought of as a reflection across the line through the point labels $20, 21, 22$.
- ς swaps the indices. This can also be thought of as a reflection across the line through the point labels $00, 11, 22$.
- $\tau = (\omega^2, \omega)$ is a translation by $(-1, 1)$ in the Cartesian plane.

We represent this as follows:



Note that we use the same symbols for the generators of $\mathrm{Aut}(\mathfrak{N})$; this is in fact coordinated:

Lemma 5.4.8. *The linear sum structure is isomorphic to the nine point diagram structure via the following map $\phi : \mathfrak{L}_{\boxplus} \to \mathfrak{N}$ which is defined on point labels as*

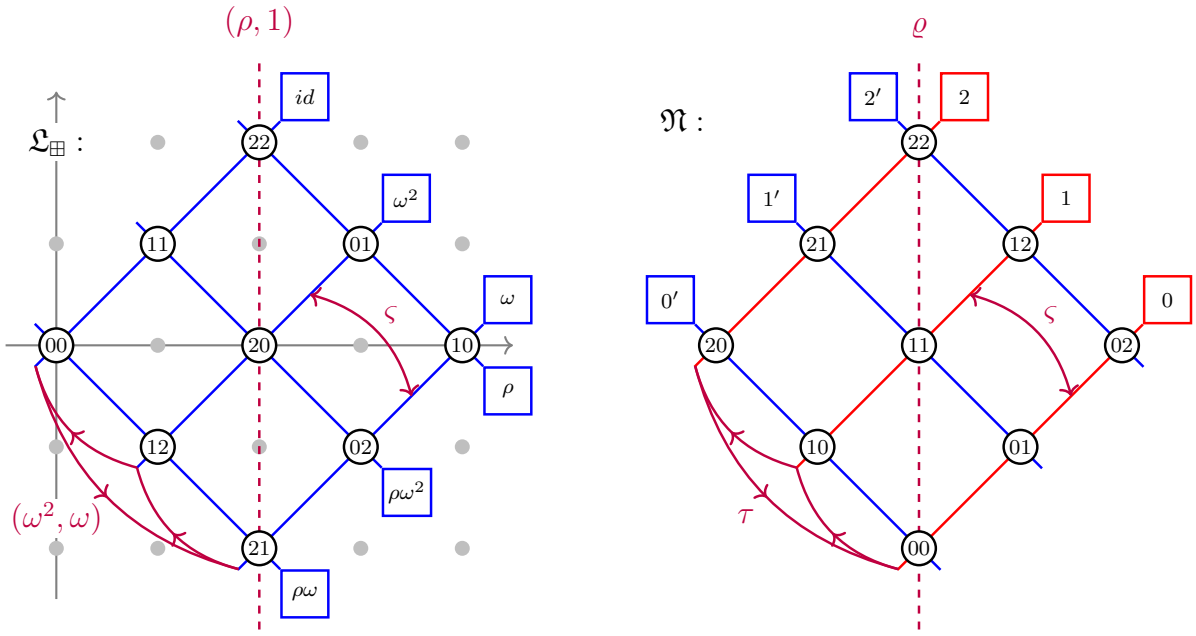
$$\phi : ij \mapsto (i - j - 1)(-i - j)$$

in modulus 3, and on line labels as

$$\phi : \ \omega^k \mapsto k - 1, \ \ \rho\omega^k \mapsto (k - 1)'$$

Furthermore, we can identify the automorphism groups via conjugation by ϕ. That is, the symbol ς will represent both the commutation automorphism on $\mathfrak{L}_{\boxplus}$ and the element of $\mathrm{Aut}(\mathfrak{N})$ that permutes the line labels as (01); we also make the identifications $\varrho = (\rho, id)$ and $\tau = (\omega^2, \omega)$.

We can represent this pictorially with the nine point diagram structure rotated 135° counterclockwise relative to our usual representation, and with different representatives for the point labels of $\mathfrak{L}_{\boxplus}$ in the Cartesian plane:



For completeness, we note other translations between $\mathrm{Aut}(\mathfrak{N})$ and $\mathrm{Aut}(\mathfrak{L}_{\boxplus})$; namely $\varsigma' = \sigma(\rho, \rho)$ and $\tau' = (\omega, \omega)$; and in the other direction $\varrho = (\rho, id)$, $\varrho\varsigma'\varsigma = (id, \rho)$, $\tau(\tau')^{-1} = (\omega, id)$ and $\tau^{-1}(\tau')^{-1} = (id, \omega)$.

5.4.3 Diagrammatic Sum

Now we are ready to define a more general analogue of a linear sum diagram:

Definition 5.4.9. *The* diagrammatic sum $\mathcal{D}_1 \boxplus \mathcal{D}_2$ *between* $\mathcal{D}_1, \mathcal{D}_2 \in \mathcal{L}^S_{\mathfrak{D}}(E)$ *is the* S*-diagrammatic sum* $\mathcal{D}_1^\circ \boxplus_S \mathcal{D}_2^\circ$*, under the action of the symmetry group generated by* $S \times S$ *and the commutation automorphism* ς*. Explicitly, the underlying structure is* $\mathfrak{D} \boxplus_S \mathfrak{D}$*, whose point/line labels are:*

$$\begin{aligned} &\{(i, \phi(i)) \ : \ i \in \mathfrak{P}, \ \phi \in S\} \\ &\{(k, \phi^{-1}) \ : \ k \in \mathfrak{L}, \ \phi \in S\} \end{aligned}$$

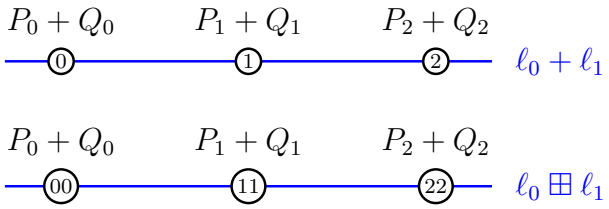
and incidence is given by $(i, \phi(i)) \in (k, \phi^{-1})$ *for any* $\phi \in S$ *whenever* $i \in k$ *in* $\mathfrak{D}$*. The point/line labels are assigned points/linear sets as follows:*

$$\begin{aligned} \mathfrak{p}_{ij}(\mathcal{D}_1^\circ \boxplus_S \mathcal{D}_2^\circ) =& \mathfrak{p}_i(\mathcal{D}_1^\circ) + \mathfrak{p}_j(\mathcal{D}_2^\circ) \\ \mathfrak{l}_{k,\phi^{-1}}(\mathcal{D}_1^\circ \boxplus_S \mathcal{D}_2^\circ) =& \mathfrak{l}_k\left(\mathcal{D}_1^\circ + \phi^{-1}\mathcal{D}_2^\circ\right) \\ =& \mathfrak{l}_k\left(\mathcal{D}_1^\circ\right) + \mathfrak{l}_{\phi(k)}\left(\mathcal{D}_2^\circ\right) \end{aligned}$$

The symmetry group of $\mathcal{D}_1 \boxplus \mathcal{D}_2$ is generated by $S \times S$ along with the commutation automorphism ς:

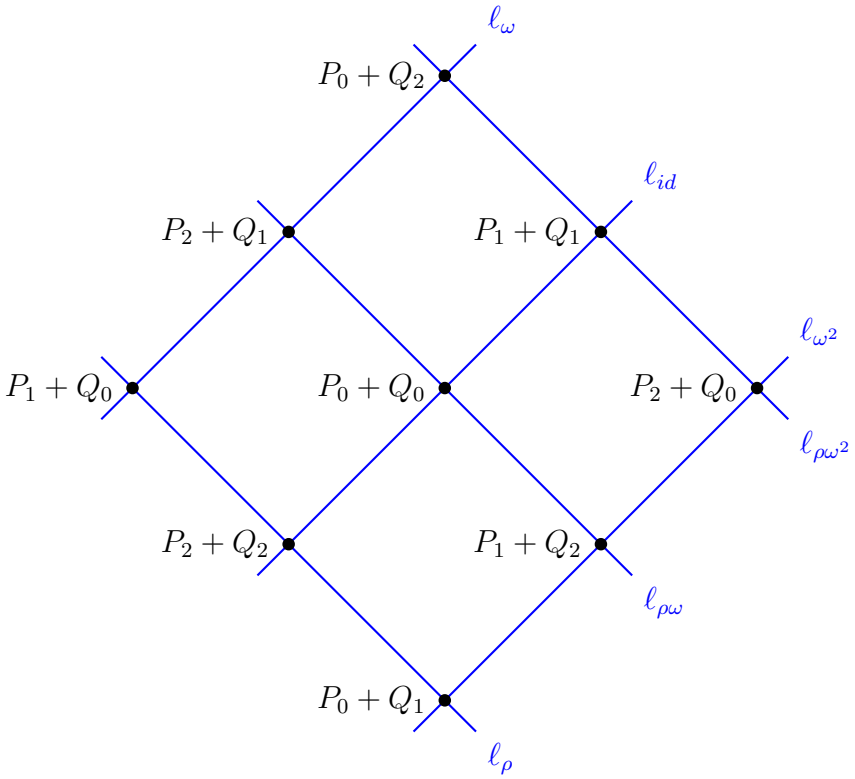
$$\begin{aligned}(\sigma_1, \sigma_2)(i,j) =& (\sigma_1(i), \sigma_2(j)), & (\sigma_1, \sigma_2)(k, \phi^{-1}) =& \left(\sigma_1(k), \sigma_1 \circ \phi^{-1} \circ \sigma_2^{-1}\right) \\ \varsigma(i,j) =& (j,i), & \varsigma(k, \phi^{-1}) =& (\phi(k), \phi)\end{aligned}$$

For example, consider labeled lines ℓ_0, ℓ_1 with respective points P_i, Q_i for $i = 0, 1, 2$. Then the diagrammatic sum $\ell_0 \boxplus \ell_1$ is essentially the same as the labeled line sum $\ell_0 + \ell_1$:



This is because a labeled line has trivial symmetry group, so the points must be paired together in the only possible way. We will in fact make this identification between $u + v$ and $u \boxplus v$ for labeled lines u, v.

For unlabeled lines $\ell_0^\bullet, \ell_1^\bullet \in \mathcal{L}_3^\bullet(E)$ represented by $\ell_0, \ell_1 \in \mathcal{L}_3^\circ(E)$ with respective points P_i, Q_i on label i, we get the following diagrammatic sum:



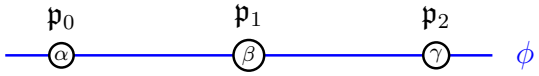
The lines in this diagrammatic sum are $\ell_\sigma = (u^\circ + \sigma v^\circ)^\bullet$ for $\sigma \in S_3$, at the label σ. This is in fact an unlabeled nine point diagram, since its symmetry group is the full automorphism group of the underlying structure $\mathfrak{L}_\boxplus$.

5.5 Homomorphisms of Diagrams

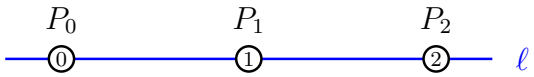
Our next step in understanding diagrammatic arithmetic is to take a closer look at the structure that appears in the diagrams we consider. Our main tools for this will be *diagrammatic homomorphisms*, which we will define in this section. We will use diagrammatic homomorphisms to express relations between various quantities involved in a diagrammatic addition. For example, the forward difference of a cyclically oriented line is given by a diagrammatic homomorphism, and can also be recovered from the linear sum diagram via a homomorphism. We will work with a general abelian group G here rather than E; the benefits of this will soon become clear.

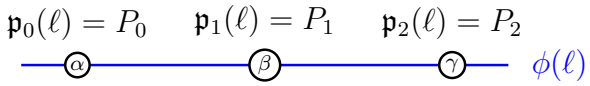
First we note that given an isomorphism $\phi : \mathfrak{D} \to \mathfrak{D}'$ of incidence structures, we have already seen how to define a *structural* isomorphism $\phi : \mathcal{L}^\circ_\mathfrak{D} \to \mathcal{L}^\circ_{\mathfrak{D}'}$. In this section, we will think of this as follows: for a label i of $\mathfrak{D}$, think of $\mathfrak{p}_i$ as a function that assigns a group element of G to a diagram from $\mathcal{L}^\circ_\mathfrak{D}(G)$. Then we define a diagram on $\mathfrak{D}'$, where to a point label i', we assign the function $\mathfrak{p}_{\phi^{-1}i}$. Then when we "plug" a diagram $\mathcal{D}$ in, we get the labeled diagram $\phi(\mathcal{D})$ on $\mathfrak{D}'$.

For example, if $\phi : \mathfrak{L}_3 \to \mathfrak{L}_{\{\alpha,\beta,\gamma\}}$ maps $0 \mapsto \alpha$, $1 \mapsto \beta$, $2 \mapsto \gamma$, then the structural isomorphism ϕ is represented as:

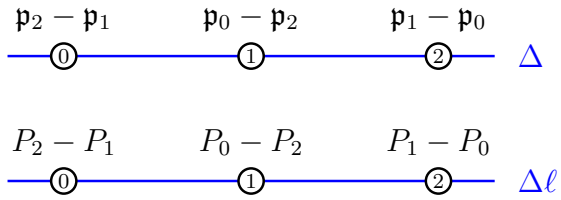


and by plugging in the following ℓ, we get $\phi(\ell)$:

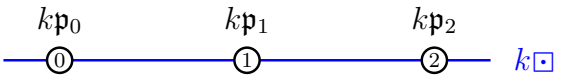




More generally, for a diagrammatic homomorphism $H : \mathcal{L}^\circ_\mathfrak{D} \to \mathcal{L}^\circ_{\mathfrak{D}'}$, to a label of $\mathfrak{D}'$ we will assign a linear combination of the functions $\mathfrak{p}_i$ from $\mathfrak{D}$. For example, the forward difference homomorphism $\Delta : \mathcal{L}^\circ_3 \to \mathcal{L}^\circ_3$ is given as follows, along with its application to the labeled line ℓ from earlier:



Another example that we have seen is the multiplication by k map $k\boxdot$ is a diagrammatic homomorphism on any structure, with $k\boxdot : \mathcal{L}_3^\circ \to \mathcal{L}_3^\circ$ represented as:



Precisely, these assignments will come from the following group:

Definition 5.5.1. *To each incidence structure $\mathfrak{D}$, we associate an abelian group $\langle\mathfrak{D}\rangle$ which is called the* diagrammatic group*, and is presented as follows:*

- *For each $i \in \mathfrak{P}$, there is a generator $\mathfrak{p}_i$*
- *For each $j \in \mathfrak{L}$, there is a relation $\sum_{i\in j} \mathfrak{p}_i = 0$*

For example, $\langle\mathfrak{L}_3\rangle$ is generated by $\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_2$, and those satisfy $\mathfrak{p}_0 + \mathfrak{p}_1 + \mathfrak{p}_2 = 0$. Now we simply define a diagrammatic homomorphism $H : \mathcal{L}_\mathfrak{D}^\circ \to \mathcal{L}_{\mathfrak{D}'}^\circ$ to be a labeled diagram on $\mathcal{L}_{\mathfrak{D}'}^\circ$ with point label i' of $\mathfrak{D}'$ being assigned a value from the diagrammatic group $\langle\mathfrak{D}\rangle$. In other words, $H \in \mathcal{L}_{\mathfrak{D}'}^\circ(\langle\mathfrak{D}\rangle)$:

Definition 5.5.2. *A* diagrammatic homomorphism $H : \mathcal{L}_\mathfrak{D}^\circ \to \mathcal{L}_{\mathfrak{D}'}^\circ$ *is an element $H \in \mathcal{L}_{\mathfrak{D}'}^\circ(\langle\mathfrak{D}\rangle)$.*

For a group G, a diagrammatic homomorphism $H : \mathcal{L}_\mathfrak{D}^\circ \to \mathcal{L}_{\mathfrak{D}'}^\circ$ gives rise to a map $H : \mathcal{L}_\mathfrak{D}^\circ(G) \to \mathcal{L}_{\mathfrak{D}'}^\circ(G)$. To describe this, start with $\mathcal{D} \in \mathcal{L}_\mathfrak{D}^\circ(G)$ which assigns $\mathfrak{p}_i(\mathcal{D}) \in G$ to a point label i of $\mathfrak{D}$. Then in the diagram H, if each instance of $\mathfrak{p}_i$ is replaced with $\mathfrak{p}_i(\mathcal{D})$, then the diagram $H(\mathcal{D}) \in \mathcal{L}_{\mathfrak{D}'}^\circ(G)$ is obtained. We will make this more precise in the next subsection.

5.5.1 Algebraic Definition of Diagrammatic Homomorphisms

To more precisely define diagrammatic homomorphisms, we start with a more algebraic definition of a labeled diagram:

Definition 5.5.3. *Given an abelian group G, a* labeled diagram $\mathcal{D}$ *over G with structure $\mathfrak{D}$ corresponds to a group homomorphism $\Gamma_{\mathcal{D}} : \langle \mathfrak{D} \rangle \to G$. Equivalently,*

- *A group element $\mathfrak{p}_i(\mathcal{D}) := \Gamma_{\mathcal{D}}(\mathfrak{p}_i) \in G$ is assigned each $i \in \mathfrak{P}$*
- *For each $j \in \mathfrak{L}$, the assignments are subject to the constraint $\sum_{i \in j} \mathfrak{p}_i(\mathcal{D}) = 0$*

The collection of all labeled diagrams over G with structure $\mathfrak{D}$ will be denoted $\mathcal{L}^{\circ}_{\mathfrak{D}}(G)$.

Now we reconsider our definition of a diagrammatic homomorphism $H \in \mathcal{L}^{\circ}_{\mathfrak{D}'}(\langle \mathfrak{D} \rangle)$. Such an H corresponds to a group homomorphism $\Gamma_H : \langle \mathfrak{D}' \rangle \to \langle \mathfrak{D} \rangle$. Thus from $\mathcal{D} \in \mathcal{L}^{\circ}_{\mathfrak{D}}(G)$, we obtain $H\mathcal{D} \in \mathcal{L}^{\circ}_{\mathfrak{D}'}(G)$ by functional composition $\Gamma_{H\mathcal{D}} := \Gamma_{\mathcal{D}} \circ \Gamma_H$:

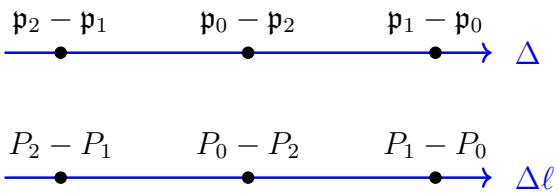
Definition 5.5.4. *Given incidence structures $\mathfrak{D}, \mathfrak{D}'$, a* diagrammatic homomorphism *$H : \mathcal{L}^{\circ}_{\mathfrak{D}} \to \mathcal{L}^{\circ}_{\mathfrak{D}'}$ is an element of $\mathcal{L}^{\circ}_{\mathfrak{D}'}(\langle \mathfrak{D} \rangle)$. For $\mathcal{D} \in \mathcal{L}^{\circ}_{\mathfrak{D}}(G)$, we define $H\mathcal{D} \in \mathcal{L}^{\circ}_{\mathfrak{D}'}(G)$ via the associated group homomorphism $\Gamma_{H\mathcal{D}} := \Gamma_{\mathcal{D}} \circ \Gamma_H$, where $\circ$ represents functional composition.*

We can apply a diagrammatic homomorphism to a diagram with symmetry, under the proper conditions. For $H : \mathcal{L}^{\circ}_{\mathfrak{D}} \to \mathcal{L}^{\circ}_{\mathfrak{D}}$, we would like to simply define $H : \mathcal{L}^{S}_{\mathfrak{D}} \to \mathcal{L}^{S'}_{\mathfrak{D}'}$, but this might run into trouble. Namely, the result should not change if we apply $\sigma \in S$ to $\mathfrak{D}$; hence $H\sigma$ should be equal to $\sigma' H$ for some $\sigma' \in S'$. But if such a condition holds for each $\sigma \in S$, then we in fact get a well-defined diagrammatic homomorphism:

Definition 5.5.5. *Given incidence structures $\mathfrak{D}, \mathfrak{D}'$, and respective symmetry groups S, S', suppose that $H : \mathcal{L}^{\circ}_{\mathfrak{D}} \to \mathcal{L}^{\circ}_{\mathfrak{D}'}$ satisfies $\Gamma_S \circ \Gamma_H \subseteq \Gamma_H \circ \Gamma_{S'}$. Then we define $H : \mathcal{L}^{S}_{\mathfrak{D}} \to \mathcal{L}^{S'}_{\mathfrak{D}'}$ to be the orbit of $H \in \mathcal{L}^{\circ}_{\mathfrak{D}'}(\langle \mathfrak{D} \rangle)$ under the action of S'.*

Note that for $\mathcal{D} \in \mathcal{L}^{S}_{\mathfrak{D}}(G)$, we will have $H\mathcal{D} \in \mathcal{L}^{S'}_{\mathfrak{D}'}(G)$ with $H\mathcal{D} = S'(H\mathcal{D}^{\circ})$ for any representative $\mathcal{D}^{\circ} \in \mathcal{L}^{\circ}_{\mathfrak{D}}(G)$.

An example of a homomorphism with symmetry is the forward difference homomorphism on cyclic line diagrams $\Delta : \mathcal{L}^{\triangleright}_{\mathfrak{D}} \to \mathcal{L}^{\triangleright}_{\mathfrak{D}}$:



5.5.2 Forgetful Homomorphisms

We have already worked with a simple example of a homomorphism of diagrams with symmetry; namely the homomorphism $(\cdot)^\bullet$ which turns an arbitrary diagram into an unlabeled diagram:

Definition 5.5.6. *For an incidence structure $\mathfrak{D}$ and symmetry groups $S_0 \subseteq S_1 \subseteq \mathrm{Aut}(\mathfrak{D})$, the following* forgetful homomorphism *is induced by the identity homomorphism:*

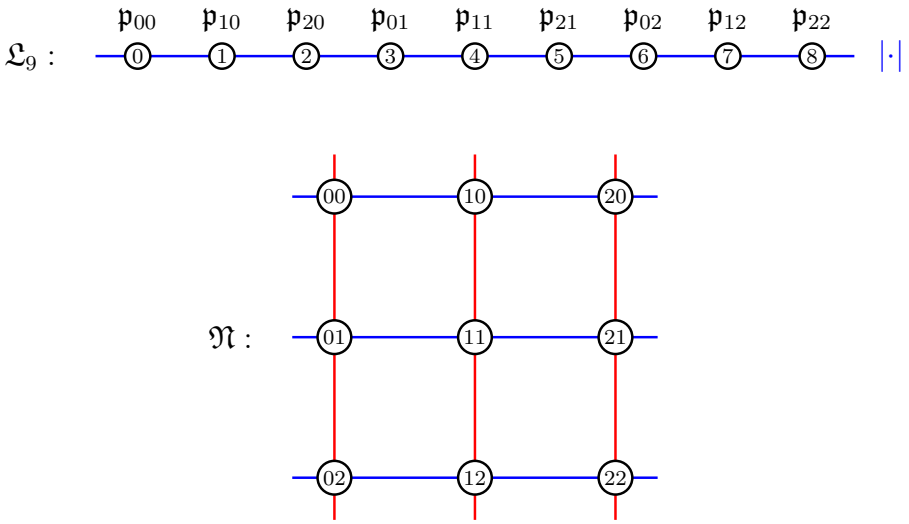
$$(\cdot)^{S_1} : \mathcal{L}_{\mathfrak{D}}^{S_0} \to \mathcal{L}_{\mathfrak{D}}^{S_1}$$

When $S_1 = \mathrm{Aut}(\mathfrak{D})$, this is denoted $(\cdot)^\bullet$.

For example, a labeled line diagram ℓ gives rise to a cyclic line diagram $\ell^{\{id,\omega,\omega^2\}}$, which we normally denote $\ell^{\triangleright}$. These examples of "forgetful" homomorphisms all leave the collection of points on a labeled diagram untouched, but there is no homomorphism which can recover the original structure.

We will more generally refer to homomorphisms with this property as *forgetful*. Another such homomorphism on a nine point diagram this outputs the unlabeled 9-line that contains the same points:

Definition 5.5.7. *The* forgetful homomorphism $|\cdot| : \mathcal{L}_{\mathfrak{N}}^{S} \to \mathcal{L}_9^\bullet$ *is defined by the following diagram (with $\mathfrak{N}$ included below as a reminder):*



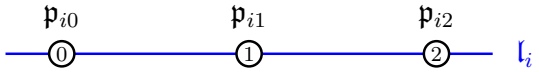
We note that this is possible because $\mathcal{N}$ can be partitioned into 3 lines; hence the points of $\mathcal{N}$ sum to $\mathcal{O}$.

The forgetful homomorphism encompasses the same information as the normalized function $\mathcal{N}(x, y) \in \mathbb{F}(E)$ that vanishes at those nine points. Hence we consider this forgetful homomorphism to be a purely diagrammatic analog to *diagram functions* that we will study in chapter 6.

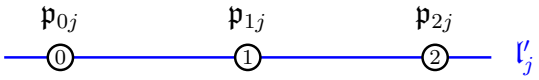
5.5.3 Line Extraction

We would like to view the lines in a nine point diagram as labeled lines in their own right. To accomplish this, we define homomorphisms to extract the lines:

Definition 5.5.8. *For $i \in \{0, 1, 2\}$, the diagrammatic homomorphism $\mathfrak{l}_i : \mathcal{L}^\circ_{\mathfrak{N}} \to \mathcal{L}^\circ_3$ is given by:*



and similarly for $j \in \{0, 1, 2\}$:

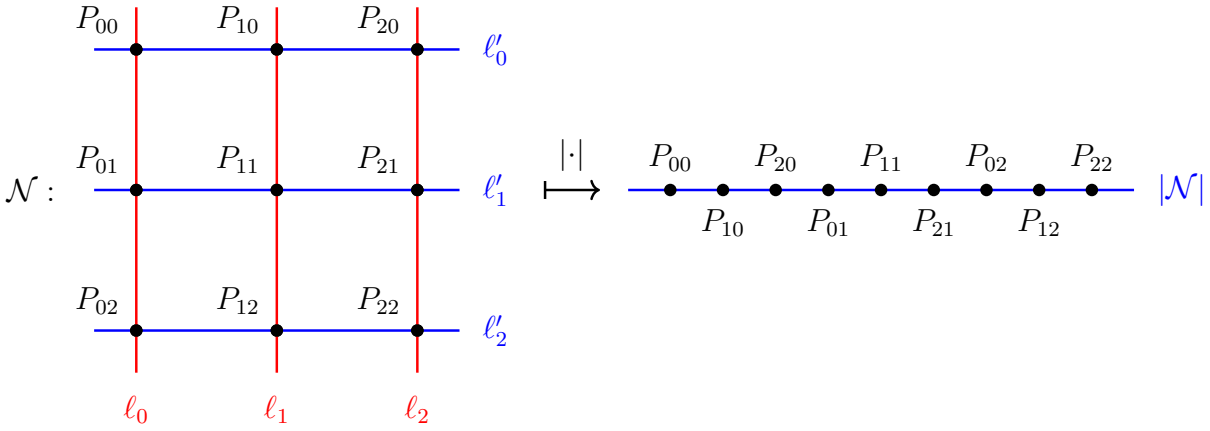


Note that $\mathfrak{l}_0 + \mathfrak{l}_1 + \mathfrak{l}_2 = \mathfrak{l}'_0 + \mathfrak{l}'_1 + \mathfrak{l}'_2 = 0$ is the zero homomorphism.

5.6 Linear Arithmetic

Here we will discuss the arithmetic of line diagrams. We will recontextualize the results of previous chapters, and outline the progress that we will make in future chapters.

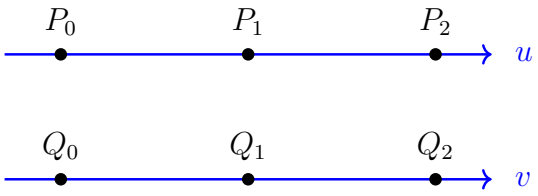
The diagrammatic sum $u \boxplus v$ for $u, v \in \mathcal{L}^\bullet_3(E)$ carries a lot of information about the line sum $u + v$ between u, v, given only the unlabeled lines themselves. In the next chapter, we will develop a diagrammatic calculus which will help us to use this additional structure. In contrast, the generic line multiplication that we have previously focused on "forgets" a lot of the structure found in the diagrammatic sum. In fact, the generic algorithm only uses the unlabeled collection of points, and thus essentially we are working in $\mathcal{L}^\bullet_n(E)$. Recall the forgetful homomorphism from definition 5.5.7:



Most of the progress we make in the following chapters focuses in one way or another on improving on generic line multiplication, by using more of the line sum structure. In particular, we will impose additional structure on lines u, v, and then take advantage of the additional structure on $u \boxplus v$ that results.

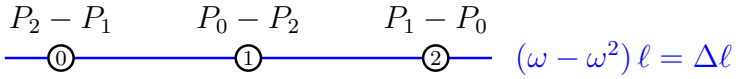
5.6.1 Cyclic Line Arithmetic

The simplest way to add structure to the line sum diagram is to add structure to the input lines. So we now reconsider cyclically oriented lines $u, v \in \mathcal{L}_3^{\triangleright}(E)$:



Now we reconsider cyclic line arithmetic of section 3.4, in terms of line diagrams. We start by noting that $1+\omega+\omega^2$ acts as 0 on labeled line diagrams. That is, $(1+\omega+\omega^2) \boxdot \ell$ is the identity element $\ell_{\mathcal{O}}$ for any labeled line diagram $\ell \in \mathcal{L}_3^{\circ}(E)$:

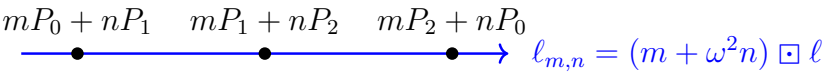
Thus we have an action of the Eisenstein integers $\mathbb{Z}[\omega]/\langle 1+\omega+\omega^2 \rangle$ on labeled line diagrams. In particular, note that $(\omega - \omega^2)\,\ell$ is the following forward difference:



Furthermore, we will notate $\sqrt{-3} := \omega - \omega^2$, noting that in the Eisenstein integers $(\omega - \omega^2)^2 = -3$.

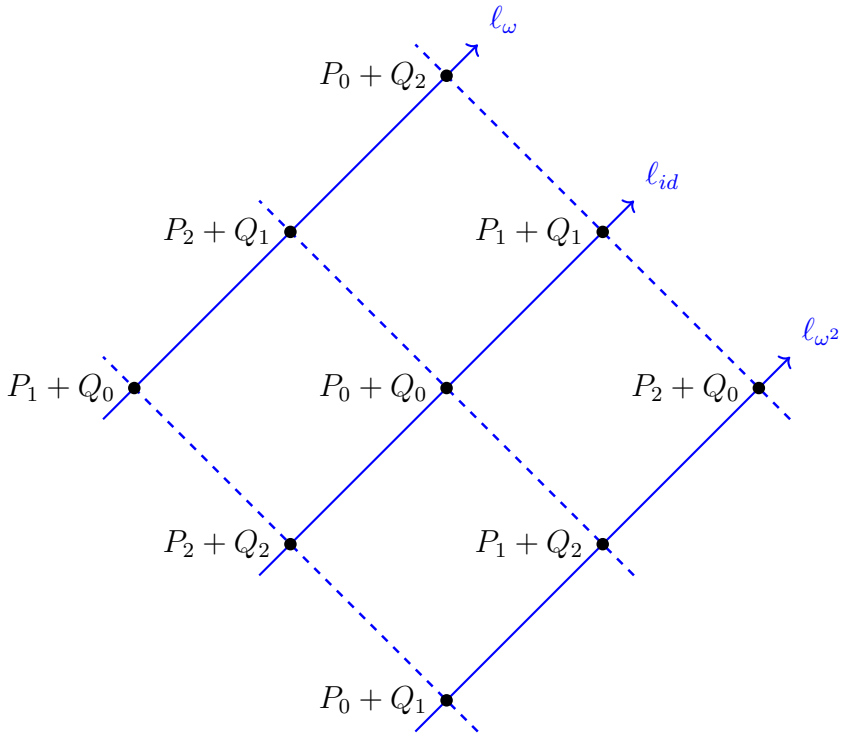
Now we can reinterpret cyclic line diagrams as orbits of $\mathcal{L}_3^\circ(E)$ under the action of the Eisenstein integers $\{1, \omega, \omega^2\}$. Then we get an action of the Eisenstein integers on cyclic line diagrams, and we simply have $\sqrt{-3} \boxdot \ell = \Delta\ell$. Note also that $\omega \boxdot \ell = \ell$ for a cyclic line diagram $\ell \in \mathcal{L}_3^\triangleright(E)$.

Given a cyclic line ℓ, suppose we want to calculate $k \boxdot \ell$ for $k \in \mathbb{Z}$. Recall the auxiliary lines $\ell_{m,n}$ that we introduced in section 3.8, with points $mP_i + nP_{i+1}$ for i in modulus 3. We can now simply define this as $\ell_{m,n} := (m + \omega^2 n) \boxdot \ell$:



This notation will simplify matters when we reconsider cyclic line multiplication. To illustrate this, observe that the transformation rules $\ell_{m,n} = \ell_{n-m,-m} = \ell_{-n,m-n}$ are more simply stated as $\mu \boxdot \ell = \omega\mu \boxdot \ell$ for an Eisenstein integer μ. If we add cyclic line diagrams $\mu \boxdot \ell$ and $\nu \boxdot \ell$, then we get three possibilities: the "good" sum $(\mu + \nu) \boxdot \ell$, or the "bad" ones $(\mu + \omega\nu) \boxdot \ell, (\mu + \omega^2\nu) \boxdot \ell$.

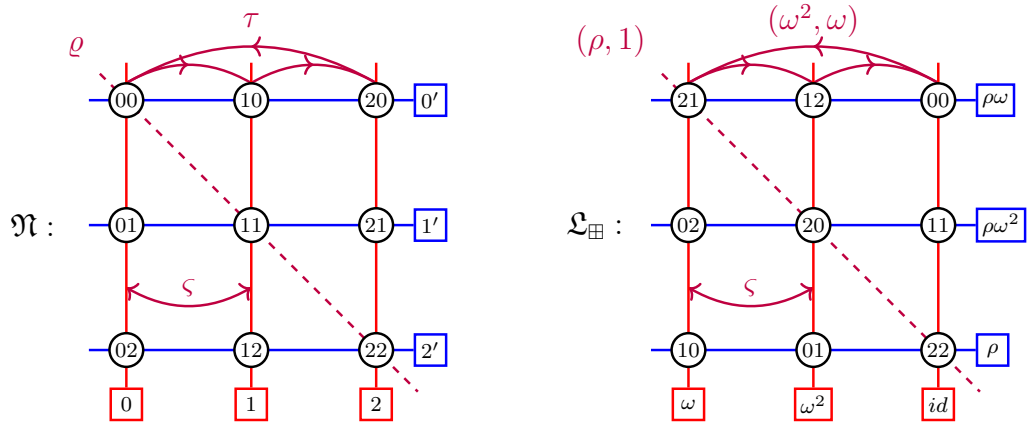
The following is the diagrammatic sum of u and v, which we notate $u^\triangleright \boxplus v^\triangleright$:



The three possible cyclic sum lines between u and v are indicated as $\ell_1, \ell_\omega, \ell_{\omega^2}$. The indices indicate that $\ell_\sigma = (u^\circ + \sigma v^\circ)^\triangleright$, with the superscript $\triangleright$ indicating that we are considering the parenthesized line diagram as being a cyclic line diagram.

Note that this diagrammatic sum has a group of 18 symmetries. In contrast, a disjoint union of three cyclic lines would have $3 * 3 * 3 * 6$ automorphisms, corresponding to shifting each line arbitrarily, and then permuting the three lines arbitrarily. The arrowheads and dotted lines indicate the extra constraints that make this distinction. Namely, the symmetries of the diagrammatic sum are exactly the nine point diagram automorphisms that take dotted lines to dotted lines, and respect the indicated line orientations.

To be more explicit, $\mathrm{Aut}(u^\triangleright \boxplus v^\triangleright) = \langle \varsigma, \tau, \tau' \rangle$. Geometrically, the commutation automorphism ς is a reflection across the diagonal in the $(1,1)$ direction; $\tau = (\omega^2, \omega)$ is a translation by $(-1,1)$ and $\tau' = (\omega, \omega)$ is a translation by $(1,1)$. A nine point diagram with the same 18 symmetries will be called a *cyclic nine point diagram*. We include the following diagram as a reminder (drawn differently from that in section 5.4.2):



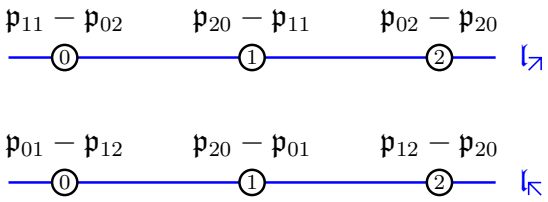
So we have $\ell_0 \leftrightarrow \ell_\omega$, $\ell_1 \leftrightarrow \ell_{\omega^2}$, $\ell_2 \leftrightarrow \ell_{id}$.

5.6.2 Forward Differences

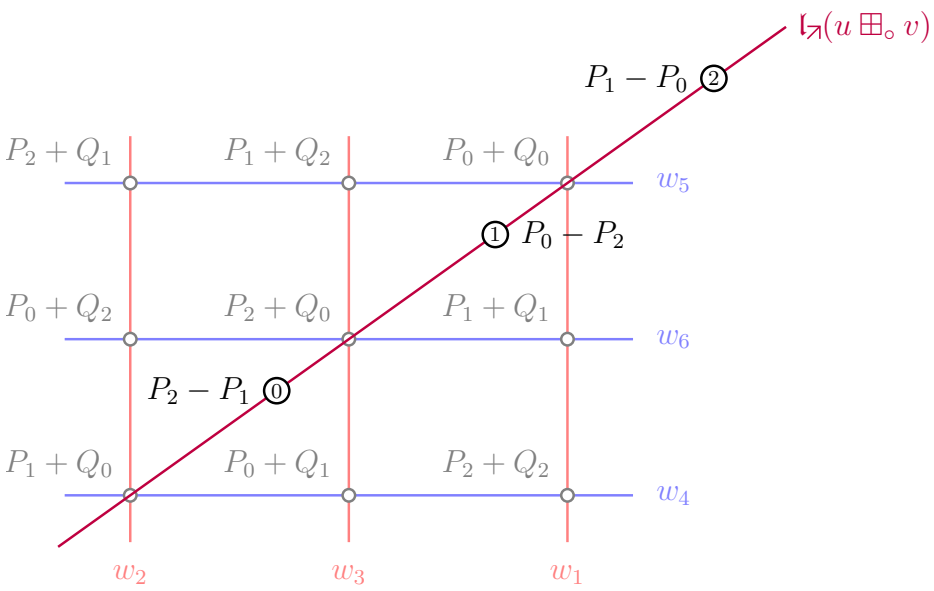
Now we consider the problem of recovering $\Delta u, \Delta v \in \mathcal{L}_3^{\triangleright}$ from the linear sum diagram. Since the point at coordinate (i, j) is $P_i + Q_j$, this is easy to accomplish. Namely, by starting at any point and taking the forward difference while traveling in the $(1, 0)$ direction, you will get Δu, since the Q_j terms will cancel out. Now we will describe this in terms of $\mathrm{Aut}(\mathfrak{N})$, since the diagram will not always be so nicely fit into a grid. Hence we take the forward difference starting in the $\tau(\tau')^{-1} = (\omega, 1)$ direction. Similarly, we get Δv by taking the forward difference in the $\tau^{-1}(\tau')^{-1}$ direction.

Now we will define these as functions of a labeled nine point diagram:

Definition 5.6.1. *The* northeast forward difference *homomorphism* $\mathfrak{l}_\nearrow : \mathcal{L}_{\mathfrak{N}}^\circ \to \mathcal{L}_3^\circ$ *and the* northwest forward difference *homomorphism* $\mathfrak{l}_\nwarrow : \mathcal{L}_{\mathfrak{N}}^\circ \to \mathcal{L}_3^\circ$ *are represented as follows:*



We can verify that $\Delta u = \mathfrak{l}_\nearrow(u \boxplus_\circ v)^\triangleright$ and $\Delta v = \mathfrak{l}_\nwarrow(u \boxplus_\circ v)^\triangleright$ when $u \boxplus_\circ v$ is identified with the following nine point diagram:



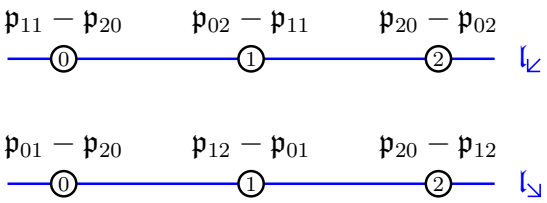
In chapter 6, we will find explicit formulas for $\mathfrak{l}_{\nearrow}(\mathcal{N})$ and $\mathfrak{l}_{\nwarrow}(\mathcal{N})$, and these will give us relations between lines involved in a line addition step.

Note that $\mathfrak{l}_{\nwarrow} = \mathfrak{l}_{\nearrow} \circ \varsigma$, which corresponds to the fact that ς changes the order of summation, when considered as an automorphism of $u \boxplus_\circ v$. In the same vein, if we apply ρ to the first summand u, the forward difference becomes:

$$\Delta \rho u = (\omega - \omega^2)\rho u = \rho(\omega^2 - \omega)u = -\rho \Delta u$$

and this corresponds to the operation $\varrho \in \mathrm{Aut}(\mathfrak{N})$. Hence we define $\mathfrak{l}_{\swarrow} = -\rho \mathfrak{l}_{\nearrow} = \mathfrak{l}_{\nearrow} \circ \varrho$ and similarly $\mathfrak{l}_{\searrow} = -\rho \mathfrak{l}_{\nwarrow}$:

Definition 5.6.2. *We define the* southwest/southeast forward differences *respectively as:*

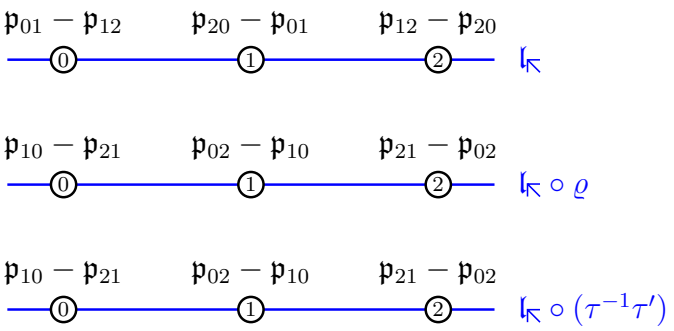


Of course, as unlabeled lines these are simply the negatives of the other two: $\mathfrak{l}^{\bullet}_{\swarrow} = -\mathfrak{l}^{\bullet}_{\nearrow}$ and $\mathfrak{l}^{\bullet}_{\searrow} = \mathfrak{l}^{\bullet}_{\nwarrow}$.

Now we note that $\mathfrak{l}_{\nearrow}(u \boxplus_\circ v) = \Delta u$ is invariant under (id, σ) for any $\sigma \in S_3$. These in fact translates into invariances of $\mathfrak{l}_{\nearrow}$ as a homomorphism (see section 5.4.2):

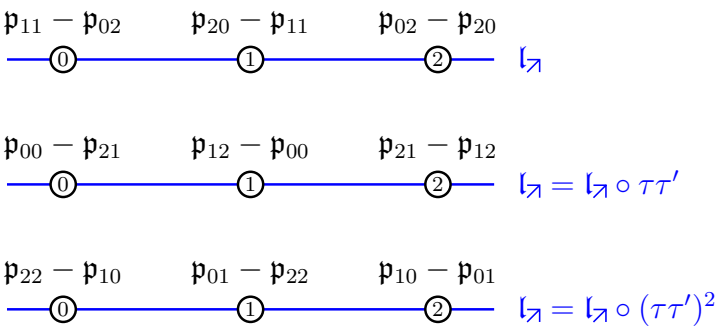
Lemma 5.6.3. *The homomorphism $\mathfrak{l}_\nearrow$ is invariant under composition on the right by $\langle \varrho\varsigma'\varsigma, \tau\tau' \rangle$, while $\mathfrak{l}_\nwarrow$ is invariant under $\langle \varrho, \tau^{-1}\tau' \rangle$.*

Proof. We verify this for $\mathfrak{l}_\nwarrow$ first:

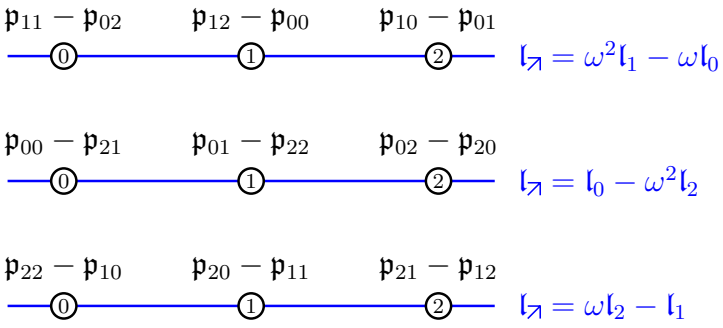


Then we note that $\mathfrak{p}_{01} - \mathfrak{p}_{12} = \mathfrak{p}_{10} - \mathfrak{p}_{21}$ holds because $0 = \mathfrak{p}_{01} + \mathfrak{p}_{11} + \mathfrak{p}_{21} = \mathfrak{p}_{10} + \mathfrak{p}_{11} + \mathfrak{p}_{12}$ by collinearity; the other two points on $\mathfrak{l}_\nwarrow$ and $\mathfrak{l}_\nwarrow \circ \varrho$ similarly match. Clearly the last two lines are the same. Then since $\mathfrak{l}_\nwarrow = \mathfrak{l}_\nearrow \circ \varsigma$, it follows that $\mathfrak{l}_\nearrow$ is invariant under $\varsigma\varrho\varsigma = \varrho\varsigma'\varsigma$ and $\varsigma\tau^{-1}\tau'\varsigma = \tau\tau'$. □

Now we compare the following three representations of $\mathfrak{l}_\nearrow$, obtained by successively composing on the right by $\tau\tau'$:



Then we notice that by mixing and matching these representations, we can express $\mathfrak{l}_\nearrow$ in terms of $\mathfrak{l}_0, \mathfrak{l}_1, \mathfrak{l}_2$ (see section 5.5.3):



Note that the equality of these expressions is a consequence of the fact that $\mathfrak{l}_0 + \mathfrak{l}_1 + \mathfrak{l}_2 = 0$. More generally:

Lemma 5.6.4.

$$\begin{aligned}\mathfrak{l}_{\nearrow} =& \omega\mathfrak{l}_2 - \mathfrak{l}_1 = \mathfrak{l}_0 - \omega^2\mathfrak{l}_2 = \omega^2\mathfrak{l}_1 - \omega\mathfrak{l}_0\\ \mathfrak{l}_{\nwarrow} =& \mathfrak{l}_1 - \omega^2\mathfrak{l}_2 = \omega\mathfrak{l}_2 - \mathfrak{l}_0 = \omega^2\mathfrak{l}_0 - \omega\mathfrak{l}_1\end{aligned}$$

Proof. The first line was already demonstrated. The second comes from $\mathfrak{l}_{\nwarrow} = \mathfrak{l}_{\nearrow} \circ \varsigma$, noting that $\mathfrak{l}_0 \circ \varsigma = \mathfrak{l}_1$, $\mathfrak{l}_1 \circ \varsigma = \mathfrak{l}_0$ and $\mathfrak{l}_2 \circ \varsigma = \mathfrak{l}_2$. □

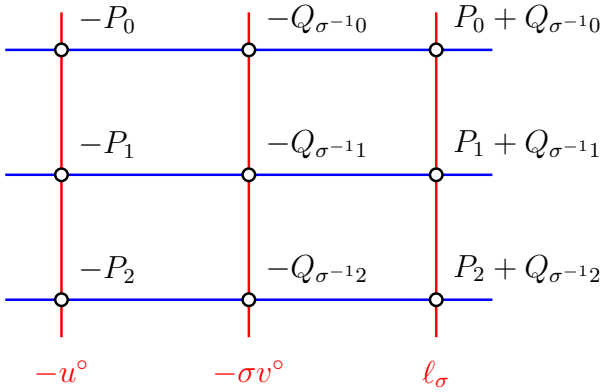
We will often use the expressions $\mathfrak{l}_{\nearrow} = \omega^2\mathfrak{l}_1 - \omega\mathfrak{l}_0, \mathfrak{l}_{\nwarrow} = \omega^2\mathfrak{l}_0 - \omega\mathfrak{l}_1$ directly, since they are easier to work with than the definitions themselves.

5.7 Nine Point Diagram Dichotomy

In this section, we discuss nine point diagrams, and elaborate on the dichotomy between viewing it as $\mathfrak{N}$ or $\mathfrak{L}_{\boxplus}$. Recall that the structure $\mathfrak{L}_{\boxplus}$ was defined to be the structure of a diagrammatic sum. This structure arises naturally as a way to organize the various sum lines ℓ_σ between two line diagrams u, v. On the other hand, the structure $\mathfrak{N}$ has been analyzed as a collection of three labeled lines which sum to zero $\mathfrak{l}_0 + \mathfrak{l}_1 + \mathfrak{l}_2 = 0$, as well as an involution ϱ.

To connect these two points of view, we start by considering a sum line ℓ_σ between lines u, v. We then note that the sum between $-u$, $-v$ and ℓ_σ vanishes, if the addition is interpreted appropriately. And that interpretation is best expressed with a nine point diagram structure on $-u, -v, \ell_\sigma$! For example we take the lines $-u^\circ, -\sigma v^\circ, \ell_\sigma$:

$(-u^\circ, -\sigma v^\circ, \ell_\sigma^\circ)$:



noting that the other three lines indicate how to connect points from $-u, -v, \ell_\sigma$ to obtain $\ell_\mathcal{O}$ as a sum.

We can in fact connect the all of the diagrams obtained this way together into a *completion diagram*. On top of that, since all sum points $P_i + Q_j$ and sum lines ℓ_σ appear, it will also be endowed with a $u \boxplus v$ diagram among those. Just as a nine point diagram contains 6 line diagrams, the completion diagram will turn out to contain 10 nine point diagrams in its 15 points. Completion diagrams connect all of the lines that appear in a step of line addition. In the next chapter, we will show that a large array of relations can be simply understood on a completion diagram.

5.7.1 Completion Diagram

We will now define the completion diagram structure, in terms of the linear sum structure $\mathfrak{L}_\boxplus$. To obtain the point labels of $\mathfrak{C}$, we start with the point labels of $\mathfrak{L}_\boxplus$, then append points $L0, L1, L2$ and $R0, R1, R2$, to represent the points of $-u, -v$ in the $(-u, -v, \ell_\sigma)$ diagrams. Then we attach two line labels L, R which are incident to Li, Ri respectively for $i = 0, 1, 2$. Lastly, for each point label ij of $\mathfrak{L}_\boxplus$, we add a line label ij which is incident to the point labels Li, Rj, ij.

Definition 5.7.1. *The* completion diagram *structure* $\mathfrak{C}$ *has point labels:*

$$\{ij \ : i, j \in \{0, 1, 2\}\} \cup \{L0, L1, L2\} \cup \{R0, R1, R2\}$$

and line labels

$$\{L, R\} \cup \{ij \ : i, j \in \{0, 1, 2\}\} \cup S_3$$

with incidences:

$$Li \in L, \quad Ri \in R, \quad Li, Rj, ij \in ij, \quad i\sigma^{-1}i \in \sigma$$

for each $i, j \in \{0, 1, 2\}$.

We attach an automorphism group to this, which acts on the lines labeled L, R. In fact, the symmetry group is the same as that for the linear sum structure $\mathfrak{L}_{\boxplus}$ and $\mathfrak{N}$, and we will reuse the notation. First we present the $\mathrm{Aut}(\mathfrak{C})$ using the notation of diagrammatic sums:

Definition 5.7.2. *The automorphism group* $\mathrm{Aut}(\mathfrak{C})$ *is generated by* $S_3 \times S_3$*, and an element* ς *of order two. The subgroup* $S_3 \times S_3$ *acts on point labels via*

$$(\sigma_L, \sigma_R): \quad Li \mapsto L\sigma_L(i), \quad Ri \mapsto R\sigma_R(i), \quad ij \mapsto \sigma_L(i)\sigma_R(j)$$

and on line labels via

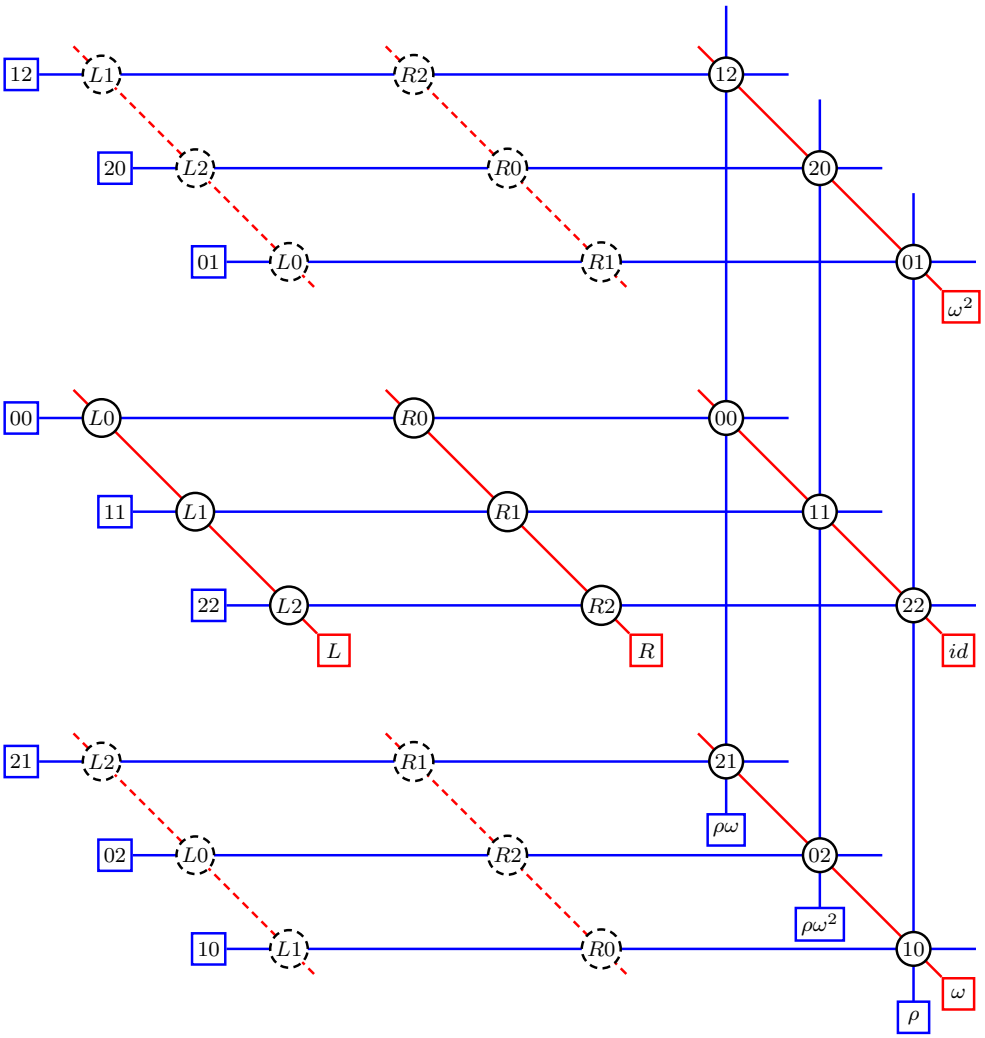
$$(\sigma_L, \sigma_R): \quad L \mapsto L,\ R \mapsto R, \quad ij \mapsto \sigma_L(i)\sigma_R(j), \quad \sigma \mapsto \sigma_L \sigma \sigma_R^{-1}$$

while ς *transposes point labels* $ij \leftrightarrow ji$ *and* $Li \leftrightarrow Ri$*; and transposes line labels* $ij \leftrightarrow ji$*,* $L \leftrightarrow R$ *and* $\sigma \leftrightarrow \sigma^{-1}$ *for* $\sigma \in S_3$*.*

We use the notation $\tau = (\omega^2, \omega)$ *and* $\varrho = (\rho, id)$*, and note that* $\mathrm{Aut}(\mathfrak{C})$ *can be identified with* $\mathrm{Aut}(\mathfrak{L}_{\boxplus})$ *and* $\mathrm{Aut}(\mathfrak{N})$ *via this notation.*

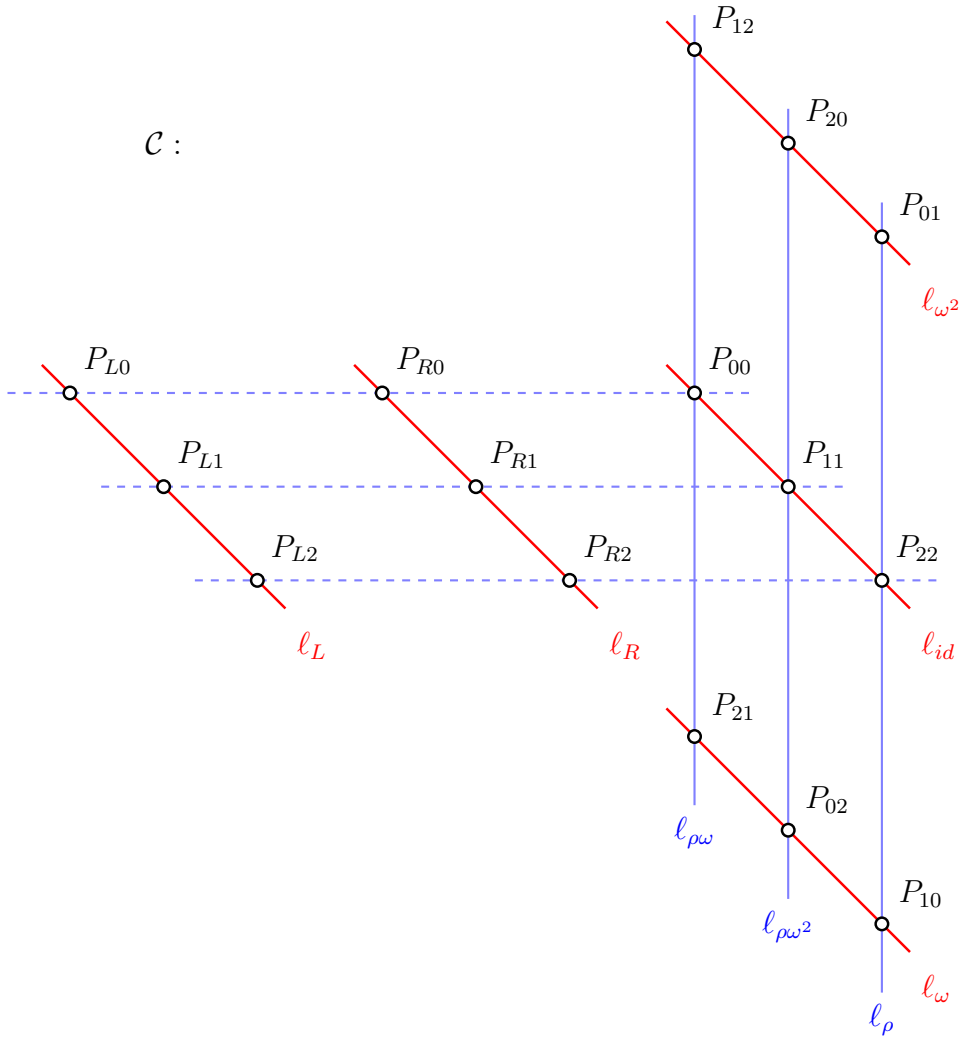
Now consider the incidence that only includes the two lines labeled L, R. In fact, that structure is diagrammatically isomorphic to $\mathfrak{C}$, since the inclusion homomorphism is inverse to a "forgetful" homomorphism; this is because all of the point/line assignments are determined by the two lines labeled L, R. We will not make explicit use of this fact, but we mention it as a good example of a non-structural diagrammatic isomorphism.

We represent the $\mathfrak{C}$ structure as follows:

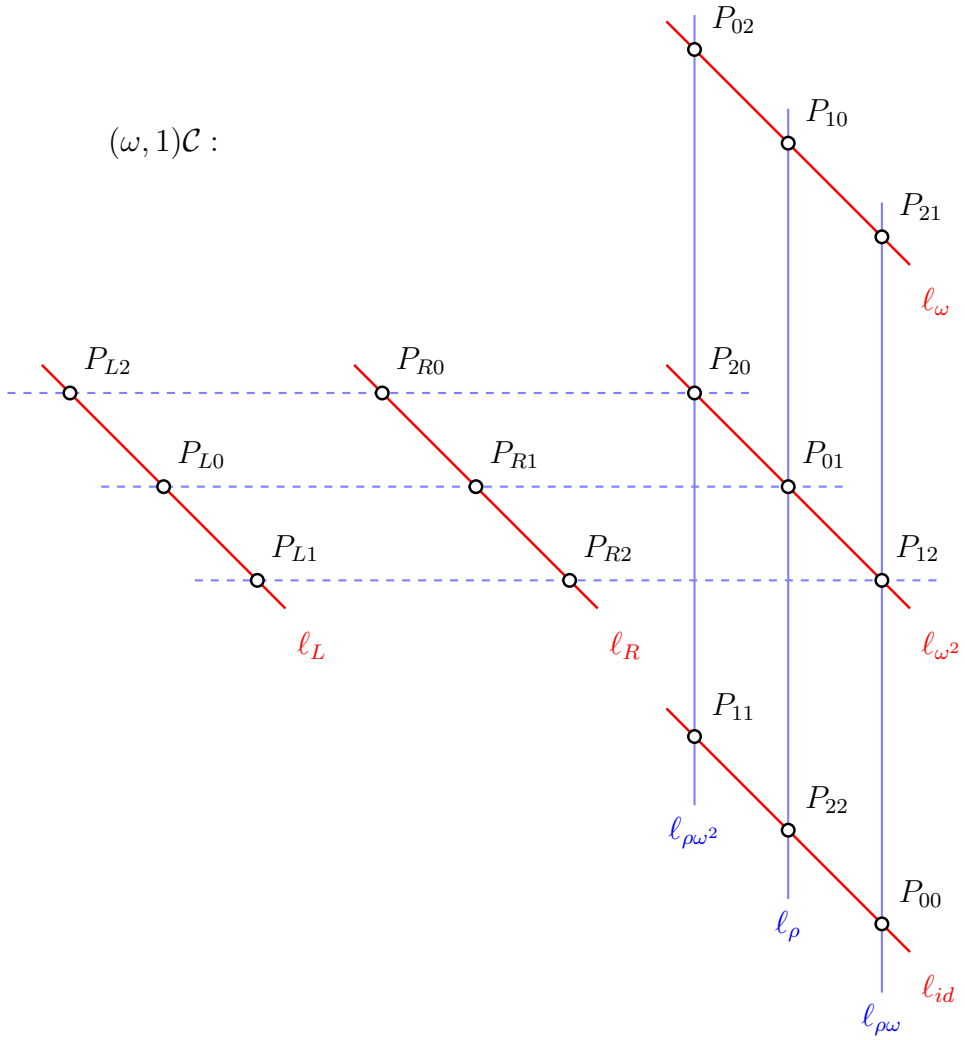


The dashed lines/points represent repeated features, and are only included to simplify the pictorial representation. We will apply the τ automorphism often, and this representation allows for a simple interpretation; τ shifts everything downwards one level wrapping around at the bottom.

We will normally use simplified representations of the following form for completion diagrams:



Where $P_{ij} = -P_{Li} - P_{Rj}$. We are most interested in the 8 solid lines, and more specifically the 5 red lines, but we will also make use of the others. When we do, we will apply a symmetry first to reveal the hidden lines. For example, we can apply $(\omega, 1)$ to get:

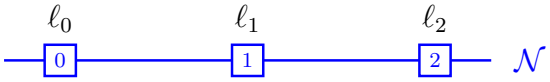


and the dashed lines have been swapped out for other hidden ones. We will revisit these diagrams in section 6.5.

5.7.2 Diagrams Within Diagrams

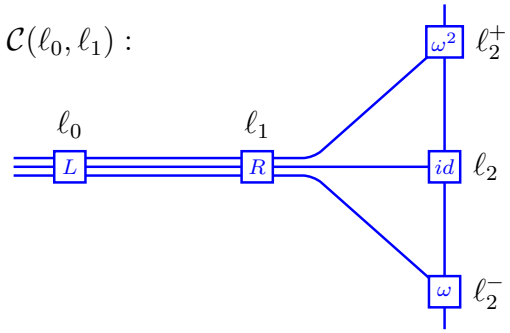
Because of the increasing complexity of our pictorial representations, we will introduce simplified representations. But rather than doing this in an arbitrary way, we will use the theory that we have developed so far. This will take advantage of the fact that we are working with an arbitrary group G.

We will interpret a nine point diagram as an element of $\mathcal{L}_3^\circ(\mathcal{L}_3^\circ(E))$:



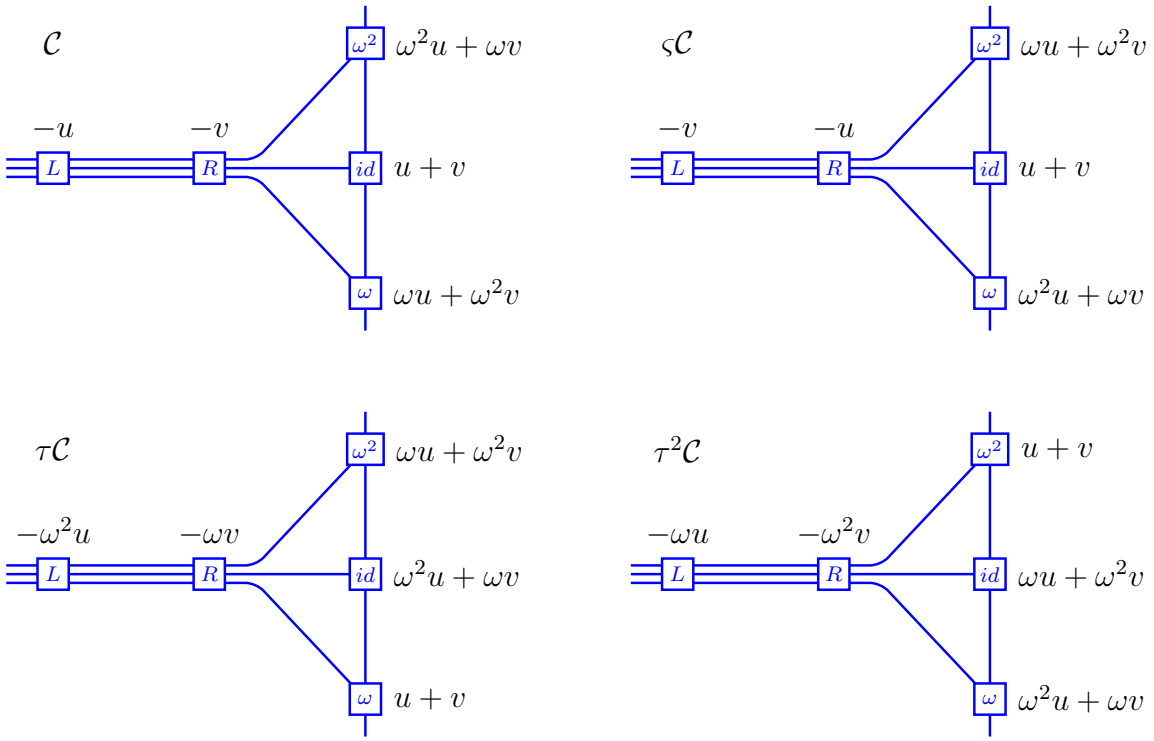
where we view $\ell_i \in \mathcal{L}_3^\circ(E)$ as a labeled line with $\mathfrak{p}_j(\ell_i) = \mathfrak{p}_{ij}(\mathcal{N})$. Then $\ell_0 + \ell_1 + \ell_2 = \ell_\mathcal{O}$ vanishes, so this is properly a labeled line diagram of labeled line diagrams!

This allows us to abbreviate completion diagrams as follows:



Note that each ℓ_i represents a labeled line, and the straight lines represent nine point diagrams thought of as elements of $\mathcal{L}_3^\circ(\mathcal{L}_3^\circ(E))$. The curved lines on the top and bottom represent the nine point diagrams with lines $\omega^2\ell_0, \omega\ell_1, \ell_2^+$ and $\omega\ell_0, \omega^2\ell_1, \ell_2^-$ respectively. The line labels $L, R, id, \omega, \omega^2$ will normally be omitted.

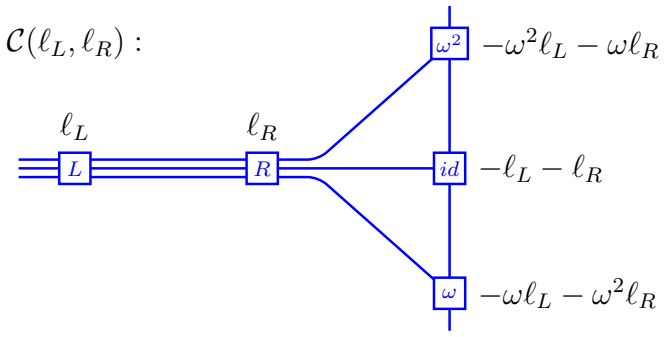
We often focus on the following automorphisms, which use the notation for $\mathrm{Aut}(\mathfrak{L}_\boxplus) = \mathrm{Aut}(\mathfrak{N})$:



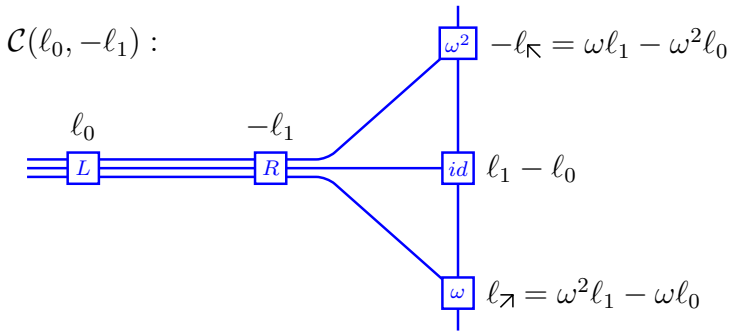
Noting that the same three labeled lines appear on the right of all of those diagrams.

5.7.3 Line Addition and Completion Diagrams

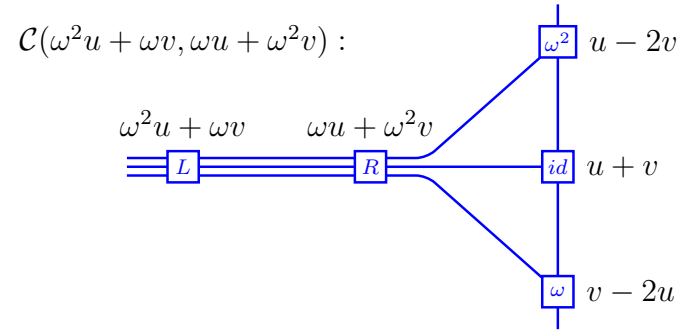
Given this simplified notation, we can now discuss line addition in simpler terms. First we note that for labeled lines $\ell_L, \ell_R \in \mathcal{L}_3^\circ(E)$, we can fill in the completion diagram as follows:

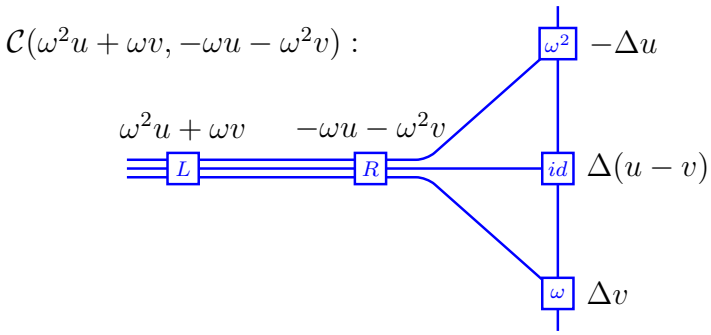


In particular, if three labeled lines form a nine point diagram $\mathcal{N} = \mathcal{N}(\ell_0, \ell_1, \ell_2)$, then the forward difference lines $\ell_\nwarrow = \mathfrak{l}_\nwarrow(\mathcal{N}), \ell_\nearrow = \mathfrak{l}_\nearrow(\mathcal{N})$ can be placed into a completion diagram. Recall from lemma 5.6.4 that $\mathfrak{l}_\nearrow = \omega^2\mathfrak{l}_1 - \omega\mathfrak{l}_0, \mathfrak{l}_\nwarrow = \omega^2\mathfrak{l}_0 - \omega\mathfrak{l}_1$, and hence:



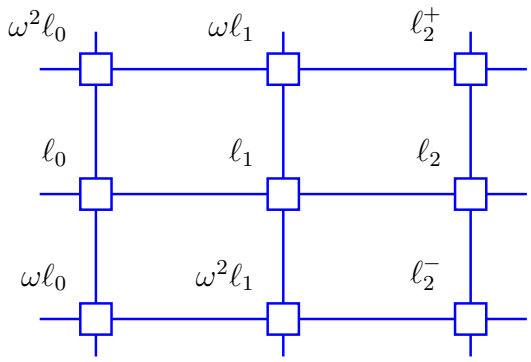
In fact, we can say much more than that. Recall from section 3.5 that in a step of a cyclic line addition, we start with lines u, v with cyclic orientations encoded via the forward difference lines $\Delta u, \Delta v$. Then to perform a step of the ladder we further assume that we are given $u - v$ and its orientation $\Delta(u - v)$, and $u - 2v$. For notational reasons, we treat these all as labeled lines. Then when we try to add u and v, we get three possibilities $u + v, \omega^2 u + \omega v, \omega u + \omega^2 v$; these appeared earlier in the completion diagram, but we will take a different point of view at the moment. Namely, *all* of the lines mentioned in addition to u, v appear in the following two completion diagrams:





In the next chapter, we will see that two completion diagrams that differ in the sign of $\mathfrak{l}_R$ are algebraically related, and this will be used for new approaches to line addition.

Lastly, we note that a completion diagram is essentially a simplified nine point diagram in $\mathcal{L}^\circ_{\mathfrak{N}}(\mathcal{L}^\circ_3(E))$:



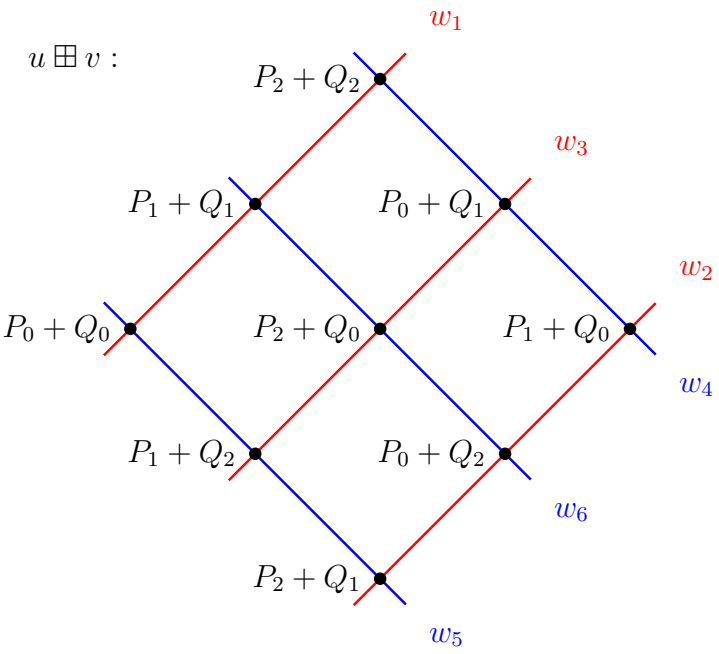
where we identify the cyclically shifted lines together. This highlights an interesting parallel; we are essentially using $\mathcal{L}^\circ_{\mathfrak{N}}(\mathcal{L}^\circ_3(E))$ to study $\mathcal{L}^\circ_3(\mathcal{L}^\circ_3(E))$, just as we used $\mathcal{L}^\circ_{\mathfrak{N}}(E)$ to study $\mathcal{L}^\circ_3(E)$.

Chapter 6

Diagrammatic Calculus

In this chapter, we will attach a *diagrammatic calculus* to the diagrammatic algebra that we developed in chapter 5. The main use of this comes when diagrams are connected together to form larger diagrams. Then the calculus will consist of formulas that express algebraic relations between the smaller diagrams.

The first important case comes when we combine six line diagrams together into a *nine point diagram*. The diagrammatic calculus will attach formulas expressing relations between the various lines involved in a nine point diagram. Recall that nine point diagrams arose in section 3.10, as a natural structure on the possible sums between points/lines of $u, v \in \mathcal{L}_3(E)$ with respective points P_0, P_1, P_2 and Q_0, Q_1, Q_2:



In section 3.10, we already had a primitive nine point diagram calculus, consisting of formulas such as:

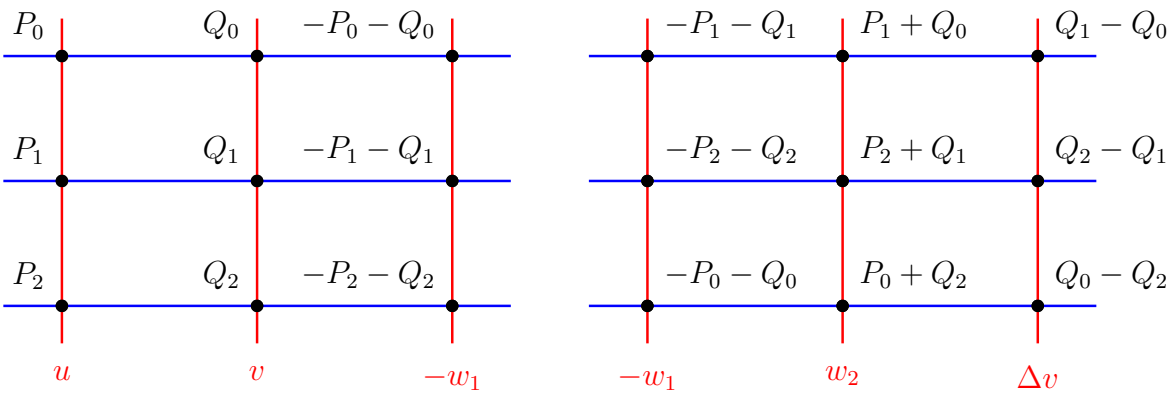
$$w_i(x, y) = y - m_i x - b_i$$
$$m_1 + m_2 + m_3 = m_4 + m_5 + m_6$$

Unfortunately, that calculus is unlikely to suffice for a line multiplication operation chain, since the lines w_4, w_5, w_6 are hard to work with.

In chapter 5, we reinterpreted the nine point diagram $u \boxplus v$ as a diagrammatic sum. This more general view allows us to see the additional structure that a nine point diagram gains when the lines u, v are given additional structure. For example, by adding cyclic line structures, we reduce the number of possible linear sum diagrams from 72 to 18. Furthermore, the cyclic orientations of u, v have a simple relation with the *orientation* $\partial(u \boxplus v)$, and this allows us to distinguish w_4, w_5, w_6 from w_1, w_2, w_3. This helps to remove a large barrier to line multiplication algorithms:

$$\partial(u \boxplus v) = \frac{m_1(b_3 - b_2) + m_2(b_1 - b_3) + m_3(b_2 - b_1)}{m_{\Delta u} - m_{\Delta v}} \tag{6.1}$$

Another quality of nine point diagrams that makes them attractive is their versatility. To illustrate this, we show that we already have multiple nine point diagram structures among the lines that we have mentioned. For example, for any possible sum line w between u and v, the lines $-u, -v, w$ form a nine point diagram. We illustrate this, as well as another example which includes sum lines and the forward difference line of v:



In fact, we can combine many of these nine point diagrams into larger diagram structures, such as the completion diagrams introduced in section 5.7.1. Then we will use the same nine point diagram calculus applied in many ways to obtain unexpected relations between various lines, all of which are relevant in line multiplication. In fact, this process

will also lead to new formulas in the nine point diagram calculus, by bootstrapping from preexisting formulas.

In chapter 7, we will develop the algebra of three torsion on E as it relates to line arithmetic. This allows for a striking occurrence of the aforementioned bootstrapping process. The following is an example of one of these relations applied to the nine point diagram of the line sum $u \boxplus v$ gives another formula for the orientation $\partial(u \boxplus v)$:

$$\frac{3b(m_1+m_2+m_3)-2a(b_1+b_2+b_3)+am_1m_2m_3+m_1b_2b_3+m_2b_1b_3+m_3b_1b_2}{m_{\Delta u}b_{\Delta v}+m_{\Delta v}b_{\Delta u}-2a}$$

By comparing this to the earlier expression (6.1) for $\partial(u \boxplus v)$, we get a relation that only involves the lines $w_i(x,y) = y - m_i x - b_i$ for $i \in \{1,2,3\}$ as well as the forward differences $\Delta u, \Delta v$ which determine the orientation of $u, v \in \mathcal{L}_3(E)$.

6.1 Diagram Functions

A major goal of this chapter is to encode structural elements of diagrams with algebraic quantities. The starting point for this is the diagram function:

Definition 6.1.1. *Given a diagram $\mathcal{D}$, the* diagram function*, also denoted $\mathcal{D}$, is the normalized function in $\mathbb{F}(E)$ that satisfies*

$$\mathrm{Div}(\mathcal{D}) = \sum_{i \in \mathfrak{D}} ((P_i) - (\mathcal{O}))$$

if such a function exists.

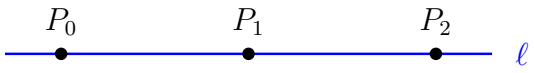
Note that the diagram function does not exist if the points of a diagram do not sum to $\mathcal{O}$. When we use diagram functions, it will normally be the case that the given diagram can be partitioned into linear sets. This is the case for a nine point diagram, whose points can be partitioned into three lines, in two different ways. In fact, in diagrams composed from multiple lines, it will very often be the case that we can perform such a partition in multiple ways, and this will give us relations between the various lines in the diagram.

A diagram function encodes the unordered tuple of points in a diagram, assuming that those sum to $\mathcal{O}$. On the other hand, the diagram function "forgets" the rest of the structure. This is analogous to the "forgetful" homomorphism (see definition 5.5.7), which takes any nine point diagram $\mathcal{N} \in \mathcal{L}_{\mathfrak{N}}(E)$, and returns an unlabeled linear diagram $|\mathcal{N}| \in \mathcal{L}_9^\bullet(E)$.

In particular, the diagram function "forgets" the symmetry group of the diagram $\mathcal{D}$. Hence we aim to attach algebraic quantities to diagrams that encode the structure that is lost in the diagram function. For example in section 3.4, the additional structure of a

cyclically oriented line u was encoded by a square root δ_u of a cubic determinant, or by a forward difference line Δu.

For unlabeled lines, the diagram function encodes the entire structure, and this is consistent with the encoding that we used in the earlier chapters:



which is the normalized function $\ell \in \mathbb{F}(E)$ satisfying

$$\text{Div}(\ell) = (P_0) + (P_1) + (P_2) - 3(\mathcal{O})$$

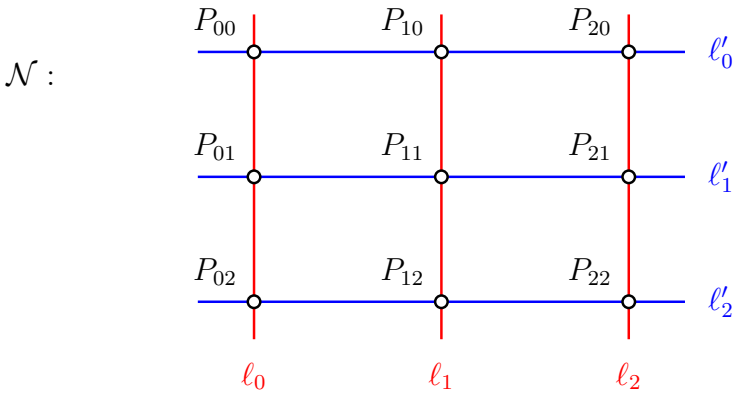
If $\mathcal{O}$ is not a point of ℓ, then we define $\alpha(\ell), \beta(\ell)$ to be the coefficients such that

$$\ell(x, y) = y - \alpha(\ell)x - \beta(\ell).$$

6.2 Nine Point Diagrams

In this section, we retread the discussion from section 3.10 to begin the development of the nine point diagram calculus. This will give us relations that exist between lines in a nine point diagram. In the following sections, we will define more general nine point diagram quantities, and these will further our understanding of the relations that exist between the lines of a nine point diagram.

We will notate our *labeled* nine point diagram as follows:



We focus on this specific representation to avoid the many ambiguities that arise when considering linear sum diagrams. In fact, some of our results are most easily understood by considering these rigid labeled diagrams first.

We focus on nine point diagrams with "typical" properties, and we will leave special cases for the appendix. To make this more precise, we first characterize the condition that allows nine points $P_{ij} \in E$ to form a nine point diagram. Recall that by definition, we need the following relations:

Lemma 6.2.1. *Nine points $P_{ij} \in E$ for $0 \leq i, j \leq 2$ form a nine point diagram $\mathcal{N}$ if and only if they satisfy the following relations:*

$$\begin{aligned} \mathcal{O} &= P_{00} + P_{01} + P_{02} = P_{10} + P_{11} + P_{12} = P_{20} + P_{21} + P_{22} \\ &= P_{00} + P_{10} + P_{20} = P_{01} + P_{11} + P_{21} = P_{02} + P_{12} + P_{22} \end{aligned} \tag{6.2}$$

Hence we will often make the implicit assumption that the points $P_{00}, P_{10}, P_{01}, P_{11}$ of $\mathcal{N}$ are linearly independent over $\mathbb{Z}$, to avoid special cases. Then by lemma 6.2.1, we have

$$\begin{aligned} P_{02} &= -P_{00} - P_{01}, \quad P_{12} = -P_{10} - P_{11} \\ P_{20} &= -P_{00} - P_{10}, \quad P_{21} = -P_{01} - P_{11} \\ P_{22} &= P_{00} + P_{01} + P_{10} + P_{11} \end{aligned}$$

The line functions of $\mathcal{N}$ will be notated $\ell_i(x, y) = y - \alpha_i x - \beta_i$ and $\ell'_i(x, y) = y - \alpha'_i x - \beta'_i$ for $i = 0, 1, 2$.

The additional assumptions will simplify the development of a nine point diagram calculus. In appendix A.7, we will deal with special cases, such as nine point diagrams that include $\mathcal{O}$.

6.2.1 Nine Point Diagram Function

Here we will discuss the nine point diagram function $\mathcal{N} \in \mathbb{F}(E)$ associated to a nine point diagram $\mathcal{N}$. This discussion will allow us to deduce relations between the lines of $\mathcal{N}$. Recall that this function is characterized as the normalized function with the following divisor:

$$\mathrm{Div}(\mathcal{N}) = \sum_{i,j \in \{0,1,2\}} (P_{ij}) - 9(\mathcal{O})$$

First we note that we can partition the divisor of a nine point diagram function $\mathcal{N}$:

$$\begin{aligned} \mathrm{Div}(\mathcal{N}) = &(P_{00}) + (P_{01}) + (P_{02}) - 3(\mathcal{O}) \\ &+ (P_{10}) + (P_{11}) + (P_{12}) - 3(\mathcal{O}) \\ &+ (P_{20}) + (P_{21}) + (P_{22}) - 3(\mathcal{O}) \end{aligned}$$

to obtain the factorization $\mathcal{N} = \ell_0\ell_1\ell_2$, since both sides are normalized. We then expand this product and reduce modulo $b + ax + x^3 - y^2$ with respect to x to obtain:

$$\begin{aligned}\mathcal{N}(x,y) =&(y - \alpha_0 x - \beta_0)(y - \alpha_1 x - \beta_1)(y - \alpha_2 x - \beta_2)\\ =& -(\beta_0\beta_1\beta_2 - b\ \alpha_0\alpha_1\alpha_2)\\ &- x\,(\alpha_0\beta_1\beta_2 + \alpha_1\beta_0\beta_2 + \alpha_2\beta_0\beta_1 - a\ \alpha_0\alpha_1\alpha_2)\\ &+ y\,(\beta_0\beta_1 + \beta_0\beta_2 + \beta_1\beta_2)\\ &- x^2\,(\alpha_0\alpha_1\beta_2 + \alpha_0\alpha_2\beta_1 + \alpha_1\alpha_2\beta_0)\\ &+ xy\,(\alpha_0(\beta_1 + \beta_2) + \alpha_1(\beta_0 + \beta_2) + \alpha_2(\beta_0 + \beta_1))\\ &- y^2\,(\alpha_0\alpha_1\alpha_2 + \beta_0 + \beta_1 + \beta_2)\\ &+ x^2y\,(\alpha_0\alpha_1 + \alpha_0\alpha_2 + \alpha_1\alpha_2)\\ &- xy^2\,(\alpha_0 + \alpha_1 + \alpha_2) + y^3 \end{aligned} \tag{6.3}$$

We will notate the coefficients as follows:

Lemma 6.2.2. *For the nine point diagram $\mathcal{N}$, we have:*

$$\mathcal{N}(x,y) = -\mathcal{N}_9 - \mathcal{N}_7 x + \mathcal{N}_6 y - \mathcal{N}_5 x^2 + \mathcal{N}_4 xy - \mathcal{N}_3 y^2 + \mathcal{N}_2 x^2 y - \mathcal{N}_1 xy^2 + y^3$$

with

$$\begin{aligned}\mathcal{N}_1 &= \alpha_0 + \alpha_1 + \alpha_2\\ \mathcal{N}_2 &= \alpha_0\alpha_1 + \alpha_0\alpha_2 + \alpha_1\alpha_2\\ \mathcal{N}_3 &= \alpha_0\alpha_1\alpha_2 + \beta_0 + \beta_1 + \beta_2\\ \mathcal{N}_4 &= \alpha_0(\beta_1 + \beta_2) + \alpha_1(\beta_0 + \beta_2) + \alpha_2(\beta_0 + \beta_1)\\ \mathcal{N}_5 &= \alpha_0\alpha_1\beta_2 + \alpha_0\alpha_2\beta_1 + \alpha_1\alpha_2\beta_0\\ \mathcal{N}_6 &= \beta_0\beta_1 + \beta_0\beta_2 + \beta_1\beta_2\\ \mathcal{N}_7 &= \alpha_0\beta_1\beta_2 + \alpha_1\beta_0\beta_2 + \alpha_2\beta_0\beta_1 - a\ \alpha_0\alpha_1\alpha_2\\ \mathcal{N}_9 &= \beta_0\beta_1\beta_2 - b\ \alpha_0\alpha_1\alpha_2\end{aligned}$$

Of course, this assumes that $\mathcal{O}$ is not a point of $\mathcal{N}$; otherwise the leading term would not be y^3.

6.2.2 Algebraic Relations Between Line Coordinates

Now we are ready to prove our first algebraic relations between the lines of a nine point diagram, again by generalizing a result from section 3.10. We start with the factorization from lemma 6.2.2; then by symmetry, we have $\mathcal{N} = \ell_0\ell_1\ell_2 = \ell'_0\ell'_1\ell'_2$ in $\mathbb{F}(E)$.

We then obtain algebraic relations between the coordinates of ℓ_i and ℓ'_i for $i = 0, 1, 2$ by comparing these two factorizations of the nine point diagram function. For $\mathcal{N}$ which does not have point $\mathcal{O}$, we get:

$$\begin{aligned}\mathcal{N}(x, y) &= (y - \alpha_0 x - \beta_0)(y - \alpha_1 x - \beta_1)(y - \alpha_2 x - \beta_2) &(6.4)\\ &= (y - \alpha'_1 x - \beta'_1)(y - \alpha'_0 x - \beta'_0)(y - \alpha'_2 x - \beta'_2) &(6.5)\end{aligned}$$

Comparing coefficients of this equality in the form of equation (6.3), we deduce the following:

Theorem 6.2.3. *For the nine point diagram $\mathcal{N}$, we have:*

$$\alpha_0 + \alpha_1 + \alpha_2 = \alpha'_1 + \alpha'_0 + \alpha'_2 \tag{6.6}$$

$$\alpha_0\alpha_1 + \alpha_0\alpha_2 + \alpha_1\alpha_2 = \alpha'_1\alpha'_0 + \alpha'_1\alpha'_2 + \alpha'_0\alpha'_2 \tag{6.7}$$

$$\alpha_0\alpha_1\alpha_2 + \beta_0 + \beta_1 + \beta_2 = \alpha'_1\alpha'_0\alpha'_2 + \beta'_1 + \beta'_0 + \beta'_2 \tag{6.8}$$

$$\begin{aligned}&\alpha_0(\beta_1 + \beta_2) + \alpha_1(\beta_0 + \beta_2) + \alpha_2(\beta_0 + \beta_1)\\ &= \alpha'_1(\beta'_0 + \beta'_2) + \alpha'_2(\beta'_1 + \beta'_2) + \alpha'_2(\beta'_1 + \beta'_0)\end{aligned} \tag{6.9}$$

$$\alpha_0\alpha_1\beta_2 + \alpha_0\alpha_2\beta_1 + \alpha_1\alpha_2\beta_0 = \alpha'_1\alpha'_0\beta'_2 + \alpha'_1\alpha'_2\beta'_0 + \alpha'_0\alpha'_2\beta'_1 \tag{6.10}$$

$$\beta_0\beta_1 + \beta_0\beta_2 + \beta_1\beta_2 = \beta'_1\beta'_0 + \beta'_1\beta'_2 + \beta'_0\beta'_2 \tag{6.11}$$

$$\begin{aligned}&\alpha_0\beta_1\beta_2 + \alpha_1\beta_0\beta_2 + \alpha_2\beta_0\beta_1 - a \cdot \alpha_0\alpha_1\alpha_2\\ &= \alpha'_1\beta'_0\beta'_2 + \alpha'_0\beta'_1\beta'_2 + \alpha'_2\beta'_1\beta'_0 - a \cdot \alpha'_1\alpha'_0\alpha'_2\end{aligned} \tag{6.12}$$

$$\beta_0\beta_1\beta_2 - b \cdot \alpha_0\alpha_1\alpha_2 = \beta'_1\beta'_0\beta'_2 - b \cdot \alpha'_1\alpha'_0\alpha'_2 \tag{6.13}$$

These are the first of many relations between nine point diagram lines that we will prove in this chapter. Given the underlying motivation of this chapter, we will have a special interest in relations that do not involve $\ell'_0, \ell'_1, \ell'_2$. That is because these do not normally correspond to lines in our line multiplication chains. So we are left with the somewhat more complicated question of finding relations between the coordinates of ℓ_0, ℓ_1, ℓ_2, as well as other quantities that figure into our operation chains.

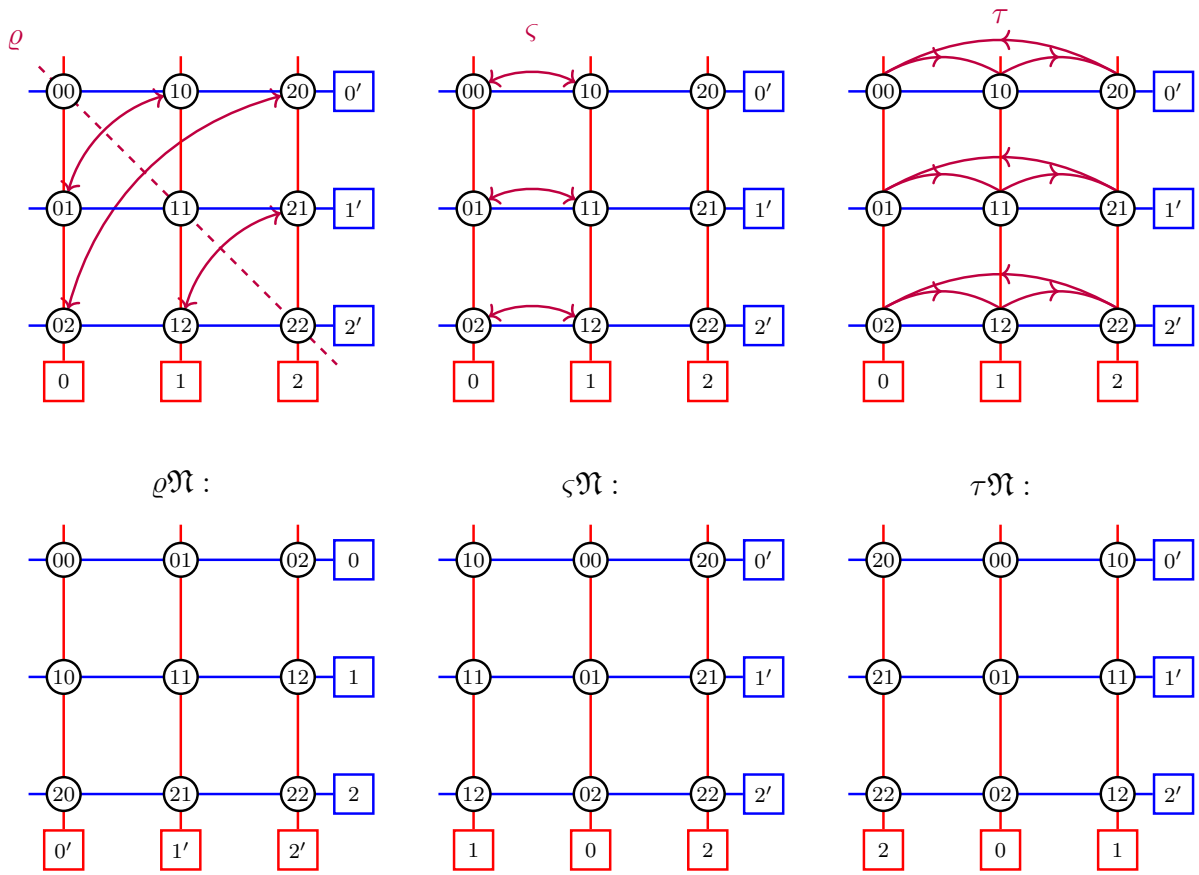
6.2.3 Nine Point Diagram Automorphisms

An important step in developing the nine point diagram calculus is to study functions that distinguish the lines $\ell'_0, \ell'_1, \ell'_2$ from ℓ_0, ℓ_1, ℓ_2. To this end, we consider the automorphisms of nine point diagram structures.

There is another reason for bringing this topic up here; it is often easiest to define properties of labeled diagrams, and then to subsequently show that they are invariant under

a symmetry group. In particular, we often define symmetric quantities as combinations of quantities that do not respect the given symmetries; rather, they transform in known ways and can be combined to achieve invariance.

Recall from section 5.1.2 that the automorphism group of the nine point diagram structure $\mathfrak{N}$ has 72 automorphisms. Furthermore, $\mathrm{Aut}(\mathfrak{N})$ is generated by ϱ, ς, τ, which are represented as follows:



We use the notation $\varsigma' = \varrho\varsigma\varrho$ for the transposition of the line labels $0', 1'$, and $\tau' = \varrho\tau\varrho$ for the cycle $(0'1'2')$. Recall then that $\langle \varsigma, \tau, \varsigma', \tau' \rangle$ is a direct product of $\langle \varsigma, \tau \rangle$ and $\langle \varsigma', \tau' \rangle$, and the two latter subgroups are isomorphic to S_3. In the next section, we will discuss a quantity which is invariant under $S_3 \times S_3$, but changes sign under the action of ϱ.

6.3 Nine Point Diagram Orientation

In this section, we define the *orientation* $\partial(\mathcal{N})$ of a nine point diagram. This quantity is invariant under the automorphisms in $S_3 \times S_3$, but changes signs under the action of ϱ;

so $\partial(\varrho\mathcal{N}) = -\partial(\mathcal{N})$, while $\partial(\varsigma\mathcal{N}) = \partial(\tau\mathcal{N}) = \partial(\mathcal{N})$. Hence this quantity will allow us to distinguish the lines ℓ_0, ℓ_1, ℓ_2 from the lines $\ell_0', \ell_1', \ell_2'$ in a nine point diagram. In fact, this quantity will be a central focus for much of our diagrammatic calculus.

Definition 6.3.1. *Given the nine point diagram $\mathcal{N}$ with $\mathcal{O} \notin \mathcal{N}$, we define the* nine point diagram orientation *to be:*

$$\partial(\mathcal{N}) = \beta_0 + \beta_1 + \beta_2 - \beta_0' - \beta_1' - \beta_2'$$

We will often use the notation $\partial(\ell_0, \ell_1, \ell_2) := \partial(\mathcal{N})$. A priori, each line ℓ_i is unlabeled, and so this notation needs justification. In fact, $\partial(\mathcal{N})$ can be expressed as a rational function of the line coefficients. An explicit expression can be found in equation (A.2) of the appendix; this lemma can be verified by a direct but tedious calculation. Note then that the property $\partial(\varrho\mathcal{N}) = -\partial(\mathcal{N})$ can be restated as $\partial(\ell_0', \ell_1', \ell_2') = -\partial(\ell_0, \ell_1, \ell_2)$.

For the remainder of this section, and much of the rest of this chapter, we focus on various formulas for nine point diagram orientations. By studying these formulas, we will be able to study related diagrams, and some surprising symmetries will emerge.

6.3.1 Formulas for Nine Point Diagram Orientation

Here we take the idea used to define $\partial(\mathcal{N})$ further to get other formulas. These are simply low hanging fruit from considering the two factorization formulas for $\mathcal{N}(x, y)$, in the vein of theorem 6.2.3.

Note that the combination $\beta_0 + \beta_1 + \beta_2$ is not $\mathrm{Aut}(\mathfrak{N})$-invariant, and this is the basis for our definition of $\partial(\mathcal{N})$. So what about starting with another non-invariant combinations, such as $\alpha_0\alpha_1\alpha_2$? It turns out that the obvious alternatives lead to closely related quantities. For example, by theorem 6.2.3 we have

$$\beta_0 + \beta_1 + \beta_2 + \alpha_0\alpha_1\alpha_2 = \beta_0' + \beta_1' + \beta_2' + \alpha_0'\alpha_1'\alpha_2'$$

and hence the non-invariance of $\alpha_0\alpha_1\alpha_2$ leads to the same indicator $\partial(\mathcal{N})$:

$$\partial(\mathcal{N}) = \beta_0 + \beta_1 + \beta_2 - \beta_0' - \beta_1' - \beta_2' = \alpha_0'\alpha_1'\alpha_2' - \alpha_0\alpha_1\alpha_2$$

We can do away with the rest of the coefficients of $\mathcal{N}(x, y)$ in one swoop. Consider the following polynomial in x, y:

$$\begin{aligned} f(x,y) =& (y - \alpha_0 x - \beta_0)(y - \alpha_1 x - \beta_1)(y - \alpha_2 x - \beta_2) \\ & - (y - \alpha_0' x - \beta_0')(y - \alpha_1' x - \beta_1')(y - \alpha_2' x - \beta_2') \\ & - (\alpha_0'\alpha_1'\alpha_2' - \alpha_0\alpha_1\alpha_2)(b + ax + x^3 - y^2) \end{aligned}$$

Notice that the first two expressions are the two factorizations of $\mathcal{N}(x, y)$ from equation (6.4). Hence it is easy to see that $f(x, y)$ is 0 as a function on E. As a consequence, it must be a multiple of $b+ax+x^3-y^2$. But the coefficient of x^3 can be checked to be 0, and hence $f(x, y)$ has degree less than 3 in x; and so it must be identically 0. Thus by combining this with the equation $\partial(\mathcal{N}) = \alpha_0'\alpha_1'\alpha_2' - \alpha_0\alpha_1\alpha_2$ we get the following supplement to theorem 6.2.3:

Lemma 6.3.2. *As polynomials in x, y, we have:*

$$\begin{aligned}\partial(\mathcal{N})(b + ax + x^3 - y^2) =&(y - \alpha_0 x - \beta_0)(y - \alpha_1 x - \beta_1)(y - \alpha_2 x - \beta_2)\\ &- (y - \alpha_0' x - \beta_0')(y - \alpha_1' x - \beta_1')(y - \alpha_2' x - \beta_2')\end{aligned}$$

By comparing coefficients, we get:

$$\begin{aligned}\partial(\mathcal{N}) =&\beta_0 + \beta_1 + \beta_2 - \beta_0' - \beta_1' - \beta_2'\\ \partial(\mathcal{N}) =&\alpha_0'\alpha_1'\alpha_2' - \alpha_0\alpha_1\alpha_2\\ a\ \partial(\mathcal{N}) =&\alpha_0'\beta_0'\beta_1' + \alpha_1'\beta_0'\beta_2' + \alpha_2'\beta_0'\beta_1' - \alpha_0\beta_0\beta_1 - \alpha_1\beta_0\beta_2 - \alpha_2\beta_0\beta_1\\ b\ \partial(\mathcal{N}) =&\beta_0'\beta_1'\beta_2' - \beta_0\beta_1\beta_2\end{aligned}$$

As an important corollary, we get the following factorizations of $\partial(\mathcal{N})$:

Theorem 6.3.3.

$$\begin{aligned}\partial(\mathcal{N}) &= (\alpha_0' - \alpha_0)(\alpha_0' - \alpha_1)(\alpha_0' - \alpha_2)\\ &= (\alpha_1' - \alpha_0)(\alpha_1' - \alpha_1)(\alpha_1' - \alpha_2)\\ &= (\alpha_2' - \alpha_0)(\alpha_2' - \alpha_1)(\alpha_2' - \alpha_2)\\ &= (\alpha_0' - \alpha_0)(\alpha_1' - \alpha_0)(\alpha_2' - \alpha_0)\\ &= (\alpha_0' - \alpha_1)(\alpha_1' - \alpha_1)(\alpha_2' - \alpha_1)\\ &= (\alpha_0' - \alpha_2)(\alpha_1' - \alpha_2)(\alpha_2' - \alpha_2)\end{aligned}$$

Proof. By plugging $y = \alpha_0' x + \beta_0'$ into the first equation of lemma 6.3.2, we get:

$$\begin{aligned}&\partial(\mathcal{N})(b + ax + x^3 - (\alpha_0' x + \beta_0')^2)\\ =&((\alpha_0' - \alpha_0)x + (\beta_0' - \beta_0))((\alpha_0' - \alpha_1)x + (\beta_0' - \beta_1))((\alpha_0' - \alpha_2)x + (\beta_0' - \beta_2))\end{aligned}$$

We get the first factorization by comparing x^3 coefficients. The others follow by symmetry. □

Note that if the line coordinates satisfy $\alpha_i = \alpha_j'$ for some $i, j \in \{0, 1, 2\}$, then in fact $\ell_i = \ell_j'$; this is because those lines are parallel and share a point. Furthermore, we have that the three lines ℓ_0, ℓ_1, ℓ_2 are the same as the three lines $\ell_0', \ell_1', \ell_2'$. Hence we can interpret theorem 6.3.3 as saying that $\partial(\ell_0, \ell_1, \ell_2)$ gives zero exactly when the diagram has a symmetry which swaps the horizontal and vertical lines. Equivalently, $\partial(\ell_0, \ell_1, \ell_2)$ indicates whether there are two non-collinear points on the nine point diagram that are equal.

6.3.2 Orientation in Terms of Two Lines

We will now prove a formula for $\partial(\mathcal{N})$ in terms of the labeled lines ℓ_0, ℓ_1. Note that for unlabeled lines, this is not generally possible, since there are multiple lines that could take the place of ℓ_2. We will study the collection of ℓ_2 such that ℓ_0, ℓ_1, ℓ_2 form a nine point diagram in section 5.7.1, and the formulas we develop here will be used to compare various related nine point diagrams.

To more easily state the formula, we need to define some quantities in terms of ℓ_0, ℓ_1. First we consider the following function, which indicates whether two lines intersect on E:

Definition 6.3.4. *For $(x, y) \in \mathbb{F}^2$, we define:*

$$e_0(x, y) = b + ax + x^3 - y^2$$

Then for any lines ℓ_0, ℓ_1 which do not have point $\mathcal{O}$, we define:

$$\begin{aligned} e_0(\ell_0; \ell_1) :=& b(\alpha_0 - \alpha_1)^3 - a(\alpha_0 - \alpha_1)^2(\beta_0 - \beta_1) - (\beta_0 - \beta_1)^3 - (\alpha_0 - \alpha_1)(\alpha_0\beta_1 - \alpha_1\beta_0)^2 \\ =& (\alpha_0 - \alpha_1)^3 e_0(\ell_0 \cap \ell_1) \end{aligned}$$

Note that this is a function of ℓ_0, ℓ_1 as unlabeled lines. As mentioned earlier, we need to use the label structure at some point, and we do so via the following:

Definition 6.3.5. *For labeled line ℓ_0, ℓ_1 with label i being assigned points*

$$P_{0i} = (x_{0i}, y_{0i}), \ P_{1i} = (x_{1i}, y_{1i})$$

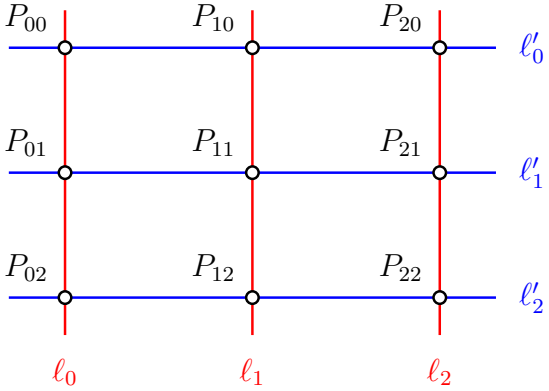
respectively, we define the following pairing indicator*:*

$$\phi(\ell_0; \ell_1) = (x_{10} - x_{00})(x_{11} - x_{01})(x_{12} - x_{02})$$

Note that the pairing indicator is invariant under the diagonal subgroup of $S_3 \times S_3$ applied to (ℓ_0, ℓ_1); that is, for any $\sigma \in S_3$, we have $\phi(\sigma\ell_0; \sigma\ell_1) = \phi(\ell_0; \ell_1)$. This is consistent with the fact that the points would be paired together in the same way after applying the same permutation to both lines.

Before stating the next theorem, we include the following diagram for reference:

$\mathcal{N}$:



Theorem 6.3.6. *The following gives a formula for $\partial(\mathcal{N}) = \partial(\ell_0, \ell_1, \ell_2)$ in terms of the lines ℓ_0, ℓ_1:*

$$\partial(\ell_0, \ell_1, \ell_2) = \frac{e_0(\ell_0; \ell_1)}{\phi_0} = \frac{\phi_1 \phi_2}{e_0(-\ell_0; \ell_1)}$$

where

$$\begin{aligned}
\phi_0 &= \phi(\ell_0; \ell_1) = (x_{10} - x_{00})(x_{11} - x_{01})(x_{12} - x_{02}) \\
\phi_1 &= \phi(\omega\ell_0; \ell_1) = (x_{10} - x_{01})(x_{11} - x_{02})(x_{12} - x_{00}) \\
\phi_2 &= \phi(\omega^2\ell_0; \ell_1) = (x_{10} - x_{02})(x_{11} - x_{00})(x_{12} - x_{01}).
\end{aligned}$$

More explicitly, we have

$$\begin{aligned}
\partial(\ell_0, \ell_1, \ell_2) &= \frac{b(\alpha_0-\alpha_1)^3 - a(\alpha_0-\alpha_1)^2(\beta_0-\beta_1) - (\beta_0-\beta_1)^3 - (\alpha_0-\alpha_1)(\alpha_0\beta_1-\alpha_1\beta_0)^2}{(x_{10}-x_{00})(x_{11}-x_{01})(x_{12}-x_{02})} \\
&= - \frac{(x_{10}-x_{01})(x_{10}-x_{02})(x_{11}-x_{00})(x_{11}-x_{02})(x_{12}-x_{00})(x_{12}-x_{01})}{b(\alpha_0+\alpha_1)^3 - a(\alpha_0+\alpha_1)^2(\beta_0+\beta_1) - (\beta_0+\beta_1)^3 - (\alpha_0+\alpha_1)(\alpha_0\beta_1-\alpha_1\beta_0)^2}
\end{aligned}$$

We will use the following lemma to prove this:

Lemma 6.3.7. *Suppose v is a (labeled) line with points Q_0, Q_1, Q_2 and $v(x, y) = y - m_v x - b_v$. Then the following holds as a polynomial in x:*

$$(x - x_{Q_0})(x - x_{Q_1})(x - x_{Q_2}) = b + ax + x^3 - (m_v x + b_v)^2.$$

For $P = (x_P, y_P) \in E$,

$$(x_P - x_{Q_0})(x_P - x_{Q_1})(x_P - x_{Q_2}) = -v(P)v(-P).$$

If u is a (labeled) line with points P_0, P_1, P_2 and $u(x, y) = y - m_u x - b_u$, then

$$v(P_0)v(P_1)v(P_2) = e_0(v; u).$$

Proof. Note that each Q_i satisfies $b + ax_{Q_i} + x_{Q_i}^3 - y_{Q_i}^2 = 0$ and $y_{Q_i} = m_v x_{Q_i} + b_v$. Hence that polynomial's roots are exactly x_{Q_i} for $i = 0, 1, 2$. Then by plugging in x_P, we get:

$$\begin{aligned}
b + ax_P + x_P^3 - (m_v x_P + b_v)^2 &= y_P^2 - (m_v x_P + b_v)^2 \\
&= -(y_P - m_v x_P - b_v)(-y_P - m_v x_P - b_v) = -v(P)v(-P)
\end{aligned}$$

For the last equality,

$$\prod_{i\in\{0,1,2\}} v(P_i) = \prod_{i\in\{0,1,2\}} (y_{P_i} - m_v x_{P_i} - b_v) = \prod_{i\in\{0,1,2\}} (b_u + m_u x_{P_i} - m_v x_{P_i} - b_v)$$
$$= -(m_u - m_v)^3 \prod_{i\in\{0,1,2\}} (-\frac{b_u - b_v}{m_u - m_v} - x_{P_i})$$
$$= -(m_u - m_v)^3 \left(b + a\left(-\frac{b_u - b_v}{m_u - m_v}\right) + \left(-\frac{b_u - b_v}{m_u - m_v}\right)^3 - \left(b_u + m_u\left(-\frac{b_u - b_v}{m_u - m_v}\right)\right)^2\right)$$
$$= -(m_u - m_v)^3 e_0(u \cap v) = -e_0(u; v) = e_0(v; u)$$

□

Now we prove the following lemma, which gives the second expression for $\partial(\ell_0, \ell_1, \ell_2)$ from the first in theorem 6.3.6:

Lemma 6.3.8.

$$\phi_0\phi_1\phi_2 = e_0(\ell_0; \ell_1)e_0(-\ell_0; \ell_1)$$

Proof. Using lemma 6.3.7:

$$\phi_0\phi_1\phi_2 = \prod_{i,j\in\{0,1,2\}} (x_{1i} - x_{0j}) = \prod_{i\in\{0,1,2\}} \left(\prod_{j\in\{0,1,2\}} (x_{1i} - x_{0j})\right)$$
$$= \prod_{i\in\{0,1,2\}} (-\ell_0(P_{1i})\ell_0(-P_{1i})) = -\left(\prod_{i\in\{0,1,2\}} \ell_0(P_{1i})\right)\left(\prod_{i\in\{0,1,2\}} \ell_0(-P_{1i})\right)$$
$$= -e_0(\ell_0; \ell_1)e_0(\ell_0; \boxminus\ell_1) = e_0(\ell_0; \ell_1)e_0(\boxminus\ell_0; \ell_1)$$

(where we use the notation $\boxminus\ell$ to distinguish line negation from negation in $\mathbb{F}(E)$.) □

And finally we prove theorem 6.3.6:

Proof. First we establish the following formula for $\alpha_0' - \alpha_0$, by substituting $y_{00} = \alpha_0 x_{00} + \beta_0$:

$$\alpha_0' - \alpha_0 = \frac{y_{10} - y_{00}}{x_{10} - x_{00}} - \alpha_0 = \frac{y_{10} - y_{00} - \alpha_0 x_{10} + \alpha_0 x_{00}}{x_{10} - x_{00}}$$
$$= \frac{y_{10} - \alpha_0 x_{10} - \beta_0}{x_{10} - x_{00}} = \frac{\ell_0(P_{10})}{x_{10} - x_{00}}$$

Then we combine this result with its conjugates under $(\tau')^2, (\tau') \in \mathrm{Aut}(\mathfrak{N})$ and use theorem 6.3.3:

$$\begin{aligned}\partial(\ell_0, \ell_1, \ell_2) =& (\alpha_0' - \alpha_0)(\alpha_1' - \alpha_0)(\alpha_2' - \alpha_0) \\ =& \frac{\ell_0(P_{10})\ell_0(P_{11})\ell_0(P_{12})}{(x_{10} - x_{00})(x_{11} - x_{01})(x_{12} - x_{02})} = \frac{e_0(\ell_0; \ell_1)}{\phi_0}\end{aligned}$$

using lemma 6.3.7. The other form follows from lemma 6.3.8. □

In section 6.5, we will combine theorem 6.3.6 with its conjugates to eliminate the ϕ_i terms using lemma 6.3.8. In the same vein, we note that by negating ℓ_1 in $\mathcal{N}$ and updating ℓ_2 accordingly, we get the same term ϕ_0 in the denominator; then by taking a quotient, we get cancellation of that factor.

Another important use of the results presented here is that we can derive a relatively simple explicit formula for $u+v$ in terms of the lines u, v, and the points on those lines. We do this in section A.1 of the appendix. This can be used to verify the formulas presented in this thesis, using a computer algebra system, or in some cases by hand.

6.3.3 Relation to Cyclic Orientation

Now we compare the notion of cyclic orientation on u, v to the orientation of $u \boxplus v$. Recall from section 3.4 that we had two ways of defining a cyclic orientation on a line $u \in \mathcal{L}_3(E)$. One was to specify a square root $\delta(u)$ of a cubic discriminant:

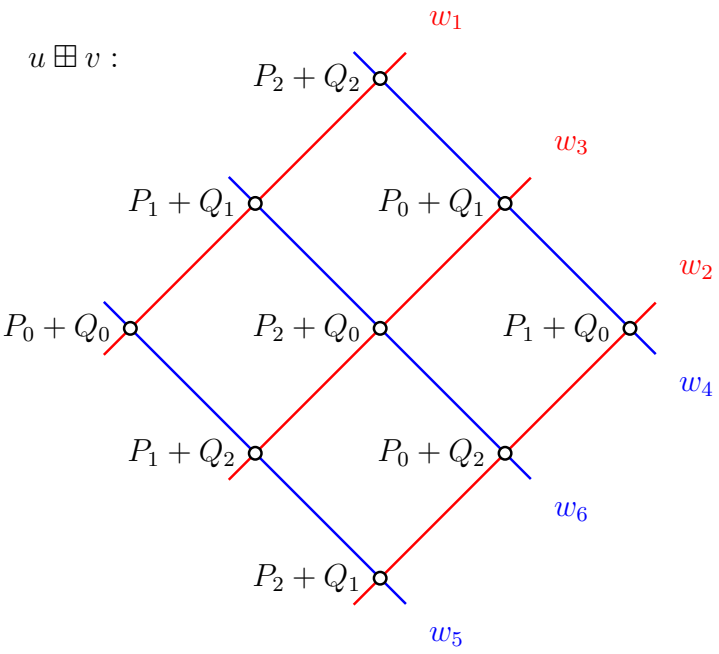
Definition 6.3.9. *For a cyclic line $\ell \in \mathcal{L}_3^{\triangleright}(E)$ with points P_0, P_1, P_2 in cyclic order, the* cyclic orientation *of ℓ is*

$$\delta(\ell) = (x_{P_1} - x_{P_0})(x_{P_2} - x_{P_1})(x_{P_0} - x_{P_2})$$

assuming that $\mathcal{O}$ is not a point of ℓ.

The cyclic orientation could also be specified via a forward difference line Δu. It turns out that both of these quantities have simple relations with the orientation of $u \boxplus v$, but in quite different ways.

First we consider the symmetries of $u^\circ, v^\circ \in \mathcal{L}_3^\circ(E)$ that preserve the function $u \boxplus v$, and those that flip it:



A transposition applied to one of the lines u, v changes the orientation of $u \boxplus v$; for example (02) applied to u°, swaps w_1 and w_6 among others. On the other hand, a 3-cycle applied to u° or v° does not affect the orientation of $u \boxplus v$. Hence the expression $\frac{\partial(u \boxplus v)}{\delta_u \delta_v}$ can be seen to be invariant under all permutations of the input lines. And as we will see in the next section, this has a simple expression in terms of the line coordinates of u, v:

$$\partial(u \boxplus v) = \pm \frac{\delta_u \delta_v}{e_0(\ell_0; -\ell_1)}$$

In the next section, we will use the *completion diagrams* from section 5.7.1 to prove this.

There turns out to be another less obvious relation as well. If $w_i(x, y) = y - m_i x - b_i$, then for the appropriate choice of signs (which need not be the same):

$$\partial(u \boxplus v) = \frac{m_1(b_3 - b_2) + m_2(b_1 - b_3) + m_3(b_2 - b_1)}{\pm m_{\Delta u} \pm m_{\Delta v}}$$

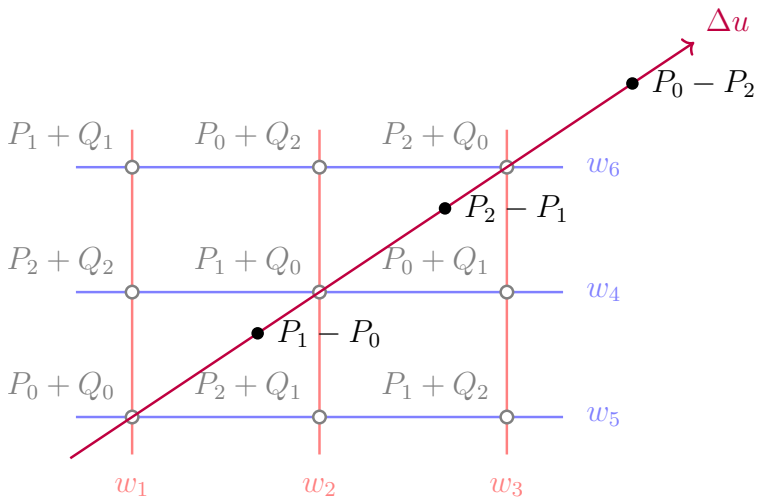
We will prove this in section 6.4, and we will explain how to determine the signs. This formula has some nice generalizations as well, that are obtained in chapter 7 by studying the action of three torsion on points and lines of E.

6.4 Forward Differences in Nine Point Diagrams

In this section, we discuss a line addition concept in terms of nine point diagrams: forward difference lines. In fact, we can recover the forward differences Δu from the $u \boxplus v$ nine

point diagram from section 3.10; see section 5.6.2. Appropriately enough, we accomplish this by taking a forward difference within the nine point diagram!

Specifically, we accomplish this by starting from the point $P_0 + Q_0$, and taking the forward difference as we travel in the northeast direction, wrapping back around at the edges. So we get the points $(P_{i+1} + Q_0) - (P_i + Q_0) = P_{i+1} - P_i$, which are the points of Δu:



In fact, despite there being nine choices of starting point, they all result in the same line Δu. So there are four possible outcomes to this process, depending on which line sum diagram was drawn, which result in the four forward difference lines $\pm\Delta u, \pm\Delta v \in \mathcal{L}_3^\bullet(E)$ for the possible orientations of u and v.

Now we define forward difference lines in terms of a nine point diagram. These will turn out to play an important role in line addition algebra. In particular, there are relations that we will demonstrate between the lines ℓ_i and these forward difference lines; notably, the three other lines ℓ_i' are not involved. This will set the stage for new cyclic line addition algorithms.

Definition 6.4.1. *For the nine point diagram $\mathcal{N}$, the* northeast forward difference line $\ell^\circ_{\nearrow}$ *is the labeled line with the following points:*

$$P_{\nearrow 0} := P_{11} - P_{02}, \quad P_{\nearrow 1} := P_{20} - P_{11}, \quad P_{\nearrow 2} := P_{02} - P_{20}$$

Similarly, the northwest/southwest/southeast forward difference lines $\ell^\circ_{\nwarrow}, \ell^\circ_{\swarrow}, \ell^\circ_{\searrow}$ *are the lines with the following points:*

$$\begin{aligned}
P_{\nwarrow 0} &:= P_{01} - P_{12}, & P_{\nwarrow 1} &:= P_{20} - P_{01}, & P_{\nwarrow 2} &:= P_{12} - P_{20} \\
P_{\swarrow 0} &:= P_{11} - P_{20}, & P_{\swarrow 1} &:= P_{02} - P_{11}, & P_{\swarrow 2} &:= P_{20} - P_{02} \\
P_{\searrow 0} &:= P_{01} - P_{20}, & P_{\searrow 1} &:= P_{12} - P_{01}, & P_{\searrow 2} &:= P_{20} - P_{12}.
\end{aligned}$$

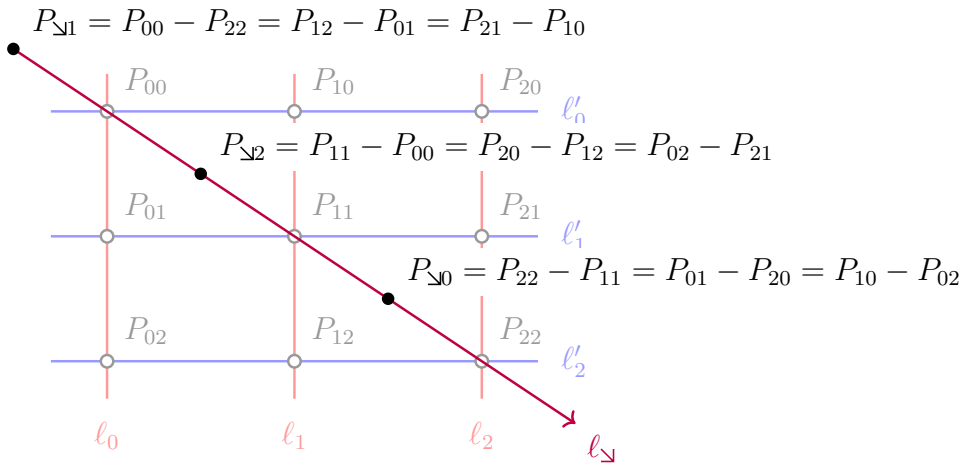
If $\mathcal{O}$ is not a point of these lines, then they have line functions $\ell_{\nearrow}(x,y) = y - \alpha_{\nearrow}x - \beta_{\nearrow}$, $\ell_{\nwarrow}(x,y) = y - \alpha_{\nwarrow}x - \beta_{\nwarrow}$, $\ell_{\swarrow}(x,y) = y - \alpha_{\swarrow}x - \beta_{\swarrow}$ and $\ell_{\searrow}(x,y) = y - \alpha_{\searrow}x - \beta_{\searrow}$.

We will mostly work with these as unlabeled lines $\ell_{\nearrow}, \ell_{\nwarrow}, \ell_{\swarrow}, \ell_{\searrow}$. In fact, as unlabeled lines these are independent of starting point, as a simple consequence of equation (6.2). For example, by considering the collinearity of the points of ℓ_1 and of ℓ'_0, we get:

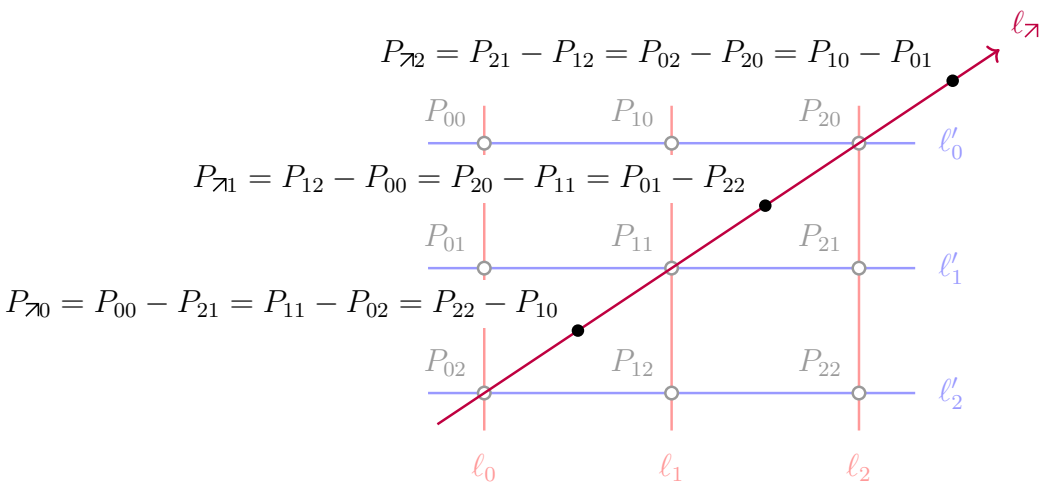
$$\begin{aligned}\mathcal{O} =& P_{00} + P_{10} + P_{20} = P_{10} + P_{11} + P_{12}\\ P_{\searrow 2} =& P_{11} - P_{00} = P_{20} - P_{12}\end{aligned}$$

Lemma 6.4.2. *As a cyclically oriented line, $\ell_{\searrow}$ (respectively $\ell_{\nearrow}$) is obtained from taking the the southeast (respectively northeast) forward difference starting from any point on the nine point diagram.*

Diagrammatically, we represent $\ell_{\searrow}$ and the various representations of its points as follows:



Similarly, we can represent $\ell_{\nearrow}$ diagrammatically as follows:



The following formulas give the slopes of the forward difference lines:

Theorem 6.4.3.

$$\alpha_\searrow = \frac{-\alpha_0\beta_1 - \alpha_1\beta_2 - \alpha_2\beta_0 + \alpha'_0\beta'_1 + \alpha'_1\beta'_2 + \alpha'_2\beta'_0}{\beta_0 + \beta_1 + \beta_2 - \beta'_0 - \beta'_1 - \beta'_2}$$
$$\alpha_\nearrow = \frac{\alpha_0\beta_2 + \alpha_1\beta_0 + \alpha_2\beta_1 - \alpha'_0\beta'_1 - \alpha'_1\beta'_2 - \alpha'_2\beta'_0}{\beta_0 + \beta_1 + \beta_2 - \beta'_0 - \beta'_1 - \beta'_2}$$

And we will prove this shortly. Observe that in theorem 6.4.3, the denominators are $\partial(\ell_0, \ell_1, \ell_2)$, and the undesirable terms α'_i, β'_i can be canceled out together:

$$\alpha_\searrow + \alpha_\nearrow = \frac{\alpha_0(\beta_2 - \beta_1) + \alpha_1(\beta_0 - \beta_2) + \alpha_2(\beta_1 - \beta_0)}{\partial(\ell_0, \ell_1, \ell_2)}$$

and this leads to a simple expression for $\partial(\ell_0, \ell_1, \ell_2)$:

Theorem 6.4.4.

$$\partial(\ell_0, \ell_1, \ell_2) = \frac{\alpha_0(\beta_2 - \beta_1) + \alpha_1(\beta_0 - \beta_2) + \alpha_2(\beta_1 - \beta_0)}{\alpha_\searrow + \alpha_\nearrow}$$

This gives us a useful tool for cyclic line addition, since the lines $\ell_\searrow, \ell_\nearrow$ will be known. In chapter 7, we will see that this result can be generalized to give new expressions for $\partial(\ell_0, \ell_1, \ell_2)$.

6.4.1 Alternate Representations

Now we will consider the forward difference lines $\ell_{\nearrow}, \ell_{\nwarrow}, \ell_{\swarrow}, \ell_{\searrow}$ as labeled lines, and express them in terms of the lines of $\mathcal{N}$. We will consider ℓ_i as a labeled line with points P_{i0}, P_{i1}, P_{i2}. Notice that we can mix and match the point representations for $\ell_{\nearrow}$ as follows: $P_{\nearrow 0} = P_{11} - P_{02}$, $P_{\nearrow 1} = P_{12} - P_{00}$, $P_{\nearrow 2} = P_{10} - P_{01}$. This can then be succinctly written as $\ell_{\nearrow} = \omega^2\ell_1 - \omega\ell_0$. Similarly, $\ell_{\nearrow} = \omega\ell_2 - \ell_1 = \ell_0 - \omega^2\ell_2$, and these representations are related by the fact that $\ell_0 + \ell_1 + \ell_2 = \ell_{\mathcal{O}}$ vanishes.

As for $\ell_{\nwarrow}$, we note that by its definition it is obtained by swapping the index $0j$ for $1j$ and vice versa wherever those appear. Equivalently, $\ell_{\nwarrow}$ is the northeast forward difference of the diagram $\varsigma\mathcal{N}$. This can be stated more precisely in the language of section 5.6.2, as $\ell_{\nwarrow} = \mathfrak{l}_{\nwarrow}(\mathcal{N}) = \mathfrak{l}_{\nearrow}(\varsigma\mathcal{N})$. Thus we can get an expression analogous to $\ell_{\nearrow} = \omega^2\ell_1 - \omega\ell_0$ as follows:

$$\begin{aligned}\ell_{\nwarrow} =& \mathfrak{l}_{\nwarrow}(\mathcal{N}) = \mathfrak{l}_{\nearrow}(\varsigma\mathcal{N}) = (\omega^2\mathfrak{l}_1 - \omega\mathfrak{l}_0)(\varsigma\mathcal{N}) \\ =& (\omega^2\mathfrak{l}_{1\varsigma} - \omega\mathfrak{l}_{0\varsigma})(\mathcal{N}) = (\omega^2\mathfrak{l}_0 - \omega\mathfrak{l}_1)(\mathcal{N}) \\ =& \omega^2\ell_0 - \omega\ell_1\end{aligned}$$

and similarly, $\ell_{\nwarrow} = \omega\ell_2 - \ell_0 = \ell_1 - \omega^2\ell_2$. For the other two forward difference lines, we have $\ell_{\swarrow} = -\rho\ell_{\nearrow}$ and $\ell_{\searrow} = -\rho\ell_{\nwarrow}$, recalling that ρ swaps the places of the points assigned to labels $0, 1$.

These representations will be useful in the following sections, since they allow for symbolic manipulation without having to do a diagram chase.

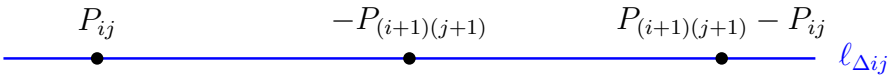
6.4.2 Proof of Theorem 6.4.3

Now we prove the first part of theorem 6.4.3:

$$\alpha_{\searrow} = \frac{-\alpha_0\beta_1 - \alpha_1\beta_2 - \alpha_2\beta_0 + \alpha_0'\beta_1' + \alpha_1'\beta_2' + \alpha_2'\beta_0'}{\beta_0 + \beta_1 + \beta_2 - \beta_0' - \beta_1' - \beta_2'}$$

Note that the denominator that appears in these expressions is $\partial(\ell_0, \ell_1, \ell_2)$. Before proving theorem 6.4.3, we first need to define auxiliary lines:

Definition 6.4.5. *For $i, j \in \{0, 1, 2\}$, the line $\ell_{\Delta ij} : \; y - \alpha_{\Delta ij}x - \beta_{\Delta ij} = 0$ contains the following three points:*

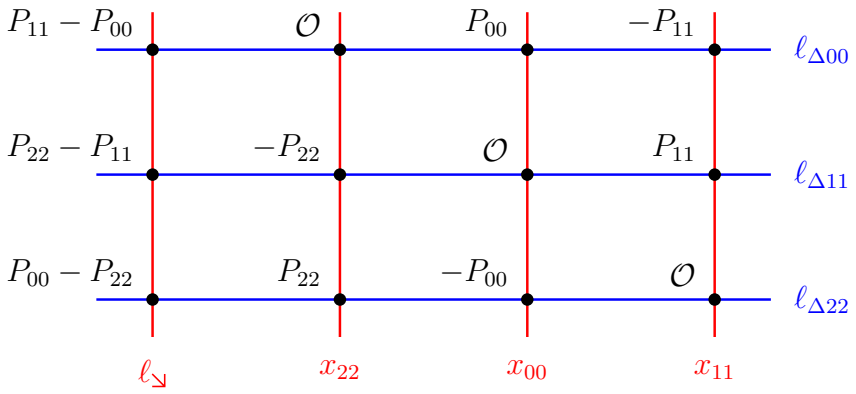


These auxiliary lines have slopes that can be combined to obtain $\alpha_{\searrow}$:

Lemma 6.4.6.

$$\alpha_{\searrow} = \alpha_{\Delta 00} + \alpha_{\Delta 11} + \alpha_{\Delta 22}$$

Proof. Consider the following diagram:



The diagram function can be factored in two ways:

$$\begin{aligned}&(y - \alpha_{\Delta 00}x - \beta_{\Delta 00})(y - \alpha_{\Delta 11}x - \beta_{\Delta 11})(y - \alpha_{\Delta 22}x - \beta_{\Delta 22})\\ &= (y - \alpha_{\searrow}x - \beta_{\searrow})(x - x_{22})(x - x_{00})(x - x_{11}).\end{aligned}$$

If we reduce this modulo $b + ax + x^3 - y^2$ with respect to x, then by comparing the coefficient for xy^2, we obtain:

$$\alpha_{\searrow} = \alpha_{\Delta 00} + \alpha_{\Delta 11} + \alpha_{\Delta 22}.$$

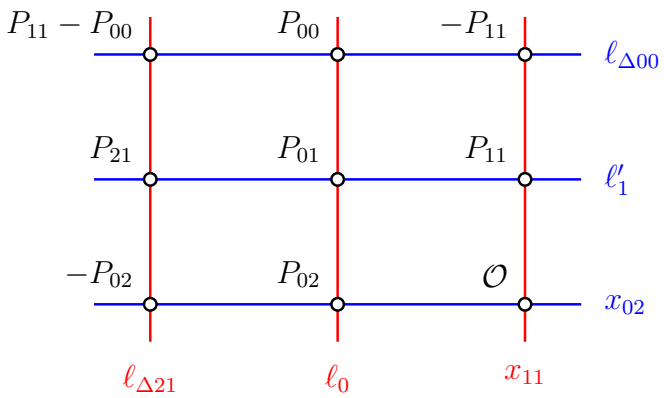
□

The next step to prove theorem 6.4.3 is to find an expression for $\alpha_{\Delta 00}$:

Lemma 6.4.7.

$$\alpha_{\Delta 00} = \frac{\alpha_0'(\beta_2' - \beta_0) - (\alpha_1' - \alpha_0 - \alpha_2)(\beta_1' - \beta_1) - \alpha_0(\beta_2 - \beta_0')}{\beta_0 + \beta_1 + \beta_2 - \beta_0' - \beta_1' - \beta_2'}$$

Proof. Again we consider the following diagram, and compare two factorizations:



We get:

$$(y - \alpha_{\Delta 21}x - \beta_{\Delta 21})(y - \alpha_0 x - \beta_0)(x - x_{11}) - (y - \alpha_{\Delta 00}x - \beta_{\Delta 00})(y - \alpha'_1 x - \beta'_1)(x - x_{02})$$
$$= (b + ax + x^3 - y^2)(x_{11} - x_{02}) = (b + ax + x^3 - y^2)(\alpha_{\Delta 21}\alpha_0 - \alpha_{\Delta 00}\alpha'_1)$$

noting that the difference between the first and the second expressions has degree less than 2 in y and is thus reduced modulo $b+ax+x^3-y^2$ with respect to y. Similarly, the difference between the first and the third expressions has degree less than 3 in x. Hence the above equalities hold as polynomials in x, y.

By comparing coefficients of x^2y and y^2, we get:

$$\begin{aligned} \alpha_0 + \alpha_{\Delta 21} &= \alpha'_1 + \alpha_{\Delta 00} \\ x_{11} - x_{02} &= \alpha_{\Delta 21}\alpha_0 - \alpha_{\Delta 00}\alpha'_1 \\ &= (\alpha'_1 - \alpha_0 + \alpha_{\Delta 00})\alpha_0 - \alpha_{\Delta 00}\alpha'_1 \\ &= (\alpha_0 - \alpha_{\Delta 00})(\alpha'_1 - \alpha_0) \end{aligned}$$

From which we isolate $\alpha_{\Delta 00}$:

$$\alpha_{\Delta 00} = \alpha_0 - \frac{x_{11} - x_{02}}{\alpha'_1 - \alpha_0} = \alpha_0 - \frac{-\frac{\beta'_1 - \beta_1}{\alpha'_1 - \alpha_1} + \frac{\beta'_2 - \beta_0}{\alpha'_2 - \alpha_0}}{\alpha'_1 - \alpha_0}$$
$$= \frac{(\alpha'_1 - \alpha_2)(\beta'_1 - \beta_1)}{(\alpha'_1 - \alpha_0)(\alpha'_1 - \alpha_1)(\alpha'_1 - \alpha_2)} - \frac{(\alpha'_0 - \alpha_0)(\beta'_2 - \beta_0)}{(\alpha'_0 - \alpha_0)(\alpha'_1 - \alpha_0)(\alpha'_2 - \alpha_0)} + \alpha_0$$

Notice that by theorem 6.3.3, the denominators are both $\partial(\ell_0, \ell_1, \ell_2)$, so we have:

$$\begin{aligned} \alpha_{\Delta 00} &= \frac{(\alpha'_1 - \alpha_2)(\beta'_1 - \beta_1) - (\alpha'_0 - \alpha_0)(\beta'_2 - \beta_0)}{\beta_0 + \beta_1 + \beta_2 - \beta'_0 - \beta'_1 - \beta'_2} + \alpha_0 \\ &= \frac{(\alpha'_1 - \alpha_2)(\beta'_1 - \beta_1) - (\alpha'_0 - \alpha_0)(\beta'_2 - \beta_0) + \alpha_0(\beta_0 + \beta_1 + \beta_2 - \beta'_0 - \beta'_1 - \beta'_2)}{\beta_0 + \beta_1 + \beta_2 - \beta'_0 - \beta'_1 - \beta'_2} \\ &= \frac{\alpha'_0(\beta_0 - \beta'_2) + (\alpha'_1 - \alpha_0 - \alpha_2)(\beta'_1 - \beta_1) + \alpha_0(\beta_2 - \beta'_0)}{\beta_0 + \beta_1 + \beta_2 - \beta'_0 - \beta'_1 - \beta'_2} \end{aligned}$$

□

Note that by symmetry, we have these formulas as well:

$$\alpha_{\Delta 11} = \frac{\alpha_1'(\beta_1 - \beta_0') + (\alpha_2' - \alpha_1 - \alpha_0)(\beta_2' - \beta_2) + \alpha_1(\beta_0 - \beta_1')}{\beta_0 + \beta_1 + \beta_2 - \beta_0' - \beta_1' - \beta_2'}$$
$$\alpha_{\Delta 22} = \frac{\alpha_2'(\beta_2 - \beta_1') + (\alpha_0' - \alpha_2 - \alpha_1)(\beta_0' - \beta_0) + \alpha_2(\beta_1 - \beta_2')}{\beta_0 + \beta_1 + \beta_2 - \beta_0' - \beta_1' - \beta_2'}$$

Now we can put everything together to prove theorem 6.4.3:

Proof. By combining the previous two lemmas, we get:

$$\begin{aligned}
\alpha_{\searrow} =& \alpha_{\Delta 00} + \alpha_{\Delta 11} + \alpha_{\Delta 22} \\
\partial(\ell_0, \ell_1, \ell_2)\alpha_{\searrow} =& \partial(\ell_0, \ell_1, \ell_2)\alpha_{\Delta 00} + \partial(\ell_0, \ell_1, \ell_2)\alpha_{\Delta 11} + \partial(\ell_0, \ell_1, \ell_2)\alpha_{\Delta 22} \\
=& \alpha_0'(\beta_0 - \beta_2') + (\alpha_1' - \alpha_0 - \alpha_2)(\beta_1' - \beta_1) + \alpha_0(\beta_2 - \beta_0') \\
&+ \alpha_1'(\beta_1 - \beta_0') + (\alpha_2' - \alpha_1 - \alpha_0)(\beta_2' - \beta_2) + \alpha_1(\beta_0 - \beta_1') \\
&+ \alpha_2'(\beta_2 - \beta_1') + (\alpha_0' - \alpha_2 - \alpha_1)(\beta_0' - \beta_0) + \alpha_2(\beta_1 - \beta_2') \\
=& \alpha_0(\beta_1 + 2\beta_2 - \beta_0' - \beta_1' - \beta_2') \\
&+ \alpha_1(2\beta_0 + \beta_2 - \beta_0' - \beta_1' - \beta_2') \\
&+ \alpha_2(\beta_1 + \beta_0 + 2\beta_1 - \beta_0' - \beta_1' - \beta_2') \\
&+ \alpha_0'(\beta_0' - \beta_2') + \alpha_1'(\beta_1' - \beta_0') + \alpha_2'(\beta_2' - \beta_1')
\end{aligned}$$

Now we rewrite this last expression so that it can be simplified using the symmetric relations from theorem 6.2.3:

$$\begin{aligned}
\partial(\ell_0, \ell_1, \ell_2)\alpha_{\searrow} =& -\alpha_0\beta_1 - \alpha_1\beta_2 - \alpha_2\beta_0 + \alpha_0'\beta_1' + \alpha_1'\beta_2' + \alpha_2'\beta_0' \\
&+ 2\left(\alpha_0(\beta_1 + \beta_2) + \alpha_1(\beta_0 + \beta_2) + \alpha_2(\beta_0 + \beta_1)\right) \\
&- 2\left(\alpha_0'(\beta_1' + \beta_2') + \alpha_1'(\beta_0' + \beta_2') + \alpha_2'(\beta_0' + \beta_1')\right) \\
&- (\beta_0' + \beta_1' + \beta_2')(\alpha_0 + \alpha_1 + \alpha_2 - \alpha_0' - \alpha_1' - \alpha_2') \\
=& -\alpha_0\beta_1 - \alpha_1\beta_2 - \alpha_2\beta_0 + \alpha_0'\beta_1' + \alpha_1'\beta_2' + \alpha_2'\beta_0'
\end{aligned}$$

Hence as desired, we have:

$$\alpha_{\searrow} = \frac{-\alpha_0\beta_1 - \alpha_1\beta_2 - \alpha_2\beta_0 + \alpha_0'\beta_1' + \alpha_1'\beta_2' + \alpha_2'\beta_0'}{\beta_0 + \beta_1 + \beta_2 - \beta_0' - \beta_1' - \beta_2'}$$

Now note that the symmetry ς which swaps ℓ_0 and ℓ_1 also has swaps $\ell_{\searrow}$ and $-\ell_{\nearrow}$ (as unlabeled lines), so by applying the above formula to $\varsigma(\mathcal{N})$, we get:

$$\alpha_{\nearrow} = \frac{\alpha_0\beta_2 + \alpha_1\beta_0 + \alpha_2\beta_1 - \alpha_0'\beta_1' - \alpha_1'\beta_2' - \alpha_2'\beta_0'}{\beta_0 + \beta_1 + \beta_2 - \beta_0' - \beta_1' - \beta_2'}$$

□

6.4.3 Cyclic Line Arithmetic

We will now connect the results from this chapter with line arithmetic. Recall from corollary 6.4.4 that we can combine the formulas for $\alpha_{\searrow}, \alpha_{\nearrow}$ to get:

$$\partial(\ell_0, \ell_1, \ell_2) = \frac{\alpha_0(\beta_2 - \beta_1) + \alpha_1(\beta_0 - \beta_2) + \alpha_2(\beta_1 - \beta_0)}{\alpha_{\searrow} + \alpha_{\nearrow}} \tag{6.14}$$

Given cyclically oriented lines u, v, the above will in fact be well defined on $u \boxplus v$, although there is a subtlety involved. Namely, the cyclic linear sum diagram has the commutation symmetry ς, which changes the order of summation. But under the action of ς on $\mathcal{N}$, two of the lines ℓ_0, ℓ_1, ℓ_2 will be transposed, and thus the numerator in equation (6.14) will change signs. Hence $\alpha_0(\beta_2 - \beta_1) + \alpha_1(\beta_0 - \beta_2) + \alpha_2(\beta_1 - \beta_0)$ is not a function of the cyclic linear sum diagram $u \boxplus v$. Similarly, ς transposes $\ell_{\searrow}$ and $-\ell_{\nearrow}$ when applied to $\mathcal{N}$, so the denominator $\alpha_{\searrow} + \alpha_{\nearrow}$ changes signs as well. But these two problems cancel each other out, since the quotient does not vary when ς is applied to $\mathcal{N}$.

Now we rewrite equation (6.14) in a more convenient form. Namely, both the numerator and denominator can be expressed as determinants:

Definition 6.4.8. *For a line ℓ, we define $[\ell]$ to be the vector such that $\ell(x, y) = [\ell]^\intercal [x\ y\ 1]^\intercal$. The following three vectors respectively represent a line ℓ without $\mathcal{O}$ as a point; a line χ with points $\mathcal{O}, P, -P$ for $P \neq \mathcal{O}$; and the line at infinity $\ell_{\mathcal{O}}$:*

$$[\ell] = \begin{bmatrix} -m_\ell \\ 1 \\ -b_\ell \end{bmatrix}, \qquad [\chi] = \begin{bmatrix} 1 \\ 0 \\ -x_P \end{bmatrix}, \qquad [\ell_{\mathcal{O}}] = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

For three lines $\ell_0, \ell_1, \ell_2 \in \mathcal{L}_3^\bullet(E)$, we define the following determinant form*:*

$$d_{\mathcal{O}}(\ell_0, \ell_1, \ell_2) := \det([\ell_0], [\ell_1], [\ell_2])$$

where we take the determinant of the matrix with the three given columns in respective order.

Then we note that in the equation (6.14), both the numerator and denominator can be written in terms of $d_{\mathcal{O}}$:

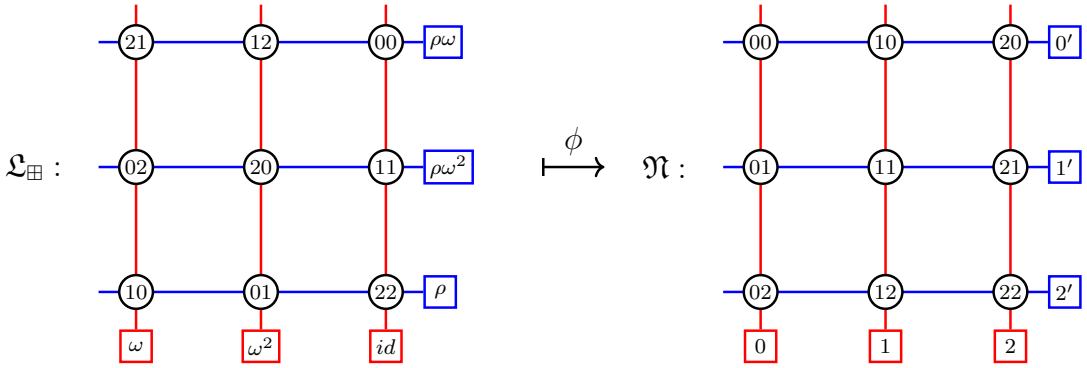
$$d_{\mathcal{O}}(\ell_0, \ell_1, \ell_2) = \begin{vmatrix} -\alpha_0 & -\alpha_1 & -\alpha_2 \\ 1 & 1 & 1 \\ -\beta_0 & -\beta_1 & -\beta_2 \end{vmatrix} = \alpha_0(\beta_2 - \beta_1) + \alpha_1(\beta_0 - \beta_2) + \alpha_2(\beta_1 - \beta_0)$$

$$d_{\mathcal{O}}(\ell_{\mathcal{O}}, -\ell_{\searrow}, \ell_{\nearrow}) = \begin{vmatrix} 0 & \alpha_{\searrow} & -\alpha_{\nearrow} \\ 0 & 1 & 1 \\ 1 & \beta_{\searrow} & -\beta_{\nearrow} \end{vmatrix} = \alpha_{\searrow} + \alpha_{\nearrow}$$

Since we are dealing with unlabeled lines now, we have $\ell_{\nwarrow} = -\ell_{\searrow}$, and so:

$$\partial(\ell_0, \ell_1, \ell_2) = \frac{d_{\mathcal{O}}(\ell_0, \ell_1, \ell_2)}{d_{\mathcal{O}}(\ell_{\mathcal{O}}, \ell_{\nwarrow}, \ell_{\nearrow})} \tag{6.15}$$

Now we discuss applying this result to cyclic line arithmetic. Suppose we have two cyclic lines, represented by $u, v \in \mathcal{L}_3^\circ(E)$ with respective points P_0, P_1, P_2 and Q_0, Q_1, Q_2. Then we assign the labeled diagram $u \boxplus v$ to the structure $\mathfrak{L}_{\boxplus}$, with $P_i + Q_j$ at label ij. We will apply this section's results to $\phi(u \boxplus v)$, where $\phi : \mathfrak{L}_{\boxplus} \to \mathfrak{N}$ is the structural isomorphism indicated below, which was defined in section 5.4.2:



Now we extract the lines that appear in equation (6.15). For example, the line ℓ_0 will correspond to $\mathfrak{l}_0(\phi(u \boxplus v))$, which has points $P_2 + Q_1, P_0 + Q_2, P_1 + Q_0$ in order. More generally:

$$\begin{aligned}
\ell_\omega &:= \mathfrak{l}_0(\phi(u \boxplus v)) = \omega u + \omega^2 v \\
\ell_{\omega^2} &:= \mathfrak{l}_1(\phi(u \boxplus v)) = \omega^2 u + \omega v \\
\ell_{id} &:= \mathfrak{l}_2(\phi(u \boxplus v)) = u + v
\end{aligned}$$

And then using lemma 5.6.4, we have $\mathfrak{l}_{\nwarrow} = \omega^2 \mathfrak{l}_0 - \omega \mathfrak{l}_1$ and $\mathfrak{l}_{\nearrow} = \omega^2 \mathfrak{l}_1 - \omega \mathfrak{l}_0$, so we confirm that:

$$\begin{aligned}
\mathfrak{l}_{\nwarrow}(\phi(u \boxplus v)) &= \omega^2(\omega u + \omega^2 v) - \omega(\omega^2 u + \omega v) = (\omega - \omega^2)v = \Delta v \\
\mathfrak{l}_{\nearrow}(\phi(u \boxplus v)) &= \omega^2(\omega^2 u + \omega v) - \omega(\omega u + \omega^2 v) = (\omega - \omega^2)u = \Delta u
\end{aligned}$$

noting that $\mathfrak{l}_{\nwarrow}$ and $\mathfrak{l}_{\nearrow}$ were defined to extract those quantities. Hence we have:

$$\partial(\ell_\omega, \ell_{\omega^2}, \ell_{id}) = \frac{d_{\mathcal{O}}(\ell_\omega, \ell_{\omega^2}, \ell_{id})}{d_{\mathcal{O}}(\ell_{\mathcal{O}}, \Delta v, \Delta u)} \tag{6.16}$$

$$\partial(\omega u + \omega^2 v, \omega^2 u + \omega v, u + v) = \frac{d_{\mathcal{O}}(\omega u + \omega^2 v, \omega^2 u + \omega v, u + v)}{d_{\mathcal{O}}(\ell_{\mathcal{O}}, \Delta v, \Delta u)} \tag{6.17}$$

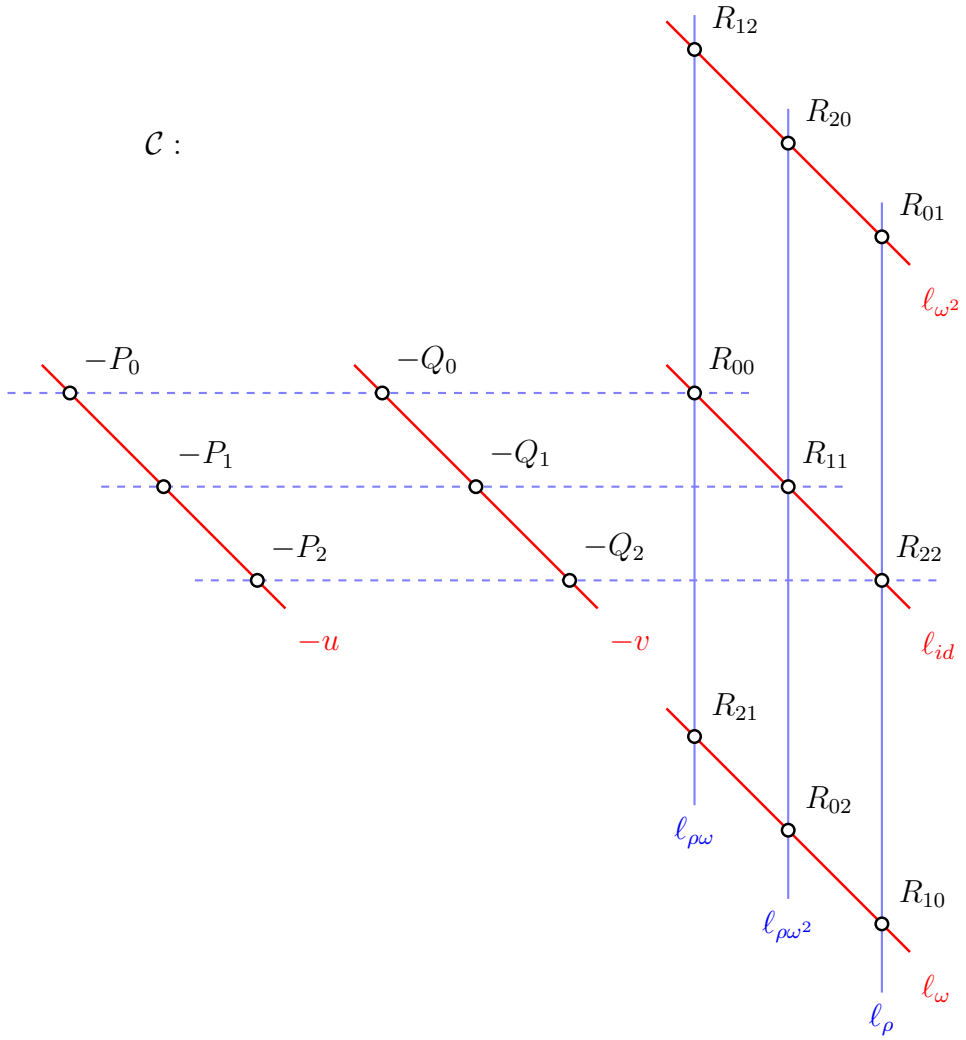
Note that all of the lines can be treated as unlabeled lines in those formulas.

In the next section, we will explain how to obtain a formula for $\partial(\ell_\omega, \ell_{\omega^2}, \ell_{id})$ from u, v and their cyclic orientations. On the other hand, the denominator is known, and this will give us enough control to perform a cyclic line multiplication.

6.5 Completion Diagrams

In this section, we combine nine point diagrams together into a *completion diagram*; these were described in section 5.7.1. Just as nine point diagrams are used to study line diagrams, we use completion diagrams to study nine point diagrams.

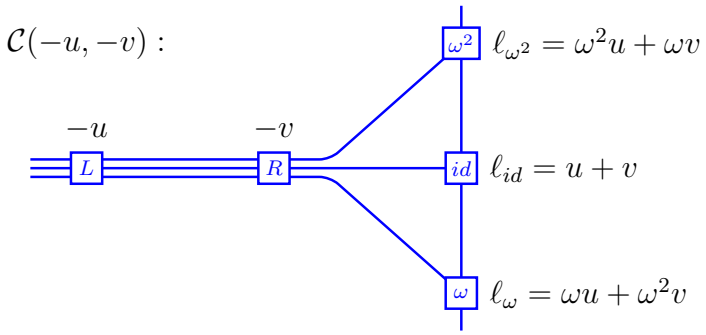
For $u, v \in \mathcal{L}_3^\circ(E)$ with respective points P_0, P_1, P_2 and Q_0, Q_1, Q_2, we represent a completion diagram as follows, where $R_{ij} = P_i + Q_j$ and as an unlabeled line ℓ_σ represents $u + \sigma v$:



Note that there are six lines which are not represented, but are implied: these are lines ℓ_{ij} with points $-P_i, -Q_j, P_i + Q_j$ for indices ij for $i, j \in \{0, 1, 2\}$.

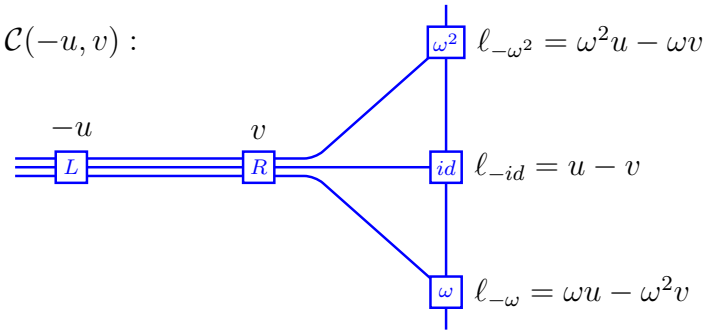
On the right side of the completion diagram, there is a vertical $u \boxplus v$ diagram. In fact, there are 10 nine point diagrams that can be found; we leave finding them as an exercise to the reader. In this section, we will combine the various formulas for $\partial(\mathcal{N})$ together to relate $\partial(u \boxplus v)$ to the cyclic orientations of u and v.

When $-u, -v$ are understood to be labeled lines with respective points $-P_i, -Q_i$ for $i = 0, 1, 2$, then we will use a simplified pictorial representation of $\mathcal{C}$:



The three lines on the right in descending order are $\ell_{\omega^2}, \ell_{id}, \ell_\omega$, which we now view as labeled lines. In a nutshell, the straight lines indicate that the three collinear labeled lines add up to $\ell_{\mathcal{O}}$; that is, they are labeled lines of labeled lines in $\mathcal{L}_3^\circ(\mathcal{L}_3^\circ(E))$, which are equivalent to nine point diagrams. The curved lines represent a similar relation, but with factors ω^i inserted; see section 5.7.2 for a precise description of the pictorial representation.

The main results of this section will be stated for the $\mathcal{C}(-u,-v)$ diagram, which is related to the line addition $u \boxplus v$, as well as the $\mathcal{C}(-u,v)$ diagram, which is related to the line addition $u \boxminus v$:



Where we notate the three labeled lines on the right as $\ell_{-\omega^2}, \ell_{-id}, \ell_{-\omega}$ in descending order, noting that without the labels, $\ell^\bullet_{-\sigma} = (u - \sigma v)^\bullet$.

First we translate the result of theorem 6.4.4 into this setting (in the form of equation (6.15)):

$$\partial(\ell_0, \ell_1, \ell_2) = \frac{d_{\mathcal{O}}(\ell_0, \ell_1, \ell_2)}{d_{\mathcal{O}}(\ell_{\mathcal{O}}, \ell_\nwarrow, \ell_\nearrow)}$$

But rather than apply this to $u \boxplus v$, we apply it to $\mathcal{N}(-u, -v, \ell_{id})$. Note that by the results of section 6.4.1, we have the following equalities of labeled lines: $\ell_\nearrow = \omega^2 \ell_1 - \omega \ell_0$

and $\ell_{\nwarrow} = \omega^2\ell_0 - \omega\ell_1$. Hence for $\mathcal{N}(-u,-v,\ell_{id})$, these translate to $\omega^2(-v) - \omega(-u) = \ell_{-\omega}$ and $\omega^2(-u) - \omega(-v) = -\ell_{-\omega^2}$. Hence we get:

$$\begin{aligned}
\partial(-u,-v,\ell_{id}) =& \frac{d_{\mathcal{O}}(-u,-v,\ell_{id})}{d_{\mathcal{O}}(\ell_{\mathcal{O}},-\ell_{-\omega^2},\ell_{-\omega})} = \frac{d_{\mathcal{O}}(-u,-v,\ell_{id})}{\alpha_{-\omega}+\alpha_{-\omega^2}} \\
\partial(-u,-v,\ell_{\omega}) =& \frac{d_{\mathcal{O}}(-u,-v,\ell_{\omega})}{\alpha_{-id}+\alpha_{-\omega^2}} \\
\partial(-u,-v,\ell_{\omega^2}) =& \frac{d_{\mathcal{O}}(-u,-v,\ell_{\omega^2})}{\alpha_{-id}+\alpha_{-\omega}}
\end{aligned}$$

For symbolic calculations, it is convenient to write this explicitly:

$$\partial(-u,-v,u+v) = \frac{d_{\mathcal{O}}(-u,-v,u+v)}{d_{\mathcal{O}}(\ell_{\mathcal{O}},\omega v-\omega^2 u,\omega u-\omega^2 v)} \tag{6.18}$$

The first main result of this section is in the same vein, and encapsulates theorems 6.5.5 and 6.5.6:

Theorem 6.5.1. *For labeled lines $u,v \in \mathcal{L}_3^\circ(E)$, consider the three sum lines $w_0 = \omega u + \omega^2 v, w_1 = \omega^2 u + \omega v, w_2 = u+v$ which form a nine point diagram, as well as their counterpart difference lines $w_0' = \omega u - \omega^2 v, w_1' = \omega^2 u - \omega v, w_2' = u - v$. Then for $i = 0,1,2$:*

$$\begin{aligned}
\frac{e_0(u;v)}{e_0(u;-v)} =& \frac{\partial(-u,-v,w_0)}{\partial(-u,v,w_0')} = \frac{\partial(-u,-v,w_1)}{\partial(-u,v,w_1')} = \frac{\partial(-u,-v,w_2)}{\partial(-u,v,w_2')} \\
e_0(u;v) =& \partial(-u,-v,w_0)\partial(-u,-v,w_1)\partial(-u,v,w_2') \\
e_0(u;-v) =& \partial(-u,v,w_0')\partial(-u,v,w_1')\partial(-u,-v,w_2)
\end{aligned}$$

This will be a fundamental tool in our nine point diagram calculus. Moreover, in chapter 7, these will be an important theoretical tool when studying the action of three torsion on points and lines.

The second main result of this section is theorem 6.5.8, which gives the following formula for the linear sum diagram's orientation, in terms of the cyclic orientations of u, v:

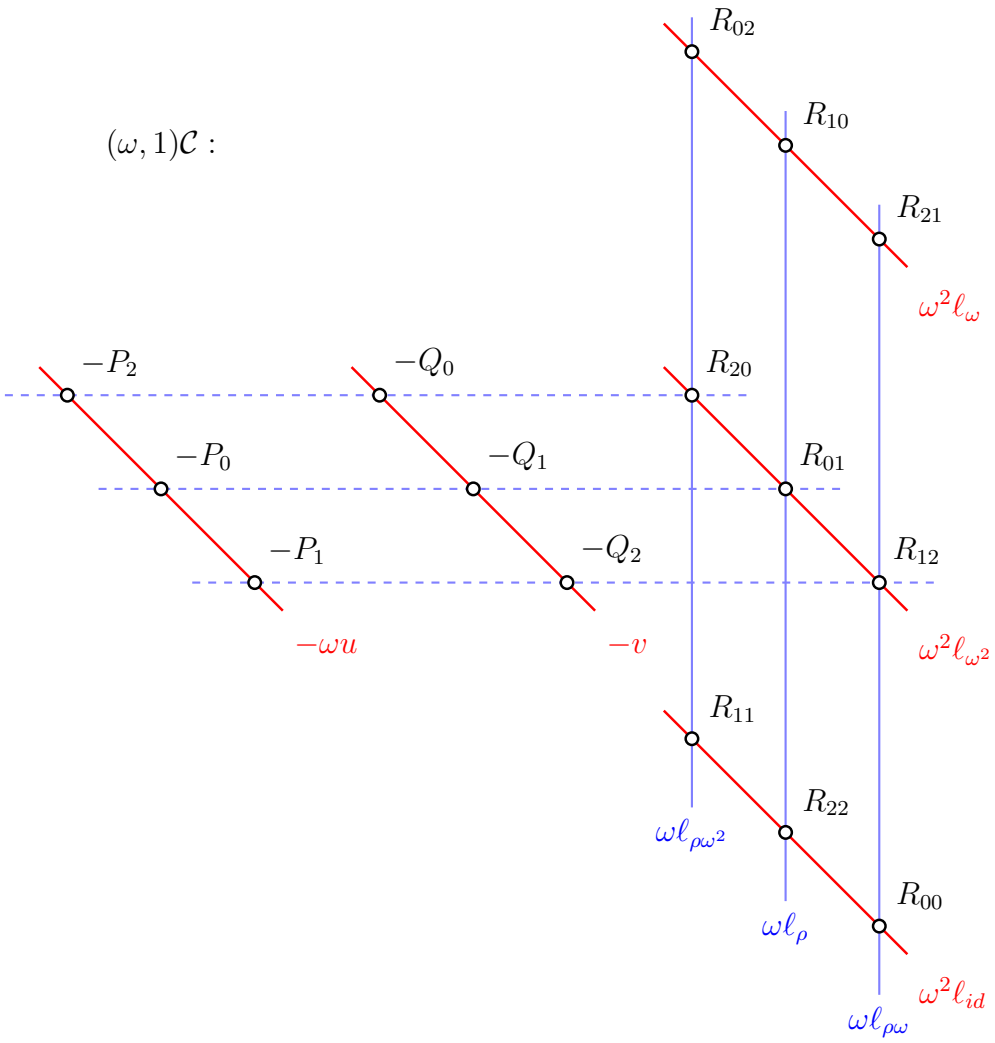
$$\partial(\ell_{id},\ell_{\omega},\ell_{\omega^2}) = \frac{-\delta_u \cdot \delta_v}{e_0(u;-v)}$$

This will be a useful tool for building cyclic line multiplication algorithms; we rewrite it in a convenient form for this purpose:

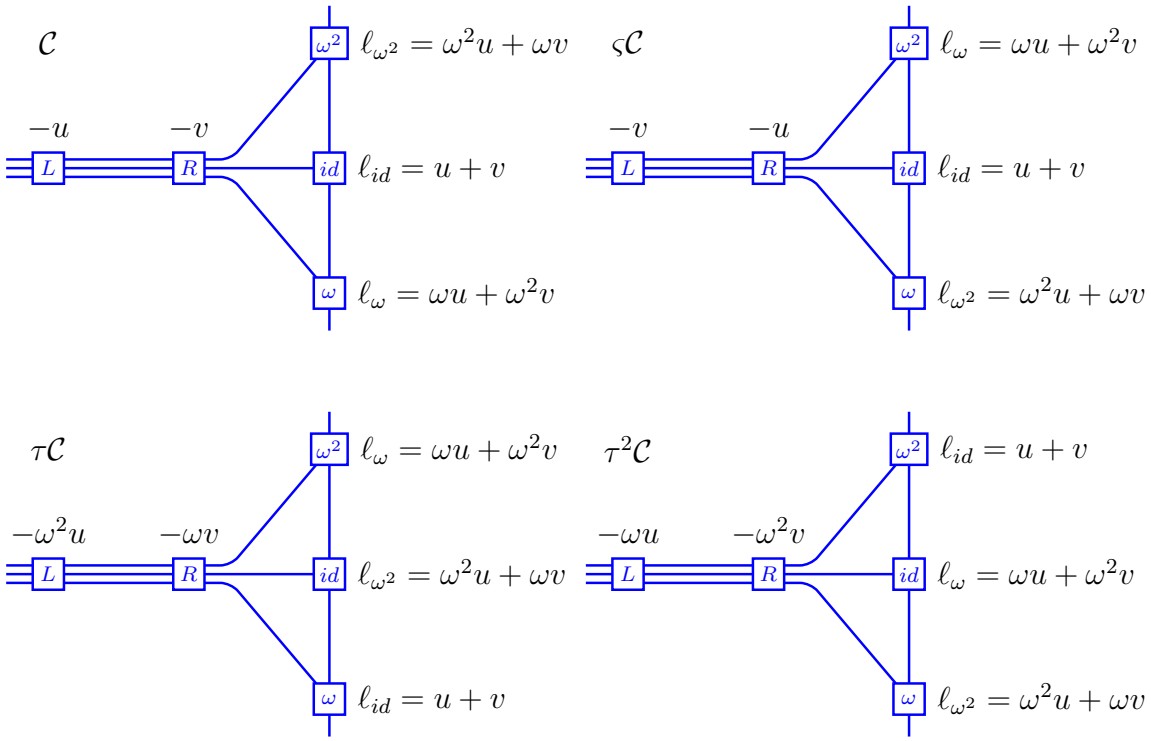
$$\partial(u+v,\omega u+\omega^2 v,\omega^2 u+\omega v) = \frac{-\delta(u)\cdot\delta(v)}{e_0(u;-v)} \tag{6.19}$$

6.5.1 Symmetries

The full symmetry group of a completion diagram encompasses all permutations of the two leftmost lines $-u, -v$, as well as swapping their places; see section 5.7.1. We will illustrate this with the cycle $\omega = (012)$ acting on the leftmost line $-u$:



In particular, we focus on the automorphisms $\tau = (\omega^2, \omega), \varsigma$, as well as $\varrho = (\rho, 1)$ when we want to consider the other orientation of $u \boxplus v$; these three automorphisms generate $\mathrm{Aut}(\mathfrak{C})$. This is because in the appropriate context, the five lines $u, v, \ell_{id}, \ell_\omega, \ell_{\omega^2}$ are all lines that appear in a line addition step. Pictorially, for labeled lines $u, v \in \mathcal{L}_3^\circ(E)$, we focus on the following:



Notice that these have exactly the same labeled lines on the right side.

6.5.2 Relations from Line Sum Function

Now we turn to the problem of describing relations between the lines in a completion diagram. As a first step, we can translate some earlier results into this context. Namely, we can use the formulas for the line sum function from theorem 3.7.3 to express relations between the 5 lines $-u, -v, \ell_{id}, \ell_\omega, \ell_{\omega^2}$ that we are most interested in. We do this briefly, since we will not use these results very much.

Let $\ell_\sigma(x, y) = y - \alpha_\sigma x - \beta_\sigma$. Then we will use the following functions to concisely express our relations:

Definition 6.5.2. *For $(x, y) \in \mathbb{F}^2$, we define:*

$$\begin{aligned} e_0(x, y) =& b + ax + x^3 - y^2 \\ e_1(x, y) =& -a^2 + 9bx + 3ax^2 + 3xy^2 \end{aligned}$$

Then for lines ℓ_0, ℓ_1, we define:

$$\begin{aligned} e_0(\ell_0;\ell_1) :=& b(\alpha_0-\alpha_1)^3 - a(\alpha_0-\alpha_1)^2(\beta_0-\beta_1) - (\beta_0-\beta_1)^3 - (\alpha_0-\alpha_1)(\alpha_0\beta_1-\alpha_1\beta_0)^2 \\ =& (\alpha_0-\alpha_1)^3 e_0(\ell_0 \cap \ell_1) \\ e_1(\ell_0;\ell_1) :=& -a^2(\alpha_0-\alpha_1)^3 - 9b(\alpha_0-\alpha_1)^2(\beta_0-\beta_1) + 3a(\alpha_0-\alpha_1)(\beta_0-\beta_1)^2 - 3(\beta_0-\beta_1)(\alpha_0\beta_1-\alpha_1\beta_0)^2 \\ =& (\alpha_0-\alpha_1)^3 e_1(\ell_0 \cap \ell_1) \end{aligned}$$

These functions allow us to express the coefficients of the line sum function in a simpler form. In fact, the denominators of line sum coefficients are $e_0(u;-v)$, and this corresponds to the fact that $\mathcal{O} \in u \boxplus v$ when $u \cap -v \in E$.

With this notation, we can rewrite the formula for γ_2 from section 3.7, and equate this to the expression from theorem 3.10.1:

$$\alpha_{id}\alpha_\omega + \alpha_{id}\alpha_{\omega^2} + \alpha_\omega\alpha_{\omega^2} = \alpha_\rho\alpha_{\rho\omega} + \alpha_\rho\alpha_{\rho\omega^2} + \alpha_{\rho\omega}\alpha_{\rho\omega^2} = \frac{e_1(u,-v)}{e_0(u;-v)}$$

In fact e_0, e_1 are cubic forms that we will study in chapter 7.

6.5.3 Pairing Indicators

Now we would like to apply theorem 6.3.6 to the completion diagram. We define the quantity ϕ_i from theorem 6.3.6 more generally, as a function of the pairing between $-u, -v$ that results in the sum ℓ_σ:

Definition 6.5.3. *For lines u, v as found in the completion diagram $\mathcal{C}$, the* pairing indicator *is*

$$\phi(\mathcal{C}) := \phi(u;v) := (x_{Q_0} - x_{P_0})(x_{Q_1} - x_{P_1})(x_{Q_2} - x_{P_2})$$

noting that this is invariant under negation of either argument. More generally, for $\sigma \in \mathrm{Aut}(\mathfrak{C})$ we define:

$$\phi_\sigma(\mathcal{C}) := \phi_\sigma(u;v) := \phi(\sigma\mathcal{C})$$

Note that ϕ is not a function of u, v as unlabeled lines. It do have invariance under the diagonal subgroup of $S_3 \times S_3 \subset \mathrm{Aut}(\mathfrak{C})$:

$$\phi_{(\sigma,\sigma)}(u;v) := \phi(\sigma u;\sigma v) := \phi(u;v)$$

which we interpret as u, v having points paired together in the same way as $\sigma u, \sigma v$ under (labeled) line addition.

In particular, $\phi_\varsigma(u;v) = \phi(v;u) = -\phi(u;v)$, and we focus on the following three quantities:

$$\begin{aligned}\phi_{id} := \phi_{id}(u;v) =&(x_{Q_0} - x_{P_0})(x_{Q_1} - x_{P_1})(x_{Q_2} - x_{P_2})\\ \phi_\tau := \phi_\tau(u;v) =&(x_{Q_2} - x_{P_1})(x_{Q_0} - x_{P_2})(x_{Q_1} - x_{P_0})\\ \phi_{\tau^2} := \phi_{\tau^2}(u;v) =&(x_{Q_1} - x_{P_2})(x_{Q_2} - x_{P_0})(x_{Q_0} - x_{P_1})\end{aligned}$$

Now we have the following corollary of theorem 6.3.6:

Lemma 6.5.4. *For the completion diagram $\mathcal{C}$, we have $\phi_{id}\phi_\tau\phi_{\tau^2} = e_0(-u;-v)e_0(u;-v)$, and*

$$\begin{aligned}\partial(-u,-v,\ell_{id}) =&\frac{e_0(-u;-v)}{\phi_{id}} = \frac{\phi_\tau\phi_{\tau^2}}{e_0(u;-v)}\\ \partial(-u,-v,\ell_\omega) =&\frac{e_0(-u;-v)}{\phi_{\tau^2}} = \frac{\phi_{id}\phi_\tau}{e_0(u;-v)}\\ \partial(-u,-v,\ell_{\omega^2}) =&\frac{e_0(-u;-v)}{\phi_\tau} = \frac{\phi_{id}\phi_{\tau^2}}{e_0(u;-v)}\end{aligned}$$

Furthermore,

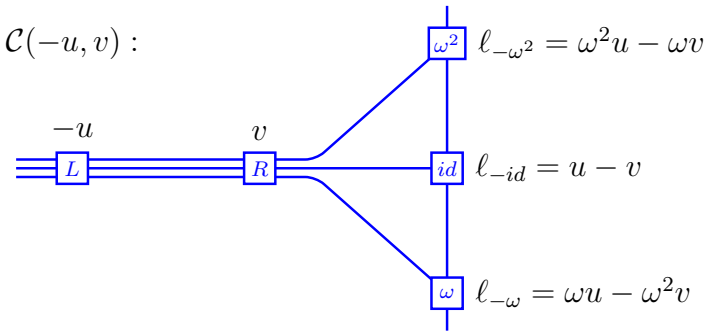
$$\partial(-u,-v,\ell_{id})\partial(-u,-v,\ell_\omega)\partial(-u,-v,\ell_{\omega^2}) =\frac{e_0(-u;-v)^2}{e_0(u;-v)}$$

Hence if we know u, v and two of their possible sum lines, then we can calculate the orientation for the diagram containing $-u, -v$ and the third possible sum line. The following form will be an important tool in our nine point diagram calculus:

Theorem 6.5.5. *For cyclically oriented lines u, v, if the three sum lines are w_1, w_2, w_3, then we have:*

$$\partial(-u,-v,w_1)\partial(-u,-v,w_2)\partial(-u,-v,w_3) =\frac{e_0(-u;-v)^2}{e_0(u;-v)}$$

Now we consider completion diagrams where the line v replaces $-v$:



Note that as unlabeled lines, $\ell_{-\sigma}$ is the difference $u - \sigma v$. Note also that the functions ϕ_σ only depend on x-coordinates, and hence they are the same when v changes signs: $\phi_\sigma(\overline{\mathcal{C}}) = \phi_\sigma(\mathcal{C})$. So by taking quotients, those terms cancel out:

$$\frac{e_0(-u;-v)}{e_0(-u;v)} = \frac{\partial(-u,-v,\ell_{id})}{\partial(-u,v,\ell_{-id})} = \frac{\partial(-u,-v,\ell_\omega)}{\partial(-u,v,\ell_{-\omega})} = \frac{\partial(-u,-v,\ell_{\omega^2})}{\partial(-u,v,\ell_{-\omega^2})}$$

More generally:

Theorem 6.5.6. *For lines u, v, if w is a sum line, and w' is a difference line, and furthermore the points of $u, \pm v$ are paired together the same way to obtain w and w', then:*

$$\frac{\partial(-u,-v,w)}{\partial(-u,v,w')} = \frac{e_0(-u;-v)}{e_0(-u;v)}$$

Note that if u, v are known, as well as one of $\partial(-u,-v,w), \partial(-u,v,w')$, then we can deduce the other. This will be considered to be an important part of our nine point diagram calculus as well.

6.5.4 Linear Sum Diagram Orientation

We will now express the orientation of the $u \boxplus v$ diagram found in $\mathcal{C}$ in terms of u, v and their cyclic orientations. We define the following quantities, which indicate the cyclic orientations of u, v; see definition 3.4.1:

Definition 6.5.7. *The cyclic orientations of the lines $-u, -v$ of $\mathcal{C}$ are:*

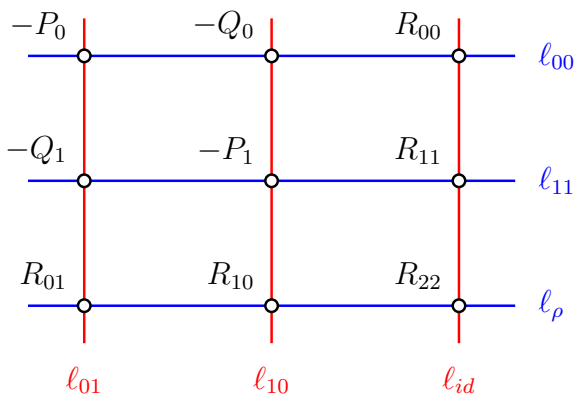
$$\begin{aligned}\delta_u &= (x_{P_1} - x_{P_0})(x_{P_2} - x_{P_1})(x_{P_0} - x_{P_2}) \\ \delta_v &= (x_{Q_1} - x_{Q_0})(x_{Q_2} - x_{Q_1})(x_{Q_0} - x_{Q_2})\end{aligned}$$

The idea is to use theorem 6.3.6 on two closely related diagrams found in $\mathcal{C}$; then by taking the quotient of their orientations, we get a lot of cancellation. For those same diagrams, we do the same using the factorization formulas in theorem 6.3.3. Then by combining all of those factorizations together, we get the following:

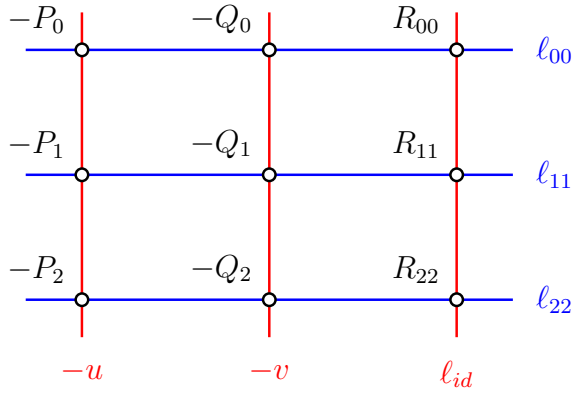
Theorem 6.5.8.

$$\partial(\ell_{id}, \ell_\omega, \ell_{\omega^2}) = \frac{-\delta_u \cdot \delta_v}{e_0(u;-v)}$$

Proof. We use the factorization formula 6.3.3 with the following two nine point diagrams consisting of lines $\ell_{00}, \ell_{11}, \ell_\rho$:



and $\ell_{00}, \ell_{11}, \ell_{22}$:



By taking the ratio of their orientations, we get cancellation:

$$\frac{\partial(\ell_{00}, \ell_{11}, \ell_\rho)}{\partial(\ell_{00}, \ell_{11}, \ell_{22})} = \frac{(\alpha_{id} - \alpha_{00})(\alpha_{id} - \alpha_{11})(\alpha_{id} - \alpha_\rho)}{(\alpha_{id} - \alpha_{00})(\alpha_{id} - \alpha_{11})(\alpha_{id} - \alpha_{22})} = \frac{(\alpha_{id} - \alpha_\rho)}{(\alpha_{id} - \alpha_{22})}$$

Similarly, we take the same ratio with respect to theorem 6.3.6:

$$\frac{\partial(\ell_{00}, \ell_{11}, \ell_\rho)}{\partial(\ell_{00}, \ell_{11}, \ell_{22})} = \frac{e_0(\ell_{00}; \ell_{11})}{(x_{Q_1} - x_{P_0})(x_{P_1} - x_{Q_0})(x_{R_{11}} - x_{R_{00}})} \frac{(x_{P_1} - x_{P_0})(x_{Q_1} - x_{Q_0})(x_{R_{11}} - x_{R_{00}})}{e_0(\ell_{00}; \ell_{11})}$$

$$\frac{(\alpha_{id} - \alpha_\rho)}{(\alpha_{id} - \alpha_{22})} = \frac{(x_{P_1} - x_{P_0})(x_{Q_1} - x_{Q_0})}{(x_{Q_1} - x_{P_0})(x_{P_1} - x_{Q_0})}$$

Now we consider the above applied to $(\omega, \omega)\mathcal{C}$. In the place of $-P_i, -Q_i$ there will be $-P_{i-1}, -Q_{i-1}$; in the place of ℓ_ρ there will be $\ell_{\omega^{-1}\rho\omega} = \ell_{\rho\omega^2}$; and in the place of ℓ_{id} there wil be $\ell_{\omega^{-1}id\omega} = \ell_{id}$. So we get:

$$\frac{(\alpha_{id} - \alpha_{\rho\omega^2})}{(\alpha_{id} - \alpha_{11})} = \frac{(x_{P_0} - x_{P_2})(x_{Q_0} - x_{Q_2})}{(x_{Q_0} - x_{P_2})(x_{P_0} - x_{Q_2})}$$

and similarly for $(\omega^2, \omega^2)\mathcal{C}$ we get:

$$\frac{(\alpha_{id} - \alpha_{\rho\omega})}{(\alpha_{id} - \alpha_{00})} = \frac{(x_{P_2} - x_{P_1})(x_{Q_2} - x_{Q_1})}{(x_{Q_2} - x_{P_1})(x_{P_2} - x_{Q_1})}$$

Then we multiply those three conjugate formulas together:

$$\begin{aligned}&\frac{(x_{P_1} - x_{P_0})(x_{P_2} - x_{P_1})(x_{P_0} - x_{P_2})(x_{Q_1} - x_{Q_0})(x_{Q_2} - x_{Q_1})(x_{Q_0} - x_{Q_2})}{(x_{Q_0} - x_{P_1})(x_{Q_0} - x_{P_2})(x_{Q_1} - x_{P_0})(x_{Q_1} - x_{P_2})(x_{Q_2} - x_{P_0})(x_{Q_2} - x_{P_1})} \\ &= \frac{\delta_u \delta_v}{\phi_\tau \phi_{\tau^2}} = -\frac{(\alpha_{id} - \alpha_\rho)(\alpha_{id} - \alpha_{\rho\omega})(\alpha_{id} - \alpha_{\rho\omega^2})}{(\alpha_{id} - \alpha_{00})(\alpha_{id} - \alpha_{11})(\alpha_{id} - \alpha_{22})}\end{aligned}$$

recalling the notation from lemma 6.5.4. Then we recognize the numerator and denominator of the last expression respectively as

$$\begin{aligned}\partial(\ell_\rho, \ell_{\rho\omega}, \ell_{\rho\omega^2}) &= -\partial(\ell_{id}, \ell_\omega, \ell_{\omega^2}) \\ \partial(\ell_{00}, \ell_{11}, \ell_{22}) &= -\partial(-u, -v, \ell_{id})\end{aligned}$$

using theorem 6.3.3. So we have:

$$\frac{\partial(\ell_{id}, \ell_\omega, \ell_{\omega^2})}{\partial(-u, -v, \ell_{id})} = -\frac{\delta_u \delta_v}{\phi_\tau \phi_{\tau^2}}$$

We multiply this with lemma 6.5.4:

$$\partial(-u, -v, \ell_{id}) = \frac{\phi_\tau \phi_{\tau^2}}{e_0(u; -v)}$$

to obtain the desired form:

$$\partial(\ell_{id}, \ell_\omega, \ell_{\omega^2}) = \frac{-\delta_u \delta_v}{e_0(u; -v)}$$

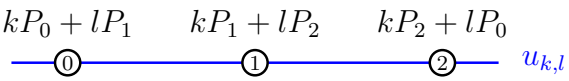
□

6.6 Diagrammatic Line Addition

Now we can use the results so far to provide an alternative to the algorithm of section 3.11. This can be used to improve the efficiency in the step where b_{u+v} is recovered. That said, we will not focus on this aspect since the improvement is small, and this requires some care. Instead, we focus on the large number of connections that exist between quantities in a line addition step. This gives very many alternatives for performing a line addition, and we hope to find efficient ways to take advantage of this in future work.

Note also that this thesis is not self-contained, since the earlier line multiplication algorithms relied on a computer algebra system to verify the formula for $u \boxplus v$. In this section, the algorithm described will not depend on any unwieldy formulas like the one for $\gamma_3(u, v)$. The only reliance left on computer verification is for the γ_1 function; this can in fact be done in less than a page by hand, using the result from section A.1 and a little trickery.

To describe our algorithm, we start with a labeled line u with points P_0, P_1, P_2. Then we use the notation $u_{k,l}(x, y) = y - m_{k,l}x - b_{k,l}$ to represent the line function associated to $u_{k,l} = (k + l\omega^2) \boxdot u$:



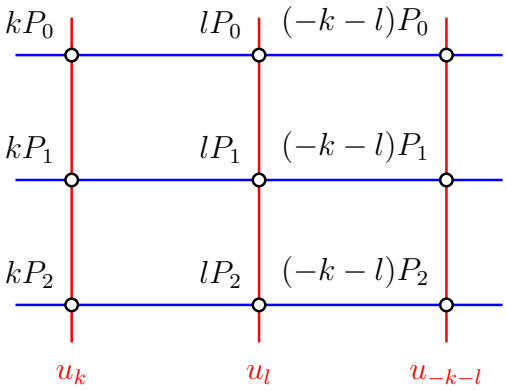
with $u_k := u_{k,0}$. Note that we define $u_{k,l}$ as a labeled line for convenience of notation. When we encounter $u_{k,l}$ in the algorithm below, that line should be thought of as an unlabeled line. So for computational purposes, $u_{k,l}$ generally represents the pair $(m_{k,l}, b_{k,l})$ of scalars.

Recall the algorithm from section 3.11, where we obtained the line sum u_{k+l} of u_k, u_l, given u_{k-l}, u_{k-2l}. In this section, we similarly make use of the following function to recover the slope m_{k+l}:

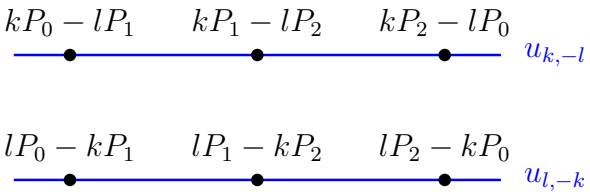
$$\gamma_1(u_k, u_l) = m_{k+l} + m_{k,l} + m_{l,k}$$

We will avoid using other coefficients γ_i of $u \boxplus v$, and instead use the results of this chapter to recover b_{k+l}.

Now we consider theorem 6.4.4 with respect to the following diagram:



The forward differences in the respective northeast and northwest directions are respectively:



so we have by corollary 6.4.4:

$$\partial(u_k, u_l, u_{-k-l}) = \frac{d_{\mathcal{O}}(u_k, u_l, u_{-k-l})}{m_{-k,l} + m_{l,-k}}$$
$$\partial(u_{-k}, u_l, u_{k-l}) = \frac{d_{\mathcal{O}}(u_{-k}, u_l, u_{k-l})}{m_{k,l} + m_{l,k}}$$

Note that in the latter expression, we will know all three lines u_{-k}, u_l, u_{k-l}, so we can compute the numerator; on the other hand, the denominator is known as a side effect of computing m_{k+l}. Hence we can calculate $\partial(u_{-k}, u_l, u_{k-l})$, and then we use lemma 6.5.6 to compute $\partial(u_k, u_l, u_{-k-l})$:

$$\partial(u_k, u_l, u_{-k-l}) = \frac{e_0(u_k; u_l)}{e_0(u_{-k}; u_l)} \partial(u_{-k}, u_l, u_{k-l})$$

And this allows us to recover b_{k+l} as follows, starting from the beginning:

1. Input: $u_k, u_l, u_{k-l}, u_{k-2l}$
2. Compute $m_{k,l} + m_{l,k} = \gamma_1(u_{k-l}, u_{-l}) - m_{k-2l}$
3. Compute $m_{k+l} = \gamma_1(u_k, u_l) - (m_{k,l} + m_{l,k})$
4. Compute $\partial(u_{-k}, u_l, u_{k-l}) = \frac{d_{\mathcal{O}}(u_{-k}, u_l, u_{k-l})}{m_{k,l} + m_{l,k}}$
5. Compute $\partial(u_k, u_l, u_{-k-l}) = \frac{e_0(u_k; u_l)}{e_0(u_{-k}; u_l)} \partial(u_{-k}, u_l, u_{k-l})$
6. Compute $m_{k,-l} + m_{-l,k} = \gamma_1(u_k, u_{-l}) - m_{k-l}$
7. Compute $\det(u_k, u_l, u_{-k-l}) = (m_{k,-l} + m_{-l,k})\partial(u_k, u_l, u_{-k-l})$
8. Since $b_{k+l}(m_k - m_l) - m_{k+l}(b_k - b_l) + (m_k b_l - m_\ell b_k) = \det(u_k, u_l, u_{-k-l})$, we compute:

$$b_{k+l} = \frac{\det(u_k, u_l, u_{-k-l}) + m_{k+l}(b_k - b_l) - (m_k b_l - m_l b_k)}{m_k - m_l}$$

Note that although we used the orientation ∂ of various nine point diagrams, we do not consider this to be a cyclic line multiplication algorithm. We will reserve that terminology for cases where we break the symmetry between $u_{k,l}$ and $u_{l,k}$.

6.7 Cyclic Line Multiplication

Now we consider cyclic line multiplication. Suppose that u is a labeled line, and that $(\omega - \omega^2) \boxdot u = \Delta u$ is known. As a starting point, take any unlabeled line multiplication algorithm. Then we can technically perform a cyclic line multiplication by computing $k \boxdot u$ from u and $k \boxdot \Delta u$ from Δu in parallel. Of course this feels like cheating! We briefly discuss improvements on this idea.

We will use the notation $u_k = k \boxdot u$, for $k \in \mathbb{Z}[\omega]/\langle 1 + \omega + \omega^2 \rangle$ in the Eisenstein integers, and consider u to be a cyclically oriented line (see section 5.6.1.) So for a line addition, we start with $u_k, u_l, u_{k-l}, u_{k-2l}$, and we also have their forward differences, with $\Delta u_k = u_{(\omega-\omega^2)k} = u_{\sqrt{-3}k}$. Note that we can compute $\partial(u_k \boxplus u_l), \partial(u_{k-l} \boxplus u_{-l})$ using theorem 6.5.8, since we know the cyclic orientations of those lines.

Then we can start by computing m_{k+l} as usual, and we do the same for the forward difference:

$$\begin{aligned} m_{k+\omega l} + m_{k+\omega^2 l} =& \gamma_1(u_{k-l}, u_{-l}) - m_{k-2l} \\ m_{\sqrt{-3}(k+\omega l)} + m_{\sqrt{-3}(k+\omega^2 l)} =& \gamma_1(u_{\sqrt{-3}(k-l)}, u_{-\sqrt{-3}(l)}) - m_{\sqrt{-3}(k-2l)} \end{aligned}$$

In fact, we outline a method to extract b_{k+l} and $b_{\sqrt{-3}(k+l)}$ with essentially the same method. This was alluded to in section 3.5.

Consider the following, thought of as a function of a nine point diagram $\mathcal{N}$:

$$\beta_\Sigma(\ell_0, \ell_1, \ell_2) := \beta_0 + \beta_1 + \beta_2 - \frac{1}{2}\partial(\ell_0, \ell_1, \ell_2)$$

Clearly this is invariant under ς, τ, since those permute the lines ℓ_0, ℓ_1, ℓ_2. But this is also invariant under ϱ, and hence all of $\mathrm{Aut}(\mathfrak{N})$:

$$\begin{aligned} \beta_\Sigma(\mathcal{N}) - \beta_\Sigma(\varrho\mathcal{N}) =& \beta_0 + \beta_1 + \beta_2 - \frac{1}{2}\partial(\mathcal{N}) - \beta_0' - \beta_1' - \beta_2' + \frac{1}{2}\partial(\varrho\mathcal{N}) \\ =& (\beta_0 + \beta_1 + \beta_2 - \beta_0' - \beta_1' - \beta_2') - \partial(\mathcal{N}) = 0 \end{aligned}$$

As a consequence, this is a function of the unlabeled nine point diagram, since it has invariance under all of the generators of the symmetry group.

Hence $\beta_\Sigma(u \boxplus v)$ has an expression as a function of u, v as unlabeled lines. So we can compute:

$$b_\Sigma(u_k \boxplus u_l) := b_{k+l} + b_{k+\omega l} + b_{k+\omega^2 l} = \beta_\Sigma(u \boxplus v) + \frac{1}{2}\partial(\boxplus v)$$

Hence by applying this to $u_{k-l} \boxplus u_{-l}$ as well, we can compute b_{k+l} just as we did for m_{k+l}:

$$\begin{aligned} b_{k+l} =& b_\Sigma(u_k \boxplus u_l) - b_\Sigma(u_{k-l} \boxplus u_{-l}) + b_{k-2l} \\ =& (b_{k+\omega l} + b_{k+\omega^2 l} + b_{k+l}) - (b_{k+\omega l} + b_{k+\omega^2 l} + b_{k-2l}) + b_{k-2l} \end{aligned}$$

Then similarly, we can compute $b_{\sqrt{-3}(k+l)}$ and this completes a cyclic line addition step.

Now we outline an alternative method in the same vein. Consider the following, thought of as a function of a nine point diagram $\mathcal{N}$:

$$\gamma(\ell_0, \ell_1, \ell_2) := \beta_0 + \beta_1 + \beta_2 - \alpha_0\alpha_1\alpha_2 - \partial(\ell_0, \ell_1, \ell_2)$$

Using the same argument as for β_Σ, this is $\mathrm{Aut}(\mathfrak{N})$-invariant:

$$\begin{aligned}\gamma(\mathcal{N}) - \gamma(\varrho\mathcal{N}) =& \beta_0 + \beta_1 + \beta_2 - \alpha_0\alpha_1\alpha_2 - \partial(\mathcal{N}) \\ & - \beta_0' - \beta_1' - \beta_2' + \alpha_0'\alpha_1'\alpha_2' + \partial(\varrho\mathcal{N}) \\ =& (\beta_0 + \beta_1 + \beta_2\beta_0' - \beta_1' - \beta_2') + (\alpha_0'\alpha_1'\alpha_2' - \alpha_0\alpha_1\alpha_2) - 2\partial(\mathcal{N}) = 0\end{aligned}$$

As a consequence, $\gamma(u \boxplus v)$ has an expression as a function of u, v as unlabeled lines. In fact, there are many expressions with similar properties, but this one was chosen because it is simpler than the others. Here it an expression for $\gamma(u \boxplus v)$, with $(X, Y) = u \cap (-v)$:

$$\begin{aligned}\gamma(u \boxplus v) =& \Big((3b + 2aX - Y^2)(2a + m_u b_v + m_v b_u) - (a + 3X^2)(3b - a m_u m_v - b_u b_v) \\ & - 2(3b(m_u - m_v) - 2a(b_u - b_v))Y \Big) / \Big((m_u + m_v)(b + aX + X^3 - Y^2) \Big)\end{aligned}$$

Using this, we get an algorithm similar to the method of section 3.11, but with the shorter expression γ rather than the huge γ_3. In fact, this can be used as an unlabeled line multiplication algorithm, if the ∂ expression is extracted as it was in the last section, for example.

In chapter 7, we will see new formulas which can be used for cyclic line multiplication. These involve trilinear forms f_0, f_1, which can replace the trilinear form $d_\mathcal{O}$:

$$\frac{d_\mathcal{O}(\ell_0, \ell_1, \ell_2)}{d_\mathcal{O}(\Delta v, \Delta u, \ell_\mathcal{O})} = \frac{f_0(\ell_0, \ell_1, \ell_2)}{f_0(\Delta v, \Delta u, \ell_\mathcal{O})} = \frac{f_1(\ell_0, \ell_1, \ell_2)}{f_1(\Delta v, \Delta u, \ell_\mathcal{O})} = \partial(\ell_0, \ell_1, \ell_2)$$

We are currently developing such algorithms.

Chapter 7

Three Torsion Algebra

Recall from chapter 3 that there is normally a six way ambiguity in adding two lines. In this chapter, we focus on a special case of line addition with no ambiguity: the addition of a triple intersection line. Such a line arises as the tangent line ℓ_T to E at a three torsion point $T \in E[3]$. Then for any line $\ell \in \mathcal{L}_3(E)$, there is a unique line sum between ℓ and ℓ_T, which is denoted $\ell^{\boxplus T}$.

The operation $\ell \mapsto \ell^{\boxplus T}$ turns out to play an important role in the algebra of line addition. For one, it provides symmetries of the line sum function:

$$u \boxplus v = u^{\boxplus T} \boxplus v^{\boxminus T}.$$

By studying invariant functions of this $E[3]$-action, we can better understand the line sum function. This is especially beneficial because the operation $\ell \mapsto \ell^{\boxplus T}$ turns out to have a simple form: it is a projective linear map, and so the coefficients of $\ell^{\boxplus T}$ can be obtained from those of ℓ via a matrix multiplication.

We then focus on an important class of functions which arise in connection to $E[3]$-invariance. These are trilinear forms which have simple transformation rules under the $E[3]$-action. These trilinear forms will provide simple relations between various lines that appear in a line addition. Furthermore, these relations have analogues in point arithmetic. This analogy is briefly mentioned here, since it is a good illustration of the central theme of this chapter.

First we note that for points satisfying $P_0 + P_1 + P_2 = \mathcal{O}$, we have $\det(P_0, P_1, P_2) = 0$ in projective coordinates due to the collinearity of those points. Then we note that for any $T \in E[3]$, we also have that $(P_0 + T) + (P_1 - T) + P_2 = \mathcal{O}$. By representing addition of three torsion with a matrix multiplication, we in fact get a cubic form $\det(M_T P_0, M_{-T} P_1, P_2)$ that vanishes for collinear points. By varying $T \in E[3]$, we can generate a 3 dimensional

vector space. By choosing a convenient basis, we get equations characterizing the relation $\det(P_0, P_1, P_2) = 0$.[1]

For example, in a Hessian form elliptic curve, we can use this principle to get simple point addition formulas. A Hessian form elliptic curve is defined by the equation:

$$E_\alpha : \ x^3 + y^3 + 1 - 3\alpha xy = 0,$$

with $\mathcal{O} = (-1 : 1 : 0)$. We can characterize collinearity of three (affine) points $P_0, P_1, P_2 \in E_\alpha$ by the vanishing of the following three cubic forms:

$$\begin{aligned} P_0 + P_1 + P_2 = \mathcal{O} \ \Leftrightarrow \ 0 =& 1 + x_0x_1x_2 + y_0y_1y_2 \\ =& x_0y_1 + x_1y_2 + x_2y_0 \\ =& x_0y_2 + x_1y_0 + x_2y_1. \end{aligned}$$

An analogous phenomenon arises in line addition, and this leads to simple line addition formulas on Hessian curves. Recall that for cyclic lines u, v with forward differences $\Delta u, \Delta v$, there are three cyclic sum lines ℓ_0, ℓ_1, ℓ_2. By theorem 6.4.4, these satisfy

$$-\frac{d_\mathcal{O}(\ell_0, \ell_1, \ell_2)}{d_\mathcal{O}(\Delta u, \Delta v, \ell_\mathcal{O})} = \partial(\ell_0, \ell_1, \ell_2) \tag{7.1}$$

Now we use the perspective from section 5.7 to similarly replace $d_\mathcal{O}$ with other trilinear forms. Suppose that $\ell_0, \ell_1, \ell_2, \Delta u, \Delta v$ are labeled lines; then because they form a nine point diagram, we have $\ell_0 + \ell_1 + \ell_2 = \ell_\mathcal{O}$ without loss of generality; furthermore, the forward differences can be taken to be $\Delta u = \text{↗}(\ell_0, \ell_1, \ell_2) = \omega^2\ell_1 - \omega\ell_0$, $\Delta v = \text{↖}(\ell_0, \ell_1, \ell_2) = \omega^2\ell_0 - \omega\ell_1$.

Then we also have $\ell_0^{\boxplus T} + \ell_1^{\boxminus T} + \ell_2 = \ell_\mathcal{O}$, using the same trick as for points. Hence $\ell_0^{\boxplus T}, \ell_1^{\boxminus T}, \ell_2$ form a nine point diagram. The forward differences are then

$$\begin{aligned} \text{↗}(\ell_0^{\boxplus T}, \ell_1^{\boxminus T}, \ell_2) =& \omega^2\ell_1^{\boxminus T} - \omega\ell_0^{\boxplus T} \\ =& \left(\omega^2\ell_1 - \omega\ell_0\right)^{\boxplus T} = (\Delta u)^{\boxplus T} \\ \text{↖}(\ell_0^{\boxplus T}, \ell_1^{\boxminus T}, \ell_2) =& \omega^2\ell_0^{\boxplus T} - \omega\ell_1^{\boxminus T} \\ =& \left(\omega^2\ell_0 - \omega\ell_1\right)^{\boxminus T} = (\Delta v)^{\boxminus T} \end{aligned}$$

So we get

$$-\frac{d_\mathcal{O}(\ell_0^{\boxplus T}, \ell_1^{\boxminus T}, \ell_2)}{d_\mathcal{O}((\Delta u)^{\boxplus T}, (\Delta v)^{\boxminus T}, \ell_\mathcal{O})} = \partial(\ell_0^{\boxplus T}, \ell_1^{\boxminus T}, \ell_2)$$

[1] See Daniel R.L. Brown's paper [2] for a different approach using cubic forms.

It turns out that by studying the transformation of ∂ under the action of $E[3]$, this last equation gives us exactly what we need! That is,

$$-\frac{\det(M_{-T}^{\intercal}[\ell_0], M_T^{\intercal}[\ell_1], [\ell_2])}{\det(M_{-T}^{\intercal}[\Delta u], M_T^{\intercal}[\Delta v], [\ell_{\mathcal{O}}])} = \partial(\ell_0, \ell_1, \ell_2)$$

and this gives a new trilinear form to replace $d_{\mathcal{O}}$! Again we get a 3 dimensional space of trilinear forms, and we can choose a convenient basis $d_{\mathcal{O}}, f_0, f_1$ with:

$$-\frac{d_{\mathcal{O}}(\ell_0, \ell_1, \ell_2)}{d_{\mathcal{O}}(\Delta u, \Delta v, \ell_{\mathcal{O}})} = -\frac{f_0(\ell_0, \ell_1, \ell_2)}{f_0(\Delta u, \Delta v, \ell_{\mathcal{O}})} = -\frac{f_1(\ell_0, \ell_1, \ell_2)}{f_1(\Delta u, \Delta v, \ell_{\mathcal{O}})} = \partial(\ell_0, \ell_1, \ell_2)$$

Now we elaborate on the transformation of ∂ under three torsion being added or subtracted from a nine point diagram. First off, if all points have T added, then the transformation is simple:

$$\partial(\ell_0^{\boxplus T}, \ell_1^{\boxplus T}, \ell_2^{\boxplus T}) = \frac{(2y_T)^3}{\ell_0(-T)\ell_1(-T)\ell_2(-T)}\partial(\ell_0, \ell_1, \ell_2)$$

which can be deduced by examining equation (7.1) under the transformation; in essence, each vector in the determinant is multiplied by the same matrix. For $\partial(\ell_0^{\boxplus T}, \ell_1^{\boxminus T}, \ell_2)$, this process would not work so cleanly, since the columns would be multiplied by different matrices. Fortunately though, we can rectify this by examining the following result of theorem 6.5.1, and its application under the transformation:

$$\begin{aligned}\partial(\ell_0, \ell_1, \ell_2)\partial(\ell_0, -\ell_1, \ell_{\nwarrow})\partial(\ell_0, -\ell_1, \ell_{\nearrow}) =& e_0(-\ell_0; \ell_1)\\ \partial(\ell_0^{\boxplus T}, \ell_1^{\boxminus T}, \ell_2)\partial(\ell_0^{\boxplus T}, (-\ell_1)^{\boxplus T}, \ell_{\nwarrow}^{\boxplus T})\partial(\ell_0^{\boxplus T}, (-\ell_1)^{\boxplus T}, \ell_{\nearrow}^{\boxplus T}) =& e_0((-\ell_0)^{\boxminus T}; \ell_1^{\boxminus T})\end{aligned}$$

Then all but the first term transform predictably; hence we can predict the transformation of the remaining term as a result. We briefly discuss a better explanation that we are developing in section 8.1.

7.1 Elliptic Curve Three Torsion

In this section, we characterize the triple intersection lines with E, since they provide a particularly simple case of line addition. In fact, the six possible sum lines mentioned in section 3.3 collapse to a single possibility if one of the summands is a triple intersection line.

Definition 7.1.1. *A triple intersection line ℓ_T for $T \in E$ is a line satisfying:*

$$\mathrm{Div}_P(\ell_T(P)) = 3(T) - 3(\mathcal{O})$$

By the characterization of principal divisors (see section 2.4), a triple intersection line ℓ_T exists for $T \in E$ if and only if $3T = \mathcal{O}$; so triple intersection lines correspond exactly to tangent lines at 3 torsion points $T \in E[3]$. We characterize $E[3]$ explicitly now, and define the notation that we use throughout this chapter:

Theorem 7.1.2. *Suppose $E: \ b + ax + x^3 - y^2 = 0$ is an elliptic curve over a field $\mathbb{F}$ of characteristic 0, with $a \neq 0$. Then E has nine three torsion points which form a subgroup that is a direct sum of two cyclic subgroups of order 3:*

$$\begin{aligned} E[3] =& \{\mathcal{O}, \pm T_0, \pm T_1, \pm T_2, \pm T_3\} \\ =& \{iT_0 + jT_1 \mid \ i, j \in \{0, 1, 2\}\end{aligned}$$

where we define $T_2 = T_0 + T_1$ and $T_3 = T_0 - T_1$.

For $T = (x_T, y_T) \in E[3]\backslash\{\mathcal{O}\}$, the triple intersection line is notated $\ell_T(x, y) = y - m_T x - b_T$ (and $\ell_{\mathcal{O}}(x, y) = 1$.) The eight slopes $z = m_T$ for $T \in E[3]\backslash\{\mathcal{O}\}$ correspond to the eight distinct roots of $-27a^2 + 108b\, z^2 + 18a\, z^4 + z^8$, and the coordinates of T and ℓ_T are:

$$\begin{aligned} T = (x_T, y_T) =& \left(\tfrac{m_T^2}{3}, \tfrac{3a + m_T^4}{6m_T}\right) \\ \ell_T(P) =& y_P - m_T x_P - b_T = y_P - m_T x_P - \tfrac{3a - m_T^4}{6m_T}. \end{aligned}$$

Note that $(m_{-T}, b_{-T}) = (-m_T, -b_T)$ and $(x_{-T}, y_{-T}) = (X_T, -y_T)$.

There is a primitive cube root of unity $\omega \in \overline{\mathbb{F}}$ (with $1 + \omega + \omega^2 = 0$) such that

$$\begin{aligned} m_{T_2} =& m_{T_0 + T_1} = \omega^2 m_{T_0} + \omega m_{T_1} \\ m_{T_3} =& m_{T_0 - T_1} = \omega m_{T_0} - \omega^2 m_{T_1} \end{aligned}$$

and furthermore m_{T_0} and m_{T_1} are related as follows for $\sqrt{-3} := \omega - \omega^2$:

$$0 = 3\sqrt{-3}a - m_{T_0}^3 m_{T_1} + \sqrt{-3} m_{T_0}^2 m_{T_1}^2 + m_{T_0} m_{T_1}^3$$

Note that as a simple corollary of theorem 7.1.2, the x-coordinates of $T \in E[3]\backslash\{\mathcal{O}\}$ are exactly the roots of the following polynomial:

Definition 7.1.3. *The third modular polynomial is:*

$$\psi_3(x) := -a^2 + 12bx + 6ax^2 + 3x^4$$

and we denote $\psi_3(Q) := \psi_3(x_Q)$.

Theorem 7.1.2 is a summary of the results of section B.1 of the appendix. In fact, the main tool that we use in our proof is the diagrammatic calculus applied to a nine point diagram formed from three triple intersection lines.

7.1.1 Action of Three Torsion

In this section, we study the action of $E[3]$ on E via translations. A crucial observation is that addition of three torsion preserves lines. This corresponds to the following action of $E[3]$ on lines:

Definition 7.1.4. *For $T \in E[3]$ and a line $\ell \in \mathcal{L}_3^\circ(E)$ with points P_0, P_1, P_2, we define the T-*shift *of ℓ to be the line $\ell^{\boxplus T}$ with points $P_0 + T, P_1 + T, P_2 + T$. This gives a map $\boxplus T : \mathcal{L}_3^\circ(E) \to \mathcal{L}_3^\circ(E)$, which is well-defined for any line diagram. We also define $\ell^{\boxminus T} := \ell^{\boxplus(-T)}$.*

We point out an important consequence of the preservation of lines; the map $\boxplus T$ is projective linear, and hence is given by a matrix multiplication in projective coordinates. A further consequence is that the translation by T map $P \mapsto P + T$ on E can also be realized by a projective linear map. To more precisely state this, we first need to establish our linear algebraic notation:

Definition 7.1.5. *For a point $P \in \overline{\mathbb{F}}^2$ and a line ℓ without $\mathcal{O}$ as a point,*

$$[P] := \begin{bmatrix} x_P \\ y_P \\ 1 \end{bmatrix}, \qquad [\ell] = \begin{bmatrix} -\alpha(\ell) \\ 1 \\ -\beta(\ell) \end{bmatrix}$$

More generally, $[\ell]$ is defined so that $\ell(P) = [\ell]^\intercal [P]$.

For example,

$$[\ell_T] = \begin{bmatrix} -m_T \\ 1 \\ -b_T \end{bmatrix} \text{ for } T \in E[3]\backslash\{\mathcal{O}\}, \text{ and } [\ell_{\mathcal{O}}] = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}.$$

Then we can explicitly express the translation by T map as a matrix multiplication in projective coordinates:

Theorem 7.1.6. *For a three torsion point $T \in E[3]$ and $P \in E\backslash\{\mathcal{O}, -T\}$:*

$$[P + T] = \left(\frac{-2y_T}{\ell_{-T}(P)}\right) M_T [P]$$

where $M_{\mathcal{O}} = I$, and M_T is the following matrix for $T \neq \mathcal{O}$:

$$M_T := \frac{1}{-2y_T} \begin{bmatrix} -b_T - y_T & x_T & x_T(b_T + 2y_T) \\ -m_T y_T & y_T & -y_T(b_T + 2y_T) \\ m_T & 1 & b_T \end{bmatrix}.$$

More precisely, for $T \in E[3]\backslash\{\mathcal{O}\}$ the following holds for functions of P in $\mathbb{F}(E)$:

$$\begin{bmatrix} x_{P+T} \\ y_{P+T} \\ 1 \end{bmatrix} = \left(\frac{-2y_T}{y_P + m_T x_P + b_T} \right) M_T \begin{bmatrix} x_P \\ y_P \\ 1 \end{bmatrix}$$

For $T \in E[3]\backslash\{\mathcal{O}\}$, the coefficient vector of $\ell^{\boxplus T}$ is:

$$[\ell^{\boxplus T}] = \frac{-2y_T}{y_T + \alpha(\ell)x_T + \beta(\ell)} M_{-T}^{\intercal}[\ell]$$

This allows us to translate points from the plane by T as well:

Definition 7.1.7. *For $T \in E[3]\backslash\{\mathcal{O}\}$ and a point $P \in \overline{\mathbb{F}}^2$ with $\ell_{-T}(P) \neq 0$, we define $P + T$ by the formula*

$$[P + T] = \left(\frac{-2y_T}{\ell_{-T}(P)} \right) M_T[P]$$

Theorem 7.1.6 is proved in section B.2 of the appendix (see theorem B.2.1 and theorem B.3.1.) The following lemma gives algebraic properties of the various matrices M_T:

Lemma 7.1.8. *For any $T, T' \in E[3]$:*

(i) $\det(M_T) = 1$

(ii) $M_T M_{T'} = \omega^i M_{T+T'}$ *for some* $i \in \{0, 1, 2\}$.

(iii) $M_T^2 = M_{-T}$

(iv) $M_T^3 = I$

This is lemma B.4.1, which is proved in section B.4 of the appendix, with more detail.

7.2 Trilinear Forms

The action of $E[3]$ is important to us because linear summation is invariant under the transformation $(u, v) \mapsto (u^{\boxplus T}, v^{\boxminus T})$:

$$u \boxplus v = u^{\boxplus T} \boxplus v^{\boxminus T}.$$

Hence we can better understand linear summation by studying $E[3]$-invariant functions. This in fact leads to simpler expressions in our line multiplication algorithms. But the benefits run much deeper, since there are arithmetic interpretations of many of the expressions that arise naturally when classifying $E[3]$-invariant functions.

We first focus on a class of expressions which transform predictably under T-shifts of their arguments. These are typified by the *determinant form*:

$$d_{\mathcal{O}}(P_0, P_1, P_2) := \det([P_0], [P_1], [P_2])$$

As a consequence of the projective linearity of T-shifts, the determinant form has a simple transformation rule under translation by $T \in E[3]\backslash\{\mathcal{O}\}$:

$$d_{\mathcal{O}}(P_0 + T, P_1 + T, P_2 + T) = \left(\prod_{i=0}^{2} \frac{-2y_T}{\ell_{-T}(P_i)}\right) d_{\mathcal{O}}(P_0, P_1, P_2)$$

This is a simple consequence of theorem 7.1.6. In fact, using the algebraic properties of the M_T matrices from lemma 7.1.8, we can define more general forms which have the same transformation formulas:

Definition 7.2.1. *For $T \in E[3]$, the* T-determinant form *is the following trilinear form for $v_1, v_2, v_3 \in \mathbb{F}^3$:*

$$d_T(v_0, v_1, v_2) := \det(v_1, M_T v_2, M_{-T} v_3).$$

We use the same terminology to denote the following associated function of $P_0, P_1, P_2 \in E$:

$$d_T(P_0, P_1, P_2) := d_T([P_0], [P_1], [P_2]) = \det([P_0], M_T[P_1], M_{-T}[P_2]).$$

We also define the cubic form $d_T(v) := d_T(v, v, v)$, and similarly $d_T(P) := d_T(P, P, P)$.

We first establish the transformation rules for these forms under T-shifts and permutations:

Theorem 7.2.2. *For any $T' \in E[3]$, the form $d_{T'}$ transforms as follows under translation of its arguments by $T \in E[3]\backslash\{\mathcal{O}\}$:*

$$d_{T'}(P_0 + T, P_1 + T, P_2 + T) = \left(\prod_{i=0}^{2} \frac{-2y_T}{\ell_{-T}(P_i)}\right) d_{T'}(P_0, P_1, P_2)$$

Furthermore, d_T is invariant under cyclic shifts:

$$d_T(P_0, P_1, P_2) = d_T(P_1, P_2, P_0) = d_T(P_2, P_0, P_1)$$

and transforms as follows under transposition of any two arguments:

$$d_T(P_0, P_2, P_1) = -d_{-T}(P_0, P_1, P_2)$$

Proof. We use the following result from theorem 7.1.6 for $T \in E[3]\backslash\{\mathcal{O}\}$:

$$[P+T] = \left(\frac{-2y_T}{y_P + m_T x_P + b_T}\right) M_T[P] = \left(\frac{-2y_T}{\ell_{-T}(P)}\right) M_T[P].$$

We also recall lemma 7.1.8, which implies that $M_{T'}M_T = \omega^i M_T M_{T'}$ for some $i \in \{0,1,2\}$, and that $M_{T'}^{-1} = M_{-T'}$. Hence

$$M_{-T'}M_T = M_{-T'}(M_T M_{T'})M_{-T'} = M_{-T'}(\omega^{-i}M_{T'}M_T)M_{-T'} = \omega^{-i}M_T M_{-T'}$$

and we can use this to demonstrate the T-shift transformation formula:

$$\begin{aligned}
&d_{T'}(P_0+T, P_1+T, P_2+T) = \det\left([P_0+T], M_{T'}[P_1+T], M_{-T'}[P_2+T]\right) \\
&= \det\left(\frac{-2y_T}{\ell_{-T}(P_0)}M_T[P_0], \frac{-2y_T}{\ell_{-T}(P_1)}M_{T'}M_T[P_1], \frac{-2y_T}{\ell_{-T}(P_2)}M_{-T'}M_T[P_2]\right) \\
&= \left(\prod_{i=0}^{2}\frac{-2y_T}{\ell_{-T}(P_i)}\right)\det\left(M_T[P_0], \omega^i M_T M_{T'}[P_1], \omega^{-i}M_T M_{-T'}[P_2]\right) \\
&= \left(\prod_{i=0}^{2}\frac{-2y_T}{\ell_{-T}(P_i)}\right)\det\left([P_0], M_{T'}[P_1], M_{-T'}[P_2]\right) = \left(\prod_{i=0}^{2}\frac{-2y_T}{\ell_{-T}(P_i)}\right) d_{T'}(P_0, P_1, P_2)
\end{aligned}$$

Where we used the fact that $\det(M_T) = 1$. We use that same property to prove the invariance of d_T under cyclic shifts:

$$\begin{aligned}
d_T(P_1, P_2, P_0) &= \det([P_1], M_T[P_2], M_{-T}[P_0]) \\
&= \det(M_T[P_1], M_T M_T[P_2], M_T M_{-T}[P_0]) \\
&= \det(M_T[P_1], M_{-T}[P_2], [P_0]) \\
&= \det([P_0], M_T[P_1], M_{-T}[P_2]) = d_T(P_0, P_1, P_2)
\end{aligned}$$

Lastly under transpositions we have:

$$\begin{aligned}
d_T(P_0, P_2, P_1) &= \det([P_0], M_T[P_2], M_{-T}[P_1]) \\
&= -\det([P_0], M_{-T}[P_1], M_T[P_2]) = -d_{-T}(P_0, P_1, P_2)
\end{aligned}$$

□

The determinant forms can be used to define functions of $P \in E$ that are invariant under translation by $T \in E[3]$. For example, the function $d_{T'}(P)/d_{T''}(P)$ is invariant under the action of $E[3]$ for fixed $T', T'' \in E[3]\backslash\{\mathcal{O}\}$. Many of those $E[3]$-invariant functions have connections to point arithmetic on E; for example the function $d_{T'}(P)/d_{T''}$ is related to $x(3P)$ by a simple transformation.

There are many other connections between determinant forms and point arithmetic. In particular, for any $T \in E[3]$ we have $d_T(P_0, P_1, P_2) = 0$ whenever $P_0 + P_1 + P_2 = \mathcal{O}$. When $T = \mathcal{O}$, this is easy to see since we are taking a determinant of a matrix whose columns represent three collinear points. More generally, d_T vanishes with those arguments since $P_0 + (P_1 + T) + (P_2 - T) = \mathcal{O}$:

Lemma 7.2.3. *For $T \in E[3]$ and $P_0, P_1, P_2 \in E$ satisfying $P_0 + P_1 + P_2 = \mathcal{O}$, the T-determinant form satisfies $d_T(P_0, P_1, P_2) = 0$.*

Proof. By definition,

$$d_T(P_0, P_2, P_1) = \det([P_0], M_T[P_1], M_{-T}[P_2])$$

and those column vectors represent the points $P_0, P_1 + T, P_2 - T$ respectively in projective coordinates, by theorem 7.1.6. The determinant thus vanishes, since those points $P_0, P_1 + T, P_2 - T$ are collinear by virtue of having sum $\mathcal{O}$. □

We can use this lemma to derive point addition formulas. Suppose that $P_0, P_1 \in E$ are given, and we would like to find $P_0 + P_1$. First we solve for $P_2 = -P_0 - P_1$ in the following system of linear equations:

$$d_{\mathcal{O}}(P_0, P_1, P_2) = d_{T_0}(P_0, P_1, P_2) = d_{T_1}(P_0, P_1, P_2) = 0$$

and then we simply negate P_2 to obtain $P_0 + P_1$. We will elaborate on this concept in section 7.2.3. For now, we focus on other arithmetic connections which we will use to prove algebraic properties of determinant forms.

7.2.1 Cyclic Orientation from Determinant Forms

We will now give another arithmetic interpretation to the determinant forms. Specifically, for $Q \in E$ and a line u with points P_0, P_1, P_2 we will prove the following in theorem 7.2.4:

$$\begin{vmatrix} x_{P_0+Q} & x_{P_1+Q} & x_{P_2+Q} \\ y_{P_0+Q} & y_{P_1+Q} & y_{P_2+Q} \\ 1 & 1 & 1 \end{vmatrix} = \frac{(x_{P_1} - x_{P_0})(x_{P_2} - x_{P_1})(x_{P_0} - x_{P_2})(-a^2 + 12bx_Q + 6ax_Q^2 + 3x_Q^4)}{(y_Q + m_u x_Q + b_u)^3}$$

This relates the determinant form to the *cyclic orientation* $\delta(u)$ of $u \in \mathcal{L}_3^{\triangleright}(E)$ which was introduced in section 3.4:

$$\delta(u) = (x_{P_1} - x_{P_0})(x_{P_2} - x_{P_1})(x_{P_0} - x_{P_2}).$$

The other factor that appears in the numerator is $\psi_3(Q)$:

$$\psi_3(Q) = -a^2 + 12bx_Q + 6ax_Q^2 + 3x_Q^4$$

recall from section 7.1 that this is the third modular polynomial, which vanishes for $Q \in E[3]\backslash\{\mathcal{O}\}$.

In section 3.4, we also talked about specifying a cyclic orientation via a forward difference line Δu. These also appear in theorem 7.2.2 when we consider more general determinant forms:

$$\frac{d_T(P_0+Q, P_1+Q, P_2+Q)}{d_{\mathcal{O}}(P_0+Q, P_1+Q, P_2+Q)} = \frac{-y_T - m_{\Delta u}x_T - b_{\Delta u}}{2y_T}$$

In fact, this formula will be used in section 7.2.2 to derive formulas for $m_{\Delta u}$ and $b_{\Delta u}$, closing the gap left in theorem 3.4.2 without the use of a computer algebra system.

Theorem 7.2.4. *Suppose the line $u \in \mathcal{L}_3^{\triangleright}(E)$ has three distinct non-zero points P_0, P_1, P_2. Then for $Q \in E\backslash\{\mathcal{O}, -P_0, -P_1, -P_2\}$ we have:*

$$d_{\mathcal{O}}(P_0+Q, P_1+Q, P_2+Q) = \frac{\delta(u)\psi_3(Q)}{-u(-Q)^3}$$

and for $T \in E[3]\backslash\{\mathcal{O}\}$ we similarly have:

$$d_T(P_0+Q, P_1+Q, P_2+Q) = \frac{\Delta u(-T)}{2y_T} \cdot \frac{\delta(u)\psi_3(Q)}{-u(-Q)^3}$$

Proof. We consider u as being fixed, and we assume that u has no point from $E[3]$. Then for each $T \in E[3]$ we define the following function $d_T \in \mathbb{F}(E)$:

$$d_T(Q) := \det\left(\begin{bmatrix} x_{P_0+Q} \\ y_{P_0+Q} \\ 1 \end{bmatrix}, M_T \begin{bmatrix} x_{P_1+Q} \\ y_{P_1+Q} \\ 1 \end{bmatrix}, M_{-T} \begin{bmatrix} x_{P_2+Q} \\ y_{P_2+Q} \\ 1 \end{bmatrix}\right)$$

Claim: For each $T \in E[3]$, there is a constant c_T such that $d_T(Q) = c_T \cdot \psi_3(Q)/u(-Q)^3$. We will prove this claim by showing that both functions have identical divisors. Recall that the third modular polynomial vanishes at non-zero three-torsion points, and $u(-Q)$ vanishes at $-P_0, -P_1, -P_2$:

$$\begin{aligned}\mathrm{Div}_Q\left(\frac{\psi_3(x_Q)}{u(-Q)^3}\right) &= \sum_{T\in E[3]} (T) - 9(\mathcal{O}) - 3\left((-P_0) + (-P_1) + (-P_2) - 3(\mathcal{O})\right) \\ &= \sum_{T\in E[3]} (T) - 3(-P_0) - 3(-P_1) - 3(-P_2)\end{aligned}$$

On the other hand, consider the expansion of $d_T(Q)$ as a polynomial in $x(P_i+Q)$ and $y(P_i+Q)$ for $i=0,1,2$. Each monomial will be of the form

$$\xi_0(P_0+Q)\xi_1(P_1+Q)\xi_2(P_2+Q)$$

where ξ_i is one of the functions x, y or 1. Hence $\mathrm{Div}(\xi_i) \geq -3(\mathcal{O})$, and as a consequence $\mathrm{Div}_Q(\xi_i(P_i+Q)) \geq -3(-P_i)$. So the monomial satisfies the following:

$$\mathrm{Div}_Q(\xi_0(P_0+Q)\xi_1(P_1+Q)\xi_2(P_2+Q)) \geq -3(-P_0)-3(-P_1)-3(-P_2)$$

It follows that $\mathrm{Div}(d_T)$ satisfies the above inequality as well. Furthermore, the function $d_T(Q)$ vanishes for each $Q \in E[3]$; this is because the columns in the determinant give the three collinear points P_0+Q, P_1+Q+T, P_2+Q-T in projective coordinates. Hence

$$\mathrm{Div}_Q(d_T(Q)) \geq \sum_{T\in E[3]}(T) - 3(-P_0) - 3(-P_1) - 3(-P_2) = \mathrm{Div}_Q\left(\frac{\psi_3(Q)}{u(-Q)^3}\right)$$

Now since all principal divisors have weight 0, the two divisors must in fact be equal. Hence the first claim is proved.

Claim: $c_{\mathcal{O}} = -(x_{P_1}-x_{P_0})(x_{P_2}-x_{P_1})(x_{P_0}-x_{P_2}) = -\delta(u)$

We will prove this by expanding the functions $d_{\mathcal{O}}(Q)$ and $\psi_3(Q)/u(-Q)^3$ locally at $\mathcal{O}$, and comparing leading coefficients. Recall from section 3.1 that the uniformizer $w := x/y$ vanishes to order 1 at $\mathcal{O}$. For functions in $\mathbb{F}(E)$, we will use the notation $f = g + O(w^k)$ to indicate that $\mathrm{Div}(f-g) \geq k(\mathcal{O})$. Note that since x, y are normalized functions of respective orders $-2, -3$ at $\mathcal{O}$, we have the expansions:

$$x = w^{-2} + O(w^{-1}), \qquad y = w^{-3} + O(w^{-2})$$

We can use the identity $y^2 = b + ax + x^3$ to bootstrap these into better expansions:

$$w^2x = w^3y = x^3y^{-2} = 1 - axy^{-2} - by^{-2} = 1 - aw^4 + O(w^5)$$

Next we expand the terms x_{P+Q} and y_{P+Q} that appear in the determinant, using the standard point addition formulas (see section 2.4.) We first expand the slope between these points:

$$\begin{aligned} m :=& \frac{y-y_P}{x-x_P} = w^{-1}\frac{w^3y - y_Pw^3}{w^2x - x_Pw^2} = w^{-1}\frac{1 - y_Pw^3 - aw^4 + O(w^5)}{1 - x_Pw^2 - aw^4 + O(w^5)} \\ =& w^{-1} + x_Pw - y_Pw^2 + x_P^2w^3 + O(w^4) \end{aligned}$$

Then we calculate the coordinates of $P+Q$:

$$\begin{aligned}
x_{P+Q} =& m^2 - x_P - x_Q \\
=& \left(w^{-2} + 2x_P - 2y_P w + 3x_P^2 w^2 + O(w^3)\right) - x_P - \left(w^{-2} - aw^2 + O(w^3)\right) \\
=& x_P - 2y_P w + (a + 3x_P^2)w^2 + O(w^3) \\
y_{P+Q} =& -m(x_{P+Q} - x_P) - y_P \\
=& -\left(w^{-1} + x_P w + O(w^2)\right)\left(-2y_P w + (a + 3x_P^2)w^2 + O(w^3)\right) - y_P \\
=& y_P - (a + 3x_P^2)w + O(w^2)
\end{aligned}$$

Finally we expand $d_{\mathcal{O}}$ as a determinant, noting that it vanishes at $Q = \mathcal{O}$:

$$\begin{aligned}
d_{\mathcal{O}} =& \begin{vmatrix} x_{P_0} - 2y_{P_0}w & x_{P_1} - 2y_{P_1}w & x_{P_2} - 2y_{P_2}w \\ y_{P_0} - (a + 3x_{P_0}^2)w & y_{P_1} - (a + 3x_{P_1}^2)w & y_{P_2} - (a + 3x_{P_2}^2)w \\ 1 & 1 & 1 \end{vmatrix} + O(w^2) \\
=& 3(x_{P_1} - x_{P_0})(x_{P_2} - x_{P_1})(x_{P_0} - x_{P_2})w + O(w^2) = 3\delta(u)w + O(w^2)
\end{aligned}$$

On the other hand,

$$\frac{\psi_3(Q)}{-u(-Q)^3} = \frac{(-a^2 + 12bx_Q + 6ax_Q^2 + 3x_Q^4)}{(y_Q + m_u x_Q + b_u)^3} = 3w + O(w^2)$$

so we have $d_{\mathcal{O}}(Q) = -\delta(u)\psi_3(Q)/u(-Q)^3$ since those functions have identical divisors and leading coefficients; thus $c_{\mathcal{O}} = -\delta(u)$.

Claim: $c_T/c_{\mathcal{O}} = \Delta u(-T)/(2y_T)$ for $T \in E[3]\backslash\{\mathcal{O}\}$

Since $d_T/d_{\mathcal{O}}$ is a constant function, we determine its value by considering $Q = -P_1$. To make the argument precise, we will consider the expansion of $d_T(Q - P_1)/d_{\mathcal{O}}(Q - P_1)$ at $Q = \mathcal{O}$. First we consider the leading term in the denominator:

$$\begin{aligned}
w^3 d_{\mathcal{O}}(Q - P_1) =& \begin{vmatrix} x_{P_0 - P_1 + Q} & w^3 x_Q & x_{P_2 - P_1 + Q} \\ y_{P_0 - P_1 + Q} & w^3 y_Q & y_{P_2 - P_1 + Q} \\ 1 & w^3 & 1 \end{vmatrix} = \begin{vmatrix} x_{P_1 - P_0} & 0 & x_{P_2 - P_1} \\ -y_{P_1 - P_0} & 1 & y_{P_2 - P_1} \\ 1 & 0 & 1 \end{vmatrix} + O(w) \\
=& (x_{P_1 - P_0} - x_{P_2 - P_1}) + O(w)
\end{aligned}$$

So $w^3 d_{\mathcal{O}}(Q - P_1)|_{Q=\mathcal{O}} = (x_{P_1 - P_0} - x_{P_2 - P_1})$. For the numerator, we proceed similarly:

$$\begin{aligned}
w^3 d_T(Q - P_1)\big|_{Q=\mathcal{O}} =& \det\left(\begin{bmatrix} x_{P_1 - P_0} \\ -y_{P_1 - P_0} \\ 1 \end{bmatrix}, M_T \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, M_{-T} \begin{bmatrix} x_{P_2 - P_1} \\ y_{P_2 - P_1} \\ 1 \end{bmatrix}\right) \\
=& \frac{-1}{4y_T^2} \begin{vmatrix} x_{P_1 - P_0} & x_T & (b_T + y_T)x_{P_2 - P_1} + x_T y_{P_2 - P_1} - x_T(b_T + 2y_T) \\ -y_{P_1 - P_0} & y_T & -m_T y_T x_{P_2 - P_1} - y_T y_{P_2 - P_1} - y_T(b_T + 2y_T) \\ 1 & 1 & -m_T x_{P_2 - P_1} + y_{P_2 - P_1} - b_T \end{vmatrix}
\end{aligned}$$

to simplify this determinant, we add $m_T x_{P_2-P_1} - y_{P_2-P_1} + (b_T + 2y_T)$ times the second column to the third one; and lastly we expand along the second column:

$$w^3 d_T(Q-P_1)\big|_{Q=\mathcal{O}} = \frac{-1}{4y_T^2}\begin{vmatrix} x_{P_1-P_0} & x_T & 2y_T x_{P_2-P_1} \\ -y_{P_1-P_0} & y_T & -2y_T y_{P_2-P_1} \\ 1 & 1 & 2y_T \end{vmatrix}$$

$$= \frac{(x_{P_1-P_0} - x_{P_2-P_1})y_T + (y_{P_2-P_1} - y_{P_1-P_0})x_T + (x_{P_1-P_0}y_{P_2-P_1} - x_{P_2-P_1}y_{P_1-P_0})}{-2y_T}$$

After dividing this by $(x_{P_1-P_0} - x_{P_2-P_1})$, we recognize the coefficients of the line Δu which passes through $P_1 - P_0$ and $P_2 - P_1$:

$$\frac{d_T(Q-P_1)}{d_{\mathcal{O}}(Q-P_1)} = \frac{y_T + m_{\Delta u}x_T + b_{\Delta u}}{-2y_T} = \frac{\Delta u(-T)}{2y_T}$$

So in fact $d_T/d_{\mathcal{O}} = c_T/c_{\mathcal{O}} = \Delta u(-T)/(2y_T)$, which proves the claim and concludes the proof of theorem 7.2.4. □

Now we generalize theorem 7.2.4 to more general arguments R_0, R_1, R_2 in the determinant forms. We can use theorem 7.2.4 by first solving for $Q \in E(\overline{\mathbb{F}})$ with $3Q = R_0+R_1+R_2$, and then taking u with points $P_i = R_i - Q$:

Corollary 7.2.5. *For $T \in E[3]\backslash\{\mathcal{O}\}$ and for distinct $R_0, R_1, R_2 \in E\backslash E[3]$ with $R_0 + R_1 + R_2 \neq \mathcal{O}$, the following holds:*

$$\frac{d_T(R_0,R_1,R_2)}{d_{\mathcal{O}}(R_0,R_1,R_2)} = \frac{-y_T - m_\Delta x_T - b_\Delta}{2y_T}$$

where $y - m_\Delta x - b_\Delta$ represents the line with points $R_1 - R_0, R_2 - R_1, R_0 - R_2$.

7.2.2 Forward Difference from Trilinear Forms

Now we consider the vector space generated by d_T as T varies over $E[3]$. We use corollary 7.2.5 as our starting point, in the following form:

$$\frac{d_T}{d_{\mathcal{O}}} = \frac{-1}{2} + m_\Delta \frac{-x_T}{2y_T} + b_\Delta \frac{-1}{2y_T} \tag{7.2}$$

where $d_T, d_{\mathcal{O}}, m_\Delta, b_\Delta$ are considered as functions of distinct $R_0, R_1, R_2 \in E\backslash E[3]$ with $R_0 + R_1 + R_2 \neq \mathcal{O}$. We consider $d_T/d_{\mathcal{O}}$ for $T = \mathcal{O}, T_0, T_1$:

$$\frac{d_{\mathcal{O}}}{d_{\mathcal{O}}} = 1$$

$$\frac{d_{T_0}}{d_{\mathcal{O}}} = \frac{-1}{2} + m_\Delta \frac{-x_{T_0}}{2y_{T_0}} + b_\Delta \frac{-1}{2y_{T_0}}$$

$$\frac{d_{T_1}}{d_{\mathcal{O}}} = \frac{-1}{2} + m_\Delta \frac{-x_{T_1}}{2y_{T_1}} + b_\Delta \frac{-1}{2y_{T_1}}$$

by solving for m_Δ, b_Δ, we obtain trilinear forms e_0, e_1 with $3e_0/d_\mathcal{O} = m_\Delta$ and $e_1/d_\mathcal{O} = b_\Delta$. Then each determinant form d_T for $T \in E\backslash\{\mathcal{O}\}$ is simply expressed as follows:

$$d_T = \frac{-1}{2} d_\mathcal{O} + \frac{-3x_T}{2y_T} e_0 + \frac{-1}{2y_T} e_1$$

see section B.5 for a more detailed argument. Note that the factor 3 is for consistency with definition 6.3.4.

Definition 7.2.6. *The trilinear forms e_0, e_1 are defined via the following:*

$$\begin{bmatrix} d_\mathcal{O} \\ e_0 \\ e_1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ \frac{-1}{2} & \frac{-3x_{T_0}}{2y_{T_0}} & \frac{-1}{2y_{T_0}} \\ \frac{-1}{2} & \frac{-3x_{T_1}}{2y_{T_1}} & \frac{-1}{2y_{T_1}} \end{bmatrix}^{-1} \begin{bmatrix} d_\mathcal{O} \\ d_{T_0} \\ d_{T_1} \end{bmatrix}$$

For points P_0, P_1, P_2 in the plane with $P_i = (x_i, y_i)$, the following gives formulas for $e_i(P_0, P_1, P_2)$:

$$\begin{aligned} e_0 =& b + \frac{a}{3}(x_0 + x_1 + x_2) + x_0x_1x_2 - \frac{1}{3}(y_0y_1 + y_0y_2 + y_1y_2) \\ e_1 =& -a^2 + 3b(x_0 + x_1 + x_2) + a(x_0x_1 + x_0x_2 + x_1x_2) + x_0y_1y_2 + x_1y_0y_2 + x_2y_0y_1 \end{aligned}$$

and we define $e_i(P) := e_i(P, P, P)$, so for $P = (x, y)$:

$$\begin{aligned} e_0(x, y) =& b + ax + x^3 - y^2 \\ e_1(x, y) =& -a^2 + 9bx + 3ax^2 + 3xy^2 \end{aligned}$$

We can now prove theorem 3.4.2, using the technique of local expansions from the proof of theorem 7.2.4:

Theorem 7.2.7. *For a line $u \in \mathcal{L}_3^\triangleright(E)$ with distinct non-zero points, the forward difference line Δu has the following coefficients:*

$$\begin{aligned} m_{\Delta u} =& \frac{9bm_u - 6ab_u + am_u^3 + 3m_ub_u^2}{(x_{P_1} - x_{P_0})(x_{P_2} - x_{P_1})(x_{P_0} - x_{P_2})} \\ b_{\Delta u} =& \frac{-2a^2m_u - 9bb_u + 2bm_u^3 - am_u^2b_u + b_u^3}{(x_{P_1} - x_{P_0})(x_{P_2} - x_{P_1})(x_{P_0} - x_{P_2})} \end{aligned}$$

Proof. As a function of Q, the expression $e_i(P_0+Q, P_1+Q, P_2+Q)/d_\mathcal{O}(P_0+Q, P_1+Q, P_2+Q)$ is constant and takes the value $m_{\Delta u}$ for $i = 0$ and $b_{\Delta u}$ for $i = 1$. To determine the value, we expand the numerators and denominators locally around $Q = \mathcal{O}$. The denominator

$d_{\mathcal{O}}(P_0+Q, P_1+Q, P_2+Q)$ expands as $3\delta(u)w + O(w^2)$, as we saw in the proof of theorem 7.2.4. Then we calculate the coefficient of w^1 in the numerators:

$$\begin{aligned} w^{-1}e_0(P_0+Q, P_1+Q, P_2+Q)\big|_{Q=\mathcal{O}} &= \sum_{\text{cyclic}} \left(\left(\frac{a}{3} + x_0x_1\right)(-2y_2) - \frac{1}{3}(y_0+y_1)(-a-3x_2^2) \right) \\ &= 9bm_u - 6ab_u + am_u^3 + 3m_ub_u^2 \end{aligned}$$

and similarly

$$\tfrac{1}{3}w^{-1}e_1(P_0+Q, P_1+Q, P_2+Q)\big|_{Q=\mathcal{O}} = -2a^2m_u - 9bb_u + 2bm_u^3 - am_u^2b_u + b_u^3$$

□

These trilinear forms e_0, e_1 have the advantage of having coefficients that do not depend on a choice of three torsion point. They have these properties inherited from the d_T:

Theorem 7.2.8. *For $i \in \{0,1\}$ and points R_0, R_1, R_2 in the plane,*

$$e_i(R_0+T, R_1+T, R_2+T) = \left(\prod_{i=0}^{2} \frac{-2y_T}{\ell_{-T}(P_i)}\right) e_i(R_0, R_1, R_2)$$

Furthermore, e_0 and e_1 are symmetric functions of their arguments.

Proof. These follow from theorem 7.2.2 and theorem B.5.2. The symmetry is clear from the definition. □

7.2.3 Point Addition and Trilinear Forms

Here we use the trilinear forms $d_{\mathcal{O}}, e_0, e_1$ to present a different point of view on elliptic curve point addition. This has similarities to the approach we take to line addition.

Recall that for $T \in E[3]$, and for $P_0, P_1, P_2 \in E$, we have $d_T(P_0, P_1, P_2) = 0$ when $P_0 + P_1 + P_2 = \mathcal{O}$. Then since e_0, e_1 are linear combinations of the d_T, this property also holds for those forms. Hence we can solve the following system of equations to derive a formula for $P_2 = -P_0 - P_1$ given points P_0, P_1 (with some special cases that are not covered):

$$d_0(P_0, P_1, P_2) = e_0(P_0, P_1, P_2) = e_1(P_0, P_1, P_2) = 0$$

So if $P_i = (x_i, y_i)$ for $i = 0, 1$, we solve for $P_2 = -P_0 - P_1 = (x_2, y_2)$ in the following system:

$$\begin{aligned} 0 &= (x_0y_1 - x_1y_0) + (y_0 - y_1)x_2 - (x_0 - x_1)y_2 \\ 0 &= \left(b + \frac{a}{3}(x_0+x_1) - y_0y_1\right) + \left(\frac{a}{3} + x_0x_1\right)x_2 - \frac{1}{3}(y_0+y_1)y_2 \\ 0 &= (-a^2 + 3b(x_0+x_1) + ax_0x_1) + (3b + a(x_0+x_1) + y_0y_1)x_2 + (x_0y_1 + x_1y_0)y_2 \end{aligned}$$

We note that there are identical addition formulas on other elliptic curves as well. For example, consider the curve E_1 defined by $e_1(P) = -a^2 + 9bx + 3ax^2 + 3xy^2 = 0$ and with base point $(0:1:0)$; note that the line $x = 0$ has a triple intersection at the base point. It follows that the T-shift of that line has a triple intersection at T; hence the three torsion points are the same for E_1 and E. Furthermore, the T-shifting formulas are also the same.

7.3 Trilinear Forms on Lines

There are also dual cubic forms, which have simple transformation properties. These will be useful to us later when discussing line addition relations.

Then we can similarly define trilinear maps:

Definition 7.3.1. *For $T \in E[3]$ and vectors v_0, v_1, v_2, we define:*

$$\widehat{d}_T(v_0, v_1, v_2) := \det\left(v_0, M_{-T}^{\intercal} v_1, M_T^{\intercal} v_2\right)$$

and for lines $\ell_0, \ell_1, \ell_2 \in \mathcal{L}_3^{\bullet}(E)$:

$$d_T(\ell_0, \ell_1, \ell_2) := \det\left([\ell_0], M_{-T}^{\intercal}[\ell_1], M_T^{\intercal}[\ell_2]\right)$$

Similarly to the trilinear forms on points, we also have a more convenient basis:

Definition 7.3.2. *We define the following two trilinear forms:*

$$\begin{aligned} f_0 =& \frac{\omega m_{T_1}(m_{T_0} - m_{T_2})^2}{6\sqrt{-3}}(\widehat{d}_{T_0} - \widehat{d}_{-T_0}) - \frac{\omega^2 m_{T_0}(m_{T_1} - m_{T_2})^2}{6\sqrt{-3}}(\widehat{d}_{T_1} - \widehat{d}_{-T_1}) \\ f_1 =& \frac{\omega b_{T_1}(m_{T_0} - m_{T_2})^2}{6\sqrt{-3}}(\widehat{d}_{T_0} - \widehat{d}_{-T_0}) - \frac{\omega^2 b_{T_0}(m_{T_1} - m_{T_2})^2}{6\sqrt{-3}}(\widehat{d}_{T_1} - \widehat{d}_{-T_1}) \end{aligned}$$

For vectors

$$v_0 = \begin{bmatrix} \alpha_0 \\ \zeta_0 \\ \beta_0 \end{bmatrix},\ v_1 = \begin{bmatrix} \alpha_1 \\ \zeta_1 \\ \beta_1 \end{bmatrix},\ v_2 = \begin{bmatrix} \alpha_2 \\ \zeta_2 \\ \beta_2 \end{bmatrix},$$

we have:

$$\begin{aligned} f_0(v_0, v_1, v_2) :=& 3b(\alpha_0\zeta_1\zeta_2 + \alpha_1\zeta_0\zeta_2 + \alpha_2\zeta_0\zeta_1) - 2a(\zeta_0\zeta_1\beta_2 + \zeta_0\zeta_2\beta_1 + \zeta_1\zeta_2\beta_0) \\ &+ a\alpha_0\alpha_1\alpha_2 + \alpha_0\beta_1\beta_2 + \alpha_1\beta_0\beta_2 + \alpha_2\beta_0\beta_1 \\ f_1(v_0, v_1, v_2) :=& -\frac{2}{3}a^2(\alpha_0\zeta_1\zeta_2 + \alpha_1\zeta_0\zeta_2 + \alpha_2\zeta_0\zeta_1) - 3b(\zeta_0\zeta_1\beta_2 + \zeta_0\zeta_2\beta_1 + \zeta_1\zeta_2\beta_0) \\ &+ 2b\alpha_0\alpha_1\alpha_2 - \frac{1}{3}a(\alpha_0\alpha_1\beta_2 + \alpha_0\alpha_2\beta_1 + \alpha_1\alpha_2\beta_0) + \beta_0\beta_1\beta_2 \end{aligned}$$

7.3.1 Trilinear Form Relations

We recall some important context: we would like to find relations between ℓ_0, ℓ_1, ℓ_2, to be used in the line addition step of our line multiplication operation chain. In particular, we will generally not assume a priori knowledge of $\ell_0', \ell_1', \ell_2'$. As a first step to rectifying this, we would like to develop formulas for $\partial(\ell_0, \ell_1, \ell_2)$ which do not involve knowledge of $\ell_0', \ell_1', \ell_2'$. Instead, we assume knowledge of ℓ_0, ℓ_1, ℓ_2, as well as the forward difference lines $\ell_{\nwarrow}, \ell_{\nearrow}$; in contrast to ℓ_i', the forward difference lines can be easily included in an operation chain, making a natural appearance in cyclic line addition.

Recall from chapter 6, that one approach was to use lemma 6.4.4. By comparing multiple nine point diagrams, we could get suitable cancellation that allowed us to perform a cyclic line addition. In this chapter, we will improve upon this. This is accomplished by developing new relations between $\ell_0, \ell_1, \ell_2, \ell_{\nwarrow}, \ell_{\nearrow}$. These are best expressed in terms of the trilinear forms on lines. In fact, they are reminiscent of the cubic form addition formulas from section 7.2.3.

These new relations come from a striking use of the formulas from chapter 6. By applying T-shifts to the arguments in judicious ways, we reveal extra symmetries. These lead to a bootstrapping process from lemma 6.4.4 to show that the trilinear form $d_{\mathcal{O}}$ can be replaced by any of the trilinear forms from section 7.2:

Theorem 7.3.3. *Using the notation from section 7.2, we have the following formulas for* $\partial(\ell_0, \ell_1, \ell_2)$*:*

$$\begin{aligned}\partial(\ell_0, \ell_1, \ell_2) &= -\frac{d_{\mathcal{O}}(\ell_0, \ell_1, \ell_2)}{d_{\mathcal{O}}(\ell_{\mathcal{O}}, \ell_{\nearrow}, \ell_{\nwarrow})} \\ &= -\frac{f_0(\ell_0, \ell_1, \ell_2)}{f_0(\ell_{\mathcal{O}}, \ell_{\nearrow}, \ell_{\nwarrow})} \\ &= -\frac{f_1(\ell_0, \ell_1, \ell_2)}{f_1(\ell_{\mathcal{O}}, \ell_{\nearrow}, \ell_{\nwarrow})}\end{aligned}$$

or explicitly:

$$\begin{aligned}\partial(\ell_0, \ell_1, \ell_2) &= \frac{\alpha_0(\beta_1 - \beta_2) + \alpha_1(\beta_2 - \beta_0) + \alpha_2(\beta_0 - \beta_1)}{\alpha_{\nearrow} - \alpha_{\nwarrow}} \\ &= \frac{3b(\alpha_0 + \alpha_1 + \alpha_2) - 2a(\beta_0 + \beta_1 + \beta_2) + a\alpha_0\alpha_1\alpha_2 + \alpha_2\beta_0\beta_1 + \alpha_1\beta_0\beta_2 + \alpha_0\beta_1\beta_2}{\alpha_{\nearrow}\beta_{\nwarrow} + \beta_{\nearrow}\alpha_{\nwarrow} - 2a} \\ &= \frac{2a^2(\alpha_0+\alpha_1+\alpha_2) + 9b(\beta_0+\beta_1+\beta_2) - 6b\alpha_0\alpha_1\alpha_2 + a(\alpha_1\alpha_2\beta_0+\alpha_0\alpha_2\beta_1+\alpha_0\alpha_1\beta_2) - 3\beta_0\beta_1\beta_2}{9b + a\alpha_{\nearrow}\alpha_{\nwarrow} + 3\beta_{\nearrow}\beta_{\nwarrow}}\end{aligned}$$

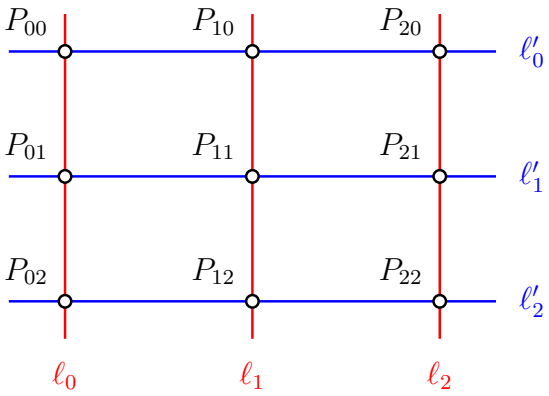
The proof follows a similar outline to that of the forward difference formulas from section 7.2. Namely, we first bootstrap from $d_{\mathcal{O}}$ to d_T for $T \in E[3]\backslash\{\mathcal{O}\}$, and then we take

linear combinations of numerators and denominators. The bootstrapping process is quite pretty in fact; it is simply a matter of combining the formulas for ∂ over various naturally arising nine point diagrams. The only finicky bit is to keep track of various factors that pop up. But the payoff is then all the more; the various factors all cancel out, leaving the elegant formulas from theorem 7.3.3.

7.3.2 Proof of Theorem 7.3.3

To prove theorem 7.3.3, we start by proving that $d_{\mathcal{O}}$ can be substituted with d_T for $T \in E[3]\backslash\{\mathcal{O}\}$. To achieve this, we start with theorem 6.5.1, which says that for this nine point diagram:

$\mathcal{N}$:



we have:

$$e_0(-\ell_0;\ell_1) = \partial(\ell_0,\ell_1,\ell_2)\partial(\ell_0,-\ell_1,-\ell_{\nwarrow})\partial(\ell_0,-\ell_1,\ell_{\nearrow})$$

Now notice that if we add T to ℓ_0 and subtract it from ℓ_1, then the factor $\partial(\ell_0,-\ell_1,-\ell_{\nwarrow})$ transforms predictably, since each argument is shifted by T. Similarly, we have a simple transformation rule for $\partial(\ell_0,-\ell_1,\ell_{\nearrow})$ and $e_0(\ell_0;-\ell_1)$. Thus to deduce the transformation rule for $\partial(\ell_0,\ell_1,\ell_2)$, we simply need to keep track of precise transformation rules for the other factors.

The first step is to establish the transformation formula for ∂ under T-shifts:

Lemma 7.3.4. *(i) The orientation $\partial(\mathcal{N})$ of a nine point diagram $\mathcal{N} = \mathfrak{N}(\ell_0,\ell_1,\ell_2)$ transforms as follows under T-shifting:*

$$\partial(\ell_0^{\boxplus T},\ell_1^{\boxplus T},\ell_2^{\boxplus T}) = \frac{(2y_T)^3}{\mathcal{N}(-T)}\partial(\ell_0,\ell_1,\ell_2)$$

(ii) The expression $e_0(\ell_0;\ell_1) = (\alpha_0-\alpha_1)^3 e_0(\ell_0\cap\ell_1)$ *transforms as follows under* T*-shifting:*

$$e_0\left(\ell_0^{\boxplus T};\ell_1^{\boxplus T}\right) = \left(\frac{2y_T}{\ell_0(-T)}\right)^3 \left(\frac{2y_T}{\ell_1(-T)}\right)^3 e_0\left(\ell_0;\ell_1\right)$$

Proof. (i) Recall theorem B.3.1:

$$[\ell^{\boxplus T}] = \frac{-2y_T}{y_T + m_\ell x_T + b_\ell} M_{-T}^{\intercal}[\ell] = \frac{2y_T}{\ell(-T)} M_{-T}^{\intercal}[\ell]$$

now we calculate the following (see section B.3):

$$\begin{aligned}
\partial(\ell_0^{\boxplus T},\ell_1^{\boxplus T},\ell_2^{\boxplus T}) =& \frac{d_{\mathcal{O}}\left(\ell_0^{\boxplus T},\ell_1^{\boxplus T},\ell_2^{\boxplus T}\right)}{d_{\mathcal{O}}\left(\ell_{\mathcal{O}},\ell_{\nwarrow},\ell_{\nearrow}\right)} = \frac{(2y_T)^3\det(M_{-T}^{\intercal}[\ell_0],M_{-T}^{\intercal}[\ell_1],M_{-T}^{\intercal}[\ell_2])}{\ell_0(-T)\ell_1(-T)\ell_2(-T)d_{\mathcal{O}}\left(\ell_{\mathcal{O}},\ell_{\nwarrow},\ell_{\nearrow}\right)} \\
=& \frac{(2y_T)^3\det([\ell_0],[\ell_1],[\ell_2])}{\mathcal{N}(-T)d_{\mathcal{O}}\left(\ell_{\mathcal{O}},\ell_{\nwarrow},\ell_{\nearrow}\right)} = \frac{(2y_T)^3 d_{\mathcal{O}}(\ell_0,\ell_1,\ell_2)}{\mathcal{N}(-T)d_{\mathcal{O}}\left(\ell_{\mathcal{O}},\ell_{\nwarrow},\ell_{\nearrow}\right)} \\
=& \frac{(2y_T)^3}{\mathcal{N}(-T)}\partial(\ell_0,\ell_1,\ell_2).
\end{aligned}$$

(ii) By a direct calculation,

$$\begin{aligned}
\alpha\left(\ell_0^{\boxplus T}\right) - \alpha\left(\ell_1^{\boxplus T}\right) =& -2y_T\frac{(\alpha_0\beta_1-\alpha_1\beta_0)-m_T(\beta_0-\beta_1)+(\alpha_0-\alpha_1)b_T}{(y_T+\alpha_0x_T+\beta_0)(y_T+\alpha_1+\beta_1)} \\
=& \frac{-2y_T\ell_{-T}(\ell_0\cap\ell_1)}{\ell_0(-T)\ell_1(-T)}(\alpha_0-\alpha_1)
\end{aligned}$$

and then we have a straightforward computation, where we use theorem 7.2.8:

$$\begin{aligned}
\frac{e_0\left(\ell_0^{\boxplus T};\ell_1^{\boxplus T}\right)}{e_0\left(\ell_0;\ell_1\right)} &= \left(\frac{\alpha\left(\ell_0^{\boxplus T}\right)-\alpha\left(\ell_1^{\boxplus T}\right)}{\alpha_0-\alpha_1}\right)^3 \frac{e_0\left(\ell_0^{\boxplus T}\cap\ell_1^{\boxplus T}\right)}{e_0\left(\ell_0\cap\ell_1\right)} \\
&= \left(\frac{-2y_T\ell_{-T}(\ell_0\cap\ell_1)}{\ell_0(-T)\ell_1(-T)}\right)^3 \frac{e_0\left((\ell_0\cap\ell_1)+T\right)}{e_0\left(\ell_0\cap\ell_1\right)} \\
&= \left(\frac{-2y_T\ell_{-T}(\ell_0\cap\ell_1)}{\ell_0(-T)\ell_1(-T)}\right)^3 \left(\frac{-2y_T}{\ell_{-T}(\ell_0\cap\ell_1)}\right)^3 \\
&= \left(\frac{2y_T}{\ell_0(-T)}\right)^3 \left(\frac{2y_T}{\ell_1(-T)}\right)^3
\end{aligned}$$

□

In theorem 7.3.3, $d_{\mathcal{O}}$ can be substituted for any T-determinantal form, for $T \in E[3]$:

Lemma 7.3.5. *For any $T \in E[3]$,*

$$\partial(\ell_0, \ell_1, \ell_2) = -\frac{d_T(\ell_0, \ell_1, \ell_2)}{d_T(\ell_\mathcal{O}, \ell_\nearrow, \ell_\nwarrow)}$$

Proof. Consider the nine point diagrams $\mathcal{N} = \mathfrak{N}(\ell_0, \ell_1, \ell_2)$ and $\mathcal{N}' = \mathfrak{N}(\ell_0^{\boxplus T}, \ell_1^{\boxminus T}, \ell_2)$. Recall from lemma 5.6.4 that $\mathfrak{l}_\nwarrow = \omega^2\mathfrak{l}_0 - \omega\mathfrak{l}_1$ and $\mathfrak{l}_\nearrow = \omega^2\mathfrak{l}_1 - \omega\mathfrak{l}_0$, so

$$\begin{aligned}\mathfrak{l}_\nwarrow(\mathcal{N}') =& \omega^2(\ell_0 + \ell_T) - \omega(\ell_1 - \ell_T) = \left(\omega^2\ell_0 - \omega\ell_1\right) - \ell_T = \ell_\nwarrow^{\boxminus T}\\ \mathfrak{l}_\nearrow(\mathcal{N}') =& \omega^2(\ell_1 - \ell_T) - \omega(\ell_0 + \ell_T) = \ell_\nearrow^{\boxplus T}\end{aligned}$$

where $\ell_\nwarrow = \mathfrak{l}_\nwarrow(\mathcal{N})$ and $\ell_\nearrow = \mathfrak{l}_\nearrow(\mathcal{N})$. Now we use theorem 6.5.1 to both $\mathcal{N}$ and $\mathcal{N}'$ to obtain:

$$\frac{e_0\left((\boxminus\ell_0)^{\boxminus T}; \ell_1^{\boxminus T}\right)}{e_0\left(\boxminus\ell_0; \ell_1\right)} = \frac{\partial\left(\ell_0^{\boxplus T}, \ell_1^{\boxminus T}, \ell_2\right)}{\partial\left(\ell_0, \ell_1, \ell_2\right)} \cdot \frac{\partial\left(\ell_0^{\boxplus T}, (\boxminus\ell_1)^{\boxplus T}, (\boxminus\ell_\nwarrow)^{\boxplus T}\right)}{\partial\left(\ell_0, \boxminus\ell_1, \boxminus\ell_\nwarrow\right)} \cdot \frac{\partial\left(\ell_0^{\boxplus T}, (\boxminus\ell_1)^{\boxplus T}, \ell_\nearrow^{\boxplus T}\right)}{\partial\left(\ell_0, \boxminus\ell_1, \ell_\nearrow\right)}$$

Next we isolate the first factor on the right hand side; the resulting expression is then simplified using lemma 7.3.4 and the identity $\boxminus\ell(P) = -\ell(-P)$:

$$\begin{aligned}\frac{\partial\left(\ell_0^{\boxplus T}, \ell_1^{\boxminus T}, \ell_2\right)}{\partial\left(\ell_0, \ell_1, \ell_2\right)} &= \frac{e_0\left((\boxminus\ell_0)^{\boxminus T}; \ell_1^{\boxminus T}\right)}{e_0\left(\boxminus\ell_0; \ell_1\right)} \cdot \frac{\partial\left(\ell_0, \boxminus\ell_1, \boxminus\ell_\nwarrow\right)}{\partial\left(\ell_0^{\boxplus T}, (\boxminus\ell_1)^{\boxplus T}, (\boxminus\ell_\nwarrow)^{\boxplus T}\right)} \cdot \frac{\partial\left(\ell_0, \boxminus\ell_1, \ell_\nearrow\right)}{\partial\left(\ell_0^{\boxplus T}, (\boxminus\ell_1)^{\boxplus T}, \ell_\nearrow^{\boxplus T}\right)}\\ &= \left(\frac{-2y_T}{\boxminus\ell_0(T)}\right)^3 \left(\frac{-2y_T}{\ell_1(T)}\right)^3 \cdot \frac{\ell_0(-T)(\boxminus\ell_1)(-T)(\boxminus\ell_\nwarrow)(-T)}{(2y_T)^3} \cdot \frac{\ell_0(-T)(\boxminus\ell_1)(-T)\ell_\nearrow(-T)}{(2y_T)^3}\\ &= \left(\frac{-2y_T}{-\ell_0(-T)}\right)^3 \left(\frac{-2y_T}{\ell_1(T)}\right)^3 \cdot \frac{\ell_0(-T)(-\ell_1(T))(-\ell_\nwarrow(T))}{(2y_T)^3} \cdot \frac{\ell_0(-T)(-\ell_1(T))\ell_\nearrow(-T)}{(2y_T)^3}\\ &= \frac{\ell_\nwarrow(T)\ell_\nearrow(-T)}{\ell_0(-T)\ell_1(T)}\end{aligned}$$

Now we use the determinantal formula from theorem 6.4.4, in the form of equation (6.15):

$$\begin{aligned}\partial\left(\ell_0, \ell_1, \ell_2\right) =& \frac{\ell_0(-T)\ell_1(T)}{\ell_\nwarrow(T)\ell_\nearrow(-T)} \cdot \partial\left(\ell_0^{\boxplus T}, \ell_1^{\boxminus T}, \ell_2\right)\\ =& \frac{\ell_0(-T)\ell_1(T)}{\ell_\nwarrow(T)\ell_\nearrow(-T)} \cdot \frac{d_\mathcal{O}\left(\ell_0^{\boxplus T}, \ell_1^{\boxminus T}, \ell_2\right)}{d_\mathcal{O}\left(\ell_\mathcal{O}, \ell_\nwarrow^{\boxminus T}, \ell_\nearrow^{\boxplus T}\right)}\\ =& \frac{\det\left(\frac{\ell_0(-T)}{2y_T}[\ell_0^{\boxplus T}], \frac{\ell_1(T)}{-2y_T}[\ell_1^{\boxminus T}], [\ell_2]\right)}{\det\left([\ell_\mathcal{O}], \frac{\ell_\nwarrow(T)}{-2y_T}[\ell_\nwarrow^{\boxminus T}], \frac{\ell_\nearrow(-T)}{2y_T}[\ell_\nearrow^{\boxplus T}]\right)}\\ =& \frac{\det\left(M_{-T}^\intercal[\ell_0], M_T^\intercal[\ell_1], [\ell_2]\right)}{\det\left([\ell_\mathcal{O}], M_T^\intercal[\ell_\nwarrow], M_{-T}^\intercal[\ell_\nearrow]\right)}\\ =& \frac{d_T(\ell_0, \ell_1, \ell_2)}{d_{-T}(\ell_\mathcal{O}, \ell_\nwarrow, \ell_\nearrow)} = -\frac{d_T(\ell_0, \ell_1, \ell_2)}{d_T(\ell_\mathcal{O}, \ell_\nearrow, \ell_\nwarrow)}\end{aligned}$$

□

Now it is a simple matter to prove theorem 7.3.3:

Proof. By lemma 7.3.5, we have that

$$\partial(\ell_0, \ell_1, \ell_2) d_T(\ell_{\mathcal{O}}, \ell_{\nearrow}, \ell_{\nwarrow}) + d_T(\ell_0, \ell_1, \ell_2) = 0$$

Since this is linear in the d_T, we can take linear combinations among those to obtain

$$\partial(\ell_0, \ell_1, \ell_2) f_i(\ell_{\mathcal{O}}, \ell_{\nearrow}, \ell_{\nwarrow}) + f_i(\ell_0, \ell_1, \ell_2) = 0$$

for $i \in \{0, 1\}$, recalling definition 7.3.2. □

Chapter 8

Conclusion and Future Work

We conclude with a discussion of past, present and future research. Our progress in this project has gone in cycles, where geometric intuition leads to algebraic results, and then algebraic experimentation leads to new geometric insights. For example, the notion of a nine point diagram arose from a need to explain certain algebraic phenomena in line addition. Then by studying the geometry of diagrams, we were able to better contextualize the trilinear forms that we had found, in terms of three torsion.

We mention some potential future applications, mostly in various areas related to elliptic curve scalar multiplication. Although we have not made significant progress, we hope to find uses for our operation that lead to new cryptographic capabilities. For example, we have considered trapdoor systems on elliptic curves in composite modulus. We even toyed with the idea of using this operation with binary pairings in composite modulus.

8.1 Geometric Interpretations

In this section, we outline some geometric observations that we are studying. First we mention the family of curves mentioned in section 7.2.3, given by the following equation for a paramater k:

$$-a^2 + 9bx + 3ax^2 + 3xy^2 - k(b + ax + x^3 - y^2) = 0$$

Note that the above is a cubic form from chapter 7. These curves all share the same three torsion, as well as the action of the three torsion. There are some interesting connections between various curves in this family. For example, we can partially explain the formula (A.2) in geometric terms. But despite much effort, these geometric explanations are most naturally expressed in terms of another curve in the family, where the line addition is "degenerate" in a sense.

There is also a dual family of elliptic curves, defined in terms of the dual cubic forms. We can use these to give a better geometric interpretation for theorem 7.3.3, which also better explains the transformation of a nine point diagram under $\ell_0, \ell_1, \ell_2 \mapsto \ell_0^{\boxplus T}, \ell_1^{\boxminus T}, \ell_2$. Unfortunately, it involves many concepts not included in the current version of this thesis, and we are currently working on a clean presentation. In a nutshell, we consider a new type of cyclic line diagram ℓ, where we consider the points $\mathfrak{p}_i$ to be in the group E, but where the identity element iT is different for each i. By cyclically shifting the line, we get 3 different unlabeled lines; but these lines can all be considered as part of the same "dual" elliptic curve, and together can be encoded via a 3-isogeny. This is the context that most cleanly explains the aforementioned $E[3]$-transformations.

8.2 Elliptic Curve Scalar Multiplication

The most natural application is for point multiplication on an elliptic curve. A direct approach would be to start with $P \in E$, then select lines $u, v \in \mathcal{L}_3(E)$ which both have P as a point. Then we would get $k \boxdot u \cap k \boxdot v = kP$ (with a few unlikely exceptions.) Of course, this operation is significantly slower than the standard point multiplication operation, since it requires two line multiplications, and each of those is more expensive than simply multiplying P by k.

To take a page out of the x-only operation, we could also obtain kP with a single line multiplication. This trick is analogous to formula 13.7 in [3]. Suppose that u has points $P, Q, -P-Q$. Then we can use our recursive line multiplication algorithms to compute $k \boxdot u$ and $(k-1) \boxdot u$, and then the following subroutine allow us to recover kP:

1. From the coordinates of $(k-1) \boxdot u$ and P, we compute a function f which vanishes at $R + P$ for each $R \in (k-1) \boxdot u$.

2. Simultaneously solve the three equations

$$\begin{aligned} f(x,y) &= 0 \\ y &= m_{k \boxdot u} x + b_{k \boxdot u} \\ y^2 &= b + ax + x^3 \end{aligned}$$

The solution is then the coordinates of kP. We note that the recovery of kP from $k \cdot u$ and $(k-1) \cdot u$ takes a fixed number of field arithmetic operations; this subroutine could also be encoded as a single explicit formula.

Now we make an important observation; once the above algorithm to compute kP is completed, we can repeat the final subroutine with $k \boxdot u$, $(k-1) \boxdot u$ and Q to compute kQ, at little extra cost. Hence we can compute kP and kQ from P and Q using only one

recursion. We hope to improve this operation to a point where it is competitive with other point multiplication algorithms for certain applications.

8.2.1 Point Multiplication in Algebraic Extension

Another setting which we consider is point multiplication in an algebraic extension. This is analogous to the algorithm that we proposed to modify Cipolla's square root finding algorithm in section 4.5. There we performed an exponentiation in an extension field using line multiplication.

As a first example, we use line multiplication to perform a point multiplication in a quadratic extension. Suppose that $P \in E(\mathbb{F}_{q^2}) \backslash E(\mathbb{F}_q)$ for an elliptic curve E over $\mathbb{F}_q$. Then computing kP normally involves working with $\mathbb{F}_{q^2}$ arithmetic, which is expensive. The line multiplication operation could be used in its place as follows:

1. Let $\overline{P} = (x(P)^q, y(P)^q)$ denote the conjugate point.
2. Let $\ell \in \mathcal{L}_3(E)$ be the line with points $P, \overline{P}, -P - \overline{P}$.
3. Compute $(k-1) \boxdot \ell, k \boxdot \ell$
4. Solve for $R = kP$ such that $R \in k \boxdot \ell$ and $R - P \in (k-1) \boxdot \ell$.

This only involves base field arithmetic. Of course this improvement needs to be weighed against the extra cost of the line multiplication operation.

Another example works in a cubic extension. Suppose that $P \in E(\mathbb{F}_{q^3}) \backslash E(\mathbb{F}_q)$ for an elliptic curve E over $\mathbb{F}_q$. Suppose that the three conjugates of P are P_0, P_1, P_2 over $\mathbb{F}_q$. These three points typically will not sum to $\mathcal{O}$, but a little trick will help us. We construct the line ℓ with points $(3P_i - P_0 - P_1 - P_2)$ for $i = 0, 1, 2$. Then again we compute $\lfloor k/3 - 1 \rfloor \boxdot \ell, \lfloor k/3 \rfloor \boxdot \ell$. Then we similarly use a recovery algorithm to compute $3\lfloor k/3 \rfloor P$, and at most one more doubling and/or addition is require to compute kP.

References

[1] Daniel J. Bernstein and Tanja Lange. Analysis and optimization of elliptic-curve single-scalar multiplication. Cryptology ePrint Archive, Report 2007/455, 2007. http://eprint.iacr.org/2007/455.

[2] Daniel R. L. Brown. Alternative cubics' rules with an algebraic appeal. *IACR Cryptology ePrint Archive*, 2015:544, 2015.

[3] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren. *Handbook of Elliptic and Hyperelliptic Curve Cryptography, Second Edition*. Chapman & Hall/CRC, 2nd edition, 2012.

[4] N. Demytko. A new elliptic curve based analogue of RSA. In Tor Helleseth, editor, *Advances in Cryptology EUROCRYPT*, volume 765 of *Lecture Notes in Computer Science*, pages 40–49. Springer Berlin Heidelberg, 1994.

[5] Thomas Little Heath and Leonhard Euler. *Diophantus of Alexandria : A study in the history of Greek algebra / Sir Thomas L. Heath*. C.V. Clay London, 1885.

[6] H. W. Lenstra. Factoring integers with elliptic curves. *Annals of Mathematics*, 126(3):649–673, 1987.

[7] Peter L. Montgomery. Speeding the Pollard and Elliptic Curve Methods of Factorization. *Mathematics of Computation*, 48(177):243–264, 1987.

[8] J. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, 2009.

Appendices

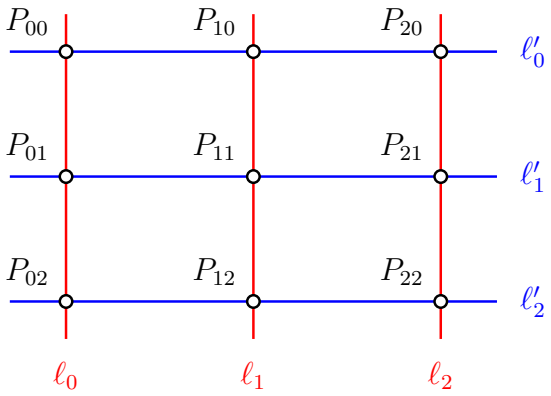
Appendix A

Table of Formulas

A.1 Explicit Line Sum

Here we derive an explicit formula for ℓ_2 in terms of ℓ_0, ℓ_1:

$\mathcal{N}$:



The following theorem uses the notation and results of section 6.3.2:

Theorem A.1.1. *The following gives an expression for the slope of ℓ_2 in terms of ℓ_0, ℓ_1:*

$$\begin{aligned}&\alpha_2 - \alpha_0\\ =&\frac{(x_{10}-x_{01})(x_{10}-x_{02})\ell_0(-P_{11})\ell_0(-P_{12}) - (x_{11}-x_{02})(x_{12}-x_{01})\ell_0(-P_{10})\ell_1(-P_{00})}{e_0(-\ell_0;\ell_1)}\end{aligned}$$

Proof. By substituting $y_{00} = \alpha_0 x_{00} + \beta_0$, we get the following expression:

$$\alpha'_0 - \alpha_0 = \frac{y_{10}-y_{00}}{x_{10}-x_{00}} - \alpha_0 = \frac{y_{10}-\alpha_0 x_{10}-\beta_0}{x_{10}-x_{00}} = \frac{\ell_0(P_{10})}{x_{10}-x_{00}}$$

We use lemma 6.3.7 to partially rationalize this, and afterwards we apply the symmetry ς:

$$\begin{aligned}\alpha_0' - \alpha_0 =& \frac{\ell_0(P_{10})}{x_{10} - x_{00}} = \frac{(x_{10} - x_{01})(x_{10} - x_{02})}{-\ell_0(-P_{10})} \\ \alpha_0' - \alpha_1 =& \frac{(x_{00} - x_{11})(x_{00} - x_{12})}{-\ell_1(-P_{00})} = \frac{(x_{11} - x_{00})(x_{12} - x_{00})}{-\ell_1(-P_{00})}\end{aligned}$$

Then we remark that the factors on the left appear in theorem 6.3.3, and those on the right appear in theorem 6.3.6:

$$\begin{aligned}\partial(\ell_0, \ell_1, \ell_2) =& (\alpha_0' - \alpha_0)(\alpha_0' - \alpha_1)(\alpha_0' - \alpha_2) \\ =& \frac{(x_{10} - x_{01})(x_{10} - x_{02})(x_{11} - x_{00})(x_{11} - x_{02})(x_{12} - x_{00})(x_{12} - x_{01})}{e_0(-\ell_0; \ell_1)}\end{aligned}$$

and thus we isolate the following expression for $\alpha_0' - \alpha_2$ in terms of ℓ_0, ℓ_1:

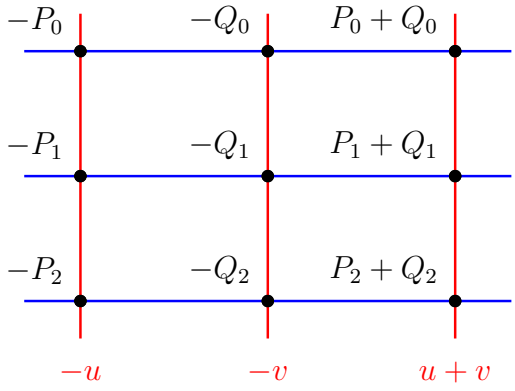
$$\alpha_0' - \alpha_2 = \frac{(x_{11} - x_{02})(x_{12} - x_{01})\ell_0(-P_{10})\ell_1(-P_{00})}{e_0(-\ell_0; \ell_1)}$$

Then we use lemma 6.3.7 again to fully rationalize $\alpha_0' - \alpha_0$:

$$\alpha_0' - \alpha_0 = \frac{(x_{10} - x_{01})(x_{10} - x_{02})}{-\ell_0(-P_{10})} = \frac{(x_{10} - x_{01})(x_{10} - x_{02})\ell_0(-P_{11})\ell_0(-P_{12})}{e_0(-\ell_0; \ell_1)}$$

Finally we get the desired result by taking the difference $(\alpha_0' - \alpha_0) - (\alpha_0' - \alpha_2)$. □

By taking $\ell_0 = -u, \ell_1 = -v$, this can be used to derive a formula for $\ell_2 = u + v$. This is useful for verifying polynomial equations on a computer algebra system. Explicitly:



and we apply our lemma to obtain the following formula for m_{u+v}:

Theorem A.1.2.

$$\begin{aligned}& m_{u+v} + m_u \\ =& \frac{(x_{Q_0} - x_{P_1})(x_{Q_0} - x_{P_2})u(-Q_1)u(-Q_2) - (x_{Q_1} - x_{P_2})(x_{Q_2} - x_{P_1})u(-Q_0)v(-P_0)}{e_0(u; -v)}\end{aligned}$$

A.2 Doubling Formula

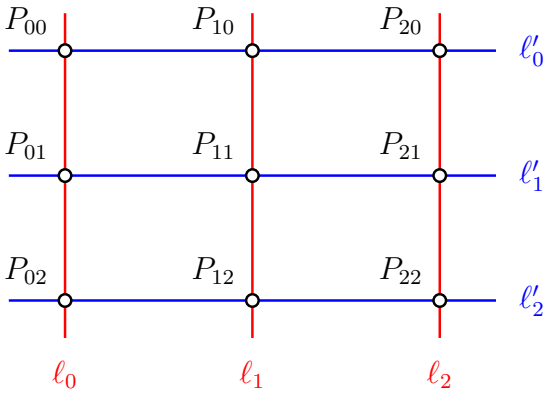
Lemma A.2.1. *The following gives the line doubling formula (see theorem 3.8.3):*

$$\begin{aligned} m_{2\boxdot\ell} =& \frac{a^2m_\ell^2 + 9bm_\ell b_\ell - 3ab_\ell^2 + m_\ell(bm_\ell^3 - am_\ell^2 b_\ell - b_\ell^3)}{2(bm_\ell^3 - am_\ell^2 b_\ell - b_\ell^3)} \\ b_{2\boxdot\ell} =& \frac{4a^3+27b^2+6abm_\ell^2-8a^2m_\ell b_\ell-18bb_\ell^2-a^2m_\ell^4-8bm_\ell^3b_\ell+2am_\ell^2b_\ell^2-b_\ell^4}{8(bm_\ell^3-am_\ell^2b_\ell-b_\ell^3)} \end{aligned} \tag{A.1}$$

A.3 Nine Point Diagram

Now we collect formulas related to the following nine point diagram:

$\mathcal{N}$:



- If $\mathcal{O} \notin P_{ij}$, then:

$$\mathcal{N}(x,y) = -\mathcal{N}_9 - \mathcal{N}_7 x + \mathcal{N}_6 y - \mathcal{N}_5 x^2 + \mathcal{N}_4 xy - \mathcal{N}_3 y^2 + \mathcal{N}_2 x^2 y - \mathcal{N}_1 xy^2 + y^3$$

  Where $\mathcal{N}_i$ represents the following:

$$\begin{aligned} \mathcal{N}_9 =& \beta_0\beta_1\beta_2 - b\cdot\alpha_0\alpha_1\alpha_2 \\ \mathcal{N}_7 =& \alpha_0\beta_1\beta_2 + \alpha_1\beta_0\beta_2 + \alpha_2\beta_0\beta_1 - a\cdot\alpha_0\alpha_1\alpha_2 \\ \mathcal{N}_5 =& \alpha_0\alpha_1\beta_2 + \alpha_0\alpha_2\beta_1 + \alpha_1\alpha_2\beta_0 \\ \mathcal{N}_4 =& \alpha_0(\beta_1+\beta_2) + \alpha_1(\beta_0+\beta_2) + \alpha_2(\beta_0+\beta_1) \\ \mathcal{N}_3 =& \alpha_0\alpha_1\alpha_2 + \beta_0 + \beta_1 + \beta_2 \\ \mathcal{N}_2 =& \alpha_0\alpha_1 + \alpha_1\alpha_2 + \alpha_2 \\ \mathcal{N}_1 =& \alpha_0 + \alpha_1 + \alpha_2 \end{aligned}$$

- The lines of $\mathcal{N}$ satisfy the following, where $\partial(\mathcal{N})$ is the diagram orientation (see section 6.3):

$$\begin{aligned}
\alpha_0 + \alpha_1 + \alpha_2 &= \alpha_1' + \alpha_0' + \alpha_2' \\
\alpha_0\alpha_1 + \alpha_0\alpha_2 + \alpha_1\alpha_2 &= \alpha_1'\alpha_0' + \alpha_1'\alpha_2' + \alpha_0'\alpha_2' \\
\alpha_0\alpha_1\alpha_2 + \beta_0 + \beta_1 + \beta_2 &= \alpha_1'\alpha_0'\alpha_2' + \beta_1' + \beta_0' + \beta_2' \\
\alpha_0(\beta_1 + \beta_2) + \alpha_1(\beta_0 + \beta_2) + \alpha_2(\beta_0 + \beta_1) & \\
= \alpha_1'(\beta_0' + \beta_2') + \alpha_2'(\beta_1' + \beta_2') + \alpha_2'(\beta_1' + \beta_0') & \\
\alpha_0\alpha_1\beta_2 + \alpha_0\alpha_2\beta_1 + \alpha_1\alpha_2\beta_0 &= \alpha_1'\alpha_0'\beta_2' + \alpha_1'\alpha_2'\beta_0' + \alpha_0'\alpha_2'\beta_1' \\
\beta_0\beta_1 + \beta_0\beta_2 + \beta_1\beta_2 &= \beta_1'\beta_0' + \beta_1'\beta_2' + \beta_0'\beta_2' \\
a \cdot \alpha_0\alpha_1\alpha_2 - (\alpha_0\beta_1\beta_2 + \alpha_1\beta_0\beta_2 + \alpha_2\beta_0\beta_1) & \\
= a \cdot \alpha_1'\alpha_0'\alpha_2' - (\alpha_1'\beta_0'\beta_2' + \alpha_0'\beta_1'\beta_2' + \alpha_2'\beta_1'\beta_0') & \\
b \cdot \alpha_0\alpha_1\alpha_2 - \beta_0\beta_1\beta_2 &= b \cdot \alpha_1'\alpha_0'\alpha_2' - \beta_1'\beta_0'\beta_2' \\
\partial(\mathcal{N}) &= \beta_0 + \beta_1 + \beta_2 - \beta_0' - \beta_1' - \beta_2' \\
\partial(\mathcal{N}) &= \alpha_0'\alpha_1'\alpha_2' - \alpha_0\alpha_1\alpha_2 \\
b\ \partial(\mathcal{N}) &= \beta_0'\beta_1'\beta_2' - \beta_0\beta_1\beta_2 \\
a\ \partial(\mathcal{N}) &= \alpha_0'\beta_0'\beta_1' + \alpha_1'\beta_0'\beta_2' + \alpha_2'\beta_0'\beta_1' - \alpha_0\beta_0\beta_1 - \alpha_1\beta_0\beta_2 - \alpha_2\beta_0\beta_1
\end{aligned}$$

- The diagram orientation has the following expressions:

$$\begin{aligned}
\partial(\mathcal{N}) &= (\alpha_0' - \alpha_0)(\alpha_0' - \alpha_1)(\alpha_0' - \alpha_2) \\
&= (\alpha_1' - \alpha_0)(\alpha_1' - \alpha_1)(\alpha_1' - \alpha_2) \\
&= (\alpha_2' - \alpha_0)(\alpha_2' - \alpha_1)(\alpha_2' - \alpha_2) \\
&= (\alpha_0' - \alpha_0)(\alpha_1' - \alpha_0)(\alpha_2' - \alpha_0) \\
&= (\alpha_0' - \alpha_1)(\alpha_1' - \alpha_1)(\alpha_2' - \alpha_1) \\
&= (\alpha_0' - \alpha_2)(\alpha_1' - \alpha_2)(\alpha_2' - \alpha_2)
\end{aligned}$$

- $$\partial(\mathcal{N}) = \frac{(a - \mathcal{N}_4)\mathcal{N}_1\mathcal{N}_2 - 9\mathcal{N}_7 + 3\mathcal{N}_3\mathcal{N}_4 - 3\mathcal{N}_1\mathcal{N}_6 + 2\mathcal{N}_2\mathcal{N}_5 + 2\mathcal{N}_2^2\mathcal{N}_3}{9a + 3\mathcal{N}_4 + \mathcal{N}_2^2} - 2\alpha_0\alpha_1\alpha_2 \tag{A.2}$$

Lemma A.3.1.

$$\begin{aligned}
\mathfrak{l}_{\nearrow} &= \omega\mathfrak{l}_2 - \mathfrak{l}_1 = \mathfrak{l}_0 - \omega^2\mathfrak{l}_2 = \omega^2\mathfrak{l}_1 - \omega\mathfrak{l}_0 \\
\mathfrak{l}_{\nwarrow} &= \mathfrak{l}_1 - \omega^2\mathfrak{l}_2 = \omega\mathfrak{l}_2 - \mathfrak{l}_0 = \omega^2\mathfrak{l}_0 - \omega\mathfrak{l}_1 \\
\mathfrak{l}_{\swarrow} &= \rho\mathfrak{l}_1 - \rho\omega\mathfrak{l}_2 = \rho\omega^2\mathfrak{l}_2 - \rho\mathfrak{l}_0 = \rho\omega\mathfrak{l}_0 - \rho\omega^2\mathfrak{l}_1 \\
\mathfrak{l}_{\searrow} &= \rho\mathfrak{l}_1 - \rho\omega\mathfrak{l}_2 = \rho\omega^2\mathfrak{l}_2 - \rho\mathfrak{l}_0 = \rho\omega\mathfrak{l}_0 - \rho\omega^2\mathfrak{l}_1
\end{aligned}$$

A.4 Nine Point Diagram Toolbox

For labeled lines $u, v \in \mathcal{L}_3^\circ(E)$:

- From equation 6.18 (and generalized in chapter 7):

$$\begin{aligned}
\partial(-u,-v,u+v) &= \frac{d_{\mathcal{O}}(-u,-v,u+v)}{d_{\mathcal{O}}(\ell_{\mathcal{O}}, v-\omega u, u-\omega v)} \\
\partial(-u,-v,u+v) &= \frac{f_0(-u,-v,u+v)}{f_0(\ell_{\mathcal{O}}, v-\omega u, u-\omega v)} \\
\partial(-u,-v,u+v) &= \frac{f_1(-u,-v,u+v)}{f_1(\ell_{\mathcal{O}}, v-\omega u, u-\omega v)} \\
\partial(-u,v,u-v) &= \frac{d_{\mathcal{O}}(-u,v,u-v)}{d_{\mathcal{O}}(\ell_{\mathcal{O}}, -(u+\omega^2 v), u+\omega v)} \\
\partial(-u,v,u-v) &= \frac{f_0(-u,v,u-v)}{f_0(\ell_{\mathcal{O}}, -(u+\omega^2 v), u+\omega v)} \\
\partial(-u,v,u-v) &= \frac{f_1(-u,v,u-v)}{f_1(\ell_{\mathcal{O}}, -(u+\omega^2 v), u+\omega v)}
\end{aligned}$$

- From equation 6.16

$$\begin{aligned}
\partial(u+\omega v, u+\omega^2 v, u+v) &= \frac{d_{\mathcal{O}}(u+\omega v, u+\omega^2 v, u+v)}{m_{\Delta u} - m_{\Delta v}} \\
\partial(u+\omega v, u+\omega^2 v, u+v) &= \frac{f_0(u+\omega v, u+\omega^2 v, u+v)}{f_0(\ell_{\mathcal{O}}, \Delta u, \Delta v)} \\
\partial(u+\omega v, u+\omega^2 v, u+v) &= \frac{f_1(u+\omega v, u+\omega^2 v, u+v)}{f_0(\ell_{\mathcal{O}}, \Delta u, \Delta v)}
\end{aligned}$$

- From equation 6.19

$$\partial(u+\omega v, u+\omega^2 v, u+v) = \frac{-\delta_u \cdot \delta_v}{e_0(u;-v)}$$

- From theorem 6.5.1

$$\begin{aligned}
\frac{e_0(u;v)}{e_0(u;-v)} &= \frac{\partial(-u,-v,u+v)}{\partial(-u,v,u-v)} \\
e_0(u;v) &= \partial(-u,-v,u+\omega v)\partial(-u,-v,u+\omega^2 v)\partial(-u,v,u-v) \\
e_0(u;-v) &= \partial(-u,v,u-\omega v)\partial(-u,v,u-\omega^2 v)\partial(-u,-v,u+v)
\end{aligned}$$

A.5 Line Sum Function

Here we give explicit formulas for the line sum function. This includes the coefficients that were omitted from theorem 3.7.3, as well as special cases.

Suppose that $u, v \in \mathcal{L}_3(E)$ have respective points P_0, P_1, P_2 and Q_0, Q_1, Q_2, with $u(x,y) = y - m_u x - b_u$ and $v(x,y) = y - m_v x - b_v$. Then we have the following equality as functions of $R \in E$, for some non-zero normalization constant c:

$$(u \boxplus v)(x,y) = c^{-1}\left(-\gamma_9^* - \gamma_7^* x + \gamma_6^* y - \gamma_5^* x^2 + \gamma_4^* xy - \gamma_3^* y^2 + \gamma_2^* x^2 y - \gamma_1^* x y^2 + \gamma_0^* y^3\right) \tag{A.3}$$

where

$$\begin{aligned}
\gamma_0^* =& b(m_u+m_v)^3 - a(m_u+m_v)^2(b_u+b_v) - (b_u+b_v)^3 - (m_u+m_v)(m_u b_v - b_u m_v)^2 \\
\gamma_1^* =& (a^2 - 3bm_u m_v + 2a(m_u b_v + m_v b_u))(m_u+m_v)^2 - 3(a + m_u b_v + m_v b_u)(b_u+b_v)^2 \\
&+ (9b - a m_u m_v + 9 b_u b_v)(m_u+m_v)(b_u+b_v) - m_u m_v (b_v m_u - b_u m_v)^2 \\
\gamma_2^* =& -a^2(m_u+m_v)^3 - 9b(m_u+m_v)^2(b_u+b_v) + 3a(m_u+m_v)(b_u+b_v)^2 \\
&- 3(b_u+b_v)(m_u b_v - b_u m_v)^2 \\
\gamma_3^* =& 4a^3 + 4a^2 b_v m_u + 4a^2 b_u m_v - 8a^2 b_u m_u - 8a^2 b_v m_v + a^2 m_u m_v^3 + a^2 m_u^2 m_v^2 \\
&+ a^2 m_u^3 m_v - 2ab_u m_u^2 m_v^3 + 3ab_v^2 m_u^2 - 7ab_u b_v m_u^2 - 2ab_v m_u^3 m_v^2 + 3ab_u^2 m_v^2 \\
&- 7ab_u b_v m_v^2 + ab_u^2 m_u m_v + ab_v^2 m_u m_v - 6abm_u m_v + 12ab_u b_v m_u m_v + 6abm_u^2 \\
&+ 6abm_v^2 + 27b^2 - b_v^3 m_u^3 + 9bb_v m_u^3 - b_u^3 m_v^3 + 4bm_u^3 m_v^3 + 9bb_u m_v^3 - 6bb_u m_u m_v^2 \\
&- b_u^2 b_v m_u m_v^2 + 3bb_v m_u m_v^2 - b_u b_v^2 m_u^2 m_v + 3bb_u m_u^2 m_v - 6bb_v m_u^2 m_v - 3b_u b_v^3 \\
&+ 21 b_u^2 b_v^2 - 3b_u^3 b_v + 18bb_u b_v - 18bb_u^2 - 18bb_v^2 \\
\gamma_4^* =& -4a^3 m_u - 4a^3 m_v + 4a^2 b_u m_u^2 + 4a^2 b_v m_v^2 + a^2 m_u^3 m_v^2 + a^2 m_u^2 m_v^3 - 3abm_u^3 \\
&- 3abm_u^2 m_v - 3abm_u m_v^2 - 3abm_v^3 + 12ab_u^2 b_v - 3ab_u^2 m_u m_v^2 + 3ab_u^2 m_v^3 + 12ab_u b_v^2 \\
&- 6ab_u b_v m_u^2 m_v - 6ab_u b_v m_u m_v^2 + 3ab_v^2 m_u^3 - 3ab_v^2 m_u^2 m_v - 27b^2 m_u - 27b^2 m_v \\
&+ 9bb_u^2 m_u - 9bb_u^2 m_v - 18bb_u b_v m_u - 18bb_u b_v m_v + 12bb_u m_u^2 m_v^2 - 9bb_v^2 m_u \\
&+ 9bb_v^2 m_v + 12bb_v m_u^2 m_v^2 - 6b_u^3 b_v m_v + 3b_u^2 b_v^2 m_u + 3b_u^2 b_v^2 m_v - 6b_u b_v^3 m_u
\end{aligned}$$

$$
\begin{aligned}
\gamma_5^* =& 9a^2b_u^2 - 18a^2b_ub_v + 9a^2b_v^2 - 27abb_um_u + 27abb_vm_u + 3ab_u^2b_vm_u - 15ab_ub_v^2m_u \\
&+ a^3m_u^2 + 27b^2m_u^2 - 9bb_ub_vm_u^2 + 9bb_v^2m_u^2 - 3b_ub_v^3m_u^2 - a^2b_vm_u^3 + 27abb_um_v \\
&- 27abb_vm_v - 15ab_u^2b_vm_v + 3ab_ub_v^2m_v + 2a^3m_um_v - 27b^2m_um_v + 9bb_u^2m_um_v \\
&+ 36bb_ub_vm_um_v + 9bb_v^2m_um_v - 3b_u^2b_v^2m_um_v + 4a^2b_um_u^2m_v - 3a^2b_vm_u^2m_v \\
&- 3abm_u^3m_v - ab_v^2m_u^3m_v + a^3m_v^2 + 27b^2m_v^2 + 9bb_u^2m_v^2 - 9bb_ub_vm_v^2 \\
&- 3b_u^3b_vm_v^2 - 3a^2b_um_um_v^2 + 4a^2b_vm_um_v^2 + 12abm_u^2m_v^2 - 4ab_ub_vm_u^2m_v^2 \\
&- a^2b_um_v^3 - 3abm_um_v^3 - ab_u^2m_um_v^3 - a^2m_u^3m_v^3
\end{aligned}
$$

$$
\begin{aligned}
\gamma_6^* =& - 4a^3b_u - 27b^2b_u - 4a^3b_v - 27b^2b_v + 18bb_u^2b_v + 18bb_ub_v^2 - 3b_u^3b_v^2 - 3b_u^2b_v^3 \\
&- a^2b_u^2m_u + 6a^2b_ub_vm_u + 3a^2b_v^2m_u + 3abb_um_u^2 - 3abb_vm_u^2 - 6ab_ub_v^2m_u^2 - a^3m_u^3 \\
&- 9b^2m_u^3 + 9bb_v^2m_u^3 + 3a^2b_u^2m_v + 6a^2b_ub_vm_v - a^2b_v^2m_v - 6abb_um_um_v - 6abb_vm_um_v \\
&+ a^3m_u^2m_v + 9b^2m_u^2m_v + 6bb_ub_vm_u^2m_v - 3bb_v^2m_u^2m_v + 2a^2b_vm_u^3m_v - 3abb_um_v^2 \\
&+ 3abb_vm_v^2 - 6ab_u^2b_vm_v^2 + a^3m_um_v^2 + 9b^2m_um_v^2 - 3bb_u^2m_um_v^2 + 6bb_ub_vm_um_v^2 \\
&- a^2b_um_u^2m_v^2 - a^2b_vm_u^2m_v^2 - a^3m_v^3 - 9b^2m_v^3 + 9bb_u^2m_v^3 + 2a^2b_um_um_v^3
\end{aligned}
$$

$$
\begin{aligned}
\gamma_7^* =& 27ab(b_u - b_v)^2 - 12ab_u^2b_v^2 + (8a^3 - 27b^2)b_um_u - 4a^3b_vm_u + 54b^2b_vm_u + 9bb_u^2b_vm_u \\
&- 9bb_ub_v^2m_u - 3b_u^2b_v^3m_u - 9a^2bm_u^2 + 4a^2b_ub_vm_u^2 - 3abb_vm_u^3 + ab_v^3m_u^3 - 4a^3b_um_v \\
&+ 54b^2b_um_v + 8a^3b_vm_v - 27b^2b_vm_v - 9bb_u^2b_vm_v + 9bb_ub_v^2m_v - 3b_u^3b_v^2m_v \\
&+ 18a^2bm_um_v - 4a^2b_u^2m_um_v - 4a^2b_v^2m_um_v + 12abb_um_u^2m_v - 21abb_vm_u^2m_v \\
&+ ab_ub_v^2m_u^2m_v - 9b^2m_u^3m_v - 3bb_v^2m_u^3m_v - 9a^2bm_v^2 + 4a^2b_ub_vm_v^2 - 21abb_um_um_v^2 \\
&+ 12abb_vm_um_v^2 + ab_u^2b_vm_um_v^2 - 4a^3m_u^2m_v^2 + 18b^2m_u^2m_v^2 - 6bb_ub_vm_u^2m_v^2 \\
&+ a^2b_vm_u^3m_v^2 - 3abb_um_v^3 + ab_u^3m_v^3 - 9b^2m_um_v^3 - 3bb_u^2m_um_v^3 + a^2b_um_u^2m_v^3 - 4abm_u^3m_v^3
\end{aligned}
$$

$$
\begin{aligned}
\gamma_9^* =& a^3b_u^2 + 27b^2b_u^2 + 2a^3b_ub_v - 27b^2b_ub_v + a^3b_v^2 + 27b^2b_v^2 - 18bb_u^2b_v^2 \\
&- b_u^3b_v^3 + 9a^2bb_um_u - 9a^2bb_vm_u - a^2b_u^2b_vm_u - 3a^2b_ub_v^2m_u + a^4m_u^2 + 3abb_ub_vm_u^2 \\
&+ 3abb_v^2m_u^2 - a^3b_vm_u^3 - 9b^2b_vm_u^3 + bb_v^3m_u^3 - 9a^2bb_um_v + 9a^2bb_vm_v - 3a^2b_u^2b_vm_v \\
&- a^2b_ub_v^2m_v - 2a^4m_um_v - 3abb_u^2m_um_v + 12abb_ub_vm_um_v - 3abb_v^2m_um_v + 2ab_u^2b_v^2m_um_v \\
&+ 9b^2b_um_u^2m_v + a^3b_vm_u^2m_v - 18b^2b_vm_u^2m_v - 3bb_ub_v^2m_u^2m_v + a^2bm_u^3m_v + a^4m_v^2 \\
&+ 3abb_u^2m_v^2 + 3abb_ub_vm_v^2 + a^3b_um_um_v^2 - 18b^2b_um_um_v^2 + 9b^2b_vm_um_v^2 \\
&- 3bb_u^2b_vm_um_v^2 - 6a^2bm_u^2m_v^2 - a^2b_ub_vm_u^2m_v^2 + 2abb_vm_u^3m_v^2 - a^3b_um_v^3 \\
&- 9b^2b_um_v^3 + bb_u^3m_v^3 + a^2bm_um_v^3 + 2abb_um_u^2m_v^3 - 4b^2m_u^3m_v^3
\end{aligned}
$$

In particular, if $P_i + Q_j \neq \mathcal{O}$ for $i, j \in \{0, 1, 2\}$, then the leading coefficient γ_0^* is non-zero, and we get theorem 3.7.3 where $\gamma_i = \gamma_i^*/\gamma_0^*$ for $i > 0$:

$$
(u \boxplus v)(x, y) := -\gamma_9 - \gamma_7 x + \gamma_6 y - \gamma_5 x^2 + \gamma_4 xy - \gamma_3 y^2 + \gamma_2 x^2 y - \gamma_1 xy^2 + y^3
$$

A.6 Special Cases

Now we discuss the cases that were not covered in theorem 3.7.3. First we note that as long as $\mathcal{O}$ is not a point of u or v, then equation (A.3) holds, where c is the leading non-zero coefficient on the right hand side. The remaining special cases correspond to $\mathcal{O}$ being a point of u or v.

First we dispense of the case where $\mathcal{O}$ appears more than once as a point of u or v. If $\mathcal{O}$ is a point of a line more than once, then that line is the line at infinity $\ell_{\mathcal{O}}$, and $u \boxplus \ell_{\mathcal{O}} = u^3$. Otherwise, if $\mathcal{O}$ is a point of both u and v, then we have $u(x,y) = x - x_P, v(x,y) = x - x_Q$. If $P = \pm Q$, then

$$(u \boxplus v)(x,y) = (x - x_P)^2(x - x_{2P})$$

and otherwise:

$$(u \boxplus v)(x,y) = (x - x_P)(x - x_Q)(x - x_{P+Q})(x - x_{P-Q})$$

and we can expand these in terms of x_P, x_Q using the formulas from section 4.2.

Now suppose that u has points $P, -P, \mathcal{O}$, so $u(x,y) = x - x_P$, but $\mathcal{O}$ is not a point of v, so $v(x,y) = y - m_v x - b_v$. Using lemma 3.7.1, we calculate:

$$(u \boxplus v)(x,y) = c^{-1}\left(-\gamma_9^\chi - \gamma_7^\chi x + \gamma_6^\chi y - \gamma_5^\chi x^2 + \gamma_4^\chi xy - \gamma_3^\chi y^2 + \gamma_2^\chi x^2 y - \gamma_1^\chi x y^2 + \gamma_0^\chi y^3\right)$$

where

$$\begin{aligned}
\gamma_0^\chi =& b + a x_P + x_P^3 - (b_v + m_v x_P)^2 \\
\gamma_1^\chi =& 2b_v(a + 3x_P^2) - 3bm_v - m_v(b_v + m_v x_P)^2 - a m_v x_P + 3 m_v x_P^3 \\
\gamma_2^\chi =& -a^2 + 9 b x_P + 3 a x_P^2 + 3 x_P (b_v + m_v x_P)^2 \\
\gamma_3^\chi =& 9 b b_v - b_v^3 + a^2 m_v - 2 a b_v m_v^2 + 4 b m_v^3 + (7 a b_v - 3 b m_v + b_v^2 m_v + 2 a m_v^3) x_P \\
&+ m_v(a - b_v m_v) x_P^2 + (3 b_v + m_v^3) x_P^3 \\
\gamma_4^\chi =& a(-3b + 3 b_v^2 + a m_v^2) - 2(2a^2 - 3 a b_v m_v + 6 b m_v^2) x_P + 3(3b + b_v^2 - a m_v^2) x_P^2 + 6 b_v m_v x_P^3 \\
\gamma_5^\chi =& -a(a b_v + 3 b m_v + b_v^2 m_v + a m_v^3) + (9 b b_v + 3 b_v^3 - 4 a^2 m_v + 4 a b_v m_v^2) x_P \\
&+ (3 a b_v + 9 b m_v - 3 b_v^2 m_v - a m_v^3) x_P^2 + 3 b_v m_v^2 x_P^3 \\
\gamma_6^\chi =& -a^3 - 9 b^2 + 9 b b_v^2 + 2 a^2 b_v m_v + (-3 a b + 6 a b_v^2 - 6 b b_v m_v + a^2 m_v^2) x_P \\
&+ (-a^2 - 3 b m_v^2) x_P^2 + 3 b_v^2 x_P^3 \\
\gamma_7^\chi =& 3 a b b_v + a b_v^3 - 9 b^2 m_v - 3 b b_v^2 m_v + a^2 b_v m_v^2 - 4 a b m_v^3 \\
&+ (-4 a^2 b_v - 12 a b m_v - a b_v^2 m_v + 6 b b_v m_v^2 - a^2 m_v^3) x_P \\
&+ (9 b b_v - 3 b_v^3 - 4 a^2 m_v + a b_v m_v^2 - 3 b m_v^3) x_P^2 + m_v(3 b_v^2 - a m_v^2) x_P^3 \\
\gamma_9^\chi =& -a^3 b_v - 9 b^2 b_v + b b_v^3 + a^2 b m_v + 2 a b b_v m_v^2 - 4 b^2 m_v^3 \\
&+ (-3 a b b_v - 9 b^2 m_v + 3 b b_v^2 m_v + a^2 b_v m_v^2 - 2 a b m_v^3) x_P \\
&+ (-a^2 b_v - 3 a b m_v + 2 a b_v^2 m_v - 3 b b_v m_v^2) x_P^2 + (b_v^3 - b m_v^3) x_P^3
\end{aligned}$$

Again, if $P_i + Q_j \neq \mathcal{O}$ for $i, j \in \{0, 1, 2\}$, then we have the following with $\gamma_i = \gamma_i^\chi / \gamma_0^\chi$ for $i > 0$:

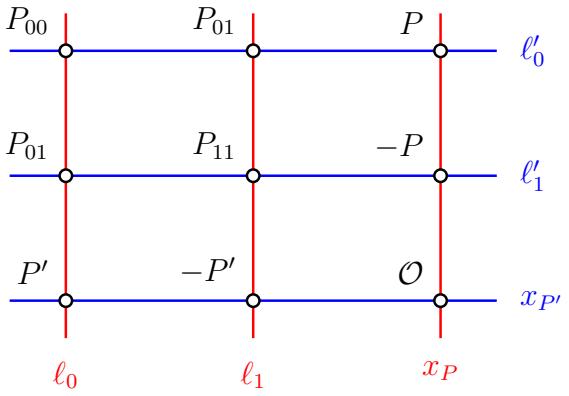
$$(u \boxplus v)(x, y) := -\gamma_9 - \gamma_7 x + \gamma_6 y - \gamma_5 x^2 + \gamma_4 xy - \gamma_3 y^2 + \gamma_2 x^2 y - \gamma_1 x y^2 + y^3$$

```
γ0x = (b + a xu + xu^3 - (bv + mv xu)^2);
γ1x = γ0x^-1 (2 bv (a + 3 xu^2) - 3 b mv - mv (bv + mv xu)^2 - a mv xu + 3 mv xu^3);
γ2x = γ0x^-1 (-a^2 + 9 b xu + 3 a xu^2 + 3 xu (bv + mv xu)^2);
γ3x = γ0x^-1 (9 b bv - bv^3 + a^2 mv - 2 a bv mv^2 + 4 b mv^3
      + (7 a bv - 3 b mv + bv^2 mv + 2 a mv^3) xu + mv (a - bv mv) xu^2 + (3 bv + mv^3) xu^3);
γ4x = γ0x^-1 (a (-3 b + 3 bv^2 + a mv^2)
      - 2 (2 a^2 - 3 a bv mv + 6 b mv^2) xu + 3 (3 b + bv^2 - a mv^2) xu^2 + 6 bv mv xu^3);
γ5x = γ0x^-1 (-a (a bv + 3 b mv + bv^2 mv + a mv^3) + (9 b bv + 3 bv^3 - 4 a^2 mv + 4 a bv mv^2) xu
      + (3 a bv + 9 b mv - 3 bv^2 mv - a mv^3) xu^2 + 3 bv mv^2 xu^3);
γ6x = γ0x^-1 (-a^3 - 9 b^2 + 9 b bv^2 + 2 a^2 bv mv
      + (-3 a b + 6 a bv^2 - 6 b bv mv + a^2 mv^2) xu + (-a^2 - 3 b mv^2) xu^2 + 3 bv^2 xu^3);
γ7x = γ0x^-1 (-3 a b bv + a bv^3 - 9 b^2 mv - 3 b bv^2 mv + a^2 bv mv^2
      - 4 a b mv^3 + (-4 a^2 bv - 12 a b mv - a bv^2 mv + 6 b bv mv^2 - a^2 mv^3) xu
      + (9 b bv - 3 bv^3 - 4 a^2 mv + a bv mv^2 - 3 b mv^3) xu^2 + mv (3 bv^2 - a mv^2) xu^3);
γ9x = γ0x^-1 (-a^3 bv - 9 b^2 bv + b bv^3 + a^2 b mv + 2 a b bv mv^2
      - 4 b^2 mv^3 + (-3 a b bv - 9 b^2 mv + 3 b bv^2 mv + a^2 bv mv^2 - 2 a b mv^3) xu
      + (-a^2 bv - 3 a b mv + 2 a bv^2 mv - 3 b bv mv^2) xu^2 + (bv^3 - b mv^3) xu^3);
LinexSumFunction = -γ9x - γ7x x + γ6x y - γ5x x^2 + γ4x x y - γ3x y^2 + γ2x x^2 y - γ1x x y^2 + y^3;
m = (-y - (mv xq + bv))/(x - xq); xs = m^2 - x - xq; ys = m (xs - x) - y;
Together@PolynomialRemainder[
  (y - mv x - bv)^3 Resultant[(xu - xs)/(xu - xq), b + a xq + xq^3 - (bv + mv xq)^2, xq] - LinexSumFunction,
  b + a x + x^3 - y^2, y]
```

Out[12]= 0

A.7 Eight Point Diagrams

Similarly, suppose that one of the points is $\mathcal{O}$. Then we instead have:



$$\begin{aligned} f(x,y) =& (y-\alpha_0 x-\beta_0)(y-\alpha_1 x-\beta_1)(x-x_P) \\ =& -(b\cdot\alpha_0\alpha_1+\beta_0\beta_1 x_P) \\ &+x\left(\beta_0\beta_1-a\cdot\alpha_0\alpha_1-(\alpha_1\beta_0+\alpha_0\beta_1)\,x_P\right) \\ &+y\left((\beta_0+\beta_1)\,x_P\right) \\ &+x^2\left(\alpha_1\beta_0+\alpha_0\beta_1-\alpha_0\alpha_1 x_P\right) \\ &-xy\left(\beta_0+\beta_1-(\alpha_0+\alpha_1)\,x_P\right) \\ &-y^2\left(x_P-\alpha_0\alpha_1\right) \\ &-x^2y\left(\alpha_0+\alpha_1\right)+xy^2 \end{aligned} \tag{A.4}$$

Theorem A.7.1. *With the above configuration of the eight point diagram, the following relations hold:*

$$\alpha_0+\alpha_1=\alpha'_0+\alpha'_1 \tag{A.5}$$

$$x_P-\alpha_0\alpha_1=x_{P'}-\alpha'_0\alpha'_1 \tag{A.6}$$

$$\beta_0+\beta_1-(\alpha_0+\alpha_1)\,x_P=\beta'_0+\beta'_1-(\alpha'_0+\alpha'_1)\,x_{P'} \tag{A.7}$$

$$\alpha_1\beta_0+\alpha_0\beta_1-\alpha_0\alpha_1 x_P=\alpha'_1\beta'_0+\alpha'_0\beta'_1-\alpha'_0\alpha'_1 x_{P'} \tag{A.8}$$

$$(\beta_0+\beta_1)\,x_P=(\beta'_0+\beta'_1)\,x_{P'} \tag{A.9}$$

$$\beta_0\beta_1-a\cdot\alpha_0\alpha_1-(\alpha_1\beta_0+\alpha_0\beta_1)\,x_P=\beta'_0\beta'_1-a\cdot\alpha'_0\alpha'_1-(\alpha'_1\beta'_0+\alpha'_0\beta'_0)\,x_{P'} \tag{A.10}$$

$$b\cdot\alpha_0\alpha_1+\beta_0\beta_1 x_P=b\cdot\alpha'_0\alpha'_1+\beta'_0\beta'_1 x_{P'} \tag{A.11}$$

So we get the following relations:

$$(y - \alpha_0 x - \beta_0)(y - \alpha_1 x - \beta_1)(x - x_P) - (y - \alpha_0' x - \beta_0')(y - \alpha_1' x - \beta_1')(x - x_{P'}) \\ = (b + ax + x^3 - y^2)(x_P - x_{P'})$$

Corollary A.7.2. *With the above configuration of the eight point diagram, the following relations hold:*

$$x_P - x_{P'} = \alpha_0\alpha_1 - \alpha_0'\alpha_1' \tag{A.12}$$
$$= (\alpha_0 - \alpha_0')(\alpha_1 - \alpha_0') = (\alpha_0 - \alpha_1')(\alpha_1 - \alpha_1') \tag{A.13}$$
$$= -(\alpha_0 - \alpha_0')(\alpha_0 - \alpha_1') = -(\alpha_1 - \alpha_0')(\alpha_1 - \alpha_1') \tag{A.14}$$

Appendix B

Three Torsion Calculation

B.1 Elliptic Curve Three Torsion

Here we fill in the gaps from section 7.1. Recall that for $T \in E[3]$, the line ℓ_T has the point T three times; geometrically, this is the tangent line to E at T, which has a triple intersection there.

Theorem B.1.1. *Suppose $E: \ b + ax + x^3 - y^2 = 0$ is an elliptic curve over a field $\mathbb{F}$ of characteristic 0, with $a \neq 0$. Then E has 9 triple intersection lines ℓ_T over $\overline{\mathbb{F}}$, corresponding to each three torsion point $T \in E[3]$. Furthermore, the 3-torsion points form a subgroup that is the direct sum of two cyclic groups of order three.*

Note that $\mathcal{O} \in E[3]$, and $\ell_{\mathcal{O}}(P) = 1$. Each other $T \in E[3]\backslash\{\mathcal{O}\}$ arises from a distinct root $z = m_T$ of $-27a^2 + 108b\,z^2 + 18a\,z^4 + z^8$, and has the following coordinates and line function:

$$T = (x_T, y_T) = \left(\frac{m_T^2}{3}, \frac{3a + m_T^4}{6m_T}\right)$$
$$\ell_T(P) = y_P - m_T x_P - b_T = y_P - m_T x_P - \frac{3a - m_T^4}{6m_T}.$$

Proof. The fact that $E[3]$ is a direct sum of two cyclic groups of order three is proved in Silverman's book [8], theorem 6.1.

For a triple intersection line ℓ_T at $T \in E\backslash\{\mathcal{O}\}$, we start by noting the following equality (of polynomials in x):

$$b + ax + x^3 - (m_T x + b_T)^2 = (x - x_T)^3$$
$$(b - b_T^2 + x_T^3) + (a - 2m_T b_T - 3x_T^2)x + (-m_T^2 + 3x_T)x^2 = 0$$

which is a restatement of the fact that ℓ_T only intersects E at T. By comparing coefficients,

$$\begin{aligned} x_T =& \frac{m_T^2}{3}, \qquad b_T = \frac{a - 3x_T^2}{2m_T} = \frac{3a - m_T^4}{6m_T} \\ 0 =& b - b_T^2 + x_T^3 = b - \left(\frac{3a - m_T^4}{6m_T}\right)^2 + \frac{m_T^6}{27} \\ =& \frac{-27a^2 + 108bm_T^2 + 18am_T^4 + m_T^8}{108m_T^2} \end{aligned}$$

So we have:

$$y_T = m_T x_T + b_T = \frac{3a + m_T^4}{6m_T}$$

And the following gives a polynomial satisfied by m_T:

$$0 = -27a^2 + 108bm_T^2 + 18am_T^4 + m_T^8.$$

Note that the condition $a \neq 0$ ensures that $m_T \neq 0$. □

Now we prove some algebraic properties of three torsion which allow us to do explicit calculations. We use the results of chapter 6 about nine point diagrams to simplify calculations.

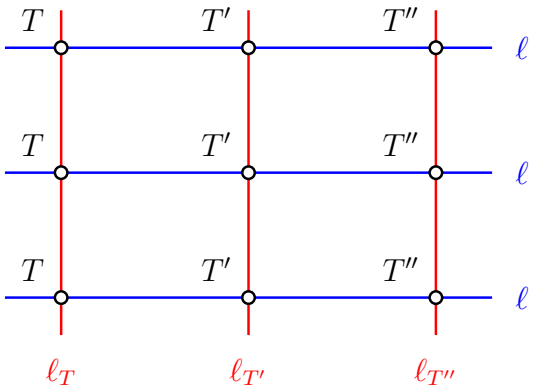
Lemma B.1.2. *Suppose that $T, T', T'' \in E[3]\backslash\{\mathcal{O}\}$ are distinct, and satisfy $T + T' + T'' = \mathcal{O}$. Then there is a primitive cube root of unity $\omega \in \overline{\mathbb{F}}$ such that*

$$m_T + \omega m_{T'} + \omega^2 m_{T''} = 0.$$

Furthermore, the line ℓ through T, T', T'' has the following slope:

$$m_\ell = \frac{1}{3}\left((1-\omega)m_T + (1-\omega^2)m_{T'}\right)$$

Proof. Consider the nine point diagram $\mathcal{N} := \mathfrak{N}(\ell_T, \ell_{T'}, \ell_{T''})$:



By theorem 6.3.3 we have the following formulas for the orientation $\partial(\mathcal{N})$:

$$\begin{aligned}\partial(\mathcal{N}) =&(m_\ell - m_T)^3 = (m_\ell - m_{T'})^3 = (m_\ell - m_{T''})^3\\ =&(m_\ell - m_T)(m_\ell - m_{T'})(m_\ell - m_{T''})\end{aligned}$$

Note that the factors $(m_\ell - m_T), (m_\ell - m_{T'}), (m_\ell - m_{T''})$ are distinct, since T, T', T'' are distinct. Furthermore, since ℓ and ℓ_T are distinct lines which share a point, they cannot be parallel; hence the three factors are also non-zero. It follows that $(m_\ell - m_T), (m_\ell - m_{T'}), (m_\ell - m_{T''})$ are related through multiplication by a primitive cube root of unity. More specifically, there is $\omega \in \overline{\mathbb{F}}$ such that:

$$\begin{aligned}(m_\ell - m_{T'}) =&\omega(m_\ell - m_T)\\ (m_\ell - m_{T''}) =&\omega^2(m_\ell - m_T)\end{aligned}$$

and hence we can isolate m_ℓ in the first equation, and subsequently solve for $m_{T''}$ in the second:

$$\begin{aligned}m_\ell =&\frac{m_{T'} - \omega m_T}{1-\omega} = \frac{(1-\omega)m_T + (1-\omega^2)m_{T'}}{3}\\ m_{T''} =& -\omega m_T - \omega^2 m_{T'}\end{aligned}$$

noting that $1 + \omega + \omega^2 = 0$, so $(1-\omega)(1-\omega^2) = 3$. □

We now define the notation for $E[3]$ that we use throughout the rest of this thesis:

Definition B.1.3. *When working with the elliptic curve $E: b + ax + x^3 - y^2 = 0$ defined over $\mathbb{F}$ of characteristic 0, we use $T_0, T_1 \in E[3]$ to denote two generators of $E[3]$:*

$$E[3] = \{iT_0 + jT_1 \mid i, j \in \{0, 1, 2\}\}.$$

We also denote $T_2 = T_0 + T_1$ and $T_3 = T_0 - T_1$. In light of lemma B.1.2, we let $\omega \in \overline{\mathbb{F}}$ denote the primitive cube root of unity satisfying:

$$m_{T_0} + \omega m_{-T_0-T_1} + \omega^2 m_{T_1} = 0$$

and note that $1 + \omega + \omega^2 = 0$. We also make frequent use of the following square root of -3:

$$\sqrt{-3} := \omega - \omega^2.$$

Lemma B.1.4.

$$\begin{aligned}m_{T_2} =&m_{T_0+T_1} = \omega^2 m_{T_0} + \omega m_{T_1}\\ m_{T_3} =&m_{T_0-T_1} = \omega m_{T_0} - \omega^2 m_{T_1}\end{aligned}$$

Proof. Since $m_{T_2} = -m_{-T_0-T_1}$, by the definition of ω, we have

$$m_{T_2} = \omega^2 m_{T_0} + \omega m_{T_1}.$$

By lemma B.1.2, the following equations hold for some $i, j \in \{1, 2\}$:

$$\begin{aligned} 0 &= m_{T_0-T_1} + \omega^i m_{T_1} - \omega^{2i} m_{T_0} \\ 0 &= m_{T_0-T_1} + \omega^j m_{T_0+T_1} + \omega^{2j} m_{T_0} \end{aligned}$$

We claim that $(i, j) = (2, 1)$. We derive a contradiction from the other three cases.

First note that for $T, T' \in E[3]\backslash\{\mathcal{O}\}$,

$$m_T = \pm m_{T'} \Rightarrow \ x_T = x_{T'} \Rightarrow \ T = \pm T'$$

since at most two points can share an x-coordinate on E. So the eight values $\pm m_{T_i}$ for $i = 0, 1, 2, 3$ are distinct.

- Now for $(i, j) = (1, 1)$ we get a contradiction by substituting

  $$\begin{aligned} m_{T_0-T_1} &= \omega^2 m_{T_0} - \omega m_{T_1} \\ m_{T_0+T_1} &= \omega^2 m_{T_0} + \omega m_{T_1} \end{aligned}$$

  to obtain:

  $$\begin{aligned} 0 &= m_{T_0-T_1} + \omega m_{T_0+T_1} + \omega^2 m_{T_0} \\ &= (1 + 2\omega^2) m_{T_0} - (\omega - \omega^2) m_{T_1} \\ &= -\sqrt{-3}(m_{T_0} + m_{T_1}) \end{aligned}$$

- Similarly for $(i, j) = (1, 2)$ we get a contradiction:

  $$\begin{aligned} 0 &= m_{T_0-T_1} + \omega^2 m_{T_0+T_1} + \omega m_{T_0} \\ &= (2\omega + \omega^2) m_{T_0} + (1 - \omega) m_{T_1} \\ &= -\omega^2\sqrt{-3}(m_{T_0} - m_{T_1}) \end{aligned}$$

- Lastly when $(i, j) = (2, 2)$, we get a contradiction by substituting

  $$\begin{aligned} m_{T_0-T_1} &= -\omega m_{T_0} - \omega^2 m_{T_0+T_1} \\ m_{T_1} &= -\omega m_{T_0} + \omega^2 m_{T_0+T_1} \end{aligned}$$

  to obtain:

  $$\begin{aligned} 0 &= m_{T_0-T_1} + \omega^2 m_{T_1} - \omega m_{T_0} \\ &= -(1 + 2\omega) m_{T_0} + (\omega - \omega^2) m_{T_0+T_1} \\ &= -\sqrt{-3}(m_{T_0} + m_{T_0+T_1}) \end{aligned}$$

□

Lemma B.1.5.

$$0 = 3\sqrt{-3}a - m_{T_0}^3 m_{T_1} + \sqrt{-3}m_{T_0}^2 m_{T_1}^2 + m_{T_0} m_{T_1}^3$$

Proof. By lemma B.1.2 applied to the line ℓ through $T_0, T_1, -T_0 - T_1$, we know that

$$m_\ell = \frac{(1-\omega^2)m_{T_0} + (1-\omega)m_{T_1}}{3}$$

and we can expand this in terms of m_{T_0}, m_{T_1} to get the desired result:

$$\begin{aligned}\frac{(1-\omega^2)m_{T_0} + (1-\omega)m_{T_1}}{3} &= \frac{y_{T_0} - y_{T_1}}{x_{T_0} - x_{T_1}} = \frac{\frac{3a+m_{T_0}^4}{6m_{T_0}} - \frac{3a+m_{T_1}^4}{6m_{T_1}}}{\frac{m_{T_0}^2}{3} - \frac{m_{T_1}^2}{3}} \\ &= \frac{-3a + m_{T_0}m_{T_1}(m_{T_0}^2 + m_{T_0}m_{T_1} + m_{T_1}^2)}{2m_{T_0}m_{T_1}(m_{T_0} + m_{T_1})}\end{aligned}$$

So:

$$\begin{aligned}0 &= -9a + m_{T_0}m_{T_1}(3m_{T_0}^2 + 3m_{T_0}m_{T_1} + 3m_{T_1}^2 - 2(m_{T_0} + m_{T_1})((1-\omega^2)m_{T_0} + (1-\omega)m_{T_1})) \\ &= -9a + m_{T_0}m_{T_1}((1+2\omega^2)m_{T_0}^2 + (-1+2\omega+2\omega^2)m_{T_0}m_{T_1} + (1+2\omega)m_{T_1}^2) \\ &= -9a + m_{T_0}m_{T_1}(-\sqrt{-3}m_{T_0}^2 - 3m_{T_0}m_{T_1} + \sqrt{-3}m_{T_1}^2) \\ &= \sqrt{-3}(3\sqrt{-3}a - m_{T_0}^3 m_{T_1} + \sqrt{-3}m_{T_0}^2 m_{T_1}^2 + m_{T_0}m_{T_1}^3)\end{aligned}$$

□

B.2 Action of the 3-torsion on Points

In this section, we fill in the gaps from section 7.1.1 to realize the translation by T map $P \mapsto P+T$ on E as a projective linear map. The following theorem explicitly demonstrates that translation by T corresponds to a matrix multiplication:

Theorem B.2.1. *For a three torsion point $T \in E[3]$ and $P \in E\backslash\{\mathcal{O}, -T\}$, the following two vectors give projective coordinates for the same point:*

$$[P+T] \propto M_T[P]$$

where $M_\mathcal{O} = I$, and M_T is the following matrix for $T \neq \mathcal{O}$:

$$M_T := \frac{1}{-2y_T}\begin{bmatrix} -b_T - y_T & x_T & x_T(b_T + 2y_T) \\ -m_T y_T & y_T & -y_T(b_T + 2y_T) \\ m_T & 1 & b_T \end{bmatrix}.$$

More precisely, for $T \in E[3]\backslash\{\mathcal{O}\}$ the following holds with coordinates as functions of P in $\mathbb{F}(E)$:

$$\begin{bmatrix} x_{P+T} \\ y_{P+T} \\ 1 \end{bmatrix} = \left(\frac{-2y_T}{y_P + m_T x_P + b_T}\right) M_T \begin{bmatrix} x_P \\ y_P \\ 1 \end{bmatrix} = \left(\frac{-2y_T}{\ell_{-T}(P)}\right) M_T[P].$$

Explicitly, we have:

$$\begin{aligned} x_{P+T} =& \frac{x_T y_P - (b_T + y_T)x_P + x_T(b_T + 2y_T)}{y_P + m_T x_P + b_T} \\ y_{P+T} =& \frac{y_T y_P - m_T y_T x_P - y_T(b_T + 2y_T)}{y_P + m_T x_P + b_T} \end{aligned}$$

Note that the factor $-1/(2y_T)$ is there so that $\det(M_T) = 1$; this will be of benefit when considering algebraic properties of these matrices.

Theorem 7.1.6 is a simple consequence of the following lemma:

Lemma B.2.2. *Suppose that $T = (x_T, y_T) \in E[3]$ is a three torsion point, with tangent line $b_T + m_T x - y = 0$. The following identities hold as functions of $P \in E$:*

$$\frac{y(P) - m_T x(P) - b_T}{y(P) + m_T x(P) + b_T} = \frac{y(P+T) + m_T x(P+T) + b_T}{2y_T} \tag{B.1}$$

$$\frac{2y_T}{y(P) + m_T x(P) + b_T} = \frac{y(P+T) - m_T x(P+T) - b_T}{-2y_T} \tag{B.2}$$

Proof. These equalities follow from comparing zeroes and poles of each side; if these coincide, then by Proposition II.3.1 of Silverman's book [8], the equality holds up to a constant factor, and hence we only need to check for equality at any point.

More precisely, we start by noting that since T and $-T$ are inflection points, their tangent lines have triple intersections with E, so:

$$\begin{aligned} \operatorname{Div}(b_T + m_T x(P) - y(P)) &= 3(T) - 3(\mathcal{O}) \\ \operatorname{Div}(b_T + m_T x(P) + y(P)) &= 3(-T) - 3(\mathcal{O}). \end{aligned}$$

Now to prove equation (B.1), we note that both sides have the same divisor:

$$\begin{aligned} \operatorname{Div}\left(\frac{y(P) - m_T x(P) - b_T}{y(P) + m_T x(P) + b_T}\right) &= (3(T) - 3(\mathcal{O})) - (3(-T) - 3(\mathcal{O})) \\ &= 3(T) - 3(-T) \\ \operatorname{Div}\left(\frac{y(P+T) + m_T x(P+T) + b_T}{2y_T}\right) &= 3(-T - T) - 3(\mathcal{O} - T) \\ &= 3(T) - 3(-T) \end{aligned}$$

and furthermore, both sides evaluate to 1 at $P = \mathcal{O}$ (recalling from section 3.1 that both the numerator and denominator are normalized functions with poles of order 3 at $\mathcal{O}$.)

Similarly, for equation (B.2), both functions have divisor $3(T) - 3(\mathcal{O})$. Furthermore, both sides evaluate to 1 at $P = T$. □

Now we can complete the proof of theorem 7.1.6:

Proof. We can restate lemma B.2.2 in matrix form:

$$\begin{bmatrix} -m_T & 1 & -b_T \\ 0 & 0 & -2y_T \\ m_T & 1 & b_T \end{bmatrix} \begin{bmatrix} x_P \\ y_P \\ 1 \end{bmatrix} = \frac{y_P + m_T x_P + b_T}{2y_T} \begin{bmatrix} m_T & 1 & b_T \\ -m_T & 1 & -b_T \\ 0 & 0 & 2y_T \end{bmatrix} \begin{bmatrix} x_{P+T} \\ y_{P+T} \\ 1 \end{bmatrix}. \quad \text{(B.3)}$$

With a direct computation, we verify that:

$$\begin{aligned} &\begin{bmatrix} m_T & 1 & b_T \\ -m_T & 1 & -b_T \\ 0 & 0 & 2y_T \end{bmatrix}^{-1} \begin{bmatrix} -m_T & 1 & -b_T \\ 0 & 0 & -2y_T \\ m_T & 1 & b_T \end{bmatrix} \\ =&\frac{1}{2m_T y_T} \begin{bmatrix} y_T & -y_T & -b_T \\ m_T y_T & m_T y_T & 0 \\ 0 & 0 & m_T \end{bmatrix} \begin{bmatrix} -m_T & 1 & -b_T \\ 0 & 0 & -2y_T \\ m_T & 1 & b_T \end{bmatrix} \\ =&\frac{1}{2m_T y_T} \begin{bmatrix} -m_T(b_T + y_T) & m_T x_T & m_T x_T (b_T + 2y_T) \\ -m_T^2 y_T & m_T y_T & -m_T y_T (b_T + 2y_T) \\ m_T^2 & m_T & m_T b_T \end{bmatrix} \\ =&\frac{m_T}{2m_T y_T}(-2y_T) M_T = -M_T. \end{aligned} \quad \text{(B.4)}$$

So we rearrange equation (B.3) to get theorem 7.1.6:

$$\begin{bmatrix} x_{P+T} \\ y_{P+T} \\ 1 \end{bmatrix} = \left(\frac{-2y_T}{y_P + m_T x_P + b_T} \right) M_T \begin{bmatrix} x_P \\ y_P \\ 1 \end{bmatrix}. \quad \text{(B.5)}$$

□

B.3 Action of 3-torsion on Lines

Now we derive a formula for $\ell^{\boxplus T}$ using the formulas for adding T to a point found in theorem 7.1.6. Informally, the argument is that $P \in \ell^{\boxplus T}$ if and only if $P - T \in \ell$, which can be equivalently expressed in linear algebraic terms:

$$0 = [\ell]^\intercal \left(M_{-T}[P] \right) = \left(M_{-T}^\intercal [\ell] \right)^\intercal [P].$$

And thus $M_{-T}^{\intercal}[\ell]$ satisfies the property that characterizes the coefficient vector of $\ell^{\boxplus T}$. We then obtain a formula for $[\ell^{\boxplus T}]$ by scaling appropriately. We make this more precise in the following theorem:

Theorem B.3.1. *For $T \in E[3]\backslash\{\mathcal{O}\}$, the coefficient vector of $\ell^{\boxplus T}$ is:*

$$[\ell^{\boxplus T}] = \frac{-2y_T}{y_T + m_\ell x_T + b_\ell} M_{-T}^{\intercal}[\ell] \tag{B.6}$$

where M_{-T} is the matrix defined in theorem B.3.1, so:

$$M_{-T}^{\intercal} := \frac{1}{2y_T} \begin{bmatrix} b_T + y_T & -m_T y_T & -m_T \\ x_T & -y_T & 1 \\ -x_T(b_T + 2y_T) & -y_T(b_T + 2y_T) & -b_T \end{bmatrix}.$$

Explicitly, we have:

$$\begin{aligned} m_{\ell^{\boxplus T}} &= \frac{-(b_T + y_T)m_\ell - m_T y_T + m_T b_\ell}{y_T + m_\ell x_T + b_\ell} \\ b_{\ell^{\boxplus T}} &= \frac{x_T(b_T + 2y_T)m_\ell - y_T(b_T + 2y_T) + b_T b_\ell}{y_T + m_\ell x_T + b_\ell}. \end{aligned}$$

Proof. Note that the coefficient vector $[\ell^{\boxplus T}]$ is characterized by the following property, up to non-zero scalar multiplication:

$$\mathrm{Div}_P([\ell^{\boxplus T}]^{\intercal}[P]) = (P_0 + T) + (P_1 + T) + (P_2 + T) - 3(\mathcal{O}).$$

We claim that the vector $M_{-T}^{\intercal}[\ell]$ has this property as well. If this claim holds, then the scaling factor can be determined by comparing the second coordinates. The second coordinate of $[\ell^{\boxplus T}]$ is 1 by definition, while for $M_{-T}^{\intercal}[\ell]$ it is

$$\frac{1}{2y_T} \begin{bmatrix} x_T \\ -y_T \\ 1 \end{bmatrix}^{\intercal} \begin{bmatrix} -m_\ell \\ 1 \\ -b_\ell \end{bmatrix} = \frac{y_T + m_\ell x_T + b_\ell}{-2y_T}.$$

This confirms that equation (B.6) has the correct scaling factor.

So all that remains is to prove our claim that:

$$\mathrm{Div}_P\left(\left(M_{-T}^{\intercal}[\ell]\right)^{\intercal}[P]\right) = (P_0 + T) + (P_1 + T) + (P_2 + T) - 3(\mathcal{O}).$$

We start by invoking theorem 7.1.6, which is the analogous result for points:

$$[P - T] = \left(\frac{2y_T}{y_P - m_T x_P - b_T}\right) M_{-T}[P].$$

From this we get a formula for $\ell(P-T)$:

$$\ell(P-T) = [\ell]^\intercal[P-T] = \left(\frac{2y_T}{y_P - m_T x_P - b_T}\right)[\ell]^\intercal M_{-T}[P],$$

which can be rearranged into:

$$\left(M_{-T}^\intercal[\ell]\right)^\intercal[P] = \frac{y_P - m_T x_P - b_T}{2y_T}\ell(P-T).$$

Finally we take divisors to obtain the desired result:

$$\begin{aligned}\mathrm{Div}\left(\left(M_{-T}^\intercal[\ell]\right)^\intercal[P]\right) =& (3(T) - 3(\mathcal{O})) + ((P_0+T) + (P_1+T) + (P_2+T) - 3(T)) \\ =& (P_0+T) + (P_1+T) + (P_2+T) - 3(\mathcal{O}).\end{aligned}$$

□

B.4 Algebraic Properties of Three Torsion Matrices

Now we will establish some algebraic properties of the M_T matrices for $T \in E[3]$ that were defined in theorem 7.1.6. This is because of their central role in the algebra of line addition. Thus these properties will be used in computations throughout the rest of this chapter. Another motivation is that we can find a more natural model of elliptic curve for line multiplication by finding conjugating these matrices; we discuss this further in section B.6.

For reference $M_{\mathcal{O}} = I$, and for $T \in E[3]\backslash\{\mathcal{O}\}$:

$$M_T = \frac{1}{-2y_T}\begin{bmatrix} -b_T - y_T & x_T & x_T(b_T + 2y_T) \\ -m_T y_T & y_T & -y_T(b_T + 2y_T) \\ m_T & 1 & b_T \end{bmatrix}$$

Recall also that $E[3] = \langle T_0, T_1 \mid T_0^3 = T_1^3 = I,\ T_0T_1 = T_1T_0\rangle$, and $T_2 = T_0+T_1$, $T_3 = T_0-T_1$.

Lemma B.4.1. *For any $T, T' \in E[3]$:*

(i) $\det(M_T) = 1$

(ii) $M_T M_{T'} = \omega^i M_{T+T'}$ *for some* $i \in \{0,1,2\}$.

(iii) $M_T^2 = M_{-T}$

(iv) $M_T^3 = I$

Proof. (i) This is a simple consequence of equation (B.4), where $-M_T$ is expressed as a product of matrices of respective determinants $(2m_T y_T)^{-1}$ and $-2m_T y_T$.

(ii) By theorem 7.1.6, the matrix $M_T M_{T'} M_{T+T'}^{-1}$ has the property that

$$[P] \propto M_T M_{T'} M_{T+T'}^{-1}[P]$$

for all but a finite number of points $P \in E$. Thus this matrix is a multiple of the identity matrix. The multiple must be a cube root of 1 since $M_T M_{T'} M_{T+T'}^{-1}$ has determinant 1.

(iii) We have $M_T^2 = \omega^i M_{-T}$ for some $i \in \{0, 1, 2\}$. We check that $i = 0$ by comparing the coordinates in the second row and second column:

$$\begin{aligned}\left(M_T^2\right)_{2,2} &= \left(\frac{1}{-2y_T}\right)^2 \left(-m_T x_T y_T + y_T^2 - y_T(b_T + 2y_T)\right) \\ &= -\frac{1}{2} = (M_{-T})_{2,2}\end{aligned}$$

(iv) Similarly, we check that $M_T^3 = M_T M_{-T} = 1$ by comparing the entries in the second row and second column.

□

In light of lemma B.4.1, we define the following:

Definition B.4.2. *For $T, T' \in E[3]$, we define $\langle T, T' \rangle \in \{1, \omega, \omega^2\}$ to be the cube root of 1 such that*

$$\langle T, T' \rangle I = M_T M_{T'} M_{-T-T'}$$

This is in fact an alternating bilinear form, and we can use it to restate the first part of lemma B.1.2 as well:

Lemma B.4.3. *Suppose $\tau_0, \tau_1 \in E[3]$ form a basis. Then for i, j, k, l in modulus 3, we have*

$$\langle i\tau_0 + j\tau_1, k\tau_0 + l\tau_1 \rangle = \langle \tau_0, \tau_1 \rangle^{il-jk} \tag{B.7}$$

$$m_{\tau_0+\tau_1} = \langle \tau_1, \tau_0 \rangle m_{\tau_0} + \langle \tau_0, \tau_1 \rangle m_{\tau_1} \tag{B.8}$$

and in particular $\langle T_0, T_1 \rangle = \omega$.

Proof. First note that by lemma B.4.1, $\langle T, T' \rangle = 1$ when the arguments are linearly dependent in modulus 3. So we suppose that they are linearly independent. We will think of equation (B.7) as follows:

$$\left\langle \begin{bmatrix} i & j \\ k & l \end{bmatrix} \begin{bmatrix} \tau_0 \\ \tau_1 \end{bmatrix} \right\rangle = \langle \tau_0, \tau_1 \rangle \begin{vmatrix} i & j \\ k & l \end{vmatrix}$$

which we will demonstrate for the identity matrix. We will also show that both sides of the equation transform equivalently under any invertible elementary row operation; hence equation (B.7) will hold for any basis.

We start by showing that $\langle -T, T' \rangle = \langle T, T' \rangle^{-1} = \langle T, -T' \rangle$ for any $T, T' \in E[3]$. Suppose that these form a basis, and compare M_T and M_{-T}; the entry in position i, j flips signs when $i + j$ is even, so we have

$$\begin{bmatrix} * & 0 & * \\ 0 & 0 & 0 \\ * & 0 & * \end{bmatrix} = I + M_T + M_{-T}$$

after checking that the $(2,2)$-entry is $1 - \frac{1}{2} - \frac{1}{2} = 0$. We ignore entries marked $*$. Next we multiply through by $M_{T'}$ on the right:

$$\begin{aligned} \begin{bmatrix} * & 0 & * \\ 0 & 0 & 0 \\ * & 0 & * \end{bmatrix} M_{T'} &= M_{T'} + M_T M_{T'} + M_{-T} M_{T'} \\ &= M_{T'} + \langle T, T' \rangle M_{T'+T} + \langle -T, T' \rangle M_{T'-T} \end{aligned} \tag{B.9}$$

and compare $(2,2)$-entries to deduce that

$$1 + \langle T, T' \rangle + \langle -T, T' \rangle = 0.$$

Since each term is among $1, \omega, \omega^2$, we deduce that all three values are represented by the three terms above (recalling that $1 + \omega + \omega^2 = 0$.) Thus $\langle -T, T' \rangle = \langle T, T' \rangle^{-1}$; a similar argument where we multiply by $M_{T'}$ on the left leads to $\langle T', -T \rangle = \langle T', T \rangle^{-1}$. From this it follows that for any $T, T' \in E[3]$ and $i, k \in \mathbb{Z}$, we have $\langle iT, kT' \rangle = \langle T, T' \rangle^{ik}$.

Next we will show that $\langle T, T' \rangle = \langle T', T \rangle^{-1}$ and $\langle T, T \pm T' \rangle = \langle T, T' \rangle = \langle T \pm T', T' \rangle$ for any $T, T' \in E[3]$. We start with the definition $\langle T, T' \rangle I = M_T M_{T'} M_{-T-T'}$, conjugate by $M_{T+T'}$, and then invert both sides:

$$\begin{aligned} \langle T, T' \rangle I &= M_{-T-T'} \langle T, T' \rangle I M_{T+T'} = M_{-T-T'} M_T M_{T'} \\ \langle T, T' \rangle^{-1} I &= M_{-T'} M_{-T} M_{T+T'} = \langle -T', T \rangle^{-1} I = \langle T', T \rangle I \end{aligned}$$

so $\langle T, T' \rangle = \langle T', T \rangle^{-1}$. The first equation then also tells us that

$$\langle T, T' \rangle = \langle -T - T', T \rangle = \langle T + T', T \rangle^{-1} = \langle T, T + T' \rangle$$

and we deduce also that $\langle T, T' - T \rangle = \langle T, T + (T' - T) \rangle = \langle T, T' \rangle$. We similarly get that

$$\langle T \pm T', T' \rangle = \langle T', T \pm T' \rangle^{-1} = \langle T', T \rangle^{-1} = \langle T, T' \rangle.$$

Lastly we demonstrate equation (B.8). Consider the entry in position $2, 1$ in equation (B.9), multiplied by -2:

$$0 = m_{T'} + \langle T, T' \rangle m_{T'+T} + \langle -T, T' \rangle m_{T'-T} \tag{B.10}$$

Fore a basis τ_0, τ_1 for $E[3]$, take $T' = -\tau_0 - \tau_1$ and $T = -\tau_0 + \tau_1$; then we have $\langle T, T' \rangle = \langle -\tau_0 + \tau_1, -\tau_0 - \tau_1 \rangle = \langle \tau_0, \tau_1 \rangle^{-1}$ and we get equation (B.8). By comparing this to definition B.1.3 we see that $\omega = \langle T_0, T_1 \rangle$ since $m_{T_0+T_1} = \omega^2 m_{T_0} + \omega m_{T_1}$. □

As an addendum, we note the following, where $n_T := 2b_T + y_T = \frac{9a + m_T^4}{6m_T}$:

Lemma B.4.4. *Suppose $\tau_0, \tau_1 \in E[3]$ form a basis. Then for i, j, k, l in modulus 3, we have*

$$\begin{aligned} m_{\tau_0+\tau_1} &= \langle \tau_1, \tau_0 \rangle m_{\tau_0} + \langle \tau_0, \tau_1 \rangle m_{\tau_1} \\ n_{\tau_0+\tau_1} &= \langle \tau_1, \tau_0 \rangle n_{\tau_0} + \langle \tau_0, \tau_1 \rangle n_{\tau_1} \end{aligned}$$

B.5 Trilinear Forms

Now we give explicit relations between the T-determinant forms, using the notation from definition B.4.2. For example, $d_{\mathcal{O}} + d_T + d_{-T} = 0$, and $d_{T_0+T_1} = -\omega d_{-T_0} - \omega^2 d_{-T_1}$:

Lemma B.5.1. *For distinct $\tau_0, \tau_1 \in E[3]$ we have*

$$d_{\tau_0+\tau_1} = -\langle \tau_0, \tau_1 \rangle d_{-\tau_0} - \langle \tau_1, \tau_0 \rangle d_{-\tau_1}$$

Proof. We first show that $d_{\mathcal{O}} + d_T + d_{-T} = 0$ for any $T \in E[3] \backslash \{\mathcal{O}\}$. Recall that $d_T(v_1, v_3, v_2) = -d_{-T}(v_1, v_2, v_3)$, and hence $d_{\mathcal{O}} + d_T + d_{-T}$ is an alternating trilinear form. So we must have $d_{\mathcal{O}} + d_T + d_{-T} = c d_{\mathcal{O}}$ for some constant c, and we will show that $c = 0$. By definition, and using the fact that $\det(M_{-T}) = 1$, we get:

$$\begin{aligned} &(d_{\mathcal{O}} + d_T + d_{-T})(M_{-T} v_1, v_2, v_3) \\ =& \det(M_{-T} v_1, v_2, v_3) + \det(M_{-T} v_1, M_T v_2, M_{-T} v_3) + \det(M_{-T} v_1, M_{-T} v_2, M_T v_3) \\ =& \det(M_{-T} v_1, v_2, v_3) + \det(v_1, M_{-T} v_2, v_3) + \det(v_1, v_2, M_{-T} v_3) \end{aligned}$$

then by plugging in $[v_1\ v_2\ v_3] = I$ we get the trace of M_{-T}, which is 0, so $d_{\mathcal{O}} + d_T + d_{-T} = 0$.

Continuing from this equation, suppose that $T' \in E[3]$. Then we get:

$$\begin{aligned}
0 =& (d_{\mathcal{O}} + d_T + d_{-T})(v_1, M_{T'}v_2, M_{-T'}v_3) \\
=& \det(v_1, M_{T'}v_2, M_{-T'}v_3) \\
&+ \det(v_1, M_T M_{T'}v_2, M_{-T}M_{-T'}v_3) \\
&+ \det(v_1, M_{-T}M_{T'}v_2, M_T M_{-T'}v_3) \\
=& \det(v_1, M_{T'}v_2, M_{-T'}v_3) \\
&+ \det(v_1, \langle T, T'\rangle M_{T+T'}v_2, \langle -T, -T'\rangle M_{-T-T'}v_3) \\
&+ \det(v_1, \langle -T, T'\rangle M_{T'-T}v_2, \langle T, -T'\rangle M_{T-T'}v_3) \\
=& \det(v_1, M_{T'}v_2, M_{-T'}v_3) \\
&+ \langle T', T\rangle \det(v_1, M_{T+T'}v_2, M_{-T-T'}v_3) \\
&+ \langle T, T'\rangle \det(v_1, M_{T'-T}v_2, M_{T-T'}v_3) \\
=& (d_{T'} + \langle T', T\rangle d_{T'+T} + \langle T, T'\rangle d_{T'-T})(v_1, v_2, v_3)
\end{aligned}$$

Hence $d_{T'} + \langle T', T\rangle d_{T'+T} + \langle T, T'\rangle d_{T'-T} = 0$ and we get the desired result by taking $T' = \tau_0 + \tau_1$ and $T = \tau_0 - \tau_1$, so $\langle T', T\rangle = \langle \tau_0 + \tau_1, \tau_0 - \tau_1\rangle = \langle \tau_0, \tau_1\rangle$. □

We now write down a convenient representation for e_0, e_1. Recall:

$$\begin{aligned}
\begin{bmatrix} d_{\mathcal{O}} \\ e_0 \\ e_1 \end{bmatrix} =& \begin{bmatrix} 1 & 0 & 0 \\ \frac{-1}{2} & \frac{-x_{T_0}}{2y_{T_0}} & \frac{-1}{2y_{T_0}} \\ \frac{-1}{2} & \frac{-x_{T_1}}{2y_{T_1}} & \frac{-1}{2y_{T_1}} \end{bmatrix}^{-1} \begin{bmatrix} d_{\mathcal{O}} \\ d_{T_0} \\ d_{T_1} \end{bmatrix} \\
=& \frac{-1}{x_{T_0} - x_{T_1}} \begin{bmatrix} -(x_{T_0} - x_{T_1}) & 0 & 0 \\ y_{T_0} - y_{T_1} & 2y_{T_0} & -2y_{T_1} \\ x_{T_0}y_{T_1} - x_{T_1}y_{T_0} & -2x_{T_1}y_{T_0} & 2x_{T_0}y_{T_1} \end{bmatrix} \begin{bmatrix} d_{\mathcal{O}} \\ d_{T_0} \\ d_{T_1} \end{bmatrix}
\end{aligned}$$

and we can simplify this as follows:

Lemma B.5.2. *e_0, e_1 can be written as linear combinations of $d_{\mathcal{O}}, d_{T_0}, d_{T_1}$. Explicitly:*

$$\begin{aligned}
e_0 =& \frac{-m_{T_3}}{3\sqrt{-3}}\ d_{\mathcal{O}} + \frac{m_{T_2} - m_{T_3}}{3\sqrt{-3}}\ d_{T_0} - \frac{m_{T_2} + m_{T_3}}{3\sqrt{-3}}\ d_{T_1} \\
e_1 =& \frac{m_{T_3}x_{T_0} - \sqrt{-3}y_{T_0}}{\sqrt{-3}}\ d_{\mathcal{O}} + \frac{(m_{T_3} - m_{T_2})x_{T_1}}{3\sqrt{-3}}\ d_{T_0} + \frac{(m_{T_2} + m_{T_3})x_{T_0}}{\sqrt{-3}}\ d_{T_1}
\end{aligned}$$

and furthermore,

$$\left(\frac{e_0}{d_{\mathcal{O}}}, \frac{e_1}{d_{\mathcal{O}}}\right) = (m_\Delta, b_\Delta)$$

B.6 Hessian Form of Elliptic Curve

The Hessian form of an elliptic curve is especially well suited to our operation. Here we have a parameter α, and our elliptic curve is given in projective form as:

$$E_\alpha \ : \ x^3 + y^3 + z^3 - 3\alpha xyz = 0$$
$$\mathcal{O} = (-1 : 1 : 0)$$

This equation for E_α makes certain symmetries apparent.

Firstly, E_α is invariant under permutations of (projective) coordinates. Secondly, a primitive cube root ω of 1 provides the symmetry $(x : y : z) \mapsto (\omega x : \omega^2 y : z)$. These operations have simple group-theoretic descriptions in E_α:

- The permutation $(x : y : z) \mapsto (y : x : z)$ corresponds to negation.
- The cyclic shift $(x : y : z) \mapsto (y : z : x)$ corresponds to addition of the three torsion point $(0 : -1 : 1)$.
- The map $(x : y : z) \mapsto (\omega x : \omega^2 y : z)$ corresponds to addition of the three torsion point $(-\omega : 1 : 0)$.

To define the addition operation on these curves, we first consider three torsion so that we can use section 7.2.3 to get nice formulas.

B.6.1 Three Torsion

The three torsion points correspond exactly to those where one of the coordinates is 0. For example, the origin $(-1 : 1 : 0)$ has triple intersection with the line $x + y + \alpha z = 0$, since that function vanishes to order three:

$$x^3 + y^3 + z^3 - 3\alpha xyz = (x + y + \alpha z)((\alpha z - x)(\alpha z - y) + (x - y)^2) - (1 - \alpha^3)z^3$$

The three torsion subgroup of $E\alpha$ can be presented as follows (in additive notation):

$$E_\alpha[3] = \langle T, T_0 \ \mid \ 3T = 3T_0 = \mathcal{O},\ T + T_0 = T_0 + T \rangle$$
$$T = (-\omega : 1 : 0)$$
$$T_0 = (0 : -1 : 1)$$

with addition table:

$+$	$\mathcal{O}$	T	$-T$
$\mathcal{O}$	$(-1 : 1 : 0)$	$(-\omega : 1 : 0)$	$(-\omega^2 : 1 : 0)$
T_0	$(0 : -1 : 1)$	$(0 : -\omega : 1)$	$(0 : -\omega^2 : 1)$
$-T_0$	$(-1 : 0 : 1)$	$(-\omega^2 : 0 : 1)$	$(-\omega : 0 : 1)$

B.6.2 Addition Formulas

Here we will derive the addition formulas (as in section 7.2.3.) To do so, we will characterize points $P_0, P_1, P_2 \in E_\alpha$ satisfying $P_0 + P_1 + P_2 = \mathcal{O}$. To simplify notation, let $x_i := x(P_i)$ and $y_i := y(P_i)$ for $i = 0, 1, 2$. First we note that summing to $\mathcal{O}$ is equivalent to the collinearity of P_0, P_1, P_2; we can express this in terms of a vanishing determinant:

$$0 = \begin{vmatrix} x_0 & x_1 & x_2 \\ y_0 & y_1 & y_2 \\ 1 & 1 & 1 \end{vmatrix} = (x_0y_1 + x_1y_2 + x_2y_0) - (x_0y_2 + x_1y_0 + x_2y_1)$$

We will obtain two further relations which will allow us to determine (x_2, y_2). To this end, note that for any $Q \in E_\alpha$, we have collinearity between $P_0, P_1 + Q, P_2 - Q$. We can now exploit the fact that adding three torsion gives a linear operator. If we take Q to be T or T_0 from section B.6.1, then we get:

$$0 = \begin{vmatrix} x_0 & \omega^2 x_1 & \omega x_2 \\ y_0 & \omega y_1 & \omega^2 y_2 \\ 1 & 1 & 1 \end{vmatrix} = \omega(x_0y_1 + x_1y_2 + x_2y_0) - \omega^2(x_0y_2 + x_1y_0 + x_2y_1)$$

$$0 = \begin{vmatrix} x_0 & y_1 & 1 \\ y_0 & 1 & x_2 \\ 1 & x_1 & y_2 \end{vmatrix} = (1 + x_0x_1x_2 + y_0y_1y_2) + (x_0y_2 + x_1y_0 + x_2y_1)$$

We can then combine these relations into a simpler form:

$$\begin{aligned} 0 &= x_0y_1 + x_1y_2 + x_2y_0 \\ 0 &= x_0y_2 + x_1y_0 + x_2y_1 \\ 0 &= 1 + x_0x_1x_2 + y_0y_1y_2 \end{aligned}$$

And these last equation allows us to solve for (x_2, y_2) in an overdetermined system:

$$\begin{aligned} (x_2, y_2) &= \left(\frac{x_1^2y_0 - x_0^2y_1}{x_0y_0 - x_1y_1}, \frac{x_0y_1^2 - x_1y_0^2}{x_0y_0 - x_1y_1} \right) \\ &= \left(\frac{x_0y_0y_1^2 - x_1}{x_0x_1^2 - y_0^2y_1}, \frac{y_0 - x_0^2x_1y_1}{x_0x_1^2 - y_0^2y_1} \right) \\ &= \left(\frac{x_1y_0^2y_1 - x_0}{x_0^2x_1 - y_0y_1^2}, \frac{y_1 - x_0x_1^2y_0}{x_0^2x_1 - y_0y_1^2} \right) \end{aligned}$$

Then we negate to get the addition operation:

$$\begin{aligned}(x_0, y_0) + (x_1, y_1) &= \left(\frac{x_0 y_1^2 - x_1 y_0^2}{x_0 y_0 - x_1 y_1}, \frac{x_1^2 y_0 - x_0^2 y_1}{x_0 y_0 - x_1 y_1}\right) \\ &= \left(\frac{y_0 - x_0^2 x_1 y_1}{x_0 x_1^2 - y_0^2 y_1}, \frac{x_0 y_0 y_1^2 - x_1}{x_0 x_1^2 - y_0^2 y_1}\right) \\ &= \left(\frac{y_1 - x_0 x_1^2 y_0}{x_0^2 x_1 - y_0 y_1^2}, \frac{x_1 y_0^2 y_1 - x_0}{x_0^2 x_1 - y_0 y_1^2}\right)\end{aligned}$$