


Spring 2020

n-cycle Splines over Sexy Rings

Jacob Tilden Cummings
Bard College

Follow this and additional works at: https://digitalcommons.bard.edu/senproj_s2020

 Part of the [Algebra Commons](#), and the [Number Theory Commons](#)



This work is licensed under a [Creative Commons Attribution-NonCommercial-No Derivative Works 4.0 License](#).

Recommended Citation

Cummings, Jacob Tilden, "n-cycle Splines over Sexy Rings" (2020). *Senior Projects Spring 2020*. 328.
https://digitalcommons.bard.edu/senproj_s2020/328

This Open Access work is protected by copyright and/or related rights. It has been provided to you by Bard College's Stevenson Library with permission from the rights-holder(s). You are free to use this work in any way that is permitted by the copyright and related rights. For other uses you need to obtain permission from the rights-holder(s) directly, unless additional rights are indicated by a Creative Commons license in the record and/or on the work itself. For more information, please contact digitalcommons@bard.edu.

n-cycle Splines over Sexy Rings

A Senior Project submitted to
The Division of Science, Mathematics, and Computing
of
Bard College

by
Jacob T. Cummings

Annandale-on-Hudson, New York
Month of Graduation, Year of Graduation

Abstract

In this project we abstract the work of previous bard students by introducing the concept of splines over non-integers, non-euclidean domains, and even non-PIDs. We focus on n -cycles for some natural number n . We show that the concept of flow up class bases exist in PID splines the same way they do in integer splines, remarking the complications and intricacies that arise when abstracting from the integers to PIDs. We also start from scratch by finding a flow up class basis for n -cycle splines over the real numbers adjoin two indeterminates, denoted $\mathbb{R}[x,y]$ which necessitate more original techniques.

Contents

Abstract	iii
Dedication	vii
Acknowledgments	ix
1 Introduction	1
2 Preliminaries	5
2.1 Number Theory	5
2.2 Ring Theory	8
3 Generalized Integer Splines	13
3.1 Definitions and Examples of Generalized Integer splines	13
3.2 Splines form a \mathbb{Z} -module over commutative rings	15
3.3 Flow-up classes	17
4 Greatest Common Divisors and Least Common Multiples in Commutative Rings	25
4.1 Gcds and Lcms in Commutative Rings	25
5 Splines over arbitrary PIDs	35
5.1 Intro	35
5.2 n-cycle splines form a module over commutative rings	36
5.3 Definition of PID Splines	37
6 Splines over $\mathbb{R}[x, y]$	43
6.1 Introduction to $\mathbb{R}[x, y]$	43
6.2 Definitions and examples of $\mathbb{R}[x, y]$ splines	44
6.3 Bases of $\mathbb{R}[x, y]$	45

7 Future Work	53
Bibliography	55

Dedication

For my parents who loved me even when I did not. For Ty and Anthony who made me laugh even when I thought I could not.

Acknowledgments

I would not be as capable in mathematics without my first professors. I was originally supposed to be a psychology major but the faculty at Bard showed me a whole new world in mathematics that I could not help but explore.

Thanks to Steve Simon for breaking me in my first semester at Bard. Thanks to Lauren Rose for so eloquently introducing me to pure mathematics. Thanks to John Cullinan for guiding me in my now (definitely not then) favorite sect of math, number theory. Thanks to Stefan Méndez-Diez for allowing me to explore applied math before I became so totally engrossed by pure math.

Finally, I cannot express the intensity of my gratitude towards Lauren Rose. Without her guidance I would have been so lost in the overwhelming body of knowledge that I encountered working on this project. When I thought my work was not substantial enough, she reaffirmed me. When I was unable to continue working, she motivated me to push on, assuring me every step of the way that I would eventually finish everything. It has truly been a pleasure to work with you, Lauren. I am lucky to have had you by my side during this particularly trying era of my Bard career.

1

Introduction

Before this project I had no idea what splines were. To a certain extent, that is still the case.

A spline is a collection of piece-wise polynomial functions meant to emulate some other function, usually one too elaborate or inefficient to use. The function to be emulated may simply have no closed form hence the need for a spline. These splines are for smoothing and data interpolation. The former is what makes it possible to conjure big beautiful symbols like the ampersand on your screen.



Figure 1.0.1. Look at that Ampersand

The latter is what enables us to take a set of data points (maybe on a Cartesian plane) and formulate a smooth, continuous, meaningful function to represent those data points. This interpolation can help us to approximate other potential data points that lie between the already existing ones.

As exciting as this all sounds pure math is always more fascinating. Thus we will be exploring a generalization of this concept. Gjonik generalized the polynomial splines to integer splines.

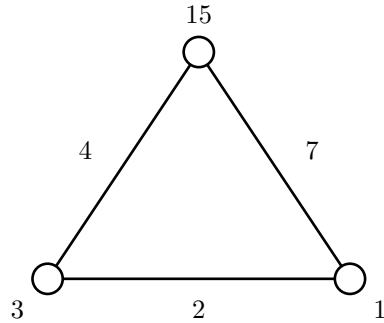


Figure 1.0.2. A three cycle spline

We have some graph whose edges and vertices are labeled with integers; fittingly the integers are called edge labels and vertex labels, respectively. If two vertices are connected by an edge then the two vertex labels must be congruent to each other modulo the edge label which connects them. Observe the graphical representation of a spline, Figure 1.0.3. Indeed, the defining system of congruences holds:

$$15 \equiv 1 \pmod{7}$$

$$1 \equiv 3 \pmod{2}$$

$$3 \equiv 15 \pmod{4}$$

Thus, it meets the qualifications and it is a spline. As the graphs get more elaborate and the edge labels more restricted things get more complicated. In this project we make another abstraction, changing the vertex and edge labels from integers to elements of an arbitrary principal ideal domain as well as a specific unique factorization domain. As the title suggests, these splines are much sexier.

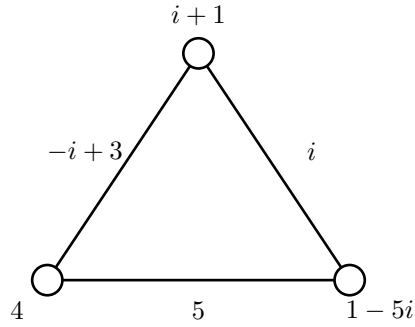


Figure 1.0.3. A three cycle spline

Above is what may or may not be a graphical representation of a spline over the set of Gaussian integers, which is of course not exactly the integers. Along with this abstraction comes interrogating everything we know about the integers and seeing what carries over to a PID like the Gaussian integers. Moreover, we must understand *how* it may carry over.

In this project we focus on n-cycle splines. That is, splines on n-cycles.

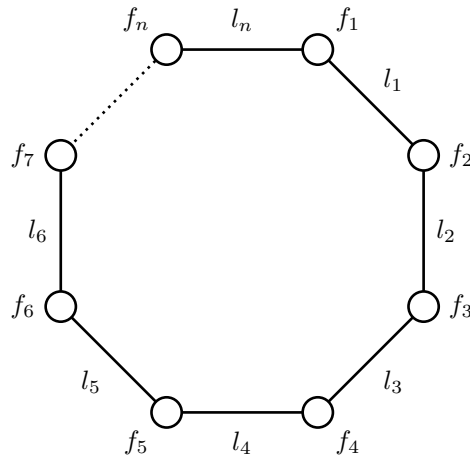


Figure 1.0.4. An n-cycle spline

Figure 1.0.4 is an edge labeled, vertex labeled, n-cycle graph. The dashed side represents the $n - 7$ edges and the $n - 8$ vertices that are between vertex f_7 and vertex f_n . Figure 1.0.4

represents a spline if and only if the defining system of congruences is satisfied.

$$\begin{aligned}
 f_1 &\equiv f_2 \pmod{l_1} \\
 f_2 &\equiv f_3 \pmod{l_2} \\
 &\vdots \\
 f_{n-1} &\equiv f_n \pmod{l_{n-1}} \\
 f_n &\equiv f_1 \pmod{l_n}
 \end{aligned}$$

We list a brief outline of our chapters:

In Chapter 2, we introduce the reader to basic number theory and ring theory.

In Chapter 3, we summarize some of the work done by Handschy, Melnick, and Reinders [7], Gjoni [5] and Madhavi [6] on Generalized integer splines to prepare the reader for the abstractions of Chapter 5 and 6.

In Chapter 4, we generalize many of our number theory concepts, like greatest common divisors and least common multiples, to more general rings like PIDs and UFDs.

In Chapter 5, we generalize many of the theorems from the work of Handschy et al., Gjoni, and Madhavi to Splines over arbitrary Principal Ideal Domains, noting similarities and complications along the way.

In Chapter 6, we start from scratch with a non-PID by approaching splines over $\mathbb{R}[x, y]$ with linearly dependant edge labels.

2

Preliminaries

2.1 Number Theory

Definition 2.1.1. Let a and $b \in \mathbb{Z}$. We say a *divides* b , denoted $a|b$, if there exists some $k \in \mathbb{Z}$ such that $ak = b$. △

Theorem 2.1.2. Let a, b and $c \in \mathbb{Z}$. If $a|b$ and $b|c$ then $a|c$.

Proof. By hypothesis $a|b$ and $b|c$. Then $ak_1 = b$ and $bk_2 = c$. Then by substitution $ak_1k_2 = c$. Then $a|c$. □

Definition 2.1.3. Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{N}$. We say a is *congruent to b modulo m* , denoted $a \equiv b \pmod{m}$, if $m|a - b$. △

Note, that, by the definition of divisibility this means there exists some $x \in \mathbb{Z}$ such that $mx = a - b$. Thus, it is valid to skip straight from $a \equiv b \pmod{m}$ to $mx = a - b$.

Theorem 2.1.4. [1, Chapter 3 Definition 3.1] Let m be an element of \mathbb{Z} . Congruence modulo m is an equivalence class. In other words, for all $a, b, c \in \mathbb{Z}$

$$(i) a \equiv b \pmod{m}, b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$$

$$(ii) a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$$

$$(iii) a \equiv a$$

Definition 2.1.5. [1, pg. 98] The *greatest common divisor* of the integers a_1, a_2, \dots, a_n , which are all not zero, is the greatest positive integer that divides all the integers a_1, a_2, \dots, a_n . \triangle

The following theorem provides another way to define greatest common divisor. We will use this definition instead of the previous one when we are in arbitrary rings that do not necessarily have a concept of "greatness" or "largeness".

Theorem 2.1.6. [1, Theorem 3.10] $d \in \mathbb{Z}$ is a **common divisor** of two elements $a_1, a_2, \dots, a_n \in R$, if $d|a_1, a_2, \dots, a_n$. Let $c \in \mathbb{Z}$. If, c is a common divisor of $a_1, a_2, \dots, a_n \Rightarrow c|d$, then d is a **greatest common divisor**.

Theorem 2.1.7. Let a_1, a_2, \dots, a_n be integers. Then $(a_1, (a_2, a_3, \dots, a_n)) = (a_1, a_2, a_3, \dots, a_n)$.

Proof. Let $d_1 = (a_1, (a_2, a_3, \dots, a_n))$, $d_2 = (a_1, a_2, a_3, \dots, a_n)$ and let D_1 be the set of all divisors of d_1 and D_2 be all the divisors of d_2 . Note that $d_1 \in D_1$ and $d_2 \in D_2$. Now let $c_1 \in D_1$. Then $c_1|d_1 = (a_1, (a_2, a_3, \dots, a_n))$. Then $c_1|a_1$ and $c_1|(a_2, a_3, \dots, a_n)$. Then $c_1|a_2, a_3, \dots, a_n$. Then $c_1|a_i$ for all i . In other words, c_1 is a common divisor of all the a_i . Then by Theorem 2.1.6 we know $c_1|(a_1, a_2, a_3, \dots, a_n) = d_2$. Then $c_1 \in D_2$. Then $D_1 \subset D_2$. Now suppose that $c_2 \in D_2$. Then $c_2|d_1 = (a_1, a_2, a_3, \dots, a_n)$. Then $c_2|a_1, a_2, a_3, \dots, a_n$. Since $c_2|a_2, a_3, \dots, a_n$ we know $c_2|(a_2, a_3, \dots, a_n)$. Since $c_2|(a_2, a_3, \dots, a_n)$ and $c_2|a_1$ we know $c_2|(a_1, (a_2, a_3, \dots, a_n)) = d_1$. Then $c_2 \in D_1$. Then $D_2 \subset D_1$. Then $D_2 = D_1$. Since $d_1 \in D_2$ and $c|d_1$ for all $c \in D_2$, d_1 is a greatest common divisor of $a_1, a_2, a_3, \dots, a_n$. Since gcds are unique in the integers we know that $d_1 = (a_1, a_2, a_3, \dots, a_n) = d_2$. \square

Definition 2.1.8. [1, pg. 123] The *least common multiple* of the integers a_1, a_2, \dots, a_n , which are all not zero, is the smallest positive integer that is divisible by all the integers a_1, a_2, \dots, a_n . \triangle

The following theorem provides another way to define least common multiples. We will use this definition instead of the previous one when we are in arbitrary rings that do not necessarily have a concept of "smallness".

Theorem 2.1.9. [3, Theorem 3.8] $m \in \mathbb{Z}$ is a **common multiple** of $a_1, a_2, \dots, a_n \in \mathbb{Z}$ if $a_1, a_2, \dots, a_n | m$. If $c \in \mathbb{Z}$ is a common multiple of $a_1, a_2, \dots, a_n \Rightarrow m | c$ then m is a **least common multiple**.

Theorem 2.1.10. Let $m_1, m_2, \dots, m_k, \alpha, m^* \in \mathbb{Z}$ and m^* is a least common multiple of m_1, m_2, \dots, m_k . If $m_1, m_2, \dots, m_k | \alpha$ then $m^* | \alpha$.

Proof. By hypothesis α is a common multiple of m_1, m_2, \dots, m_k . By Theorem 2.1.9 m^* divides every common multiple of m_1, m_2, \dots, m_k . Then $m^* | \alpha$. \square

Because of the nature of splines, we will be working with systems of congruences often. The following corollary will be useful when we need to make generalizations regarding particular components of our splines.

Corollary 2.1.11. Let $m_1, m_2, \dots, m_n, \alpha, \theta \in \mathbb{Z}$. If

$$\begin{aligned} \alpha &\equiv \theta \pmod{m_1} \\ \alpha &\equiv \theta \pmod{m_2} \\ \alpha &\equiv \theta \pmod{m_3} \\ &\vdots \\ \alpha &\equiv \theta \pmod{m_n} \end{aligned}$$

then $\alpha \equiv \theta \pmod{d_k}$ where d_k is a least common multiple of m_1, m_2, \dots, m_n .

Proof. We know by hypothesis that $\alpha \equiv \theta \pmod{m_i}$ for all $1 \leq i \leq n$. Then $m_i | \alpha - \theta$ for all i . Then by Theorem 2.1.10, $d_k | \alpha - \theta$ where d_k is a least common multiple of m_1, m_2, \dots, m_n . Then $\alpha \equiv \theta \pmod{d_k}$ by the definition of congruence. \square

Theorem 2.1.12 (The Chinese Remainder Theorem for non-coprime moduli). [5, Theorem 2.1.23] *Let $x, z_1, z_2, \dots, z_r, m_1, m_2, \dots, m_r$ be integers. The system of congruences*

$$\begin{cases} x \equiv z_1 \pmod{m_1} \\ x \equiv z_2 \pmod{m_2} \\ \vdots \\ x \equiv z_r \pmod{m_r} \end{cases}$$

has a solution if and only if $(m_i, m_j) | z_i - z_j$ for every pair of integers (i, j) where $1 \leq i < j \leq r$.

This theorem, like corollary 2.1.11, will be essential for generalizing the form of some of our splines. We will abstract this theorem to PIDs as well.

2.2 Ring Theory

Recall that a ring is a set with two binary operations, usually referred to as addition and multiplication, in which the distributive law and associative law exist. The commutative law also exists for addition but not necessarily for multiplication. Now we will define the most general type of ring that will be discussed in this paper.

Definition 2.2.1. [4, Chapter 1 Definition 1.1] A ring in which multiplication is also commutative is called a *commutative ring*. △

Unless otherwise stated, rings in this document will be assumed to be commutative.

Definition 2.2.2. Let e be an element of a commutative ring, R . If, for all $r \in R$, $er = r$, e is a *multiplicative identity element*. △

From now on an identity element of a ring will be denoted by either 1 or occasionally 1_R and we will assume that every ring we encounter has a multiplicative identity element.

Definition 2.2.3. Let u be an element of some commutative ring, R . If u has a multiplicative inverse, u^{-1} , such that $uu^{-1} = 1_R$, then u is a *unit*. △

Definition 2.2.4. [4, Chapter 3 Definition 3.1] Let a and b be elements of a commutative ring, R . If $a|b$ and $b|a$ then b is an *associate* of a and vice versa. △

Theorem 2.2.5. *Let a be an element of a commutative ring, R . Let U be the set of all units of R . Then for all $u \in U$ au is an associate of a .*

Proof. To prove this we must show that $a|au$ and $au|a$. We know $au(u^{-1}) = a(1) = a$. Then $au|a$. Also $a(u) = au$. Then $a|au$ by definition. Thus, a and au are associates. \square

Definition 2.2.6. [4, Chapter 1 Definition 1.3] A nonzero element, a , of a commutative ring, R , is said to be a *zero divisor* if there exists a nonzero element $b \in R$ such that $ab = 0$. \triangle

It is easy to verify that a ring R has no zero divisors if and only if the right and left cancellation laws hold in R ; that is, for all $a, b, c \in R$ with $a \neq 0$,

$$ab = ac \text{ or } ba = ca \Rightarrow b = c$$

The concept of 'division' is not always present in rings which makes the cancellation property particularly valuable in these arbitrary rings. We will now define rings that have the cancellation property.

Definition 2.2.7. A commutative ring R with no zero divisors is called an *integral domain*. \triangle

We now define irreducibles and primes.

Definition 2.2.8. [3, 45.4] An element, p , of an integral domain R is an *irreducible* if for every factorization, $p = ab$, either a or b is unit. \triangle

Definition 2.2.9. [3, Definition 45.13] A nonzero, nonunit element of an integral domain R is a *prime* if, for all $a, b \in R$, $p|ab \Rightarrow p|a$ or $p|b$. \triangle

Definition 2.2.10. [4, Chapter 3 Definition 3.5] An integral domain R is a *Unique Factorization Domain* or UFD provided that:

- (i) any non-unit, non-zero element can be expressed as a product of irreducibles.
- (ii) If for all $a \in R$ $a = c_1c_2 \dots c_n$ and $a = d_1d_2 \dots d_m$, (c_i, d_i are irreducibles) then $n = m$ and for some permutation σ of $\{1, 2, \dots, n\}$, c_i and $d_{\sigma(i)}$ are associates for every i . \triangle

Essentially this means that if x is an element of a UFD then it can be factored into irreducibles. Moreover, any other factorization of x into irreducibles must have irreducibles that are associates of the irreducibles in the original factorization. That is the scope of the uniqueness.

Corollary 2.2.11. *The ring of all real numbers is a UFD.*

Proof. The real numbers has no nonzero, nonunit elements. Thus it fits the definition of a UFD. \square

Theorem 2.2.12. [3, pg. 394] *Every irreducible element of a UFD is prime.*

Definition 2.2.13. [4, Chapter 3 Definition 2.1] Let R be a ring and S a nonempty subset of R that is closed under the operations of addition and multiplication in R . If S is itself a ring under these operations then S is called a subring of R . A subring I of a ring R is an *ideal* provided,

$$r \in R \text{ and } x \in I \Rightarrow rx \in I$$

\triangle

Theorem 2.2.14. [4, Chapter 3 Theorem 2.2] *A nonempty I subset of a ring R is an ideal if and only if for all $a, b \in I$ and $r \in R$.*

$$(i) a, b \in I \Rightarrow a - b \in I \tag{2.2.1}$$

$$(ii) a \in I, r \in R \Rightarrow ra \in I \tag{2.2.2}$$

Note that, since rings have additive inverses, the first equation could just as easily be $a + b$ instead of $a - b$.

Definition 2.2.15. Let x_1, x_2, \dots, x_n be an element of a ring R . Then $\langle x_1, x_2, \dots, x_n \rangle$, called the *set generated by x_1, x_2, \dots, x_n* , is precisely equal to $\{x | x = r_1x_1 + r_2x_2 + \dots + r_nx_n\}$ for $r_1, r_2, \dots, r_n \in R$. In other words, $\langle x_1, x_2, \dots, x_n \rangle$ is the set of all linear combinations of x_1, x_2, \dots, x_n . \triangle

Theorem 2.2.16. *Let x_1, x_2, \dots, x_n be an element of a ring R . Then $\langle x_1, x_2, \dots, x_n \rangle$ is an ideal.*

Proof. We will use Theorem 2.2.14 to prove this theorem. Let $I = \langle x_1, x_2, \dots, x_n \rangle$. We will first show that for all $a, b \in I$, it is the case that $a - b \in I$. Note that since $a, b \in I$, we know that for some $r_1, r_2, \dots, r_n, s_1, s_2, \dots, s_n \in R$, $a = r_1x_1 + r_2x_2 + \dots + r_nx_n$ and $b = s_1x_1 + s_2x_2 + \dots + s_nx_n$. Then $a - b = (r_1x_1 + r_2x_2 + \dots + r_nx_n) - (s_1x_1 + s_2x_2 + \dots + s_nx_n) = (r_1 - s_1)x_1 + (r_2 - s_2)x_2 + \dots + (r_n - s_n)x_n$. Since $r_i - s_i \in R$ we know that $a - b$ is generated by x_1, x_2, \dots, x_n . Thus $a - b \in I$.

Now we will show that for all $a \in I$ and $k \in R$ $ak \in I$. Note that since $a \in I$ that $a = r_1x_1 + r_2x_2 + \dots + r_nx_n$. Then $ak = k(r_1x_1 + r_2x_2 + \dots + r_nx_n) = kr_1x_1 + kr_2x_2 + \dots + kr_nx_n$. Since $k, r_i \in R$ for all i , we know $kr_i \in R$. Then $ak \in I$. Then by Theorem 2.2.14 we conclude that $I = \langle x_1, x_2, \dots, x_n \rangle$ is an ideal. \square

This theorem will be very useful when navigating splines over PIDs, as many theorems about PIDs use this $\langle \rangle$ concept.

We now define PIDs.

Definition 2.2.17. [3, Definition 45.7] R is a *Principal Ideal Domain* or PID if it is an integral domain of which every ideal is principal. i.e. For all $x_1, x_2, \dots, x_n \in R$ there exists some $c \in R$ such that $\langle x_1, x_2, \dots, x_n \rangle = \langle c \rangle$. \triangle

Theorem 2.2.18. [4, Chapter 3 Theorem 3.7] *Every Principal Ideal Domain R is a Unique Factorization Domain.*

Theorem 2.2.19. [3, Corollary 45.30] *If R is a UFD then $R[X_1, X_2, \dots, X_n]$ is also a UFD for $n \in \mathbb{N}$.*

Definition 2.2.20. [4, Chapter 4 Definition 1.1] Let R be a commutative ring. An *R -Module* is an additive abelian group, A , together with a function $R \times A \rightarrow A$ (the image of (r, a) being denoted ra) such that for all $r, s \in R$ and $a, b \in A$:

$$(i) \ r(a+b) = ra + rb$$

$$(ii) \ (r+s)a = ra + sa$$

$$(iii) \ r(sa) = (rs)a$$

If R has an identity element 1_R and

$$(iv) 1_R a = a$$

then A is said to be a *unitary R -module*.

\triangle

Every ring we work with will have an identity element thus every R -module we encounter will be a unitary R -module. So, we will use the term “ R -module” to mean “unitary R -module”.

3

Generalized Integer Splines

3.1 Definitions and Examples of Generalized Integer splines

Definition 3.1.1. Let G be a graph with k edges e_1, e_2, \dots, e_k and n vertices v_1, v_2, \dots, v_n . For $1 \leq i \leq k$, let $l_i \in \mathbb{N}$ be the label on edge e_i so that $L = \{l_1, l_2, \dots, l_k\}$ is the set of edge labels. Then, (G, L) is called an *edge-labeled graph*. \triangle

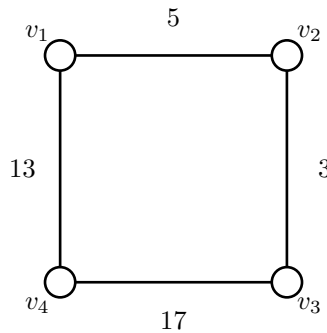
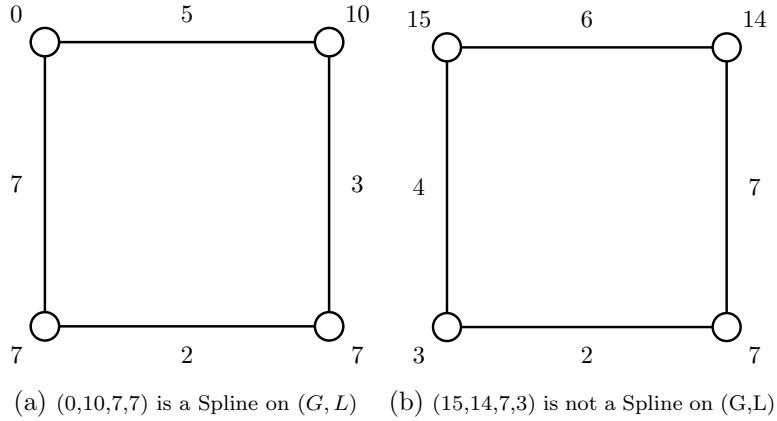


Figure 3.1.1. Edge-labeled 4-cycle graph

As you can see, the figure above is an edge-labeled graph with $L = \{l_1, l_2, l_3, l_4\} = \{5, 3, 17, 13\}$ being the set of edge labels. Note that the difference between e_i and l_i , for any i , is that l_i is a value that we associate with the edge, whereas e_i is referring to the edge itself.

Definition 3.1.2. Let (G, L) be an edge-labeled graph. A *generalized integer spline* is a vertex labeling, $(f_1, f_2, \dots, f_n) \in \mathbb{Z}^n$, such that if vertices v_i and v_j are connected by edge e_k then $f_i \equiv f_j \pmod{l_k}$. We denote the set of all splines on (G, L) by $\mathbb{S}_{(G,L)}$.



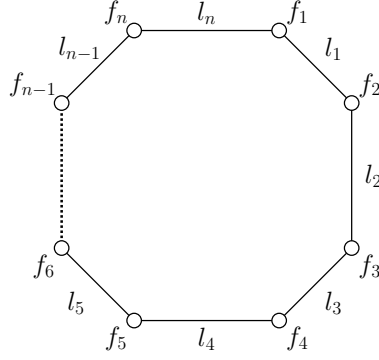
△

Figure (a) is a Spline because $0 \equiv 10 \pmod{5}$, $10 \equiv 7 \pmod{3}$, $7 \equiv 7 \pmod{2}$, and $7 \equiv 0 \pmod{7}$. Figure (b) however is not a spline because $15 \not\equiv 14 \pmod{6}$.

Definition 3.1.3. Let (G, L) be an n -cycle graph with $L = l_1, l_2, \dots, l_n$. An *n -cycle spline* is a vertex labeling $(f_1, f_2, \dots, f_n) \in \mathbb{Z}^n$ such that the following system of congruences holds,

$$\begin{aligned} f_1 &\equiv f_2 \pmod{l_1} \\ f_2 &\equiv f_3 \pmod{l_2} \\ &\vdots \\ f_{n-1} &\equiv f_n \pmod{l_{n-1}} \\ f_n &\equiv f_1 \pmod{l_n} \end{aligned}$$

△



These graphs are useful for proving general theorems about splines that lie on any cycle, i.e. when we prove a theorem for n -cycle splines we also prove that same theorem for 2-cycle splines, 3-cycle splines, 4-cycle splines and so on.

Before we continue, we present a conventional way to number the vertices and edges of an n -cycle graph. In general, vertices v_i and v_{i+1} are connected by edge e_i for $1 \leq i \leq n - 1$ and vertices v_n and v_1 are connected by edge e_n as shown in the edge labeled graph above. The dashed line represents the sequential vertices and edges that lie between f_6 and f_{n-1} .

3.2 Splines form a \mathbb{Z} -module over commutative rings

Theorem 3.2.1. *Let $L = l_1, l_2, \dots, l_n$ where $l_1, l_2, \dots, l_n \in \mathbb{Z}$ and let G be some graph. Let $\mathbb{S}_{(G,L)}$ be the set of all splines with vertex and edge labels in \mathbb{Z} . Then $\mathbb{S}_{(G,L)}$ is a \mathbb{Z} -module.*

Proof. According to definition 3.2.1 to prove this we must show that $\mathbb{S}_{(G,L)}$ is an additive abelian group and for $r, s \in \mathbb{Z}$ and $F, G_1 \in \mathbb{S}_{(G,L)}$ the following four equations hold.

$$(i) \quad r(F + G_1) = rF + rG_1$$

$$(ii) \quad (r + s)F = rF + sF$$

$$(iii) \quad r(sa) = (rs)a$$

$$(iv) \quad 1F = F$$

(the subscript in G_1 is to differentiate the spline G_1 from the graph G) First we will show that $\mathbb{S}_{(G,L)}$ is an abelian group. Let $F = (f_1, f_2, \dots, f_n)$ and $G_1 = (g_1, g_2, \dots, g_n)$ be splines on $\mathbb{S}_{(G,L)}$.

We will first prove the existence of the identity element E . Let $E = (0, 0, \dots, 0)$. Observe that $F + E = (f_1 + 0, f_2 + 0, \dots, f_n + 0) = (f_1, f_2, \dots, f_n) = F$. Thus E is the identity element.

Next we will prove that the additive inverse of an arbitrary element of $\mathbb{S}_{(G,L)}$ is also an element of $\mathbb{S}_{(G,L)}$. Let $-F = (-f_1, -f_2, \dots, -f_n)$. Since F is a spline we know that the following equations hold true.

$$\begin{aligned} f_i &\equiv f_{i+1} \pmod{l_i} \text{ for } 1 \leq i \leq (n-1) \\ f_n &\equiv f_1 \pmod{l_n} \end{aligned}$$

Thus $l_i | f_i - f_{i+1}$ for $1 \leq i \leq n-1$ and $l_n | f_n - f_1$. Thus $f_i - f_{i+1} = p(l_i)$ and $f_n - f_1 = q(l_n)$ for $p, q \in \mathbb{Z}$. Then by multiplying by -1 we get $-f_i - (-f_{i+1}) = -p(l_i)$ and $-f_n - (-f_1) = -q(l_n)$. Then $l_i | -f_{i+1} - (-f_i)$ and $l_n | -f_1 - (-f_n)$. Then $-f_i \equiv -f_{i+1} \pmod{l_i}$ for $1 \leq i \leq (n-1)$ and $-f_n \equiv -f_1 \pmod{l_n}$. Thus $-F \in S_{G,L}$. Because $F + (-F) = E$, we know that every element $F \in S_{G,L}$ has an inverse. Next we will show that $S_{G,L}$ is closed under addition. $F = (f_1, f_2, \dots, f_n) \in S_{G,L}$ and $G = (g_1, g_2, \dots, g_n) \in S_{G,L} \Rightarrow f_i \equiv f_{i+1} \pmod{l_i}$ for $i \leq (n-1)$, $f_n \equiv f_1 \pmod{l_n}$ and $g_i \equiv g_{i+1} \pmod{l_i}$ for $i \leq (n-1)$ $g_n \equiv g_1 \pmod{l_n}$ respectively. Then $f_i - f_{i+1} = m(l_i)$ and $f_n - f_1 = n(l_n)$ for some $m, n \in \mathbb{Z}$ and $g_i - g_{i+1} = p(l_i)$ and $g_n - g_1 = q(l_n)$ for some $p, q \in \mathbb{Z}$. Then by summing the first and third equation we get $(f_i + g_i) - (f_{i+1} + g_{i+1}) = (m + p)(l_i)$. Also, by summing the second and fourth equation we get $(f_n + g_n) - (f_1 + g_1) = (n + q)(l_n)$. Then $l_i | (f_i + g_i) - (f_{i+1} + g_{i+1})$ and $l_n | (f_n + g_n) - (f_1 + g_1)$. Then $(f_i + g_i) \equiv (f_{i+1} + g_{i+1}) \pmod{l_i}$ and $(f_n + g_n) \equiv (f_1 + g_1) \pmod{l_n}$. Then $F + G = (f_1 + g_1, f_2 + g_2, \dots, f_n + g_n) \in \mathbb{S}_{(G,L)}$. Then $\mathbb{S}_{(G,L)}$ is closed under addition.

Then $\mathbb{S}_{(G,L)}$ forms a group under addition. Note that $F + G = (f_1 + g_1, f_2 + g_2, \dots, f_n + g_n) = (g_1 + f_1, g_2 + f_2, \dots, g_n + f_n) = G + F$. Thus $S_{G,L}$ forms an Abelian group.

Next we will prove that $\mathbb{S}_{(G,L)}$ is closed under scalar multiplication. We know $f_i \equiv f_{i+1} \pmod{l_i}$ for $1 \leq i \leq (n-1)$ and $f_n \equiv f_1 \pmod{l_n} \Rightarrow f_i - f_{i+1} = p(l_i)$ and $f_n - f_1 = q(l_n)$ for some $p, q \in \mathbb{Z}$. Then by multiplying each side of both equations by an element of \mathbb{Z} , r , we get $rf_i - rf_{i+1} = rp(l_i)$ and $rf_n - rf_1 = rq(l_n) \Rightarrow l_i | rf_i - rf_{i+1}$ for $i \leq n-1$ and $l_n | rf_n - rf_1 \Rightarrow rf_i \equiv rf_{i+1} \pmod{l_i}$ for $1 \leq i \leq n-1$ and $rf_n \equiv rf_1 \pmod{l_n}$. Then $rF = (rf_1, rf_2, \dots, rf_n) \in S_{G,L}$. Thus we have shown

that $F \in S_{G,L}$ and $r \in Z \Rightarrow rF \in \mathbb{S}_{(G,L)}$ or as the mathematicians say $\mathbb{S}_{(G,L)}$ is closed under scalar multiplication.

Now we will prove equation 1) holds. We know $r \cdot (F + G) = r \cdot (f_1 + g_1, f_2 + g_2, \dots, f_n + g_n) = (r(f_1 + g_1), r(f_2 + g_2), \dots, r(f_n + g_n)) = (rf_1 + rg_1, rf_2 + rg_2, \dots, rf_n + rg_n) = rF + rG$. Thus 1) holds.

Now we will prove equation 2) holds. We know $(r + s) \cdot F = ((r + s)f_1, (r + s)f_2, \dots, (r + s)f_n) = (rf_1 + sf_1, rf_2 + sf_2, \dots, rf_n + sf_n) = r \cdot F + s \cdot F$. Then equation 2) holds.

Now we will prove equation 3) holds. We know $(rs) \cdot F = ((rs)f_1, (rs)f_2, \dots, (rs)f_n) = (r(sf_1), r(sf_2), \dots, r(sf_n)) = r \cdot (sf_1, sf_2, \dots, sf_n) = r \cdot (s \cdot (f_1, f_2, \dots, f_n)) = r \cdot (s \cdot (f_1, f_2, \dots, f_n))$. Then equation 3) holds.

Now we will prove equation 4) holds. $1 \cdot F = (1f_1, 1f_2, \dots, 1f_n) = (f_1, f_2, \dots, f_n) = F$. Then equation 4) holds.

Then integer splines for a \mathbb{Z} -module. □

This means if I take some splines over \mathbb{Z} , let's call them F, G and H, and integers, let's call them x, y and z, I can combine them yielding another spline. i.e. $xF + yG + zH$ is a spline. This will be crucial for proving the existence bases.

3.3 Flow-up classes

Flow-up classes are the essential concept for finding the bases that we will be discussing in this project as each element of a basis will fall into a unique flow-up class.

Definition 3.3.1. Fix the edge labels on (G,L) . Let $1 \leq i \leq n$ (Recall n is the number of vertices as well as the number of edges because we are working with n-cycle graphs). The *i*th flow-up class, denoted by \mathbb{F}_i is the set of all splines with *i* leading zeros. △

Example 3.3.2. Let $F = (0, 0, f_3, \dots, f_n)$ be a spline on (G,L) with $f_3 \neq 0$. Then $F \in \mathbb{F}_2$. Note that f_3 must not be 0 because there must be precisely 2 leading zeroes and if f_3 were zero then

there would be more than 2 leading zeros. With that said, f_4, f_5, \dots, f_n may or may not be zero. Whatever fulfils the congruences suffices enough to be a spline. \diamond

Definition 3.3.3. Let G be an n -cycle with a set of edge labels L . Let \mathbb{F}_i , where $1 \leq i \leq n-1$, be a flow-up class (over integers). Then $f \in \mathbb{F}_i$ is the smallest flow up class element in \mathbb{F} if the leading term f_i of F is less than or equal to the leading term of any other flow up class element in \mathbb{F} . \triangle

The following two theorems are important for proving that potential basis elements span for the integers. We will generalize these theorems to PID splines in the next chapter

Theorem 3.3.4. Let G be an n -cycle. Fix the edge labels on (G, L) , where $L = \{l_1, l_2, \dots, l_n\}$. Let $i \in [1, n] \cap \mathbb{Z}$ and let $F_i = (0, \dots, 0, f_{i+1}, f_{i+2}, \dots, f_n)$ be a an element of \mathbb{F}_i in $\mathbb{S}_{(G, L)}$. Then the leading term, f_{i+1} , is a multiple of $[l_i, (l_{i+1}, \dots, l_n)]$ and $f_{i+1} = [l_i, (l_{i+1}, \dots, l_n)]$ is the smallest value satisfying the l_i and l_{i+1} conditions.

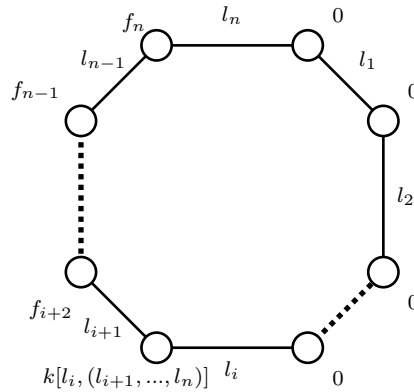


Figure 3.3.1. Element of \mathbb{F}_i

Proof. Figure 3.3.1 represents our $F_i \in \mathbb{F}_i$ with k of course being some integer.

We will use proof by induction for the bulk of this proof. Assume $F_i = (0, \dots, 0, f_{i+1}, f_{i+2}, \dots, f_n)$ is a spline. Then the following system of congruences must hold true.

$$\begin{aligned}
0 &\equiv 0 \pmod{l_1} \\
0 &\equiv 0 \pmod{l_2} \\
&\vdots \\
0 &\equiv f_{i+1} \pmod{l_i} \\
f_{i+1} &\equiv f_{i+2} \pmod{l_{i+1}} \\
&\vdots \\
f_{n-3} &\equiv f_{n-2} \pmod{l_{n-3}} \\
f_{n-2} &\equiv f_{n-1} \pmod{l_{n-2}} \\
f_{n-1} &\equiv f_n \pmod{l_{n-1}} \\
f_n &\equiv 0 \pmod{l_n}
\end{aligned}$$

Figure 3.3.2.

By Theorem 2.1.12 we know that if we take any subsection

$$\begin{aligned}
f_j &\equiv f_{j+1} \pmod{l_j} \\
f_{j+1} &\equiv f_{j+2} \pmod{l_{j+1}}
\end{aligned}$$

where $i \leq j \leq n-1$ (note $f_i = 0$), of two consecutive congruences from the system above, it must be the case that $f_j \equiv f_{j+2} \pmod{(l_j, l_{j+1})}$. The same is true for the last case of

$$\begin{aligned}
f_{n-1} &\equiv f_n \pmod{l_{n-1}} \\
f_n &\equiv 0 \pmod{l_n}
\end{aligned}$$

in which it must be the case that $f_{n-1} \equiv 0 \pmod{(l_{n-1}, l_n)}$. We will approach this case first, the base case. We know that f_n may only exist if $f_{n-1} \equiv 0 \pmod{(l_{n-1}, l_n)}$.

Now for the inductive case. Suppose that

$$\begin{aligned}
f_j &\equiv f_{j+1} \pmod{l_j} \\
f_{j+1} &\equiv 0 \pmod{(l_{j+1}, l_{j+2}, \dots, l_n)}
\end{aligned}$$

and $2 \leq j \leq n-2$ ($j = n-1$ is the base case). By Theorem 2.1.12 it must be the case that $f_j \equiv 0 \pmod{(l_j, (l_{j+1}, l_{j+2}, \dots, l_n))}$. Note, by Theorem 2.1.7 $(l_j, (l_{j+1}, l_{j+2}, \dots, l_n)) = (l_j, l_{j+1}, \dots, l_n)$.

Additionally, observing the first system of congruences in this proof, Figure 3.3.2, we know $f_{j-1} \equiv f_j \pmod{l_{j-1}}$. Then we know the system of congruences

$$\begin{aligned} f_{j-1} &\equiv f_j \pmod{l_{j-1}} \\ f_j &\equiv 0 \pmod{(l_j, l_{j+1}, \dots, l_n)} \end{aligned}$$

holds true. Then by induction $f_j \equiv 0 \pmod{(l_j, l_{j+1}, \dots, l_n)}$ for all $0 \leq j \leq n$.

This means that $f_{i+1} \equiv 0 \pmod{(l_{i+1}, l_{i+2}, \dots, l_n)}$. By the first system in the proof, Figure 3.3.2 we know that $0 \equiv f_{i+1} \pmod{l_i}$. Then by Corollary 2.1.11, we know that $f_{i+1} \equiv 0 \pmod{[l_i, (l_{i+1}, l_{i+2}, \dots, l_n)]}$. Then $[l_i, (l_{i+1}, l_{i+2}, \dots, l_n)] | f_{i+1}$. Then our leading element f_{i+1} is a multiple of $[l_i, (l_{i+1}, l_{i+2}, \dots, l_n)]$. By definition $[l_i, (l_{i+1}, l_{i+2}, \dots, l_n)]$ is the smallest multiple of itself. \square

Theorem 3.3.5. *Fix the edge labels on (G, L) , where $L = \{l_1, l_2, \dots, l_n\}$. $F = (0, \dots, 0, f_n)$ be spline and an element of the $n - 1^{\text{th}}$ flow-up class, \mathbb{F}_{n-1} , in $\mathbb{S}_{(G, L)}$. Then the leading term, f_n , is a multiple of $[a_{n-1}, a_n]$ and $f_n = [a_{n-1}, a_n]$ is the smallest value satisfying the l_n and l_{n-1} conditions.*

Proof. In order for F to be a spline the following system of congruences must be satisfied,

$$\begin{aligned} 0 &\equiv 0 \pmod{l_1} \\ 0 &\equiv 0 \pmod{l_2} \\ &\vdots \\ 0 &\equiv f_n \pmod{l_{n-1}} \\ f_n &\equiv 0 \pmod{l_n} \end{aligned}$$

Figure 3.3.3.

Obviously the first $n - 2$ congruences hold as $0 \equiv 0$ regardless of our modulus. This leaves us with the last two congruences.

$$\begin{aligned} 0 &\equiv f_n \pmod{l_{n-1}} \\ f_n &\equiv 0 \pmod{l_n} \end{aligned}$$

By Corollary 2.1.11, this means that $f_n \equiv 0 \pmod{[l_{n-1}, l_n]}$. Thus $[l_{n-1}, l_n] | f_n$ and f_n is a multiple of $[l_{n-1}, l_n]$. By definition $[l_{n-1}, l_n]$ is the smallest multiple of itself. \square

In the last two theorems the term “the smallest value” is used to describe one potential leading term. They will not be used in the generalization of those theorems to PIDs because the concept of order doesn’t exist in all commutative rings. Luckily, the “smallest” quality of the leading term is not what we need when forming the basis. The important thing is that for any flow-up class \mathbb{F}_i , excluding \mathbb{F}_0 , there exists a spline, F , whose leading term divides the leading term of every other spline in \mathbb{F}_i . F will be the “smallest element” of its flow-up class and will thus be one of the smallest flow-up class basis elements. It will be employed in a theorem about PID spline bases similarly to how its integer spline counterpart is employed in the following theorem. You’ll see.

Theorem 3.3.6. *Let G be a three-cycle and let edge labels $L = \{l_1, l_2, l_3\}$. Then the smallest flow up class elements of $\mathbb{S}_{(G,L)}$ (That is the smallest element of each flow-up class) form a basis for $\mathbb{S}_{(G,L)}$.*

Proof. Let $F_0 = (1, 1, 1)$. This is always our trivial smallest element of \mathbb{F}_0 in every set of splines over a commutative ring, not just integer splines. Let $F_1 = (0, [l_1, (l_2, l_3)], \beta)$. By Theorem 3.3.4, F_1 is the smallest flow-up class element of \mathbb{F}_1 . Let $F_2 = (0, 0, [l_2, l_3])$. By Theorem 3.3.5, F_2 is the smallest flow-up class element of \mathbb{F}_2 .

First, note that if we were to place these splines into one matrix like so,

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & [l_1, (l_2, l_3)] & \beta \\ 0 & 0 & [l_2, l_3] \end{bmatrix}$$

we would get nice, clean upper triangular matrix. Recall from your first linear algebra class that the determinant of an upper triangular matrix is the product of its diagonal components, in this case $(1) \cdot ([l_1, (l_2, l_3)]) \cdot ([l_2, l_3])$. This is very much not zero, thus these vectors (splines) are linearly independent. Then the vectors which represent each spline are linearly independent.

Now we need only show that this basis spans.

Let $F = (f_1, f_2, f_3)$ be a spline on $\mathbb{S}_{(G,L)}$. Let $F^2 = F - f_1 F_0$ (note the superscript is not an exponent but just another way to index things other than using a subscript). Then

$$F^2 = F - f_1 F_0 = \begin{bmatrix} f_1 \\ f_2 \\ f_3 \end{bmatrix} - \begin{bmatrix} (f_1)1 \\ (f_1)1 \\ (f_1)1 \end{bmatrix} = \begin{bmatrix} 0 \\ f_2 - f_1 \\ f_3 - f_1 \end{bmatrix}$$

By Theorem 3.2.1, we know that this linear combination over the integers of splines, namely F^2 , must also be a spline. F^2 is clearly an element of \mathbb{F}_1 as it has precisely one leading zero. By Theorem 3.3.4 we know that its leading term must be a multiple of $[l_1(l_2, l_3)]$. Then for some integer k , $F^2 = (0, f_2 - f_1, f_3 - f_1) = (0, k[l_1(l_2, l_3)], f_3 - f_1)$. Then let $F^3 = F^2 - kF_1$ (Again, don't freak out about the superscript). Then

$$F^3 = F^2 - kF_1 = \begin{bmatrix} 0 \\ k[l_1(l_2, l_3)] \\ f_3 - f_1 \end{bmatrix} - \begin{bmatrix} (k)0 \\ (k)[l_1, (l_2, l_3)] \\ (k)\beta \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ f_3 - f_1 - (k)\beta \end{bmatrix}$$

By Theorem 3.2.1, F^3 must also be a spline. It is also an element of \mathbb{F}_2 . Then by Theorem 3.3.5, we know that the leading term must be a multiple of $[l_2, l_3]$. Then for some integer j , $F^3 = (0, 0, f_3 - f_1 - (k)\beta) = (0, 0, j[l_2, l_3])$. Okay now check this out.

$$F^3 - jF_3 = \begin{bmatrix} 0 \\ 0 \\ j[l_2, l_3] \end{bmatrix} - \begin{bmatrix} (j)0 \\ (j)0 \\ (j)[l_2, l_3] \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Then we have reached this conclusion,

$$0 = F^3 - jF_3 = F^2 - kF_2 - jF_3 = F - f_1 F_1 - kF_2 - jF_3.$$

Then $F = f_1 F_1 + kF_2 + jF_3$. We have shown that any spline in $\mathbb{S}_{(G,L)}$ is in the span of the elements F_1, F_2 , and F_3 . Then those splines form a basis for $\mathbb{S}_{(G,L)}$. □

We now generalize this theorem to n-cycle splines.

Theorem 3.3.7. *Let G be an n -cycle and the set of edge labels $L = \{l_1, l_2, \dots, l_n\}$. Then the smallest flow up class elements of $\mathbb{S}_{(G,L)}$ form a basis.*

Proof. Let $F_0 = (1, 1, \dots, 1)$, $F_{n-1} = (0, 0, \dots, 0, [l_{n-1}, l_n])$. For $1 \leq i \leq n-2$ and $j = i$ let $F_i = (0, \dots, [l_i, (l_{i+1}, \dots, l_n)], f_{j+1}^i, f_{j+2}^i, \dots, f_{n-1}^i, f_n^i)$. This means F_i is the smallest element of \mathbb{F}_i ;

it has i leading zeros. The i in the super script of each integer is to associate that integer with its spline whereas the $j + c$ (c is a constant) is to associate the integer with its spot in the spline.

Now that we have our basis elements (fingers crossed) we must first declare that they are linearly independent. We place the splines into a matrix.

$$\begin{bmatrix} 1 & 1 & 1 & \dots & 1 & 1 & 1 \\ 0 & [l_1, (l_2, l_3, \dots, l_n)] & f_3^1 & \dots & f_{n-2}^1 & f_{n-1}^1 & f_n^1 \\ 0 & 0 & [l_2, (l_3, l_4, \dots, l_n)] & \dots & f_{n-2}^2 & f_{n-1}^2 & f_n^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & [l_{n-3}, (l_{n-2}, l_{n-1}, l_n)] & f_{n-1}^{n-3} & f_n^{n-3} \\ 0 & 0 & 0 & \dots & 0 & [l_{n-2}, (l_{n-1}, l_n)] & f_n^{n-2} \\ 0 & 0 & 0 & \dots & 0 & 0 & [l_{n-1}, l_n] \end{bmatrix}$$

Again, we get an *attractive* upper triangular matrix whose determinant will be nonzero. Then the splines are linearly independent.

Let $H = (h_1, h_2, \dots, h_n) \in \mathbb{S}_{(G,L)}$. Let $H_1 = H - h_1 F_0$. Then

$$H_1 = H - h_1 F_0 = \begin{bmatrix} h_1 \\ h_2 \\ \vdots \\ h_n \end{bmatrix} - \begin{bmatrix} h_1 \\ h_1 \\ \vdots \\ h_1 \end{bmatrix} = \begin{bmatrix} 0 \\ h_2 - h_1 \\ \vdots \\ h_n - h_1 \end{bmatrix}$$

Then $H_1 = (0, h_2 - h_1, h_3 - h_1, \dots, h_n - h_1)$. We will now use induction to continue this sort of deconstruction of G .

We will start with the base case. Note that $H_1 \in \mathbb{F}_1$ is a spline by Theorem 3.2.1. Then by Theorem 3.3.4 the leading term of H_1 is a multiple of $[l_1, (l_2, l_3, \dots, l_n)]$. Then for some integer k_1 we know $H_1 = (0, h_2 - h_1, h_3 - h_1, \dots, h_n - h_1) = (0, k_1[l_1, (l_2, l_3, \dots, l_n)], h_3 - h_1, \dots, h_n - h_1)$. Then let $H_2 = H_1 - k_1 F_1$. So,

$$H_2 = H_1 - k_1 F_1 = \begin{bmatrix} 0 \\ k_1[l_1, (l_2, l_3, \dots, l_n)] \\ h_3 - h_1 \\ \vdots \\ h_n - h_1 \end{bmatrix} - \begin{bmatrix} 0 \\ k_1[l_1, (l_2, l_3, \dots, l_n)] \\ f_3^1 \\ \vdots \\ f_n^1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ h_3 - h_1 - f_3^1 \\ \vdots \\ h_n - h_1 - f_n^1 \end{bmatrix}$$

Then $H_2 \in \mathbb{F}_2$ is a spline by Theorem 3.2.1. Now for the inductive step. Suppose we have some $H_i \in \mathbb{F}_i$. Let $H_i = (0, 0, \dots, h_{i+1}^*, \dots, h_n^*)$. Since H_i has exactly i leading zeros we know h_{i+1}^* , the leading term, is the $i + 1$ th term. By Theorem 3.3.4 we know that the lead-

ing term of H_i is multiple of $[l_i, (l_{i+1}, \dots, l_n)]$. Then for some integer k_i it is the case that $H_i = (0, 0, \dots, h_{i+1}^*, \dots, h_n^*) = ((0, 0, \dots, k_i[l_i, (l_{i+1}, \dots, l_n)], h_{i+2}^*, \dots, h_n^*)$. Let $H_{i+1} = H_i - k_i F_i$.

Then

$$H_{i+1} = H_i - k_i F_i = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ k_i[l_i, (l_{i+1}, \dots, l_n)] \\ h_{i+2}^* \\ h_{i+3}^* \\ \vdots \\ h_n^* \end{bmatrix} - \begin{bmatrix} (k_i)0 \\ (k_i)0 \\ \vdots \\ (k_i)[l_i, (l_{i+1}, \dots, l_n)] \\ (k_i)f_{j+2}^i \\ (k_i)f_{j+3}^i \\ \vdots \\ (k_i)f_n^i \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ (k_i)f_{j+2}^i \\ (k_i)f_{j+3}^i \\ \vdots \\ h_n^* - (k_i)f_n^i \end{bmatrix}$$

Then $H_{i+1} \in \mathbb{F}_{i+1}$ is a spline by Theorem 3.2.1. This concludes the inductive step.

Then we have shown that we may subtract $\sum_{i=1}^{n-2} k_i F_i$ from H_1 to yield a new spline $H_{n-1} \in \mathbb{F}_{n-1}$. Using algebraic language, $H_{n-1} = H_1 - \sum_{i=1}^{n-2} k_i F_i \in \mathbb{F}_{n-1}$. Because H_{n-1} is in the $n-1$ th flow up class we know that there are $n-1$ leading zeros and, by theorem 3.3.5 the leading term is a multiple of $[l_{n-1}, l_n]$. Then for some integer k_{n-1} we know that $H_{n-1} = (0, 0, \dots, 0, k_{n-1}[l_{n-1}, l_n])$. Then $H_{n-1} - k_{n-1} F_{n-1} = (0, 0, \dots, 0, k_{n-1}[l_{n-1}, l_n]) - (0, 0, \dots, 0, k_{n-1}[l_{n-1}, l_n]) = (0, 0, \dots, 0, 0)$. Then $0 = H_{n-1} - k_{n-1} F_{n-1} = H_1 - \sum_{i=1}^{n-2} k_i F_i - k_{n-1} F_{n-1} = H - h_1 F_0 - \sum_{i=1}^{n-2} k_i F_i - k_{n-1} F_{n-1}$. Then $H = h_1 F_0 + \sum_{i=1}^{n-2} k_i F_i + k_{n-1} F_{n-1}$. Then every spline H is in the span of F_1, F_2, \dots, F_{n-1} . Then we have found a basis. \square

Take note of this process because it is, in a sense, the *juicy* part of the document. The process of this proof occurs again for a flow-up class basis for the set of all PID splines on an edge-labeled graph and then again for the set of all splines over $\mathbb{R}[x, y]$. Next we will show that this theorem, which we have just proved, holds for all PID splines as well. This is because the PID quality of the integers is the crucial quality which makes this particular proof possible. This is also why the PID analogue of this theorem will have a nearly identical proof. However, we cannot simply state this. We must prove it rigorously. This means that we must reorient every integer-based tool we have used to prove this theorem, (gcds, lcms, bezout's theorem, and of course the chinese remainder theorem with noncoprime moduli) so that they work in PID splines as they did in integer splines. This will be the substance of the next chapter.

4

Greatest Common Divisors and Least Common Multiples in Commutative Rings

4.1 Gcds and Lcms in Commutative Rings

Theorem 4.1.1. *Let d , a and b be elements of a commutative ring, R and d is a greatest common divisor of a and b . Then, every associate of d is also a greatest common divisor of a and b .*

Proof. Let e be an associate of d and let c be a common divisor of a and b . Since, $e|d$ and $d|a$ and $d|b$, we know that $e|a$ and $e|b$. Then, e is a common divisor of a and b . We know $c|d$ by definition of greatest common divisors. Then, since $d|e$ we can deduce that $c|e$. Then, e is a common divisor of a and b and every common divisor of a and b divides e . Thus, e is a greatest common divisor. □

Using the previous theorem we can show that Theorem 2.1.7 also holds for UFDs (thus also PIDs).

Theorem 4.1.2. *Let a_1, a_2, \dots, a_n be elements of a UFD with d being a greatest common divisor of a_2, \dots, a_n . Then a greatest common divisor of a_1, a_2, \dots, a_n is also a greatest common divisor of a_1 and d .*

Proof. Let d_1 be a greatest common divisor of a_1 and d and d_2 be a greatest common divisor of $a_1, a_2, a_3, \dots, a_n$ and let D_1 be the set of all divisors of d_1 and D_2 be all the divisors of d_2 . Note that $d_1 \in D_1$ and $d_2 \in D_2$. Now let $c_1 \in D_1$. Then $c_1|d_1$. Then $c_1|a_1$ and $c_1|d$. Then $c_1|a_2, a_3, \dots, a_n$. Then $c_1|a_i$ for all i . In other words, c_1 is a common divisor of all the a_i . Then by Definition 2.1.6 we know $c_1|d_2$. Then $D_1 \subset D_2$. Now, suppose that $c_2 \in D_2$. Then $c_2|d_2$. Then $c_2|a_1, a_2, a_3, \dots, a_n$. Since $c_2|a_2, a_3, \dots, a_n$ we know $c_2|d$. Since $c_2|d$ and $c_2|a_1$ we know $c_2|d_1$. Then $c_2 \in D_1$. Then $D_2 \subset D_1$. Then $D_2 = D_1$. Since $d_1 \in D_2$ and $c|d_1$ for all $c \in D_2$, d_1 is a greatest common divisor of $a_1, a_2, a_3, \dots, a_n$. Similarly, since $d_2 \in D_1$ and $c|d_2$ for all $c \in D_1$, d_2 is a greatest common divisor of a_1 and d . \square

Definition 4.1.3. Let R be a UFD. $d \in R$ is a *common divisor* of $a_1, a_2, \dots, a_n \in R$, if $d|a_1, d|a_2, \dots, d|a_n$. If $c \in R$ is a common divisor of all the $a_i \Rightarrow c|d$, then d is a *greatest common divisor*. \triangle

This theorem also holds in PIDs since all PIDs are UFDs. This next theorem is a more convenient way to define greatest common divisors in PIDs.

Definition 4.1.4. Let R be a PID with $d, a_1, a_2, \dots, a_n \in R$. Then $\langle d \rangle = \langle a_1, a_2, a_3, \dots, a_n \rangle \iff d$ is a *greatest common divisor* of $a_1, a_2, a_3, \dots, a_n$. \triangle

Proof. Let R be PID with $d, a_1, a_2, \dots, a_n \in R$. We will show that $\langle d \rangle = \langle a_1, a_2, a_3, \dots, a_n \rangle \Rightarrow d$ is a greatest common divisor of $a_1, a_2, a_3, \dots, a_n$ and $\langle d \rangle = \langle a_1, a_2, a_3, \dots, a_n \rangle \Leftarrow d$ is a greatest common divisor of $a_1, a_2, a_3, \dots, a_n$, using 4.1.3 as our definition of greatest common divisor.

\Rightarrow Assume that $\langle d \rangle = \langle a_1, a_2, a_3, \dots, a_n \rangle$. Since for all $1 \leq i \leq n$ we know $a_i \in \langle a_1, a_2, a_3, \dots, a_n \rangle$, we can conclude that a_i is a multiple of d . Thus $d|a_i$ for all i . Then d is a common divisor of a_1, a_2, \dots, a_n . Now suppose that c is a common divisor of a_1, a_2, \dots, a_n . Then $c|a_1, c|a_2, \dots, c|a_n$. Then for some $k_1, k_2, \dots, k_n \in R$, $ck_1 = a_1, ck_2 = a_2, \dots, ck_n = a_n$. We know every element of $\langle d \rangle$, i.e. every multiple of d , is of the form $a_1x_1 + a_2x_2 + \dots + a_nx_n = ck_1x_1 + ck_2x_2 + \dots + ck_nx_n = c(k_1x_1 + k_2x_2 + \dots + k_nx_n)$. Then c divides every multiple of d . Since d is a multiple of d we know that c divides d . Then d is a greatest common divisor of a_1, a_2, \dots, a_n .

\Rightarrow Assume d is a greatest common divisor of a_1, a_2, \dots, a_n . Since R is a PID we know that for some $p \in R$, $\langle a_1, a_2, a_3, \dots, a_n \rangle = \langle p \rangle$. Then, as we showed earlier in this proof, p is a greatest common divisor of a_1, a_2, \dots, a_n . Then, by the definition of greatest common divisor, $p|d$ and $d|p$. Since d is a multiple of p we know that $d \in \langle p \rangle$. Then $\langle d \rangle \subset \langle p \rangle$. Since p is a multiple of d we know that $p \in \langle d \rangle$. Then $\langle p \rangle \subset \langle d \rangle$. Then $\langle d \rangle = \langle p \rangle = \langle a_1, a_2, a_3, \dots, a_n \rangle$. \square

Theorem 4.1.5 (Generalization of Euclid's Lemma). *Let n, a, b be elements of a PID, R . If $n|ab$ and 1 is a greatest common divisor of a and n , then $n|b$.*

Proof. Since n and a , with a greatest common divisor of 1 , are elements of a PID we know that $\langle a, n \rangle = 1$. Then for some $x, y \in R$, $1 = xa + yn$. Multiply both sides by b yielding $b = xab + ynb$. Note that since $n|ab$ we know for some $k \in R$, $nk = ab$. Then $b = xab + ynb = xnk + ynb$. Factor n out of the right side yielding $b = n(ak + yb)$. Then $n|b$. \square

Definition 4.1.6. Let R be a ring with $m \in R$ is a *common multiple* of $a_1, a_2, \dots, a_n \in R$ if $a_1, a_2, \dots, a_n|m$. If $c \in R$ is a common multiple of $a_1, a_2, \dots, a_n \Rightarrow m|c$ then m is a *least common multiple*. \triangle

Theorem 4.1.7. *Let R be a PID with $m, a_1, a_2, \dots, a_n \in R$. Then m is an least common multiple of $a_1, a_2, \dots, a_n \iff \langle m \rangle = \langle a_1 \rangle \cap \langle a_2 \rangle \cap \dots \cap \langle a_n \rangle$.*

Proof. First note that, $\langle a_1 \rangle \cap \langle a_2 \rangle \cap \dots \cap \langle a_n \rangle$ is an intersection of a finite number of ideals thus it is an ideal. Because it is an ideal in a PID, we know this ideal is principal. Then there exists some m in R such that $\langle m \rangle = \langle a_1 \rangle \cap \langle a_2 \rangle \cap \dots \cap \langle a_n \rangle$. Now we will approach the if and only if statement.

\Leftarrow Assume $\langle m \rangle = \langle a_1 \rangle \cap \langle a_2 \rangle \cap \dots \cap \langle a_n \rangle$. Since $m \in \langle m \rangle$, we know $m \in \langle a_1 \rangle \cap \langle a_2 \rangle \cap \dots \cap \langle a_n \rangle$. Then $m \in \langle a_1 \rangle, m \in \langle a_2 \rangle, \dots, m \in \langle a_n \rangle$ by definition of set intersection. $m \in \langle a_i \rangle \Rightarrow m = a_i k_i$ for some k_i in $R \Rightarrow a_i|m$ for all $1 \leq i \leq n$. Then m is a common multiple of a_1, a_2, \dots, a_n . Now suppose we have another common multiple of a_1, a_2, \dots, a_n , call it m^* . Then $a_i|m^*$ for all i . Then $m^* \in \langle a_i \rangle$ for all i . Then $m^* \in \langle a_1 \rangle \cap \langle a_2 \rangle \cap \dots \cap \langle a_n \rangle = \langle m \rangle$. Because $m^* \in \langle m \rangle$ we know that $m^* = mk$ for some $k \in R$. Then $m|m^*$. Then m is a least common multiple.

\Rightarrow Assume m is a least common multiple of a_1, a_2, \dots, a_n . Since $\langle a_1 \rangle \cap \langle a_2 \rangle \cap \dots \cap \langle a_n \rangle$ is an ideal we know it is principal and it may be generated by a single element, call it p . Then $\langle a_1 \rangle \cap \langle a_2 \rangle \cap \dots \cap \langle a_n \rangle = \langle p \rangle$. As shown earlier in this proof, p is then a least common multiple. By definition of least common multiples, $g|p$ and $p|g$. These two statements respectively imply $p \in \langle g \rangle$ and $g \in \langle p \rangle$ which then implies $\langle p \rangle \subset \langle g \rangle$ and $\langle p \rangle \subset \langle g \rangle$. Since these sets are subsets of each other they are equal. Then $\langle m \rangle = \langle p \rangle = \langle a_1 \rangle \cap \langle a_2 \rangle \cap \dots \cap \langle a_n \rangle$

Theorem 4.1.8. [4, Chapter 3 Theorem 3.11] *If R is a Unique Factorization Domain, then $a_1, a_2, \dots, a_n \in R$ have a greatest common divisor.*

Theorem 4.1.9. *Let a, b be elements of a UFD, R . Let d be a greatest common divisor of a and b so that for some $k_1, k_2 \in R, a = dk_1$ and $b = dk_2$. Then 1 is a greatest common divisor of k_1, k_2 .*

Proof. Suppose t is a greatest common divisor of k_1, k_2 and t is not a unit. Then $t|k_1$ and $t|k_2$. Then there exists some $l_1, l_2 \in R$ such that $tl_1 = k_1$ and $tl_2 = k_2$. Multiply both sides by d yielding $tl_1d = k_1d = a$ and $tl_2d = k_2d = b$. Then $td|a$ and $td|b$. Since td is a common divisor of a and b it must divide d a greatest common divisor. However, we also know that d must divide td (because $td = dt$). Because $td|d$ and $d|td$, then $td = du$ where u is an arbitrary unit of R . Then by the cancellation property of integral domains $t = u$. Then t is a unit, thus we have reached a contradiction. Then t is a unit. However, by Theorem 4.1.1, a greatest common divisor multiplied by a unit is also a greatest common divisor. Since t is a unit we know that t^{-1} is also a unit. Then $tt^{-1} = 1$ is also a greatest common divisor. \square

Theorem 4.1.10. [2, Property 4.2.g] *Let R be a ring. Any nonempty finite set of elements in R has a least common multiple if and only if every pair of elements has a least common multiple.*

Theorem 4.1.11. *Let R be a UFD. Any nonempty finite set of elements in R has a least common multiple.*

Proof. To prove this we will show that any pair of elements in R has a least common multiple and then use Theorem 4.1.10.

Let R be a UFD with $a, b, u \in R$ and u is a unit. Then $a = up_1^{r_1} \cdot p_2^{r_2} \cdot \dots \cdot p_n^{r_n}$ and $b = p_1^{s_1} \cdot p_2^{s_2} \cdot \dots \cdot p_m^{s_m}$, p_i all being irreducibles. We write the products as having the same bases because we allow some of the exponents to be zero under the condition that the exponent's base does not occur as a factor in that value. For example $-50 = -1 \cdot 7^0 \cdot 5^2 \cdot 3^0 \cdot 2^1$ and $42 = 7^1 \cdot 5^0 \cdot 3^1 \cdot 2^1$ are two values that don't share the same set of prime factors but we may still write them as having factorizations with the same bases.

Anywho, consider the value $l = p_1^{\max[r_1, s_1]} \cdot p_2^{\max[r_2, s_2]} \cdot \dots \cdot p_n^{\max[r_n, s_n]}$. The $\max[x, y]$ function spits out the largest integer, x or y . Clearly $a|l$ and $b|l$. So l is a common multiple of a and b . Let c be a common multiple of a and b . Then $c|a$ and $c|b$. Then for some k_1 and $k_2 \in R$, $ak_1 = u \cdot p_1^{r_1} \cdot p_2^{r_2} \cdot \dots \cdot p_n^{r_n} \cdot k_1 = c = p_1^{s_1} \cdot p_2^{s_2} \cdot \dots \cdot p_m^{s_m} \cdot k_2 = bk_2$. For all p_i we know that $p_i^{r_i} | l$ and $p_i^{s_i} | l$ so obviously $p_i^{\max[r_i, s_i]} | l$ since either either $\max[r_i, s_i] = r_i$ or $\max[r_i, s_i] = s_i$. Then $l|c$. Then l is a least common multiple by 4.1.6. Since a pair of elements always has a least common multiple in a UFD, we may conclude, by Theorem 4.1.10, that any finite nonempty set of elements in a UFD has a least common multiple. \square

In splines there will be times that we need to refer to greatest common divisors and least common divisors without knowing their actual value, so their innate existence will be very convenient. Again, because every PID is also a UFD this theorem also applies to PIDs.

Theorem 4.1.12 (Bezout's Identity). *Let a, b and d be elements of a PID R such that d is a greatest common divisor of a and b . Then $d = ax + by$ for some $x, y \in R$.*

Proof. Since d is a greatest common divisor of a and b we know that $\langle d \rangle = \langle a, b \rangle$. Since $d \in \langle d \rangle$ we know $d \in \langle a, b \rangle$. Then d is of the form $ax + by$ for some $x, y \in R$. \square

Theorem 4.1.13. *Let $m_1, m_2, m_3, \dots, m_n$ be elements of an arbitrary PID, R . Let d_{n-1} be a least common multiple of m_1, m_2, \dots, m_{n-1} . Then a least common multiple of d_{n-1} and m_n is also a least common multiple of $m_1, m_2, \dots, m_{n-1}, m_n$*

Proof. By Theorem 4.1.7 we know that a least common multiple of d_{n-1} and m_n is any element, $r \in R$, such that $\langle r \rangle = \langle d_{n-1} \rangle \cap \langle m_n \rangle$. Recall, however, that d_{n-1} is a least common multiple of m_1, m_2, \dots, m_{n-1} . Then, by Theorem 4.1.7 $\langle d_{n-1} \rangle = \langle m_1 \rangle \cap \langle m_2 \rangle \cap \dots \cap \langle m_{n-1} \rangle$. Then by substitution $\langle r \rangle = \langle d_{n-1} \rangle \cap \langle m_n \rangle = [\langle m_1 \rangle \cap \langle m_2 \rangle \cap \dots \cap \langle m_{n-1} \rangle] \cap \langle m_n \rangle$. Since set intersection is associative, $[\langle m_1 \rangle \cap \langle m_2 \rangle \cap \dots \cap \langle m_{n-1} \rangle] \cap \langle m_n \rangle = \langle m_1 \rangle \cap \langle m_2 \rangle \cap \dots \cap \langle m_{n-1} \rangle \cap \langle m_n \rangle$. All the m_i are elements of R , a PID. Then the intersection of their ideals is also an ideal. Then for some p in R , $\langle m_1 \rangle \cap \langle m_2 \rangle \cap \dots \cap \langle m_{n-1} \rangle \cap \langle m_n \rangle = \langle p \rangle$. Then p is a least common multiple of m_1, m_2, \dots, m_n and $\langle r \rangle = \langle p \rangle$. Thus r is also a least common multiple of m_1, m_2, \dots, m_n . \square

Theorem 4.1.14. *Let $m_1, m_2, \dots, m_k, \alpha, m^* \in R$, where R is a PID, and m^* is a least common multiple of m_1, m_2, \dots, m_k . If $m_1, m_2, \dots, m_k | \alpha$ then $m^* | \alpha$.*

Proof. By hypothesis α is a common multiple of m_1, m_2, \dots, m_k . By definition m^* divides every common multiple of m_1, m_2, \dots, m_k then $m^* | \alpha$. \square

Corollary 4.1.15. *Let $m_1, m_2, \dots, m_n, \alpha, \theta \in R$, where R is a PID. If*

$$\begin{aligned} \alpha &\equiv \theta \pmod{m_1} \\ \alpha &\equiv \theta \pmod{m_2} \\ \alpha &\equiv \theta \pmod{m_3} \\ &\vdots \\ \alpha &\equiv \theta \pmod{m_n} \end{aligned}$$

then $\alpha \equiv \theta \pmod{d_k}$ where d_k is a least common multiple of m_1, m_2, \dots, m_n .

Proof. We know by hypothesis that $\alpha \equiv \theta \pmod{m_i}$ for all $1 \leq i \leq n$. Then $m_i | \alpha - \theta$ for all i . Then by Theorem 4.1.14, $d_k | \alpha - \theta$ where d_k is a least common multiple of m_1, m_2, \dots, m_n . Then $\alpha \equiv \theta \pmod{d_k}$ by the definition of congruence. \square

Theorem 4.1.16 (Chinese Remainder Theorem for Arbitrary PIDs: non-coprime moduli). *Let $x, z_1, z_2, \dots, z_r, m_1, m_2, \dots, m_r$ be elements of an arbitrary PID, R . Let $d_{i,j}$ be a greatest common*

divisor of m_i and m_j . Then, the following system

$$\begin{cases} x \equiv z_1 \pmod{m_1} \\ x \equiv z_2 \pmod{m_2} \\ \vdots \\ x \equiv z_r \pmod{m_r} \end{cases}$$

has a solution for x if and only if for all m_i, m_j such that $i \neq j$, $d_{i,j} | z_i - z_j$.

Uniqueness is much more complicated in general PIDs than in the integers or, even more so, the natural numbers. Luckily, we only want to use this theorem to show that certain values exist; we do not care whether the value is unique. That is why this Theorem does have the “unique mod $[m_1, m_2, \dots, m_r]$ ” which is often present in presentation of the integer analogue of this theorem.

To prove this we will first show that it is true for a system of two congruences and then show that it can be generalized to an arbitrary amount of congruences.

Lemma 4.1.17. *Let $z_1, z_2, m_1, m_2 \in R$ where R is a PID. Let d be a greatest common divisor of m_1 and m_2 . Then the system*

$$\begin{cases} x \equiv z_1 \pmod{m_1} \\ x \equiv z_2 \pmod{m_2} \end{cases}$$

has a solution if and only if $d | z_1 - z_2$.

Proof. \Leftarrow Since $d | z_1 - z_2$ we know $dk = z_1 - z_2$ for $k \in R$. Then by Bezout’s identity, for some $r, s \in R$ $dk = (m_1r + m_2s)k = z_1 - z_2$. Then $m_1kr + m_2ks = z_1 - z_2$. Then $m_1kr + z_2 = -m_2ks + z_1$. Let $x = m_1kr + z_2 = -m_2ks + z_1$. Then $x \equiv m_1kr + z_2 \equiv (0)kr + z_2 \equiv z_2 \pmod{m_2}$ and $x \equiv -m_2ks + z_1 \equiv (0)ks + z_1 \equiv z_1 \pmod{m_1}$. Thus the congruences hold.

\Rightarrow Suppose the system has a solution for x . Then $x \equiv z_1 \pmod{m_1}$ and $x \equiv z_2 \pmod{m_2}$. Then for some $n_1, n_2 \in R$ we know $m_1n_1 = x - z_1$ and $m_2n_2 = x - z_2$. Then $x = m_1n_1 + z_1 = m_2n_2 + z_2$. Now we have established that $m_1n_1 + z_1 = m_2n_2 + z_2$. Then $m_2n_2 - m_1n_1 = z_2 - z_1$. Recall d is a greatest common divisor of m_1 and m_2 . Then $d | m_1, d | m_2$. Then $dk_1 = m_1$ and $dk_2 = m_2$. Then $m_2n_2 - m_1n_1 = dk_2n_2 - dk_1n_1 = d(k_2n_2 - k_1n_1) = z_2 - z_1$. Then $d | z_2 - z_1$. \square

$m_j n_j - m_i n_i = z_j - z_i$. Let d be a greatest common divisor of m_i and m_j . Then $d|m_i$, $d|m_j$. Then for some $k_i, k_j \in R$ we know $dk_i = m_i$ and $dk_j = m_j$. Then $m_j n_j - m_i n_i = dk_j n_j - dk_i n_i = d(k_j n_j - k_i n_i) = z_j - z_i$. Then $d|z_j - z_i$. \square

5

Splines over arbitrary PIDs

5.1 Intro

Now that we adequately understand how our essential theorems carry over to commutative rings from the integers we can dive head first into some PID splines.

What we know about graphs will not change. The only dissimilar aspect is the new family of edge and vertex labels. Where once they were integers, they will now be elements of a PID or, in more general cases, an arbitrary PID.

The following are a few reminders about which theorems and definitions will remain functionally identical to their integer analogues.

Definition 5.1.1. Let R be a PID. Let $a, b \in R$. We say a *divides* b , denoted $a|b$, if there exists some $k \in R$ such that $ak = b$. △

Theorem 5.1.2. Let R be a PID. Let a, b and $c \in R$. If $a|b$ and $b|c$ then $a|c$.

Proof. By hypothesis $a|b$ and $b|c$. Then for some $k_1, k_2 \in R$, $ak_1 = b$ and $bk_2 = c$. Then by substitution $ak_1k_2 = c$. Then $a|c$. □

Definition 5.1.3. Let R be a PID. Let $a, b, m \in R$. We say a is *congruent to b modulo m* , denoted $a \equiv b \pmod{m}$, if $m|a - b$. △

Modular arithmetic involving non-integers may seem unfamiliar and therefore daunting but the concept of divisibility and subtraction does not change. Since, congruence follows directly from divisibility and subtraction it will not be very difficult to navigate.

Note again that, by the definition of divisibility this means there exists some $x \in R$ such that $mx = a - b$. Thus, it is valid to skip straight from $a \equiv b \pmod{m}$ to $mx = a - b$.

Theorem 5.1.4. *Let R be a PID. Let m be an element of R . Congruence modulo m is an equivalence class. In other words, for all $a, b, c \in R$*

$$a \equiv b \pmod{m}, b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$$

$$a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$$

$$a \equiv a$$

5.2 n-cycle splines form a module over commutative rings

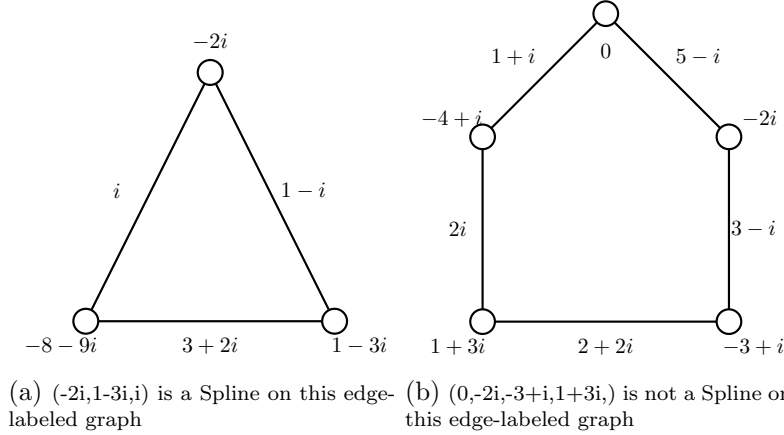
Theorem 5.2.1. *Let R be a commutative ring. Let $L = l_1, l_2, \dots, l_n$ where $l_1, l_2, \dots, l_n \in R$ and let G be an n -cycle. Let $\mathbb{S}_{(G,L)}$ be the set of all splines with vertex and edge labels in R . Then $\mathbb{S}_{(G,L)}$ is a unitary R -module.*

This theorem was proved for integer splines, (Theorem 3.2.1). The proof for this theorem is almost identical with the exception of the ring \mathbb{Z} instead being a commutative ring R . Thus we will not add the proof here.

Since $\mathbb{S}_{(G,L)}$ forms an R -module we know that $\mathbb{S}_{(G,L)}$ is closed under addition as well as scalar multiplication by elements of R , R being the ring that the edge labels and vertex labels belong to. This means if I take some splines over R , let's call them F , G and H , and elements of R , let's call them x , y and z , I can combine them yielding another spline. $Fx + Gy + Hz$ will be a spline. This will be crucial for proving bases.

5.3 Definition of PID Splines

Definition 5.3.1. Let R be a PID. Let (G, L) be an edge-labeled graph. A **generalized PID spline** is a vertex labeling, $(f_1, f_2, \dots, f_n) \in R^n$, such that if vertices v_i and v_j are connected by edge e_k then $f_i \equiv f_j \pmod{l_k}$. We denote the set of all splines on (G, L) by $\mathbb{S}_{(G,L)}$. \triangle



Example 5.3.2. Figure (a) is a Spline because

$$(1-i)(-1)1-3i - (-2i) = 1-i \Rightarrow 1-3i \equiv -2i \pmod{1-i}$$

$$(3+2i)(-3) - 8-9i - (1-3i) = -9-6i \Rightarrow -8-9i \equiv 1-3i \pmod{3+2i}$$

$$i(8i-7) = -8-9i - (-2i) = -8-7i \Rightarrow -8-9i \equiv -2i \pmod{i}$$

Figure (b), however is not a spline because $5-i \nmid -2i-0$. Suppose the opposite were true. Then $\frac{2i}{5-i}$ would be a Gaussian integer. Then $\frac{2i}{5-i} \cdot 1 = \frac{2i}{5-i} \cdot \frac{5+i}{5+i} = \frac{(2i)(5+i)}{(5-i)(5+i)} = \frac{10i+2i^2}{25-i^2} = \frac{10i-2}{26} = \frac{10}{26}i + \frac{2}{26}$. The RHS of this equation however is not a Gaussian integer. Thus $5-i \nmid -2i-0$. Thus $2i \not\equiv 0 \pmod{5-i}$. \diamond

Unlike the definition of a smallest flow-up class element for splines over the integers, the PID analogue will not make use of order.

Definition 5.3.3. Let R be a PID. Let G be an n -cycle with a set of edge labels $L = \{l_1, l_2, \dots, l_n\}$ with $l_1, l_2, \dots, l_n \in R$. Let \mathbb{F}_i , where $1 \leq i \leq n-1$, be a flow-up class. Then $f \in \mathbb{F}_i$ is a *smallest*

flow-up class element in F if the leading term f_i of f divides the leading term of any other flow up class element of \mathbb{F}_i . △

Again “smallness” implies “order” which is a fallacy within an arbitrary PID. However we use the term “smallest” to associate the following two theorems with their integer analogues.

Theorem 5.3.4. *Fix the edge labels on (G,L) , where $L = \{l_1, l_2, \dots, l_n\}$. Let $i \in [1, n] \cap \mathbb{N}$ and let $F_i = (0, \dots, 0, f_{i+1}, f_{i+2}, \dots, f_n)$ be an element of \mathbb{F}_i in $\mathbb{S}_{(G,L)}$. Let d_{i+1} be a greatest common divisor of l_{i+1}, \dots, l_n . Then the leading term, f_{i+1} , is a multiple of a least common multiple, m , of l_i and d_{i+1} . Also $f_{i+1} = m$ is a smallest flow-up class element satisfying the conditions.*

Proof. We will use proof by induction for the bulk of this proof. Assume $F_i = (0, \dots, 0, f_{i+1}, f_{i+2}, \dots, f_n)$ is a spline. Then the following system of congruences must hold true.

Figure 5.3.2. Caption

$$\begin{aligned}
 0 &\equiv 0 \pmod{l_1} \\
 0 &\equiv 0 \pmod{l_2} \\
 &\vdots \\
 0 &\equiv f_{i+1} \pmod{l_i} \\
 f_{i+1} &\equiv f_{i+2} \pmod{l_{i+1}} \\
 &\vdots \\
 f_{n-3} &\equiv f_{n-2} \pmod{l_{n-3}} \\
 f_{n-2} &\equiv f_{n-1} \pmod{l_{n-2}} \\
 f_{n-1} &\equiv f_n \pmod{l_{n-1}} \\
 f_n &\equiv 0 \pmod{l_n}
 \end{aligned}$$

By Theorem 4.1.16 we know that if we take any subsection

$$\begin{aligned}
 f_j &\equiv f_{j+1} \pmod{l_j} \\
 f_{j+1} &\equiv f_{j+2} \pmod{l_{j+1}}
 \end{aligned}$$

where $i \leq j \leq n - 1$ (note $f_i = 0$), of two consecutive congruences from the system above, it must be the case that $f_j \equiv f_{j+2} \pmod{d_j}$, where d is a greatest common divisor of l_j, l_{j+1} . The same is true for the last case of

$$\begin{aligned} f_{n-1} &\equiv f_n \pmod{l_{n-1}} \\ f_n &\equiv 0 \pmod{l_n} \end{aligned}$$

in which it must be the case that $f_{n-1} \equiv 0 \pmod{d_n}$ where d_n is a greatest common divisor of l_{n-1} and l_n . We will approach this case first, the base case. We know that f_n may only exist if $f_{n-1} \equiv 0 \pmod{d_{n-1}}$ where d_{n-1} is a gcd of l_{n-1} and l_n .

Now for the inductive case. Suppose that

$$\begin{aligned} f_j &\equiv f_{j+1} \pmod{l_j} \\ f_{j+1} &\equiv 0 \pmod{d_{j+1}} \end{aligned}$$

where d_{j+1} is a greatest common divisor of $l_j + 1, l_{j+2}, \dots, l_n$ and $2 \leq j \leq n - 2$ ($j = n - 1$ is the base case). We know that in order for this system to be true it must be the case that $f_j \equiv 0 \pmod{d_j}$ where d_j is a greatest common divisor of l_j and d_{j+1} . Note, by Theorem 4.1.2 d_j is also a greatest common divisor of l_j, l_{j+1}, \dots, l_n . Additionally, observing the first system of congruences in this proof, Figure 5.3.2, we know $f_{j-1} \equiv f_j \pmod{l_{j-1}}$. Then we know the system of congruences

$$\begin{aligned} f_{j-1} &\equiv f_j \pmod{l_{j-1}} \\ f_j &\equiv 0 \pmod{d_j} \end{aligned}$$

holds true. Then by induction $f_j \equiv 0 \pmod{d_j}$ for all $j \in [0, n] \cap \mathbb{N}$ where d_j is a greatest common divisor of l_j, l_{j+1}, \dots, l_n .

This means that $f_{i+1} \equiv 0 \pmod{d_{i+1}}$ where d_{i+1} is a greatest common divisor of $l_{i+1}, l_{i+2}, \dots, l_n$. By the first system in the proof we know that $0 \equiv f_{i+1} \pmod{l_j}$. Then by Corollary 4.1.15, we know that $f_{i+1} \equiv 0 \pmod{\theta}$ where θ is a least common multiple of l_j and d_{i+1} . \square

Theorem 5.3.5. *Fix the edge labels on (G,L) , where $L = \{l_1, l_2, \dots, l_n\}$. $F = (0, \dots, 0, f_n)$ be an element of the $n - 1^{\text{th}}$ flow-up class, \mathbb{F}_{n-1} , in $\mathbb{S}_{(G,L)}$. Then the leading term, f_n , is a multiple of a least common multiple, m , of l_n and l_{n-1} . Furthermore, $f_n = m$ is a smallest flow-up class element satisfying the l_n and l_{n-1} conditions.*

Proof. Since $F = (0, \dots, 0, f_n)$ is a spline we know that $f_n \equiv 0 \pmod{l_{n-1}}$ and $f_n \equiv 0 \pmod{l_n}$. Then $l_{n-1} | f_n$ and $l_n | f_n$. F is a spline if and only f_n fulfills those two properties. Then f_n is any common multiple of l_n and l_{n-1} . Then by definition we know that a least common multiple of l_{n-1} and l_n , m , divides f_n . In other words f_n is a multiple of m . Since m is also a common multiple of l_n and l_{n-1} we know that $f_n = m$ is also one acceptable value that allows F to be a spline. Of course m divides every multiple of m thus $f_n = m$ is a smallest flow up class element. □

We now have all the necessary tools to show the existence of a general flow-up class basis for splines over PIDs. I hope you are as excited as I am.

Theorem 5.3.6. *Let R be a PID. Let G be an n -cycle. Let $l_1, l_2, \dots, l_n \in R$ be our sequential set of edge labels, L . That is, $L = \{l_1, l_2, \dots, l_n\}$. Then the smallest flow-up class elements of $\mathbb{S}_{(G,L)}$ form a basis.*

Proof. The symbol 1 (one) will denote the multiplicative identity element of R and 0 the additive identity element, except when they appear as a superscript or subscript. Let $F_0 = (1, 1, \dots, 1)$ and $F_{n-1} = (0, 0, \dots, 0, [l_{n-1}, l_n])$. For $1 \leq i \leq n - 2$ and $j = i$ let $F_i = (0, \dots, [l_i, (l_{i+1}, \dots, l_n)], f_{j+1}^i, f_{j+2}^i, \dots, f_{n-1}^i, f_n^i)$. This means F_i is the smallest element of \mathbb{F}_i ; it has i leading zeros. Again, the i in the super script of each element is to associate that element with its spline whereas the $j + c$ (c is a constant) is to associate the element with its component-spot in the spline.

Now we show that our splines are linearly independent. We place the splines into a matrix.

$k_i \in R$ it is the case that $H_i = (0, 0, \dots, h_{i+1}^*, \dots, h_n^*) = (0, 0, \dots, k_i[l_i, (l_{i+1}, \dots, l_n)], h_{i+2}^*, \dots, h_n^*)$.

Let $H_{i+1} = H_i - k_i F_i$. Then

$$H_{i+1} = H_i - k_i F_i = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ k_i[l_i, (l_{i+1}, \dots, l_n)] \\ h_{i+2}^* \\ h_{i+3}^* \\ \vdots \\ h_n^* \end{bmatrix} - \begin{bmatrix} (k_i)0 \\ (k_i)0 \\ \vdots \\ (k_i)[l_i, (l_{i+1}, \dots, l_n)] \\ (k_i)f_{j+2}^i \\ (k_i)f_{j+3}^i \\ \vdots \\ (k_i)f_n^i \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ (k_i)f_{j+2}^i \\ (k_i)f_{j+3}^i \\ \vdots \\ h_n^* - (k_i)f_n^i \end{bmatrix}$$

Then $H_{i+1} \in \mathbb{F}_{i+1}$ is a spline by Theorem 5.2.1. This concludes the inductive step.

Then we have shown that we may subtract $\sum_{i=1}^{n-2} k_i F_i$ from H_1 to yield a new spline $H_{n-1} \in \mathbb{F}_{n-1}$. In algebraic language, $H_{n-1} = H_1 - \sum_{i=1}^{n-2} k_i F_i \in \mathbb{F}_{n-1}$. Because H_{n-1} is in the $n-1$ th flow up class we know that there are $n-1$ leading zeros and, by theorem 5.3.5 the leading term is a multiple of $[l_{n-1}, l_n]$. Then for some $k_{n-1} \in R$ we know that $H_{n-1} = (0, 0, \dots, 0, k_{n-1}[l_{n-1}, l_n])$. Then $H_{n-1} - k_{n-1} F_{n-1} = (0, 0, \dots, 0, k_{n-1}[l_{n-1}, l_n]) - (0, 0, \dots, 0, k_{n-1}[l_{n-1}, l_n]) = (0, 0, \dots, 0, 0)$. Then $0 = H_{n-1} - k_{n-1} F_{n-1} = H_1 - \sum_{i=1}^{n-2} k_i F_i - k_{n-1} F_{n-1} = H - h_1 F_0 - \sum_{i=1}^{n-2} k_i F_i - k_{n-1} F_{n-1}$. Then $H = h_1 F_0 + \sum_{i=1}^{n-2} k_i F_i + k_{n-1} F_{n-1}$. Then every spline $H \in \mathbb{S}_{(G,L)}$ is in the span of F_1, F_2, \dots, F_{n-1} . Then we have found a basis. \square

6

Splines over $\mathbb{R}[x, y]$

My original intent was to focus on Splines over Gaussian integers but it became clear that that ring was too similar to the regular integers and my project would be a nearly identical copy of previous projects with different ingredients. My solution was to work with a particularly different ring. One that was not euclidean or better yet not a PID. So, I chose $\mathbb{R}[x, y]$. However, I thought it would also be fun/substantial to show that most of the findings from Gjoni and Mahdavi's project could be generalized to PIDs with some work, thus solidifying the idea that non PIDs, like $\mathbb{R}[x, y]$ is the new frontier.

This first section will be an introduction to the ring $\mathbb{R}[x, y]$.

6.1 Introduction to $\mathbb{R}[x, y]$

$\mathbb{R}[x, y]$ is the set of all polynomials with 2 indeterminates and with real coefficients. We use x and y to represent our respective indeterminates. Then for all $n, m \in \mathbb{N}$ and $j_i, k_i, c \in \mathbb{R}$, $\sum_{i=1}^n j_i x^{k_i} + \sum_{i=1}^m k_i y^{j_i} + c \in \mathbb{R}[x, y]$.

Example 6.1.1. The following is an example of an element of $\mathbb{R}[x, y]$:

$$\pi x^2 + 3x - \sqrt{7}y^3 + y + 3\sqrt{2}$$

◇

Though $\pi, \sqrt{7}, 3\sqrt{2} \in \mathbb{Q}'$, (elements of the irrational numbers) they are still real.

Note that since $\mathbb{Z} \subset \mathbb{R}$ we may deduce $\mathbb{Z}[x, y] \subset \mathbb{R}[x, y]$.

Example 6.1.2. The following is an example of an element of $\mathbb{R}[x, y]$:

$$5x^5 + 2x^2 + 3y + 5$$

$$4x^2 + 2x + 3y^3 + 1$$

$$x^2 + 7x + 2y + 4$$

◇

Corollary 6.1.3. *Note that from Corollary 2.2.11 and Theorem 2.2.19, $\mathbb{R}[x, y]$ is a UFD.*

This means that any theorem we have proved for UFDs will apply to $\mathbb{R}[x, y]$. For example by Theorem 4.1.8 we know we may still take the gcd of elements in $\mathbb{R}[x, y]$. By Theorem 4.1.11 we know we may still take the lcm of elements in $\mathbb{R}[x, y]$. By Theorem 5.2.1 we know the sum or difference of scalar multiples of splines over $\mathbb{R}[x, y]$ are themselves splines over $\mathbb{R}[x, y]$.

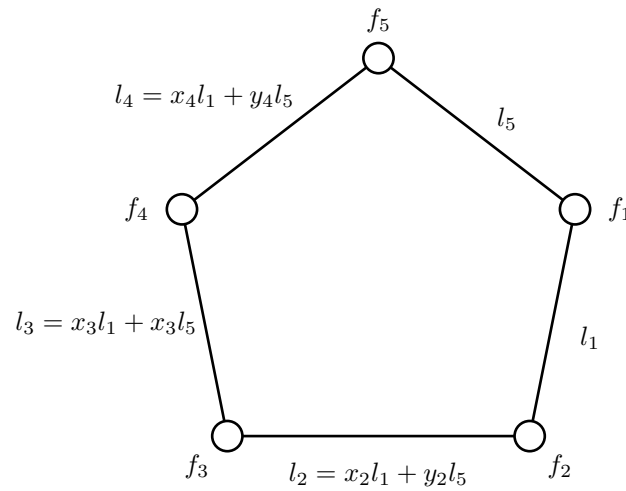
6.2 Definitions and examples of $\mathbb{R}[x, y]$ splines

Definition 6.2.1. Let $L = \{l_1, l_2, \dots, l_m\}$ and let G be some graph. A generalized $\mathbb{R}[x, y]$ spline is a vertex labeling $(f_1, f_2, \dots, f_n) \in \mathbb{R}^n[x, y]$, such that if vertices v_i and v_j are connected by edge e_k then $f_i \equiv f_j \pmod{l_k}$. We denote the set of all splines on (G, L) by $\mathbb{S}_{(G, L)}$. △

We will mostly be looking at splines on edge-labeled graphs whose edge labels are linear combinations over \mathbb{R} of other edges. We provide an example of what this means.

Example 6.2.2. Let G be a five-cycle and let $L = \{l_1, l_2, l_3, l_4, l_5\}$ be our set of edge labels, each element of $\mathbb{R}[x, y]$. Let $x_2, x_3, x_4, y_2, y_3, y_4 \in \mathbb{R}$. Then let $l_2 = x_2l_1 + y_2l_5$, $l_3 = x_3l_1 + y_3l_5$, and $l_4 = x_4l_1 + y_4l_5$. Then (G, L) is a type of edge-labeled graph we would encounter.

Figure 6.2.1. 5-cycle edge labeled graph



◇

As is visible from Figure 6.2.1, the edge labels l_2, l_3 and l_4 are each of the form $x_i l_1 + y_i l_5$ where i is equal to 2, 3 and 4, respectively. If there were not of that form, if they were random elements of $\mathbb{R}[x, y]$, then there would be no way to determine the form of the vertices. In PIDs we have Theorem 5.3.4 which allows us to determine the form of the leading terms of most of our basis elements. They also assure us that, with leading terms of that form, the rest of the vertices will have potential values that satisfy that defining system congruences. Theorem 5.3.4 requires the Chinese remainder theorem which we do not have in $\mathbb{R}[x, y]$. The basis elements of the set of all splines over $\mathbb{R}[x, y]$ require a different method for discovery.

6.3 Bases of $\mathbb{R}[x, y]$

It should be noted that flow up classes are still defined the same way. The i th flow up class is the set of all splines with i leading zeros. Again, Theorem 5.3.4 is not available for these splines. We can, however, generalize Theorem 5.3.5 to splines over $\mathbb{R}[x, y]$ because it does not use the Chinese remainder theorem we will include it without rigorous proof because the proof is nearly identical to that of Theorem 5.3.5.

Theorem 6.3.1. Fix the edge labels on (G, L) , where $L = \{l_1, l_2, \dots, l_n\}$. $F = (0, \dots, 0, f_n)$ be an element of the $n - 1^{\text{th}}$ flow-up class, \mathbb{F}_{n-1} , in $\mathbb{S}_{(G, L)}$. Then the leading term, f_n , is a multiple of a least common multiple, m , of l_n and l_{n-1} . Furthermore, $f_n = m$ is a smallest flow-up class element satisfying the l_n and l_{n-1} conditions.

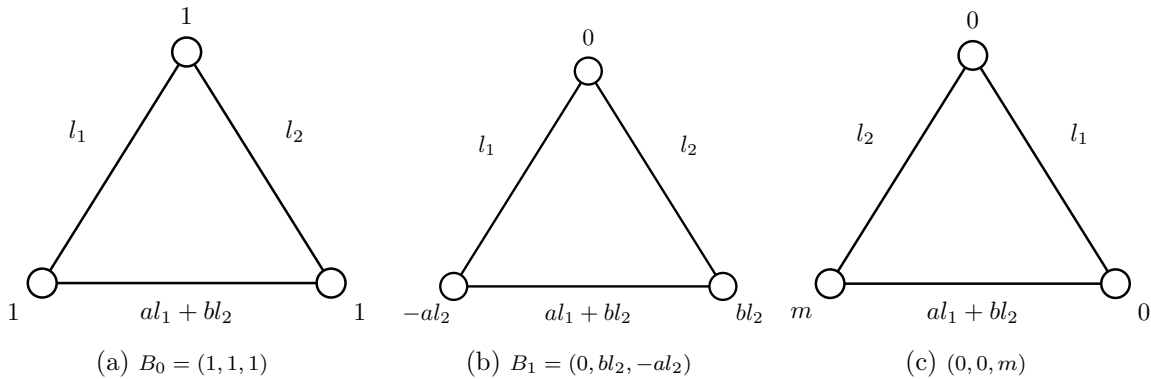
A rough proof to sway any doubts about this theorem:

Proof. Assuming F is a spline we know that

$$\begin{aligned} f_n &\equiv 0 \pmod{l_n} \\ 0 &\equiv f_n \pmod{l_{n-1}} \end{aligned}$$

Then $l_n | f_n - 0 = f_n$ and $l_{n-1} | f_n - 0 = f_n$. Then f_n may be any common multiple of l_n and l_{n-1} . Then by Definition 4.1.6 we know that f_n must be a multiple of a least common multiple, m , of l_n and l_{n-1} . \square

Theorem 6.3.2. Let G be a 3-cycle graph. Let $l_1, l_2 \in \mathbb{R}[x, y] - 0$ and $a, b \in \mathbb{R}$ with $a, b \neq 0$. Let $L = \{l_2, al_1 + bl_2, l_1\}$ be our set of edge labels. Let m be a least common multiple of $al_1 + bl_2$ and l_1 . Let $B_0 = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$, $B_1 = \begin{bmatrix} 0 \\ bl_2 \\ -al_1 \end{bmatrix}$, $B_2 = \begin{bmatrix} 0 \\ 0 \\ m \end{bmatrix}$ be sets of vertex labels on the (G, L) . Then B_0, B_1, B_2 are splines that form a basis for all splines on (G, L) , $\mathbb{S}_{(G, L)}$.



Proof. Firstly, we need to show that B_0, B_1, B_2 are indeed splines on (G, L) . B_0 is so obviously a spline, $1 \equiv 1 \pmod{m}$ for all $m \in \mathbb{R}[x, y]$. As for B_1 , we know $0 \equiv bl_2 \pmod{l_2}$, and $0 \equiv -al_1$

mod l_1 . Also $-al_1 - bl_2 = (-1)(al_1 + bl_2)$. Then $al_1 + bl_2 \mid -al_1 - bl_2$ thus B_1 is a spline. It is also trivial to see that B_2 is a spline.

Now to show that these splines form a basis for $\mathbb{S}_{(G,L)}$. By hypothesis that $a, b \neq 0$. Let $F = (f_1, f_2, f_3)$. Then let $F' = F - f_1B_0$. Then,

$$F' = F - f_1B_0 = \begin{bmatrix} f_1 \\ f_2 \\ f_3 \end{bmatrix} - \begin{bmatrix} f_1 \\ f_1 \\ f_1 \end{bmatrix} = \begin{bmatrix} 0 \\ f_2 - f_1 \\ f_3 - f_1 \end{bmatrix}$$

We know splines on n -cycle graphs form an $R[x, y]$ module. Then since F' is a linear combination over $\mathbb{R}[x, y]$ of splines on (G, L) we know that it is itself a spline, by Theorem 5.2.1. Since F' is a spline we know that $f_2 - f_1 \equiv 0 \pmod{l_2}$. Thus $l_2 \mid f_2 - f_1$. Then there exists some $m \in \mathbb{R}[x, y]$ such that $l_2m = f_2 - f_1$. Then $F' = (0, f_2 - f_1, f_3 - f_1) = (0, l_2m, f_3 - f_1)$. Now let $F'' = F' - \frac{m}{b}B_1$. Then

$$F'' = F' - \frac{m}{b}B_1 \begin{bmatrix} 0 \\ l_2m \\ f_3 - f_1 \end{bmatrix} - \begin{bmatrix} 0 \\ l_2m \\ -\frac{aml_1}{b} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ f_3 - f_1 + \frac{aml_1}{b} \end{bmatrix}$$

Note that $m/b \in \mathbb{R}[x, y]$ then F'' is a linear combination over $\mathbb{R}[x, y]$ of splines. Thus it also a spline by Theorem 5.2.1. Then $f_3 - f_1 + \frac{aml_1}{b} \equiv 0 \pmod{al_1 + bl_2}$ and $f_3 - f_1 + \frac{aml_1}{b} \equiv 0 \pmod{l_1}$. Then $f_3 - f_1 + \frac{aml_1}{b}$ is a common multiple of $al_1 + bl_2$ and l_1 . Then $m \mid f_3 - f_1 + aml_1$. Then for some $n \in \mathbb{R}[x, y]$ it is the case that $mn = f_3 - f_1 + aml_1$. Then $F'' = (0, 0, f_3 - f_1 + \frac{aml_1}{b}) = (0, 0, mn)$. Let $F''' = F'' - nB_2$. Then

$$F''' = F'' - nB_2 = \begin{bmatrix} 0 \\ 0 \\ mn \end{bmatrix} - \begin{bmatrix} 0 \\ 0 \\ mn \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Then $F = F' + f_1B_0 = F'' + \frac{m}{b}B_1 + f_1B_0 = nB_2 + \frac{m}{b}B_1 + f_1B_0$. Thus any spline in $\mathbb{S}_{(G,L)}$ is in the span of B_0, B_1, B_2 when $L = \{l_2, al_1 + bl_2, l_1\}$ and $a, b \neq 0$. Thus B_0, B_1, B_2 is a basis. \square

Theorem 6.3.3. *Let G be an n -cycle graph with a set of edge labels, $L = \{l_1, l_2, l_3, \dots, l_n\}$ where $l_i = a_i l_1 + b_i l_n$ and $a_i, b_i \in \mathbb{R} - 0$ for all $2 \leq i \leq n - 1$ and $l_1, l_n \in \mathbb{R}[x, y] - 0$ are not multiples of each other. Let m be a least common multiple of l_{n-1} and l_n . Let $B_0 = \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix}$. Let*

$$B_1 = \begin{bmatrix} 0 \\ l_1 \\ l_1 \\ \vdots \\ \frac{b_{n-2}(a_{n-1}-1)}{a_{n-2}}l_n + a_{n-1}l_1 \\ (\frac{b_{n-2}(a_{n-1}-1)}{a_{n-2}} - b_{n-1})l_n \end{bmatrix} \quad \text{Let } B_i = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ l_i \\ l_i \\ \vdots \\ (\frac{-a_i+a_{n-1}}{a_{n-2}}b_{n-2} + b_i)l_n + a_{n-1}l_1 \\ (b_{n-1} + \frac{-a_i+a_{n-1}}{a_{n-2}}b_{n-2} + b_i)l_n \end{bmatrix} \quad \text{for } 2 \leq i \leq n-3$$

$$\text{Let } B_{n-2} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ l_{n-2} = a_{n-2}l_1 + b_{n-2}l_n \\ (b_{n-2} - \frac{a_{n-2}}{a_{n-1}}b_{n-1})l_n \end{bmatrix} \quad \text{Let } B_{n-1} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ m \end{bmatrix} \quad \text{Then all } B_j \text{ for } 1 \leq j \leq n-1 \text{ are}$$

splines that form a basis for $\mathbb{S}(G, L)$.

Proof. First, we will show that all B_j are splines. Recall that in order to do this we must show that for each spline, the i th vector component is congruent to the $(i+1)$ th vector component modulo l_i for $1 \leq i \leq n-1$ and the n th vector component is congruent to the first vector component modulo l_n . Since, $1 \equiv 1 \pmod{m}$ for all $m \in R[x, y] - 0$ we know B_0 is a spline.

Now we will show that B_1 is a spline. We know $0 \equiv l_1 \pmod{l_1}$ and $l_1 \equiv l_1 \pmod{m}$ for all m . Because $(\frac{b_{n-2}(a_{n-1}-1)}{a_{n-2}}l_n + a_{n-1}l_1) - l_1 = (\frac{b_{n-2}(a_{n-1}-1)}{a_{n-2}}l_n + (a_{n-1}-1)l_1) = \frac{(a_{n-1}-1)}{a_{n-2}}(b_{n-2}l_n + a_{n-2}l_1)$, we know that $b_{n-2}l_n + a_{n-2}l_1 | (\frac{b_{n-2}(a_{n-1}-1)}{a_{n-2}}l_n + a_{n-1}l_1) - l_1$. Then by definition $\frac{b_{n-2}(a_{n-1}-1)}{a_{n-2}}l_n + a_{n-1}l_1 \equiv l_1 \pmod{b_{n-2}l_n + a_{n-2}l_1}$. We know $\frac{b_{n-2}(a_{n-1}-1)}{a_{n-2}}l_n + a_{n-1}l_1 - (\frac{b_{n-2}(a_{n-1}-1)}{a_{n-2}} - b_{n-1})l_n = (\frac{b_{n-2}(a_{n-1}-1)}{a_{n-2}} - \frac{b_{n-2}(a_{n-1}-1)}{a_{n-2}} + b_{n-1})l_n + a_{n-1}l_1 = b_{n-1}l_n + a_{n-1}l_1 = b_{n-1}l_n + a_{n-1}l_1$. Then by definition $b_{n-1}l_n + a_{n-1}l_1 | \frac{b_{n-2}(a_{n-1}-1)}{a_{n-2}}l_n + a_{n-1}l_1 - (\frac{b_{n-2}(a_{n-1}-1)}{a_{n-2}} - b_{n-1})l_n$. Then $\frac{b_{n-2}(a_{n-1}-1)}{a_{n-2}}l_n + a_{n-1}l_1 \equiv (\frac{b_{n-2}(a_{n-1}-1)}{a_{n-2}} - b_{n-1})l_n \pmod{b_{n-1}l_n + a_{n-1}l_1}$. We know that $(\frac{b_{n-2}(a_{n-1}-1)}{a_{n-2}} - b_{n-1})l_n \equiv 0 \pmod{l_n}$ since $(\frac{b_{n-2}(a_{n-1}-1)}{a_{n-2}} - b_{n-1})l_n$ is a multiple of l_n . Then B_1 is a spline.

Now we will show B_i is a spline for $2 \leq i \leq n-3$. The leading term of B_i is obviously the $(i+1)$ th vector component since there is i leading zeroes. We know $0 \equiv 0 \pmod{m}$ for all $m \in \mathbb{R}[x, y] - 0$, $0 \equiv l_i \pmod{l_i}$, and $l_i \equiv l_i \pmod{h}$ for all $h \in \mathbb{R}[x, y] - 0$. Note that $l_i = a_i l_1 + b_i l_n$. Then, $(\frac{-a_i+a_{n-1}}{a_{n-2}}b_{n-2} + b_i)l_n + a_{n-1}l_1 - l_i = (\frac{-a_i+a_{n-1}}{a_{n-2}}b_{n-2} + b_i)l_n + a_{n-1}l_1 - (a_i l_1 + b_i l_n) = (\frac{-a_i+a_{n-1}}{a_{n-2}}b_{n-2} + b_i - b_i)l_n + (a_{n-1} - a_i)l_1 = (\frac{-a_i+a_{n-1}}{a_{n-2}}b_{n-2})l_n + (a_{n-1} - a_i)l_1 = (\frac{-a_i+a_{n-1}}{a_{n-2}})(b_{n-2}l_n +$

$a_{n-2}l_1$). Then $b_{n-2}l_n + a_{n-2}l_1 | (\frac{-a_i+a_{n-1}}{a_{n-2}}b_{n-2} + b_i)l_n + a_{n-1}l_1 - l_i$. Then $(\frac{-a_i+a_{n-1}}{a_{n-2}}b_{n-2} + b_i)l_n + a_{n-1}l_1 \equiv l_i \pmod{b_{n-2}l_n + a_{n-2}l_1}$. We know that $(\frac{-a_i+a_{n-1}}{a_{n-2}}b_{n-2} + b_i)l_n + a_{n-1}l_1 - (b_{n-1} + \frac{-a_i+a_{n-1}}{a_{n-2}}b_{n-2} + b_i)l_n = (\frac{-a_i+a_{n-1}}{a_{n-2}}b_{n-2} + b_i - b_{n-1} - \frac{-a_i+a_{n-1}}{a_{n-2}}b_{n-2} + b_i) + a_{n-1} = b_{n-1}l_n + a_{n-1}$. Then $b_{n-1}l_n + a_{n-1} | (\frac{-a_i+a_{n-1}}{a_{n-2}}b_{n-2} + b_i)l_n + a_{n-1}l_1 - (b_{n-1} + \frac{-a_i+a_{n-1}}{a_{n-2}}b_{n-2} + b_i)l_n$. Then $(\frac{-a_i+a_{n-1}}{a_{n-2}}b_{n-2} + b_i)l_n + a_{n-1}l_1 \equiv (b_{n-1} + \frac{-a_i+a_{n-1}}{a_{n-2}}b_{n-2} + b_i)l_n \pmod{b_{n-1}l_n + a_{n-1}}$. Finally, since $(b_{n-1} + \frac{-a_i+a_{n-1}}{a_{n-2}}b_{n-2} + b_i)l_n$ is a multiple of l_n we can deduce that $(b_{n-1} + \frac{-a_i+a_{n-1}}{a_{n-2}}b_{n-2} + b_i)l_n \equiv 0 \pmod{l_n}$. Then B_i is a spline for $2 \leq i \leq n-3$.

Now we will show B_{n-2} is a spline. Again we know $0 \equiv 0 \pmod{m}$ for all $m \in \mathbb{R}[x, y] - 0$ and $0 \equiv l_{n-2} \pmod{l_{n-2}}$. Since $a_{n-2}l_1 + b_{n-2}l_n - (b_{n-2} - \frac{a_{n-2}}{a_{n-1}}b_{n-1})l_n = a_{n-2}l_1 + (b_{n-2} - b_{n-2} + \frac{a_{n-2}}{a_{n-1}}b_{n-1})l_n = a_{n-2}l_1 + (\frac{a_{n-2}}{a_{n-1}}b_{n-1})l_n = (\frac{a_{n-2}}{a_{n-1}})(a_{n-1}l_1 + b_{n-1}l_n)$ we know that $a_{n-1}l_1 + b_{n-1}l_n | a_{n-2}l_1 + b_{n-2}l_n - ((b_{n-2} - \frac{a_{n-2}}{a_{n-1}}b_{n-1})l_n)$. Then $a_{n-2}l_1 + b_{n-2}l_n \equiv (b_{n-2} - \frac{a_{n-2}}{a_{n-1}}b_{n-1})l_n \pmod{a_{n-1}l_1 + b_{n-1}l_n}$. Finally, since $(b_{n-2} - \frac{a_{n-2}}{a_{n-1}}b_{n-1})l_n$ is a multiple of l_n we know that $(b_{n-2} - \frac{a_{n-2}}{a_{n-1}}b_{n-1})l_n \equiv 0 \pmod{l_n}$. Then B_{n-2} is a spline.

Now, will show B_{n-1} is a spline. We know $0 \equiv 0 \pmod{m}$ for all $m \in \mathbb{R}[x, y] - 0$. We know m is a multiple l_{n-1} and l_n then $m \equiv 0 \pmod{l_{n-1}}$ and $m \equiv 0 \pmod{l_n}$. Then B_{n-1} is a spline.

Now we will show that the proposed basis spans.

Let $G = (g_1, g_2, \dots, g_n)$ be a spline on (G, L) with $g_i \in \mathbb{R}[x, y] - 0$ for $1 \leq i \leq n$. Then define G_1 as

$$G_1 = G - g_1 G_0 = \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_n \end{bmatrix} - \begin{bmatrix} g_1 \\ g_1 \\ \vdots \\ g_1 \end{bmatrix} = \begin{bmatrix} 0 \\ g_2 - g_1 \\ \vdots \\ g_n - g_1 \end{bmatrix}$$

By Theorem 3.2.1, we know that G_1 is a spline. Then $g_2 - g_1 \equiv 0 \pmod{l_1}$. Then $g_2 - g_1 = g_2^* l_1$

for some $g_2^* \in \mathbb{R}[x, y]$. Define G_2 as

$$G_2 = G_1 - g_2^* B_1 = \begin{bmatrix} 0 \\ g_2^* l_1 \\ g_3 - g_1 \\ \vdots \\ g_{n-1} - g_1 \\ g_n - g_1 \end{bmatrix} - \begin{bmatrix} 0 \\ g_2^* l_1 \\ g_2^* l_1 \\ \vdots \\ g_2^* \frac{b_{n-2}(a_{n-1}-1)}{a_{n-2}} l_n + a_{n-1} l_1 \\ g_2^* (\frac{b_{n-2}(a_{n-1}-1)}{a_{n-2}} - b_{n-1}) l_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ g_3 - g_1 - g_2^* l_1 \\ \vdots \\ g_{n-1} - g_1 - g_2^* \frac{b_{n-2}(a_{n-1}-1)}{a_{n-2}} l_n + a_{n-1} l_1 \\ g_n - g_1 - g_2^* (\frac{b_{n-2}(a_{n-1}-1)}{a_{n-2}} - b_{n-1}) l_n \end{bmatrix}$$

Now, note that since G_2 is a spline $g_3 - g_1 - g_2^* l_1 \equiv 0 \pmod{l_2}$. Thus $g_3 - g_1 - g_2^* l_1 = g_3^* l_2$ for some $g_3^* \in \mathbb{R}[x, y]$. Then define G_3 to be

$$G_3 = G_2 - g_3^* B_2 = \begin{bmatrix} 0 \\ 0 \\ g_3^* l_2 \\ g_4 - g_1 - g_2^* l_1 \\ \vdots \\ g_{n-1} - g_1 - g_2^* \frac{b_{n-2}(a_{n-1}-1)}{a_{n-2}} l_n + a_{n-1} l_1 \\ g_n - g_1 - g_2^* \left(\frac{b_{n-2}(a_{n-1}-1)}{a_{n-2}} - b_{n-1} \right) l_n \end{bmatrix} - \begin{bmatrix} 0 \\ 0 \\ g_3^* l_2 \\ g_3^* l_2 \\ \vdots \\ g_3^* \left(\left(\frac{-a_2 + a_{n-1}}{a_{n-2}} b_{n-2} + b_2 \right) l_n + a_{n-1} l_1 \right) \\ g_3^* \left((b_{n-1} + \frac{-a_2 + a_{n-1}}{a_{n-2}} b_{n-2} + b_2) l_n \right) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ g_4 - g_1 - g_2^* l_1 - g_3^* l_2 \\ \vdots \end{bmatrix}$$

Some of the column vector components, like the $(n-1)$ th and n th components of G_3 , are not explicitly stated because they are far too long and complicated to fully write out. Moreover, they will be expressed differently, and more concisely, later in the proof based on values to which they are congruent. So, there is not really any point in putting the reader through such a terrible experience. The important thing is that each difference of splines is also spline. Thus G_3 is still a spline. Then $g_4 - g_1 - g_2^* l_1 - g_3^* l_2 \equiv 0 \pmod{l_3}$ and $g_4 - g_1 - g_2^* l_1 - g_3^* l_2 = g_4^* l_3$ for some $g_4^* \in \mathbb{R}[x, y]$ which leads us to defining G_4 as $G_4 = G_3 - g_4^* B_3$. We can iterate this process until we define G_{n-3} as $G_{n-2} = G_{n-3} - g_{n-2}^* B_3$ for some $g_{n-2}^* \in \mathbb{R}[x, y]$. G_{n-2} will be an element of \mathbb{F}_{n-2} on (G, L) . This means the leading term of G_{n-2} is the $n-1$ th (2nd to last) vector component; let's call it α for now. While we're at it, let's refer to the n th component of G_{n-2} as β . Since α is the leading term we know that $\alpha \equiv 0 \pmod{l_{n-2}}$. Then $\alpha = g_{n-1}^* l_{n-2}$. Define G_{n-1} as

$$G_{n-1} = G_{n-2} - g_{n-1}^* B_{n-2} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ \alpha = g_{n-1}^* l_{n-2} \\ \beta \end{bmatrix} - \begin{bmatrix} 0 \\ 0 \\ \vdots \\ g_{n-1}^* l_{n-2} \\ g_{n-1}^* (b_{n-2} - \frac{a_{n-2}}{a_{n-1}} b_{n-1}) l_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ \beta - g_{n-1}^* (b_{n-2} - \frac{a_{n-2}}{a_{n-1}} b_{n-1}) l_n \end{bmatrix}$$

Since G_{n-1} is a spline we know that $\beta - (b_{n-2} - \frac{a_{n-2}}{a_{n-1}} b_{n-1}) l_n \equiv 0 \pmod{l_{n-1}}$ and $\beta - (b_{n-2} - \frac{a_{n-2}}{a_{n-1}} b_{n-1}) l_n \equiv 0 \pmod{l_{n-1}}$. Then $\beta - (b_{n-2} - \frac{a_{n-2}}{a_{n-1}} b_{n-1}) l_n \equiv 0 \pmod{l_{n-1}}$ is a common multiple of l_{n-1} and l_n . Then for some $g_n^* \in \mathbb{R}[x, y]$ we know $m | \beta - (b_{n-2} - \frac{a_{n-2}}{a_{n-1}} b_{n-1}) l_n$. by definition of divisibility. Then $(b_{n-2} - \frac{a_{n-2}}{a_{n-1}} b_{n-1}) l_n = g_n^* m$. Then

$$G_{n-1} - g_n^* B_{n-1} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ g_n^* m \end{bmatrix} - \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ g_n^* m \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{bmatrix}$$

We have arrived at $G - g_1 B_0 - \sum_{i=2}^n g_i^* B_{i-1} = 0$. Then $G = g_1 B_0 + \sum_{i=2}^n g_i^* B_{i-1}$. Then any spline $G \in \mathbb{S}[x, y]$ is in the span of B_j .

Now we will show that the proposed basis is linearly independent. Fret not, however; this is the easy part. It also gives us the opportunity to put our basis elements into a matrix. This allows me to end the project with what might very well be the most disgusting matrix in the history of Bard Senior Projects. This is very exciting.

$$\begin{bmatrix}
 1 & 0 & 0 & 0 & \dots & 0 \\
 1 & l_1 & 0 & 0 & \dots & 0 \\
 1 & l_1 & l_2 & 0 & \dots & 0 \\
 1 & l_1 & l_2 & l_3 & \dots & 0 \\
 \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
 1 & l_1 & l_2 & l_3 & \dots & l_{n-4} \\
 1 & l_1 & l_2 & l_3 & \dots & l_{n-4} \\
 1 & \frac{b_{n-2}(a_{n-1}-1)}{a_{n-2}} l_n + a_{n-1} l_1 & (\frac{-a_2+a_{n-1}}{a_{n-2}} b_{n-2} + b_2) l_n + a_{n-1} l_1 & (\frac{-a_3+a_{n-1}}{a_{n-2}} b_{n-2} + b_3) l_n + a_{n-1} l_1 & \dots & (\frac{-a_{n-4}+a_{n-1}}{a_{n-2}} b_{n-2} + b_{n-4}) l_n + a_{n-1} l_1 \\
 1 & (\frac{b_{n-2}(a_{n-1}-1)}{a_{n-2}} - b_{n-1}) l_n & (b_{n-1} + \frac{-a_2+a_{n-1}}{a_{n-2}} b_{n-2} + b_2) l_n & (b_{n-1} + \frac{-a_3+a_{n-1}}{a_{n-2}} b_{n-2} + b_3) l_n & \dots & (b_{n-1} + \frac{-a_{n-4}+a_{n-1}}{a_{n-2}} b_{n-2} + b_{n-4}) l_n
 \end{bmatrix}$$

Figure 6.3.2. We're gonna need a bigger boat

Observe Figure 6.3.2. The smallest font provided by $\text{L}^{\text{A}}\text{T}_{\text{E}}\text{X}$ is still too large to contain the entire matrix on one page. Instead we will note that because each spline, which falls into each column of the above matrix, is a sequence of elements from ascending flow up classes (\mathbb{F}_0 then \mathbb{F}_1 then ... then \mathbb{F}_{n-1}), we know that the matrix is lower triangular. Thus its determinant will be the product of the diagonal components all of which are not zero. Thus the product will not be zero. Thus the splines are linearly independent. \square

7

Future Work

With more time we would have looked at the following:

1. Can we abstract theory of integer splines on the diamond graph to PID splines on the diamond graph the same way we did with n-cycle splines?
2. Can we generalize our theory on $\mathbb{R}[x, y]$ splines on n-cycles to arbitrary UFDs on n-cycles. Instead of a_i and b_i being real numbers they would be units of our UFD.

I encourage any future Bard math seniors to explore these topics because I believe they would both be Rather promising. I mean come on, every mathematician likes generalizations.

Bibliography

- [1] Kenneth Rosen, *Elementary Number Theory & its applications*, Pearson, Boston, MA, 2011.
- [2] Kenneth Auslander and David Buchsbaum, *Groups, Rings, Modules*, Harper and Row, New York, NY, 1974.
- [3] John Fraleigh, *A First Course in Abstract Algebra*, Addison-Wesley, Reading, MA, 1982.
- [4] Thomas Hungerford, *Algebra*, 2nd ed., Springer, New York, NY, 2000.
- [5] Ester Gjoni, *Basis Criteria for n -cycle Integer Splines*, 2015, Bard senior project.
- [6] Emmet Mahdavi, *Integer Generalized Splines on the Diamond Graph*, 2016, Bard senior project.
- [7] Madeline Handschy, Julie Melnick, and Stephanie Reinders, *Integer Generalized Splines on Cycles*. arXiv:1409.1481.