

Louisiana State University

LSU Scholarly Repository

LSU Historical Dissertations and Theses

Graduate School

1997

Graphs and Number Theory.

Brian Heck

Louisiana State University and Agricultural & Mechanical College

Follow this and additional works at: https://repository.lsu.edu/gradschool_disstheses

Recommended Citation

Heck, Brian, "Graphs and Number Theory." (1997). *LSU Historical Dissertations and Theses*. 6491.
https://repository.lsu.edu/gradschool_disstheses/6491

This Dissertation is brought to you for free and open access by the Graduate School at LSU Scholarly Repository. It has been accepted for inclusion in LSU Historical Dissertations and Theses by an authorized administrator of LSU Scholarly Repository. For more information, please contact gradetd@lsu.edu.

INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

UMI

**A Bell & Howell Information Company
300 North Zeeb Road, Ann Arbor MI 48106-1346 USA
313/761-4700 800/521-0600**

GRAPHS AND NUMBER THEORY

A Dissertation

**Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy**

in

The Department of Mathematics

**by
Brian Heck
B.S., McMurry College, 1990
M.S., Louisiana State University, 1994
August 1997**

UMI Number: 9808748

UMI Microform 9808748
Copyright 1997, by UMI Company. All rights reserved.

**This microform edition is protected against unauthorized
copying under Title 17, United States Code.**

UMI
300 North Zeeb Road
Ann Arbor, MI 48103

ACKNOWLEDGEMENTS

I would first like to thank my adviser, Dr. Jurgen Hurrelbrink. In addition to his wisdom and knowledge, his support, guidance and especially his patience were invaluable. I also want to thank Dr. P. E. Conner for all his help and advise and I am thankful to Dr. Bogdan Oporowski for his help with the computer computations and preparation of this dissertation.

Finally, I wish to extend a very special thank you to my fiancée, Jennifer Sommers. I thank her for her love, her encouragement and her unconditional support. This accomplishment means so much more because she is in my life.

TABLE OF CONTENTS

ACKNOWLEDGMENTS	ii
ABSTRACT	iv
INTRODUCTION	1
CHAPTER	
1 CIRCULANT GRAPHS	5
1: Preliminaries	5
2: The Invariant $c(\Gamma)$	9
3: Circulant Graphs	16
4: The Group $G(S)$	34
5: The Role of $2 \in (\mathbb{Z}/p\mathbb{Z})^*$	41
6: The Automorphism Group of a Circulant Graph	48
2 QUOTIENT GRAPHS	61
1: The Deleted Graph and the Quotient Graph	61
2: The Quotient Graph $Q(S)$	68
3: Idempotence and the Quotient Graph	74
4: The Modified Quotient Graph	80
5: The Characteristic Polynomial of $Q(S)$	86
6: Examples	91
3 FORMAL QUOTIENT GRAPHS	108
1: The General Situation	108
2: How Many Formal Quotient Graphs Are There?	114
3: Examples	122
4: Generating Idempotent Formal Quotient Graphs	126
5: Summary	133
BIBLIOGRAPHY	139
APPENDIX	142
VITA	144

ABSTRACT

In the 1930's, L. Rédei and H. Reichardt used certain matrices to aid in the determination of the structure of ideal class groups of quadratic number fields. This is a classical number theoretic problem which in general presents difficulties. Ideal class groups are finite abelian groups, and it is a result of Gauss that allows us to determine their 2-rank, in other words the number of cyclic factors of even order. Rédei and Reichardt worked on determining the 4-rank, the number of factors of order divisible by 4. Later, the classical study of circulant graphs was utilized to further help this determination. In particular, if we relate a certain circulant graph G to a quadratic number field, then the number of Eulerian Vertex Decompositions of G is closely related to the 4-rank of the ideal class group of the quadratic number field.

Circulant graphs however become large rather quickly. Recently, P. E. Conner and J. Hurrelbrink developed the concept of quotient graphs. These are significantly smaller graphs, yet by analyzing their structure, one can determine much of the same number theoretic information, including the 4-rank of the ideal class group of the related quadratic number field, as one can from the underlying circulant graph. Formal quotient graphs are a generalization of quotient graphs and are a useful tool in determining how many graphs on a given number of vertices can be realized as quotient graphs.

In Chapter 1, we develop the background information on circulant graphs and explore their structure. We then utilize circulant graphs in Chapter 2 with

the development of quotient graphs. In this chapter we determine exactly which graphs on 2, 3, 4, 5 and 7 vertices are quotient graphs. Finally in Chapter 3, we develop the concept of formal quotient graphs as a generalization of quotient graphs. By analyzing the general situation, we are able to count how many formal quotient graphs there are on 11, 13, 17 and 19 vertices and realize many of these graphs as actual quotient graphs.

INTRODUCTION

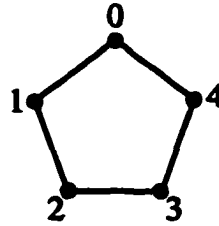
It is often surprising yet exciting when two distinct areas of mathematics are brought together and one is utilized to make progress in classical areas of the other. Seemingly unrelated topics become relevant and questions previously thought to be out of reach suddenly seem achievable. Such is the case with topics in graph theory and number theory. Recently, see for example [M] and [K], graphs and tournaments (simple complete directed graphs) have been used to make progress towards two questions from algebraic number theory:

- (1) What is the structure of ideal class groups of quadratic number fields?
- (2) What is the number of solutions to Diophantine equations over finite fields?

While these questions have yet to be fully answered, graph theory has enabled us to learn a great deal about the solutions. In this dissertation, we further explore the relevant graphs which hold information pertaining to algebraic number theory.

In Chapter 1, we discuss certain types of graphs called **circulant graphs**. By a **graph**, we mean a simple graph with a nonempty, finite set of vertices. So we will only consider graphs with no loops or multiple edges. A circulant graph is a graph with the property that for some labeling of its vertices, the adjacency matrix is a circulant matrix. We can state this another way. Define a set $S \subseteq (\mathbb{Z}/p\mathbb{Z})^*$ with the property that $(-1)S = S$. The circulant graph $\Gamma(S)$ is a graph with vertex set $V = \{0, 1, \dots, n-1\}$ and edges defined by the following condition: two vertices i and j are adjacent if and only if $i - j \in S$.

Example: Let $n = 5$ and $S = \{\pm 1\}$. Then the circulant graph $\Gamma(S)$ is



In this chapter, we explore an invariant of graphs, denoted by $c(\Gamma)$, and explain its importance to both graph theorists and number theorists. In short, for a given graph Γ , we consider a vertex decomposition of Γ . This is an unordered pair $\{U_1, U_2\}$ of subsets of the vertex set V such that $U_1 \cup U_2 = V$ and $U_1 \cap U_2 = \emptyset$. If every vertex is adjacent to an even number of vertices in the subset to which it does not belong, then the vertex decomposition is called an **Eulerian Vertex Decomposition (EVD)**. A question graph theorists deal with is:

For a given graph, how many EVD's does it have?

We show in Chapter 1 that this number is always a power of 2 and denote the exponent by $c(\Gamma)$. Therefore,

$$\# \text{ EVD's of } \Gamma = 2^{c(\Gamma)}.$$

There is a number theoretic reason to determine this number $c(\Gamma)$ also. For a given quadratic number field, determining the structure of the ideal class group is a classical problem. We know that ideal class groups are always finite and abelian. So we know that they are finite products of cyclic groups of prime power order. Gauss discovered a formula for determining the **2-rank** of the ideal class group of a given quadratic number field. The 2-rank is the number of cyclic factors of even order. Then in the 1930's, L. Rédei and H. Reichardt used certain matrices

to make significant progress by determining the **4-rank**, the number of cyclic factors of order divisible by 4. What does this have to do with $c(\Gamma)$? Let E be a quadratic number field, with ideal class group $C(E)$. A consequence of Rédei and Reichardt's work is that we can relate a graph, Γ_E , to E and then it has been proved that

$$\text{4-rank } C(E) = c(\Gamma).$$

In fact, by Dirichlet's Theorem on primes in arithmetic progressions, we know that *any* graph can be viewed as the associated graph to some quadratic number field. So we study this number $c(\Gamma)$, in the context of circulant graphs, extensively in Chapter 1 to gain insight towards the classical problem of determining the structure of ideal class groups.

Circulant graphs created in this fashion tend to be quite large. So in Chapter 2, we introduce the concept of **quotient graphs**. These graphs are significantly smaller graphs (more specifically, much fewer vertices), yet we can still determine the same number theoretic information. Namely, if $\Gamma(S)$ is a circulant graph, and $Q(S)$ is its related quotient graph, we will show that

$$c(Q(S)) = \frac{c(\Gamma(S))}{\#S}.$$

Counting the number of EVD's of $Q(S)$ is much easier than counting this number for $\Gamma(S)$ (since $Q(S)$ has so many fewer vertices), so our study of quotient graphs enables us to understand the 4-rank question even better than before. We determine in this chapter exactly which graphs on 2, 3, 4, 5 and 7 vertices are quotient graphs, and therefore we know all values for $c(Q(S))$ (and hence $c(\Gamma(S))$)

in these cases. In addition, quotient graphs shed some light on the second classical number theoretic question about Diophantine equations. In particular, given a Diophantine equation, we can relate to it a quotient graph and then the existence (or non-existence) of an edge between two vertices in the quotient graph will determine whether there are an odd (or an even) number of solutions in certain finite fields to the given Diophantine equation.

Even these graphs, however, get rather large quickly. So we then generalize the situation in Chapter 3 and develop the idea of **formal quotient graphs**. In this chapter, we show that every quotient graph, Q , is in fact a formal quotient graph, FQ , and we count how many formal quotient graphs there are on 11, 13, 17 and 19 vertices. Then we can determine all the values of $c(FQ)$, and hence we know what the *possible* values of $c(Q)$ are for many more classes of quotient graphs. Finally we are able to use a computer and in several cases realize many formal quotient graphs as actual quotient graphs.

With regards to notation: lemmas, propositions, corollaries, theorems, definitions and examples are all numbered consecutively within each section. For example, if the third item in Section 4 of Chapter 2 is a lemma, then it is labeled Lemma 2.4.3 and the next item (which is a proposition) is labeled Proposition 2.4.4. A black box (■) is used to indicate the end of a proof.

CHAPTER 1: CIRCULANT GRAPHS

Section 1: Preliminaries

To completely understand and discuss circulant graphs, which will be defined later (see 1.3.1), we first need to define the terminology and notation we will be using. We begin with some definitions and results from graph theory.

(1.1.1) **Definition:** Let Γ be a graph with $V = V(\Gamma)$ denoting the vertex set. For each vertex $v \in V$, we define the **set of neighbors of v** to be the set

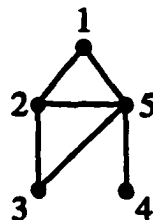
$$N(v) = \{w \in V : v \text{ is adjacent to } w \text{ in } \Gamma\}.$$

Hence we have that the **degree** of the vertex v is $\#N(v)$.

(1.1.2) **Definition:** A **vertex decomposition** of a graph Γ is an unordered pair of subsets, $\{U_1, U_2\}$, of the vertex set V of Γ with (1) $U_1 \cup U_2 = V$ and (2) $U_1 \cap U_2 = \emptyset$. We will usually write $U = U_1$ and $V \setminus U = U_2$.

(1.1.3) **Definition:** A vertex is **special with respect to the vertex decomposition** $\{U, V \setminus U\}$ if it is adjacent to an odd number of vertices in the subset to which it does not belong. We define the set $P(\Gamma, U)$ to be the set of vertices in the graph Γ which are special with respect to the vertex decomposition $\{U, V \setminus U\}$.

(1.1.4) **Example:** Consider the following graph, Γ :



If we let $U = \{1, 2\}$ and $V \setminus U = \{3, 4, 5\}$, then we see that the vertex 1 is adjacent

to only one vertex (the vertex 5) in $V \setminus U$ and the vertex 3 is adjacent to only one vertex (the vertex 2) in U . All other vertices are adjacent to an even number of vertices in the subset to which they do not belong. Therefore, for this vertex decomposition $P(\Gamma, U) = \{1, 3\}$. If we let $U = \{1, 3\}$, then $P(\Gamma, U) = \emptyset$.

We now point out several basic facts which follow directly from these definitions and can be easily verified.

(1.1.5) Remarks:

(1) $P(\Gamma, U) = P(\Gamma, V \setminus U)$.

(2) $P(\Gamma, \emptyset) = \emptyset$.

(3) If Γ_{td} is a totally disconnected graph (i.e. a graph with no edges), then $P(\Gamma_{td}, U) = \emptyset$, for any subset $U \subseteq V$.

(4) If K_n is a complete graph with an even number of vertices, then for any subset $U \subseteq V$ with $\#U$ odd, we have $P(K_n, U) = V$.

(5) If K_n is a complete graph with an odd number of vertices, then for any subset $U \subseteq V$ with $U \neq \emptyset$ or V , $P(K_n, U) \neq \emptyset$.

We now will consider a subgraph of Γ by utilizing the vertex decomposition $\{U, V \setminus U\}$. We denote this subgraph by Γ_U and define it as follows: Γ_U has the same set of vertices as Γ , but two distinct vertices are adjacent in Γ_U if and only if they are adjacent in Γ *and* they lie in different subsets of the vertex decomposition. Clearly a vertex $v \in V$ will be special in Γ with respect to the vertex decomposition $\{U, V \setminus U\}$ if and only if v has *odd* degree in the subgraph Γ_U .

(1.1.6) **Lemma:** For any subset $U \subseteq V$, we have

$$\#P(\Gamma, U) \equiv 0(2).$$

Proof: The “Handshake Lemma” (see Corollary 1.1 in [BM]) says that the number of vertices of odd degree in any graph is always even. In particular, the number of vertices in Γ_U of odd degree is even for any U . Therefore, the number of special vertices in Γ is even as well. ■

(1.1.7) **Definition:** A vertex decomposition $\{U, V \setminus U\}$ is called an **Eulerian Vertex Decomposition (EVD)** if $P(\Gamma, U) = \emptyset$.

In other words, $\{U, V \setminus U\}$ is an EVD if and only if every vertex is adjacent to an *even* number of vertices in the subset of V to which it does not belong. The name “Eulerian Vertex Decomposition” is the natural choice since we see that by the way the subgraph Γ_U was defined, a vertex decomposition is Eulerian if the subgraph Γ_U associated to it is an Eulerian graph. Remark 1.1.5(2) implies that the trivial vertex decomposition $\{\emptyset, V\}$ is always an EVD, and Remark 1.1.5(5) implies that the only EVD for a complete graph with an odd number of vertices is the trivial one. For Eulerian graphs we have another characterization of special vertices.

(1.1.8) **Lemma:** Let Γ be an Eulerian graph. Then $v \in V$ is a special vertex with respect to the vertex decomposition $\{U, V \setminus U\}$ if and only if v is adjacent to an odd number of vertices in the subset of V to which it *does* belong.

Proof: In an Eulerian graph, every vertex has even degree. Therefore a vertex is adjacent to an odd number of vertices in one subset of a vertex decomposition if

and only if it is also adjacent to an odd number of vertices in the other. ■

Now for any graph Γ on an ordered set of vertices $V = \{v_1, v_2, \dots, v_n\}$ we have the familiar adjacency matrix of Γ . This is an $n \times n$ matrix $A = (a_{ij})$ over \mathbf{F}_2 defined by the condition

$$a_{ij} = 1 \iff v_i \text{ and } v_j \text{ are adjacent.}$$

We will now define the Rédei matrix, which is a modification of this matrix.

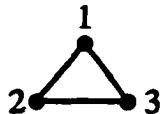
(1.1.9) **Definition:** Let Γ be a graph with $V = \{v_1, v_2, \dots, v_n\}$. The **Rédei matrix** $M = (m_{ij})$ is the $n \times n$ matrix over the field \mathbf{F}_2 given by

$$m_{ij} = \begin{cases} 1 & \text{if } i \neq j \text{ and } v_i \text{ is adjacent to } v_j \text{ in } \Gamma, \\ 0 & \text{if } i \neq j \text{ and } v_i \text{ is not adjacent to } v_j \text{ in } \Gamma, \\ \#N(v_i) \bmod 2 & \text{if } i = j \end{cases}$$

Clearly the Rédei matrix M of any graph Γ will be a symmetric matrix over the field \mathbf{F}_2 . The entries of M will be identical to the entries of the usual adjacency matrix A except perhaps along the diagonal.

(1.1.10) **Examples:**

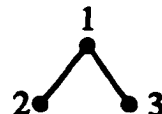
(1) If Γ is the graph



then its Rédei matrix is

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

(2) If Γ is the graph



then its Rédei matrix is

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

We can consider the Rédei matrix M to be the adjacency matrix with an adjustment along the diagonal so that each row (and each column) will sum to

0 in \mathbb{F}_2 . Notice that if a vertex has even degree, then its row in the adjacency matrix *already* adds up to 0 in \mathbb{F}_2 . Hence M and A will be identical if and only if every vertex of the graph has even degree. Since the rows of the Rédei matrix M sum to 0 in \mathbb{F}_2 , M is not of maximal rank over \mathbb{F}_2 . In other words, for any graph Γ on n vertices,

$$\text{rank}_{\mathbb{F}_2} M < n.$$

We will explain the connection between the above two concepts (Eulerian vertex decompositions and Rédei matrices) in the next section by showing that the rank of the Rédei matrix and the number of distinct EVD's of a graph determine each other.

Section 2: The Invariant $c(\Gamma)$

What does the number of EVD's of a graph have to do with its Rédei matrix?

For an indication, consider Γ_{td} , the totally disconnected graph with n vertices. The number of EVD's of Γ_{td} is as large as possible, namely 2^{n-1} , while the rank of its Rédei matrix is as small as possible, namely 0. In this section, we will explain this relationship.

For this entire section, let Γ be a graph with vertex set $V = \{v_1, v_2, \dots, v_n\}$ and Rédei matrix M . Let W be the n -dimensional vector space over \mathbb{F}_2 . We will consider the elements of W to be $n \times 1$ column matrices $\bar{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ with entries in \mathbb{F}_2 . Define $\bar{w} = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$. We see that the Rédei matrix M defines a linear

operator

$$(1.2.1) \quad T: W \longrightarrow W \text{ defined by}$$

$$T(\bar{x}) = M\bar{x}.$$

Notice that since each row of M sums to 0 in \mathbf{F}_2 , we have $\bar{w} \in \text{Ker}(T)$. We now present a lemma which will be useful later in Chapter 2.

(1.2.2) **Lemma:** If \bar{y} is in the image of T , then $\bar{y} \cdot \bar{y} = 0$.

Proof: We will show that the number of nonzero entries of \bar{y} is even. Let $\bar{y} = (y_i)$ be in the image of T . Then there exists a vector $\bar{x} = (x_i)$ such that

$$M\bar{x} = \bar{y}.$$

Consider the sum

$$\sum_{i=1}^n y_i.$$

This sum will equal 1 if and only if $y_i = 1$ for an odd number of indices. Since

$$y_i = \sum_{j=1}^n (m_{ij}x_j)$$

the sum $\sum_{i=1}^n y_i = 1$ if and only if $m_{ij}x_j = 1$ for an odd number of pairs of indices. However, $m_{ij}x_j = 1$ if and only if both $x_j = 1$ and $m_{ij} = 1$. By the definition of M , this is impossible. For any fixed j , the number of indices i with $m_{ij} = 1$ is even. So for each $x_j = 1$ there are an even number of m_{ij} which also equal 1. Therefore, $\sum_{i=1}^n y_i = 0$ and hence $\bar{y} \cdot \bar{y} = 0$. ■

Let \mathcal{S} be the set of all subsets of $V = \{v_1, v_2, \dots, v_n\}$. With respect to symmetric difference, \mathcal{S} is an elementary abelian 2-group of rank n , and as such,

it is an n -dimensional vector space over \mathbb{F}_2 . For $U \in \mathcal{S}$, we define an element $\bar{x}_U = (x_i) \in W$ in a natural way: let $x_i = 1$ if and only if $v_i \in U$. We therefore have an isomorphism:

$$(1.2.3) \quad \mathcal{S} \xrightarrow{\cong} W \text{ given by}$$

$$U \mapsto \bar{x}_U.$$

We can now describe the linear operator $T: W \rightarrow W$ given by the Rédei matrix of Γ by determining $T(\bar{x}_U)$ for *every* subset $U \subseteq V$.

(1.2.4) **Proposition:** For any subset $U \subseteq V$,

$$T(\bar{x}_U) = \bar{x}_{P(\Gamma, U)}.$$

Proof: Let $U \subseteq V$. Let $\bar{x}_U = (x_i)$, $M = (m_{ij})$ and $\bar{x}_{P(\Gamma, U)} = (z_i)$. Then

$$T(\bar{x}_U) = M\bar{x}_U = (y_i) \text{ with}$$

$$y_i = \sum_{j=1}^n m_{ij}x_j = m_{ii}x_i + \sum_{j \neq i} m_{ij}x_j.$$

So what we wish to show is that

$$y_i = z_i \text{ for every } i.$$

Recall that for $i \neq j$,

$$(1.2.5) \quad \begin{aligned} m_{ij}x_j = 1 &\iff m_{ij} = 1 \text{ and } x_i = 1 \\ &\iff v_i \text{ is adjacent to } v_j \text{ in } \Gamma \text{ and } v_j \in U. \end{aligned}$$

Also,

$$(1.2.6) \quad \begin{aligned} m_{ii}x_i = 1 &\iff m_{ii} = 1 \text{ and } x_i = 1 \\ &\iff v_i \text{ has odd degree in } \Gamma \text{ and } v_i \in U. \end{aligned}$$

Since $\bar{x}_{P(\Gamma, U)} = (z_i)$ we know that

$$(1.2.7) \quad z_i = 1 \iff v_i \in P(\Gamma, U).$$

Suppose $v_i \notin U$. Then by (1.2.6), $m_{ii}x_i = 0$. Therefore $y_i = \sum_{j \neq i} m_{ij}x_j$. So

$$\begin{aligned} y_i = 1 &\iff m_{ij}x_j = 1 \text{ an odd number of times} \\ &\iff v_i \text{ is adjacent to an odd number of vertices of } U \\ &\iff v_i \in P(\Gamma, U) \\ &\iff z_i = 1. \end{aligned}$$

Now suppose $v_i \in U$. Then

$$y_i = 1 \iff (1) \ m_{ii}x_i = 1 \text{ and } \sum_{j \neq i} m_{ij}x_j = 0$$

or

$$(2) \ m_{ii}x_i = 0 \text{ and } \sum_{j \neq i} m_{ij}x_j = 1.$$

In Case (1), $m_{ii}x_i = 1$ implies v_i has odd degree, and $\sum_{j \neq i} m_{ij}x_j = 0$ implies v_i is adjacent to an even number of vertices of U . Together that implies that v_i is adjacent to an odd number of vertices not in U .

In Case (2), $m_{ii}x_i = 0$ implies v_i has even degree, and $\sum_{j \neq i} m_{ij}x_j = 1$ implies v_i is adjacent to an odd number of vertices of U . Together that implies that v_i is adjacent to an odd number of vertices not in U .

Therefore, in either case,

$$\begin{aligned} y_i = 1 &\iff v_i \in P(\Gamma, U) \\ &\iff z_i = 1, \end{aligned}$$

which proves the proposition. ■

(1.2.8) **Corollary:** The subsets $U \subseteq V$ for which

$$P(\Gamma, U) = U$$

form an additive subgroup of \mathcal{S} which is isomorphic to $\text{Ker}(T + I)$.

Proof: By the previous proposition, we know that $P(\Gamma, U) = U$ if and only if $T(\bar{x}_U) = \bar{x}_U$. In other words,

$$P(\Gamma, U) = U \iff (T + I)(\bar{x}_U) = \bar{0},$$

which proves the corollary. ■

(1.2.9) **Corollary:** For any subset $U \subseteq V$, $\{U, V \setminus U\}$ is an EVD of Γ if and only if $\bar{x}_U \in \text{Ker}(T)$.

Proof: Simply recall that

$$\{U, V \setminus U\} \text{ is an EVD of } \Gamma \iff P(\Gamma, U) = \emptyset$$

$$\iff \bar{x}_{P(\Gamma, U)} = \bar{0}$$

$$\iff T(\bar{x}_U) = \bar{0}$$

$$\iff \bar{x}_U \in \text{Ker}(T). \quad \blacksquare$$

We will now use these results to count the number of Eulerian vertex decompositions of a graph Γ . By this last corollary, we can do this by determining the size of the kernel of T . However, since complementary subsets of V give rise to the same EVD, we have

$$(1.2.10) \quad \# \text{ EVD's} = \frac{\# \text{Ker}(T)}{2}.$$

This will give us an explicit description of the number of EVD's of a graph in terms of the rank of its Rédei matrix.

(1.2.11) **Theorem:** Let Γ be a graph with n vertices and Rédei matrix M . Then

$$\# \text{ EVD's} = 2^{n-1-\text{rank}_{\mathbb{F}_2} M}.$$

Proof: From the definition of T , we know that the dimension of $\text{Ker}(T)$ over \mathbb{F}_2 is given by $n - \text{rank}_{\mathbb{F}_2} M$. So $\# \text{ Ker}(T) = 2^{n-\text{rank}_{\mathbb{F}_2} M}$. Therefore by 1.2.10,

$$\# \text{ EVD's} = \frac{\# \text{ Ker}(T)}{2} = 2^{n-1-\text{rank}_{\mathbb{F}_2} M}. \quad \blacksquare$$

In number theory, there is more motivation for being interested in the number of EVD's of graphs. Let us discuss one of the applications of this by recalling the connection to the structure of ideal class groups (See [RR]).

Consider a real quadratic number field $E = \mathbb{Q}(\sqrt{p_1 p_2 \cdots p_n})$ with $n \geq 1$ distinct prime numbers $p_i \equiv 1(4)$. Let $C(E)$ denote the narrow ideal class group of E . We denote the number of cyclic factors of $C(E)$ of order divisible by 4 by $4\text{-rk } C(E)$. Associate to E the graph Γ_E on an ordered set of vertices $V = \{v_1, v_2, \dots, v_n\}$ and define edges by the following condition: v_i is adjacent to v_j if and only if $i \neq j$ and the Legendre symbol $\left(\frac{p_i}{p_j}\right)$ is equal to -1 . We know from Dirichlet's Theorem that *every* graph Γ is a graph Γ_E for some quadratic number field E . Then we have the following theorem.

(1.2.12) **Theorem (Rédei-Reichardt):** Let E be a quadratic number field as described above and let Γ_E be its associated graph. Then

$$\# \text{ EVD's of } \Gamma_E = 2^{4\text{-rk } C(E)}.$$

For the proof of this we refer to [RR] and to the vast literature dealing with Rédei-Reichardt's 4-rank formula for ideal class groups. We have an immediate consequence of 1.2.11 and 1.2.12.

With E , Γ_E , $C(E)$ and M as above, we have

$$(1.2.13) \quad \begin{aligned} 4\text{-rk } C(E) &= n - 1 - \text{rank}_{\mathbb{F}_2} M \\ &= \text{corank}_{\mathbb{F}_2} M - 1. \end{aligned}$$

This formula can be traced back to 1934 and it allows us to define a graph invariant as follows.

(1.2.14) **Definition:** Let Γ be a graph on an ordered set of n vertices $V = \{v_1, v_2, \dots, v_n\}$. Let M be the Rédei matrix of Γ . We define a graph invariant $c(\Gamma)$ by

$$\begin{aligned} c(\Gamma) &= 4\text{-rk } C(E) = n - 1 - \text{rank}_{\mathbb{F}_2} M \\ &= \text{corank}_{\mathbb{F}_2} M - 1. \end{aligned}$$

In other words,

$$(1.2.15) \quad \# \text{ EVD's of } \Gamma = 2^{c(\Gamma)}.$$

Naturally, $c(\Gamma)$ is independent of the ordering of the vertices of Γ and is an invariant of the isomorphism class of the graph. We see that if $\#V = n$, then

$$(1.2.16) \quad 0 \leq c(\Gamma) \leq n - 1.$$

We can also express the invariant $c(\Gamma)$ in the following way:

$$(1.2.17) \quad c(\Gamma) = \dim \text{Ker}(T) - 1.$$

Notice that if $c(\Gamma) = n - 1$, then by definition $\text{rank}_{\mathbb{F}_2} M = 0$. So M is the zero matrix and hence Γ is the totally disconnected graph. At the other extreme, if $c(\Gamma) = 0$ then (by 1.2.15) Γ has only the trivial EVD given by $\{\emptyset, V\}$. Since a

disconnected graph always has a nontrivial EVD (simply choose the set U to be a connected component), we see that $c(\Gamma) = 0$ implies that Γ is a connected graph.

Finally, we wish to discuss the idempotence of the Rédei matrix M . Let

$$(1.2.18) \quad d(\Gamma) = \dim \operatorname{Ker}(T + I).$$

(1.2.19) **Lemma:** Let Γ be a graph. The Rédei matrix M is idempotent if and only if

$$c(\Gamma) + d(\Gamma) = n - 1.$$

Proof: Recall that a matrix M over \mathbf{F}_2 is idempotent if and only if M is diagonalizable over \mathbf{F}_2 . However, we know that the linear operator T associated to M is diagonalizable if and only if

$$\dim \operatorname{Ker}(T) + \dim \operatorname{Ker}(T + I) = n.$$

Using the fact that $c(\Gamma) = \dim \operatorname{Ker}(T) - 1$ and the definition of $d(\Gamma)$, the lemma follows. ■

We will investigate this graph invariant $c(\Gamma)$ further in Section 3 with our study of circulant graphs.

Section 3: Circulant Graphs

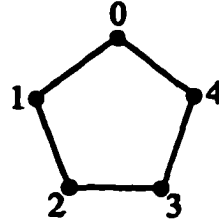
We define a circulant graph in the following way.

(1.3.1) **Definition:** Let p be a prime number. Let $S \subseteq (\mathbf{Z}/p\mathbf{Z})^*$ be a subset which is symmetric in the sense that $(-1)S = S$. Then we define a **circulant graph** $\Gamma(S)$ to be the graph with vertex set $V = 0, 1, \dots, p - 1$ and edges defined by the following condition: two vertices $i, j \in V$ are adjacent if and only if $i - j \in S$.

(1.3.2) **Examples:**

(1) Let $p = 5$ and $S = \{\pm 1\} \subseteq (\mathbb{Z}/5\mathbb{Z})^*$.

Then the circulant graph $\Gamma(S)$ is

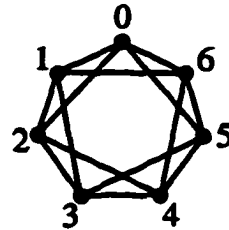


and its Rédei matrix M is

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

(2) Let $p = 7$ and $S = \{\pm 1, \pm 2\} \subseteq (\mathbb{Z}/7\mathbb{Z})^*$.

Then the circulant graph $\Gamma(S)$ is



and its Rédei matrix M is

$$\begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

A circulant graph $\Gamma(S)$ is an example of the general class of graphs known as **Cayley Graphs** (see [Bo]). We note that $\Gamma(S)$ is a connected graph if and only if $S \neq \emptyset$ since any non-empty set of units additively generates $\mathbb{Z}/p\mathbb{Z}$.

A circulant graph defined in this way is always regular. To see this notice that if $S = \{v_1, v_2, \dots, v_n\}$, then for any vertex x of $\Gamma(S)$, the vertices $x - v_1, x - v_2, \dots, x - v_n$ are all adjacent to x . Furthermore, if y is any vertex adjacent to x , then $x - y \in S$ (by definition of $\Gamma(S)$). So $x - y = v_i$ for some i . But that implies $y = x - v_i$. So in fact $\{x - v_1, x - v_2, \dots, x - v_n\}$ is the complete set of neighbors of x . Therefore every vertex of $\Gamma(S)$ has degree $n = \#S$.

Since $(-1)S = S$ and $0 \notin S$, we see that $\#S \equiv 0(2)$. So in fact if $S \neq \emptyset$,

(1.3.3) $\Gamma(S)$ is a regular *Eulerian* graph.

Also notice that the Rédei matrices of circulant graphs are circulant matrices (in fact, this is how the name “circulant” graph originated). We will now examine how the invariant $c(\Gamma(S))$ for circulant graphs on p vertices can be described via investigation of the group ring $\mathbf{F}_2[C_p]$ where C_p denotes the cyclic group of order p . This is most natural since, as we will show (see 1.3.35), the group ring $\mathbf{F}_2[C_p]$ is isomorphic to the ring of $p \times p$ circulant matrices.

To begin our discussion of the group ring $\mathbf{F}_2[C_p]$, we start with the polynomial ring $\mathbf{F}_2[x]$. For an odd prime p , the polynomial $x^p + 1$ generates the principal ideal $(x^p + 1) \subseteq \mathbf{F}_2[x]$. If C_p is the multiplicatively written cyclic group of order p with generator t , then recall that

$$\mathbf{F}_2[C_p] \simeq \mathbf{F}_2[x]/(x^p + 1)$$

by the identification $t \mapsto x$. We will use this isomorphism to analyze the structure of the group ring $\mathbf{F}_2[C_p]$. An element of this group ring can be uniquely written

in the form

$$\sum_{j=0}^{p-1} a_j t^j \quad \text{with } a_j \in \mathbf{F}_2 \quad \text{for all } j.$$

We now utilize the **augmentation homomorphism**:

$$(1.3.4) \quad \epsilon : \mathbf{F}_2[C_p] \longrightarrow \mathbf{F}_2 \quad \text{defined by}$$

$$\epsilon\left(\sum_{j=0}^{p-1} a_j t^j\right) = \sum_{j=0}^{p-1} a_j.$$

Since ϵ is onto, $\mathbf{F}_2[C_p]/\text{Ker}(\epsilon) \simeq \mathbf{F}_2$, so $\text{Ker}(\epsilon)$ is a maximal ideal of $\mathbf{F}_2[C_p]$. Now in $\mathbf{F}_2[x]$, we have the factorization

$$x^p + 1 = (x + 1)\phi_p(x)$$

where $\phi_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1$ is the *p-th cyclotomic polynomial*. Note that the factors are relatively prime. We want to examine the corresponding factors in $\mathbf{F}_2[C_p]$. Consider the map

$$\mathbf{F}_2[x]/(x^p + 1) \longrightarrow \mathbf{F}_2 \quad \text{determined by}$$

$$x \longmapsto 1.$$

The kernel of this map is the ideal $(x + 1)$. Since $\mathbf{F}_2[x]/(x^p + 1) \simeq \mathbf{F}_2[C_p]$ and the ideal $(x + 1)$ corresponds to the ideal $(t + 1)$ in $\mathbf{F}_2[C_p]$, we see that $\text{Ker}(\epsilon) = (t + 1)$.

Then the other factor, $\phi_p(x) \in \mathbf{F}_2[x]$, of $x^p + 1$ must correspond to the familiar

$$\Omega = t^{p-1} + t^{p-2} + \dots + t + 1 \in \mathbf{F}_2[C_p].$$

Note that multiplying Ω by t^j for any j simply permutes the terms of Ω . In other words,

$$(t^j)\Omega = \Omega \quad \text{for any } j.$$

So for any $\alpha \in \mathbf{F}_2[C_p]$, we have

$$(1.3.5) \quad \alpha\Omega = \epsilon(\alpha)\Omega.$$

In particular, $\Omega^2 = \Omega$ (since $\epsilon(\Omega) = 1$). Therefore the ideal generated by Ω consists only of Ω and 0 (i.e. $(\Omega) = \{0, \Omega\}$). Hence

$$(1.3.6) \quad \text{Ker}\epsilon \cap (\Omega) = (t+1) \cap (\Omega) = \{0\}.$$

Since $x+1$ and $\phi_p(x)$ are relatively prime in $\mathbf{F}_2[x]$, and using the Chinese Remainder Theorem we have

$$(1.3.7) \quad \begin{aligned} \mathbf{F}_2[C_p] &\simeq \mathbf{F}_2[x]/(x^p+1) \simeq \mathbf{F}_2[x]/(x+1) \oplus \mathbf{F}_2[x]/(\phi_p(x)) \\ &\simeq \mathbf{F}_2 \oplus \mathbf{F}_2[x]/(\phi_p(x)). \end{aligned}$$

We want to understand the second factor of this decomposition.

Let $\xi = e^{\frac{2\pi i}{p}}$. Then $\mathbf{Z}[\xi]$ will be the ring of integers of the p -th cyclotomic extension

$$\begin{array}{c} \mathbf{Q}(\xi) \\ | \\ \mathbf{Q} \end{array}$$

Clearly in $\mathbf{Z}[\xi]$, we have $\mathbf{Z}[x]/(\phi_p(x)) \simeq \mathbf{Z}[\xi]$ by the identification $x \mapsto \xi$. But we are interested in $\phi_p(x) \in \mathbf{F}_2[x]$. We can map

$$\mathbf{Z}[\xi] \simeq \mathbf{Z}[x]/(\phi_p(x)) \longrightarrow \mathbf{F}_2[x]/(\phi_p(x))$$

by reduction modulo 2 and then the kernel is $2\mathbf{Z}[\xi]$. Since this is clearly onto, we get

$$R = \mathbf{Z}[\xi]/2\mathbf{Z}[\xi] \simeq \mathbf{F}_2[x]/(\phi_p(x)).$$

Therefore 1.3.7 becomes,

$$(1.3.8) \quad \mathbf{F}_2[C_p] \simeq \mathbf{F}_2 \oplus R.$$

However $\phi_p(x)$ is not necessarily irreducible in $\mathbf{F}_2[x]$. To examine how $\phi_p(x)$ splits in $\mathbf{F}_2[x]$, we'll examine the splitting of the rational prime 2 in the p -th cyclotomic extension.

The $\text{Gal}(\mathbf{Q}(\xi)|\mathbf{Q}) \simeq (\mathbf{Z}/p\mathbf{Z})^*$. For $g \in (\mathbf{Z}/p\mathbf{Z})^*$, the corresponding automorphism σ_g of $\mathbf{Q}(\xi)$ is determined by

$$\sigma_g(\xi) = \xi^g.$$

In fact, $\mathbf{Z}[\xi]$ has a normal basis over \mathbf{Z} , namely $\{\xi, \xi^2, \dots, \xi^{p-1}\}$. In other words, $(\mathbf{Z}[\xi], +)$ is a free $\mathbf{Z}[\text{Gal}(\mathbf{Q}(\xi)|\mathbf{Q})]$ -module of rank 1.

Now $2 \in (\mathbf{Z}/p\mathbf{Z})^*$. Since 2 does not divide the discriminant of the field extension, the ideal $2\mathbf{Z}[\xi]$ *decomposes* in $\mathbf{Q}(\xi)$. So $2\mathbf{Z}[\xi] = P_1 P_2 \cdots P_r$ is a product of r distinct prime ideals. These are transitively permuted by the action of $(\mathbf{Z}/p\mathbf{Z})^*$. Let $\frac{p-1}{r} = f$. Then at each P_i , the decomposition subgroup has order f and hence each residue field $k_i = \mathbf{Z}[\xi]/P_i$ is an extension of \mathbf{F}_2 of degree f . In fact we know that $f \in \mathbf{N}$ is the least positive integer for which $2^f \equiv 1 \pmod{p}$. Then 2 generates a cyclic subgroup in $(\mathbf{Z}/p\mathbf{Z})^*$ of order f . So we have that each decomposition subgroup *equals* $(2) \subseteq (\mathbf{Z}/p\mathbf{Z})^*$.

Then in terms of $\phi_p(x) \in \mathbf{F}_2[x]$, there is a unique factorization

$$\phi_p(x) = q_1(x) \cdots q_r(x)$$

into a product of r distinct monic irreducible polynomials of degree f . So

$$\mathbf{F}_2[x]/(\phi_p(x)) \simeq R = \mathbf{Z}[\xi]/2\mathbf{Z}[\xi] = \mathbf{Z}[\xi]/P_1 P_2 \cdots P_r.$$

By the Chinese Remainder Theorem, we see

$$R = \mathbf{Z}[\xi]/2\mathbf{Z}[\xi] = \mathbf{Z}[\xi]/(P_1 \cdots P_r) \simeq (\mathbf{Z}[\xi]/P_1) \oplus \cdots \oplus (\mathbf{Z}[\xi]/P_r).$$

Therefore we have expressed R as a direct sum of residue fields,

$$(1.3.9) \quad R \simeq \bigoplus_{i=1}^r k_i$$

where $k_i = \mathbf{Z}[\xi]/P_i$.

(1.3.10) **Theorem:** The group ring $\mathbf{F}_2[C_p]$ is a commutative semi-simple algebra over \mathbf{F}_2 and

$$\mathbf{F}_2[C_p] \xrightarrow{\simeq} \mathbf{F}_2 \oplus R \xrightarrow{\simeq} \mathbf{F}_2 \oplus \bigoplus_{i=1}^r k_i.$$

Proof: Clear by 1.3.8 and 1.3.9. ■

We now introduce a second ring homomorphism

$$(1.3.11) \quad \nu : \mathbf{F}_2[C_p] \longrightarrow R \text{ given by}$$

$$\nu\left(\sum_{j=0}^{p-1} a_j t^j\right) = \sum_{j=0}^{p-1} a_j \xi^j \in R.$$

Recall the ring homomorphism $\epsilon : \mathbf{F}_2[C_p] \longrightarrow \mathbf{F}_2$. Notice that the $\text{Ker}(\epsilon)$ contains a multiplicative identity $1 + \Omega$ since for any $x \in \text{Ker}(\epsilon)$

$$(x)(1 + \Omega) = x + x\Omega = x + \epsilon(x)\Omega = x \quad (\text{see 1.3.5}).$$

In view of this we have the following corollary.

(1.3.12) **Corollary:** The restriction of ν to $\text{Ker}(\epsilon)$ produces a ring isomorphism,

$$\nu : \text{Ker}(\epsilon) \simeq R.$$

Proof: Since $\text{Ker}(\nu) = (\Omega)$ and as already noted, $\text{Ker}(\epsilon) \cap (\Omega) = \{0\}$ (see 1.3.6), ν restricted to the $\text{Ker}(\epsilon)$ is one-to-one. Now since $\text{Ker}(\epsilon)$ and R both have dimension $p - 1$ as vector spaces over \mathbf{F}_2 , ν is onto also. ■

We now go over the action of $(\mathbf{Z}/p\mathbf{Z})^*$ as a group of ring homomorphisms. First $(\mathbf{Z}/p\mathbf{Z})^*$ acts on $\mathbf{F}_2[C_p]$ as a group of automorphisms. Namely, for $g \in (\mathbf{Z}/p\mathbf{Z})^*$, the automorphism σ_g is defined by:

$$(1.3.13) \quad \sigma_g(t) = t^g.$$

For example if $g = -1$, then

$$\sigma_{-1}(t) = t^{-1}$$

yields the canonical involution of the group ring. We note that for $\alpha \in \mathbf{F}_2[C_p]$,

$$\epsilon(\sigma_g(\alpha)) = \epsilon(\alpha).$$

We have already noted that $(\mathbf{Z}/p\mathbf{Z})^*$ acts on $\mathbf{Z}[\xi]$ as the Galois group of the cyclotomic extension. The quotient ring

$$R = \mathbf{Z}[\xi]/2\mathbf{Z}[\xi]$$

inherits this action. Indeed, $(R, +)$ is a free $\mathbf{F}_2[(\mathbf{Z}/p\mathbf{Z})^*]$ -module of rank 1. We can use $\{1, \xi, \xi^2, \dots, \xi^{p-2}\} \in R$ as the \mathbf{F}_2 -basis. Now $\nu : \mathbf{F}_2[C_p] \longrightarrow R$ commutes

with this action of $(\mathbf{Z}/p\mathbf{Z})^*$. Since $\mathbf{F}_2[C_p]$ is a commutative \mathbf{F}_2 -algebra, we have a *Frobenius automorphism*:

$$x \mapsto x^2.$$

Clearly $\sigma_2(x) = x^2$ and similarly in R , $\sigma_2(y) = y^2$. Thus we do know how the subgroup $(2) \subseteq (\mathbf{Z}/p\mathbf{Z})^*$ acts on $\mathbf{F}_2[C_p]$ and R .

Now recall the group \mathcal{S} , the elementary abelian 2-group of all subsets of $\mathbf{Z}/p\mathbf{Z}$ with respect to symmetric difference. We are interested in the natural additive isomorphism

$$\mathcal{S} \simeq \mathbf{F}_2[C_p]$$

described as follows: For a subset $A \subseteq \mathbf{Z}/p\mathbf{Z}$, let $\chi_A : \mathbf{Z}/p\mathbf{Z} \rightarrow \mathbf{F}_2$ be the characteristic function of A and define

$$(1.3.14) \quad d_A = \sum_{j=0}^{p-1} \chi_A(j) t^j \in \mathbf{F}_2[C_p].$$

(1.3.15) **Lemma:** The map $d : \mathcal{S} \rightarrow \mathbf{F}_2[C_p]$ defined by $d(A) = d_A$ is an isomorphism.

Proof: Since $d(A) = 0 \iff \chi_A(j) = 0$ for every $j \iff A = \emptyset$, we see that d is one-to-one. Since d is also clearly onto, the lemma is proved. ■

Note that for any set $A \in \mathcal{S}$,

$$(1.3.16) \quad \epsilon(d_A) \equiv \#A \pmod{2} \quad (\text{see 1.3.4}).$$

In particular,

$$(1.3.17) \quad \epsilon(d_S) \equiv \#S \equiv 0 \pmod{2}.$$

Naturally, $(\mathbb{Z}/p\mathbb{Z})^*$ acts as a group of additive automorphisms on \mathcal{S} , namely, for $g \in (\mathbb{Z}/p\mathbb{Z})^*$ and $A \in \mathcal{S}$ we have a group action σ_g defined by

$$(1.3.18) \quad \sigma_g(A) = gA \in \mathcal{S}.$$

Notice that the isomorphism $d : \mathcal{S} \xrightarrow{\cong} \mathbb{F}_2[C_p]$ commutes with the action of $(\mathbb{Z}/p\mathbb{Z})^*$. That is, for $A \in \mathcal{S}$ we have

$$(1.3.19) \quad \sigma_g(d_A) = d_{\sigma_g(A)} = d_{gA}.$$

In particular,

$$(1.3.20) \quad \sigma_{-1}(d_S) = d_S \quad (\text{see 1.3.1}).$$

Remark: When d_A is squared, the coefficients of all the “crossterms” are multiples of 2, so in $\mathbb{F}_2[C_p]$ they are 0. Therefore,

$$\sigma_2(d_A) = (d_A)^2 = d_{2A}.$$

Similarly,

$$(1.3.21) \quad \sigma_{2^i}(d_A) = (d_A)^{2^i} = d_{2^i A} \quad \text{for any } i.$$

Also note that,

$$(1.3.22) \quad \sigma_g(A) = A \iff \sigma_g(d_A) = d_A.$$

(1.3.23) **Remark** We define \mathcal{S}_* to be the subgroup of \mathcal{S} consisting of all subsets of $(\mathbb{Z}/p\mathbb{Z})^*$.

Note that as a vector space over \mathbf{F}_2

$$\dim_{\mathbf{F}_2} \mathcal{S}_* = p - 1.$$

Using this fact, we will show that $\mathcal{S}_* \simeq R$.

Define a homomorphism

$$(1.3.24) \quad \gamma : \mathcal{S}_* \longrightarrow R \text{ by}$$

$$\gamma(L) = \nu(d_L)$$

where the homomorphisms ν and d are as defined in 1.3.11 and 1.3.14 respectively.

We write $\gamma_L = \nu(d_L)$.

(1.3.25) **Lemma:** The additive homomorphism $\gamma : \mathcal{S}_* \longrightarrow R$ given by $\gamma(L) = \gamma_L$ is an isomorphism which commutes with the action of $(\mathbf{Z}/p\mathbf{Z})^*$.

Proof: Recall that $\text{Ker}(\nu) = (\Omega) = \{0, \Omega\}$. Now since $\Omega = d_{\mathbf{Z}/p\mathbf{Z}}$, we see that for any $L \in \mathcal{S}_*$, $\gamma_L = \nu(d_L) = 0 \iff L = \emptyset$. So γ is a monomorphism. Since

$$\dim_{\mathbf{F}_2} \mathcal{S}_* = \dim_{\mathbf{F}_2} R = p - 1,$$

γ is in fact an isomorphism. Finally, since d commutes with the action of $(\mathbf{Z}/p\mathbf{Z})^*$, clearly γ does also. ■

So we see that in $R = \mathbf{Z}[\xi]/2\mathbf{Z}[\xi]$,

$$(1.3.26) \quad \sigma_g(\gamma_L) = \gamma_{gL}$$

In fact, modulo 2,

$$(1.3.27) \quad \sigma_{2^i}(\gamma_L) = (\gamma_L)^{2^i} = \gamma_{2^i L} \text{ for any } i \text{ (see 1.3.21).}$$

Now let G be a subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$. Since $(\mathbb{Z}/p\mathbb{Z})^*$ is a cyclic group of order $p-1$, $G \subseteq (\mathbb{Z}/p\mathbb{Z})^*$ is also cyclic, and $\#G$ must divide $p-1$. Let $\#G = m$ and $\frac{p-1}{m} = n$. Then the quotient group is $\Pi = (\mathbb{Z}/p\mathbb{Z})^*/G$ and

$$\#\Pi = [(\mathbb{Z}/p\mathbb{Z})^* : G] = \frac{p-1}{m} = n.$$

In fact we can conclude that

$$(1.3.28) \quad G = (\mathbb{Z}/p\mathbb{Z})^{*n} = \text{the subgroup of } (\mathbb{Z}/p\mathbb{Z})^* \text{ of } n\text{-th powers.}$$

(1.3.29) **Definition:** Let $\mathcal{S}_*^G \subseteq \mathcal{S}_*$ be the subgroup of all G -fixed elements in \mathcal{S}_* ; that is, the subgroup of all $L \in \mathcal{S}_*$ for which $gL = L$ for all $g \in G$.

The quotient group $\Pi = (\mathbb{Z}/p\mathbb{Z})^*/G$ will then act on \mathcal{S}_*^G as a group of automorphisms. Hence \mathcal{S}_*^G is an $\mathbb{F}_2[\Pi]$ -module. In fact it is a free $\mathbb{F}_2[\Pi]$ -module of rank 1. Simply observe $G \subseteq (\mathbb{Z}/p\mathbb{Z})^*$ and therefore $G \in \mathcal{S}_*^G$. So this is a basis of \mathcal{S}_*^G over $\mathbb{F}_2[\Pi]$.

(1.3.30) **Lemma:** As a vector space over \mathbb{F}_2 , \mathcal{S}_* has dimension $n = [(\mathbb{Z}/p\mathbb{Z})^* : G]$.

Proof: Simply notice that the cosets of G in $(\mathbb{Z}/p\mathbb{Z})^*$ form a basis of \mathcal{S}_*^G over \mathbb{F}_2 . ■

Recall our additive isomorphism $\gamma : \mathcal{S}_* \xrightarrow{\sim} R$ which commutes with the action of $(\mathbb{Z}/p\mathbb{Z})^*$ (see 1.3.25). If $R^G \subseteq R$ denotes the subring of G -fixed elements in $R = \mathbb{Z}[\xi]/2\mathbb{Z}[\xi]$, then

$$(1.3.31) \quad \mathcal{S}_*^G \simeq R^G$$

and in particular R^G is a free $\mathbb{F}_2[\Pi]$ -module. To understand this, consider the following: If we think of $(\mathbb{Z}/p\mathbb{Z})^* = \text{Gal}(\mathbb{Q}(\xi)|\mathbb{Q})$ then associated to the subgroup

$G \subseteq (\mathbf{Z}/p\mathbf{Z})^*$ is a fixed field F ,

$$\mathbf{Q} \subseteq F \subseteq \mathbf{Q}(\xi)$$

which is a cyclic field extension of \mathbf{Q} of degree n with $\text{Gal}(\mathbf{Q}(\xi)|F) = G$ and $\text{Gal}(F|\mathbf{Q}) = \Pi$. The ring of integers $\mathcal{O}_F \subseteq F$ is a subring of $\mathbf{Z}[\xi]$. In fact $\mathcal{O}_F = \mathbf{Z}[\xi]^G$ is the subring of $\mathbf{Z}[\xi]$ of G -fixed elements. Also note that for any $x \in \mathbf{Z}[\xi]$, we have

$$2x \in \mathbf{Z}[\xi]^G \iff x \in \mathbf{Z}[\xi]^G.$$

Thus

$$\mathbf{Z}[\xi]^G \cap 2\mathbf{Z}[\xi] = 2\mathbf{Z}[\xi]^G$$

Therefore, we can think of

$$\mathcal{O}_F/2\mathcal{O}_F = \mathbf{Z}[\xi]^G/2\mathbf{Z}[\xi]^G \subseteq \mathbf{Z}[\xi]/2\mathbf{Z}[\xi] = R$$

and hence we have $\mathcal{O}_F/2\mathcal{O}_F \subseteq R^G$. But notice that both $\mathcal{O}_F/2\mathcal{O}_F$ and R^G have dimension 2 as vector spaces over \mathbf{F}_2 . Therefore

$$(1.3.32) \quad \mathcal{O}_F/2\mathcal{O}_F = R^G.$$

We know that $\{\xi, \xi^2, \dots, \xi^{p-1}\}$ is a normal basis for $\mathbf{Z}[\xi]$ over \mathbf{Z} . Thus $\mathbf{Z}[\xi]$ is a free $\mathbf{Z}[(\mathbf{Z}/p\mathbf{Z})^*]$ -module of rank 1 and ξ is a basis. The following was observed by Hilbert (see [Hi]):

(1.3.33) As a $\mathbf{Z}[\Pi]$ -module, \mathcal{O}_F is *also* free of rank 1 and $\text{tr}_{\mathbf{Q}(\xi)|F}(\xi) \in \mathcal{O}_F$ is a basis.

Next let us recall $G \in \mathcal{S}_*^G \subseteq \mathcal{S}_*$. Then in $R^G = \mathcal{O}_F/2\mathcal{O}_F$ we have

$$\begin{aligned}\gamma_G &= \sum_{j=1}^{p-1} \chi_G(j) \xi^j \\ &= \text{tr}_{\mathbf{Q}(\xi)|F}(\xi) \in R^G.\end{aligned}$$

The point is \mathcal{S}_*^G is a free $\mathbf{F}_2[\Pi]$ -module of rank 1 with $G \in \mathcal{S}_*^G$ a basis. Then $R^G = \mathcal{O}_F/2\mathcal{O}_F$ is also a free $\mathbf{F}_2[\Pi]$ -module with basis $\text{tr}_{\mathbf{Q}(\xi)|F}(\xi)$. In fact the $\mathbf{F}_2[\Pi]$ -module isomorphism $\gamma : \mathcal{S}_* \xrightarrow{\cong} R$ induces an isomorphism

$$(1.3.34) \quad \gamma_* : \mathcal{S}_*^G \xrightarrow{\cong} R^G \quad \text{defined by}$$

$$\gamma_*(G) = \gamma_G.$$

Certainly the ring structure in $\mathbf{F}_2[C_p]$ does *not* correspond to set intersection in \mathcal{S} . The investigation of the relation between multiplication in the group ring and the subsets of $\mathbf{Z}/p\mathbf{Z}$ is our study of circulant graphs.

We will now show that the group ring $\mathbf{F}_2[C_p]$ is isomorphic to the ring of $p \times p$ circulant matrices.

(1.3.35) **Proposition:** The group ring $\mathbf{F}_2[C_p]$ is isomorphic to the ring of $p \times p$ circulant matrices over \mathbf{F}_2 .

Proof: As noted in 1.3.15, $d : \mathcal{S} \longrightarrow \mathbf{F}_2[C_p]$ given by $d(A) = d_A$ is an isomorphism. So we will show that \mathcal{S} is isomorphic to the ring of $p \times p$ matrices in order to prove the proposition.

Let $A \in \mathcal{S}$. Then associate a matrix $M_A = (m_{ij})$ as follows:

$$m_{ij} = \begin{cases} 0, & \text{if } i - j \notin A; \\ 1, & \text{if } i - j \in A \end{cases}$$

Note that M_A is a $p \times p$ circulant matrix. Therefore we have a map

$$M: \mathcal{S} \longrightarrow \{\text{ring of } p \times p \text{ circulant matrices}\} \text{ given by}$$

$$M(A) = M_A.$$

M is clearly one-to-one, and by choosing A appropriately, M can easily be seen to be onto as well. ■

(1.3.36) **Remark** Note that if $S \in \mathcal{S}$ is symmetric, then the matrix associated to d_S is identical to the Rédei matrix of $\Gamma(S)$.

(1.3.37) **Proposition:** Let $\Gamma(S)$ be a circulant graph as defined in 1.3.1. If $L \in \mathcal{S}_*$ (i.e. $L \subseteq V$), then in $\mathbb{F}_2[C_p]$,

$$d_{P(\Gamma(S), L)} = d_S \cdot d_L.$$

Proof: Recall the convolution product $\chi_S * \chi_L$ of χ_S and χ_L :

for $c \in (\mathbb{Z}/p\mathbb{Z})^*$,

$$(\chi_S * \chi_L)(c) \equiv \sum_{i+j=c} \chi_S(i) \chi_L(j) \pmod{2}.$$

So we have

$$\begin{aligned} d_S \cdot d_L &= \left(\sum_{i=0}^{p-1} \chi_S(i) t^i \right) \left(\sum_{j=0}^{p-1} \chi_L(j) t^j \right) \\ &= \sum_{c=0}^{p-1} \left(\sum_{i+j=c} \chi_S(i) \chi_L(j) \right) t^c \\ &= \sum_{c=0}^{p-1} (\chi_S * \chi_L)(c) t^c. \end{aligned}$$

So to prove the proposition, we want to show

$$(1.3.38) \quad \chi_{P(\Gamma(S), L)}(c) = (\chi_S * \chi_L)(c) \text{ for all } c \in (\mathbb{Z}/p\mathbb{Z})^*.$$

Now $\chi_S(i)\chi_L(j) = 1 \iff i \in S \text{ and } j \in L$. Since $i + j = c$ (i.e. $c - j = i \in S$), we have

$$\chi_S(i)\chi_L(j) = 1 \iff c \text{ is adjacent to } j \in L \text{ in } \Gamma(S).$$

Therefore:

$$(\chi_S * \chi_L)(c) = 1 \iff \chi_S(i)\chi_L(j) = 1 \text{ an odd number of times.}$$

$$\iff c \text{ is adjacent to an odd number of vertices in } L.$$

So if $c \notin L$, then that implies $c \in P(\Gamma(S), L)$.

If $c \in L$, recall that $\Gamma(S)$ is an Eulerian graph (see 1.3.3). So by Lemma 1.1.8, $c \in P(\Gamma(S), L)$.

Therefore $(\chi_S * \chi_L)(c) = 1 \iff c \in P(\Gamma(S), L) \iff \chi_{P(\Gamma(S), L)}(c) = 1$. So 1.3.38 (and hence the proposition) is proved. ■

Clearly to count the number of EVD's of $\Gamma(S)$, we could count the number of sets L with $P(\Gamma(S), L) = \emptyset$ (i.e. $d_{P(\Gamma(S), L)} = 0$). So by Proposition 1.3.37, that amounts to counting the number of sets $L \in \mathcal{S}_*$ with

$$d_S \cdot d_L = 0.$$

Since $\epsilon(d_S) = 0$ (see 1.3.17), we see that $\epsilon(d_S \cdot d_L) = 0$ also. Therefore

$$d_S \cdot d_L \in \text{Ker}(\epsilon),$$

so by Corollary 1.3.12, we have

$$(1.3.39) \quad d_S \cdot d_L = 0 \iff \gamma_S \cdot \gamma_L = 0 \in R = \mathbb{Z}[\xi]/2\mathbb{Z}[\xi].$$

Therefore to determine the number of sets $L \in \mathcal{S}_*$ with $d_S \cdot d_L = 0$, we'll compute the order of $\text{Ann}(\gamma_S)$.

Recall we have $2\mathbb{Z}[\xi] = P_1 P_2 \cdots P_r$ and for each i , $1 \leq i \leq r$, there is a residue map

$$\eta_i: R \longrightarrow k_i = \mathbb{Z}[\xi]/P_i.$$

Now if $\eta_i(\gamma_S) \neq 0 \in k_i$, then $\eta_i(\gamma_S \cdot \gamma_L) = 0 \iff \eta_i(\gamma_L) = 0$. However, if $\eta_i(\gamma_S) = 0 \in k_i$, then there is no condition on $\eta_i(\gamma_L)$ (i.e. $\eta_i(\gamma_S \cdot \gamma_L) = 0$ for all $L \in \mathcal{S}_*$. So $\gamma_L \in \text{Ann}(\gamma_S)$ for all $L \in \mathcal{S}_*$). Therefore to compute the order of $\text{Ann}(\gamma_S)$, we only need to count the number N of indices for which $\eta_i(\gamma_S) = 0$. Then since

$$\eta = \bigoplus_{i=1}^r \eta_i: R \xrightarrow{\cong} \bigoplus_{i=1}^r k_i \quad (\text{see 1.3.9})$$

is an isomorphism and $\#k_i = 2^f$ for all i , we get that

$$(1.3.40) \quad \#\text{Ann}(\gamma_S) = 2^{fN}.$$

(1.3.41) **Proposition:** If $\Gamma(S)$ is the circulant graph associated to the symmetric subset $S \in \mathcal{S}_*$ and N is the number of indices for which $\eta_i(\gamma_S) = 0$, then

$$c(\Gamma(S)) = fN.$$

Proof: As we have seen, determining the invariant $c(\Gamma(S))$ is equivalent to simply counting the number of EVD's of the circulant graph $\Gamma(S)$ (see 1.2.15), which as noted in the above discussion, can be done by computing the order of the annihilator of γ_S . In other words,

$$2^{c(\Gamma(S))} = \# \text{ of EVD's of } \Gamma(S) = \#\text{Ann}(\gamma_S) = 2^{fN} \quad (\text{see 1.3.40}),$$

which proves the proposition. ■

Here is the interpretation in terms of algebraic integers of $\mathbf{Q}(\xi)$. We have an algebraic integer

$$\gamma_S = \sum_{j=0}^{p-1} \chi_S(j) \xi^j \in \mathbf{Z}[\xi].$$

Then N is simply the number of distinct dyadic primes P_i dividing the ideal (γ_S) .

Each prime has inertia degree f (i.e. $[\mathbf{Z}[\xi]/P_i : \mathbf{Z}/2\mathbf{Z}] = f$). So

$$N_{\mathbf{Q}(\xi)|\mathbf{Q}}(P_i) = \#(\mathbf{Z}[\xi]/P_i) = 2^f.$$

If we form the greatest common divisor, in the sense of ideals, of (γ_S) and (2) then

$$\gcd(\gamma_S, 2) = (\gamma_S, 2) = P_{i_1} P_{i_2} \cdots P_{i_N}$$

and so by the Chinese Remainder Theorem, we get

$$N_{\mathbf{Q}(\xi)|\mathbf{Q}}(\gamma_S, 2) = \#(\mathbf{Z}[\xi]/P_{i_1} \cdots P_{i_N}) = \#(\mathbf{Z}[\xi]/P_{i_1} \oplus \cdots \oplus \mathbf{Z}[\xi]/P_{i_N}).$$

So

$$N_{\mathbf{Q}(\xi)|\mathbf{Q}}(\gamma_S, 2) = 2^{fN} = 2^{c(\Gamma(S))}.$$

Consequently $c(\Gamma(S)) = 0 \iff N_{\mathbf{Q}(\xi)|\mathbf{Q}}(\gamma_S, 2) = 1$.

In closing, let us note that $\Gamma(S)$ is the totally disconnected graph if and only if $S = \emptyset$, which implies that $\gamma_S = 0$. Hence $N = r$, and by Theorem 1.3.41, $c(\Gamma(S)) = fN = fr = p - 1$. Therefore,

$$(1.3.42) \quad \Gamma(S) \text{ is totally disconnected} \iff c(\Gamma(S)) = p - 1$$

as previously stated.

Section 4: The Group $G(S)$

We now wish to improve upon Theorem 1.3.41. Given a symmetric subset $S \subseteq (\mathbf{Z}/p\mathbf{Z})^*$, we define the subgroup $G(S) \subseteq (\mathbf{Z}/p\mathbf{Z})^*$ to be the set of all $g \in (\mathbf{Z}/p\mathbf{Z})^*$ for which $\sigma_g(S) = gS = S$. Equivalently,

$$(1.4.1) \quad G(S) = \{g \in (\mathbf{Z}/p\mathbf{Z})^* \mid \sigma_g(d_S) = d_S\} \quad (\text{see 1.3.22}).$$

Clearly by the definition of symmetry (see 1.3.1), we have $-1 \in G(S)$. So $\{\pm 1\} \subseteq G(S)$ and therefore

$$(1.4.2) \quad \#G(S) \equiv 0 \pmod{2},$$

and if F is the fixed field of the subgroup $G(S) \subseteq (\mathbf{Z}/p\mathbf{Z})^* = \text{Gal}(\mathbf{Q}(\xi)|\mathbf{Q})$ then $\{\pm 1\} \subseteq G(S)$ implies that

$$\mathbf{Q} \subseteq F \subseteq \mathbf{Q}(\xi)^+ \subseteq \mathbf{Q}(\xi)$$

where $\mathbf{Q}(\xi)^+$ is the maximal real subfield of $\mathbf{Q}(\xi)$.

Now with $G(S)$ and F as above, recall from 1.3.32 that we can identify the ring $\mathcal{O}_F/2\mathcal{O}_F$ with the elements of $R = \mathbf{Z}[\xi]/2\mathbf{Z}[\xi]$ which are fixed by the action of $G(S)$. Namely, $\mathcal{O}_F/2\mathcal{O}_F = R^{G(S)}$. Since $\gamma_S \in R$ is fixed by $G(S)$ (by definition and 1.3.26), we see that

$$(1.4.3) \quad \gamma_S \in \mathcal{O}_F/2\mathcal{O}_F$$

so we will consider γ_S to be the reduction modulo 2 of $\gamma_S \in \mathcal{O}_F \subseteq \mathbf{Z}[\xi]$.

Now as we pointed out in Section 3, $\deg F|\mathbf{Q} = [(\mathbf{Z}/p\mathbf{Z})^* : G(S)] = n$, $G(S) = (\mathbf{Z}/p\mathbf{Z})^{*n}$ and

$$\text{Gal}(F|\mathbf{Q}) = \Pi = (\mathbf{Z}/p\mathbf{Z})^*/G(S).$$

Define $b > 0$ to be the least positive integer for which

$$(1.4.4) \quad 2^b \in G(S).$$

Thus b is the order of the subgroup generated by 2 in the quotient group Π . Then we know that b divides f (recall that f is the least positive integer such that $2^f \equiv 1 \pmod{p}$) and for each dyadic prime $\mathcal{P} \subseteq \mathcal{O}_F$, the inertial degree of \mathcal{P} is b . That is, $\mathcal{O}_F/\mathcal{P}$ is an extension field of $\mathbb{Z}/2\mathbb{Z}$ of degree b . Therefore since F is a degree n extension of \mathbb{Q} , the number of dyadic primes in \mathcal{O}_F must be $\frac{n}{b}$. Since there is a total of r dyadic primes in $\mathbb{Z}[\xi]$ (see Section 3), we see that each dyadic prime which lies in \mathcal{O}_F must, in $\mathbb{Z}[\xi]$, split into

$$(1.4.5) \quad \frac{r}{n/b} = \frac{br}{n}$$

dyadic primes of $\mathbb{Z}[\xi]$. We shall use this to produce another computation of $c(\Gamma(S))$ (due to P.E.Conner).

Let a , $0 \leq a \leq \frac{n}{b}$, be the number of dyadic primes $\mathcal{P} \subseteq \mathcal{O}_F$ which divide the ideal $(\gamma_S) \subseteq \mathcal{O}_F$. In other words, a is the number of dyadic primes $\mathcal{P} \subseteq \mathcal{O}_F$ for which $\gamma_S \in \mathcal{O}_F/2\mathcal{O}_F$ lies in the kernel of the map

$$\mathcal{O}_F/2\mathcal{O}_F \longrightarrow \mathcal{O}_F/\mathcal{P}.$$

(1.4.6) **Theorem (Conner):** For a symmetric subset $S \subseteq (\mathbb{Z}/p\mathbb{Z})^*$ and a subgroup $G(S) \subseteq (\mathbb{Z}/p\mathbb{Z})^*$ defined by $G(S) = \{g \in (\mathbb{Z}/p\mathbb{Z})^* : gS = S\}$ we have:

$$c(\Gamma(S)) = a \cdot b \cdot \#G(S).$$

Proof: Since each \mathcal{P} splits into $\frac{br}{n}$ primes in $\mathbf{Z}[\xi]$, by Theorem 1.3.41 we have

$$c(\Gamma(S)) = N \cdot f = \left(a \cdot \frac{br}{n}\right) \cdot f = \frac{abrf}{n},$$

and since $\frac{rf}{n} = \frac{(p-1)}{n} = \#G(S)$, we get

$$c(\Gamma(S)) = \frac{abrf}{n} = a \cdot b \cdot \frac{rf}{n} = a \cdot b \cdot \#G(S). \quad \blacksquare$$

We must understand $G(S)$, a and b as described above.

(1.4.7) **Remark:** $0 \leq c(\Gamma(S)) \leq p-1$ and

$$c(\Gamma(S)) = p-1 \iff S = \emptyset \quad (\text{see 1.3.42}) \text{ and}$$

$$c(\Gamma(S)) = 0 \iff a = 0 \iff \gamma_S \in (\mathcal{O}_F/2\mathcal{O}_F)^*.$$

(1.4.8) **Corollary:** For a symmetric subset $S \subseteq (\mathbf{Z}/p\mathbf{Z})^*$,

$$c(\Gamma(S)) \equiv 0(2).$$

Proof: This follows directly from the previous theorem, since $\#G(S)$ is even. \blacksquare

In fact by utilizing Theorem 1.3.41 we know a little more than what this corollary tells us. In particular,

$$\text{if } f \equiv 0(2), \text{ then } c(\Gamma(S)) = mf \quad (\text{for some } m, 0 \leq m \leq r) \text{ and}$$

$$\text{if } f \equiv 1(2), \text{ then } c(\Gamma(S)) = 2mf \quad (\text{for some } m, 0 \leq m \leq r/2).$$

By Theorem 1.3.41, we know that $c(\Gamma(S)) = fN$, so either f is even, or N is even.

If f is even, let $m = N$ and we are done. If $f \equiv 1(2)$ then N must be even, so let $m = N/2$.

(1.4.9) **Corollary:** If $S \neq \emptyset$ and the fixed field of $G(S)$ contains exactly one dyadic prime (in other words $b = n$), then

$$c(\Gamma(S)) = 0.$$

Proof: If F contains exactly one dyadic prime \mathcal{P} , then

$$\mathcal{O}_F/2\mathcal{O}_F \simeq \mathcal{O}_F/\mathcal{P}.$$

So $\mathcal{O}_F/2\mathcal{O}_F$ is a field. Also, $S \neq \emptyset$ implies that $\gamma_S \neq 0$. Hence γ_S is a unit in $\mathcal{O}_F/2\mathcal{O}_F$. So by Remark 1.4.7, $c(\Gamma(S)) = 0$. ■

The hypothesis for the last corollary that $b = n$ implies that the quotient group Π is in fact a *cyclic* quotient group with $2S \in \Pi$ as a generator. We point out that the maximal real subfield $\mathbb{Q}(\xi)^+$ will contain only one dyadic prime if and only if either $f = p-1$ or $f \equiv 1(2)$ and $f = (p-1)/2$ (which implies $p \equiv 3(4)$). In such a case, $c(\Gamma(S)) = 0$ for all non-empty symmetric subsets (in other words, all connected circulant graphs). Therefore it can be shown that $p = 17$ is the smallest prime for which $\mathbb{Q}(\xi)^+$ contains more than one dyadic prime.

Now recall again the subgroup \mathcal{S}_* of \mathcal{S} which is a group under symmetric difference (denoted by a ∇). In Section 3 (see 1.3.34) we showed that there is an additive isomorphism

$$\mathcal{S}_*^{G(S)} \simeq \mathcal{O}_F/2\mathcal{O}_F \simeq R^{G(S)}.$$

To $L \in \mathcal{S}_*^{G(S)}$ we associate

$$\gamma_L = \sum_{j=1}^{p-1} \chi_L(j) \xi^j \in \mathcal{O}_F/2\mathcal{O}_F.$$

In particular, since $S \in \mathcal{S}_*^{G(S)}$, we showed that $\gamma_S \in \mathcal{O}_F/2\mathcal{O}_F$. For $L \in \mathcal{S}_*^{G(S)}$ we define

$$\tilde{L} = (\mathbb{Z}/p\mathbb{Z})^* \setminus L.$$

Note that also $\tilde{L} \in \mathcal{S}_*^{G(S)}$.

(1.4.10) **Lemma:** For $L \in \mathcal{S}_*^{G(S)}$,

$$\gamma_{\tilde{L}} = 1 + \gamma_L.$$

Proof: Since γ is a homomorphism,

$$\gamma_{(L \nabla \tilde{L})} = \gamma_L + \gamma_{\tilde{L}}.$$

Since $L \nabla \tilde{L} = (\mathbb{Z}/p\mathbb{Z})^*$, we have

$$1 = \gamma_{(\mathbb{Z}/p\mathbb{Z})^*} = \gamma_{(L \nabla \tilde{L})} = \gamma_L + \gamma_{\tilde{L}},$$

which proves the lemma. ■

We would now like to consider the vertex decomposition of the graph $\Gamma(S)$ given by $\{L, (\tilde{L} \cup \{0\})\}$. This should be carefully distinguished from the decomposition $\{\tilde{L}, (L \cup \{0\})\}$.

(1.4.11) **Lemma:** If $L \in \mathcal{S}_*^{G(S)}$ then $P(\Gamma(S), L) \in \mathcal{S}_*^{G(S)}$.

Proof: Recall that $P(\Gamma(S), L)$ is the set of special vertices of the circulant graph $\Gamma(S)$ with respect to the vertex decomposition $\{L, (\tilde{L} \cup \{0\})\}$. We need to show that $P(\Gamma(S), L) \in \mathcal{S}_*$ and that it is $G(S)$ -invariant. Consider the vertex 0 in the circulant graph $\Gamma(S)$. The set of vertices in L adjacent to 0 is $S \cap L$ (see 1.3.1). Since both S and L are in $\mathcal{S}_*^{G(S)}$, so is $S \cap L$. Therefore either $S \cap L = \emptyset$ or $S \cap L$

is a union of cosets of $G(S)$ (see Lemma 1.3.30). In either case, $\#(S \cap L) \equiv 0(2)$ since $\#G(S) \equiv 0(2)$. So 0 is adjacent to an even number of vertices in L , and hence is not a special point of $\Gamma(S)$. Therefore $P(\Gamma(S), L) \subseteq (\mathbb{Z}/p\mathbb{Z})^*$ and so it is in \mathcal{S}_* . Also since $i - j \in S \iff gi - gj \in S$ for all $g \in G(S)$ (by the definition of $G(S)$), we see that $P(\Gamma(S), L)$ is $G(S)$ -invariant. ■

In Section 3 (see Proposition 1.3.37), we showed that in $\mathbb{F}_2[C_p]$,

$$d_S \cdot d_L = d_{P(\Gamma(S), L)}.$$

However, S , L and $P(\Gamma(S), L)$ are all in $\mathcal{S}_*^{G(S)}$ and as noted $\mathcal{S}_*^{G(S)} \simeq \mathcal{O}_F/2\mathcal{O}_F$.

Which leads us to the following lemma.

(1.4.12) **Lemma:** If $L \in \mathcal{S}_*^{G(S)}$ then in $\mathcal{O}_F/2\mathcal{O}_F$

$$\gamma_S \cdot \gamma_L = \gamma_{P(\Gamma(S), L)}.$$

Proof: This follows immediately from Proposition 1.3.37. ■

(1.4.13) **Corollary:** If $L \in \mathcal{S}_*^{G(S)}$ then

$$P(\Gamma(S), \tilde{L}) = P(\Gamma(S), L) \nabla S.$$

Proof: By Lemma 1.4.12,

$$\gamma_{P(\Gamma(S), \tilde{L})} = \gamma_S \cdot \gamma_{\tilde{L}}.$$

From 1.4.10, we know that

$$\gamma_S \cdot \gamma_{\tilde{L}} = \gamma_S \cdot (1 + \gamma_L) = \gamma_S + \gamma_S \cdot \gamma_L,$$

and again from Lemma 1.4.12,

$$\gamma_S + \gamma_S \cdot \gamma_L = \gamma_S + \gamma_{P(\Gamma(S), L)} = \gamma_{S \nabla P(\Gamma(S), L)}.$$

Since γ is one-to-one, the corollary is proved. ■

(1.4.14) **Proposition:** The vector space of all subsets $L \in \mathcal{S}_*^{G(S)}$ for which $\{L, (\bar{L} \cup \{0\})\}$ is a $G(S)$ -invariant EVD of the circulant graph $\Gamma(S)$ is an additive subgroup of $\mathcal{S}_*^{G(S)}$ whose dimension over \mathbb{F}_2 is given by

$$ab = \frac{c(\Gamma(S))}{\#G(S)}.$$

Proof: For $L \in \mathcal{S}_*^{G(S)}$, $\{L, (\bar{L} \cup \{0\})\}$ is an EVD of the circulant graph $\Gamma(S)$ if and only if in $\mathcal{O}_F/2\mathcal{O}_F$ we have $\gamma_S \cdot \gamma_L = 0$, and in fact clearly in this case, it would be a $G(S)$ -invariant EVD. Such subsets form an additive subgroup of $\mathcal{S}_*^{G(S)}$, and since $\mathcal{S}_*^{G(S)} \simeq \mathcal{O}_F/2\mathcal{O}_F$, this subgroup is additively isomorphic to the annihilator ideal of $\gamma_S \in \mathcal{O}_F/2\mathcal{O}_F$. So we only need to compute the dimension over \mathbb{F}_2 of this ideal.

Recall that a is the number of dyadic prime ideals $\mathcal{P}_i \subseteq \mathcal{O}_F$ in which γ_S is mapped to 0. Since each residue field $\mathcal{O}_F/\mathcal{P}_i$ has order 2^b , the order of the annihilator ideal in $\mathcal{O}_F/2\mathcal{O}_F$ of γ_S is

$$2^{ab}$$

which proves the proposition. ■

As noticed several times, the element $2 \in (\mathbb{Z}/p\mathbb{Z})^*$ is of great importance.

In the next section we will investigate its significance.

Section 5: The Role of $2 \in (\mathbb{Z}/p\mathbb{Z})^*$

The cyclic subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$ generated by 2 contains -1 if and only if f is even. Recall from Section 3 that $f \in \mathbb{N}$ is the least positive integer for which $2^f \equiv 1 \pmod{p}$. If f is odd, then

$$(-2)^f = -1 \quad \text{and so}$$

$$(-2)^{f+1} = 2.$$

So the cyclic subgroup generated by -2 contains both 2 and -1 .

(1.5.1) Definition: Let H be the smallest subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$ which contains both 2 and -1 . In other words, if f is even, we define H to be the subgroup generated by 2. If f is odd, we define H to be the subgroup generated by -2 .

From this definition, we see that the order of H is either f (if H is generated by 2) or $2f$ (if H is generated by -2).

(1.5.2) Proposition: If S is a symmetric subset of $(\mathbb{Z}/p\mathbb{Z})^*$, then the following are equivalent:

$$(1) \ d_S^2 = d_S \in \mathbb{F}_2[C_p]$$

$$(2) \ \gamma_S^2 = \gamma_S \in R$$

$$(3) \ 2 \in G(S)$$

$$(4) \ H \subseteq G(S)$$

$$(5) \ \text{the Rédei matrix } M \text{ associated to } \Gamma(S) \text{ is an idempotent matrix.}$$

Proof: Recall that

$$d_S^2 = \sigma_2(d_S) = d_{2S}$$

$$\gamma_S^2 = \sigma_2(\gamma_S) = \gamma_{2S} \quad (\text{see 1.3.21, 1.3.27}).$$

Then since $2 \in G(S)$ if and only if $2S = S$, we get the equivalence of (1), (2) and (3). Also, since H is generated either by 2 or by -2 and $-1 \in G(S)$ we have that $2 \in G(S)$ if and only if $H \subseteq G(S)$ which shows the equivalence of (4) to the first three. Finally, since M is the $p \times p$ circulant matrix associated with d_S (see 1.3.36), (5) follows as well. ■

Hence we know when the Rédei matrix M of a circulant graph is idempotent.

We would like a more geometric result.

(1.5.3) Proposition: Let Γ be a graph on a finite set of vertices. The Rédei matrix of Γ is idempotent if and only if

- (1) every vertex of Γ has even degree, and
- (2) Γ has the property that any two distinct vertices are adjacent if and only if they have an odd number of common neighbors in Γ .

Proof: We first consider the diagonal entries. For $1 \leq i \leq n$, the i -th diagonal entry of M^2 is given by

$$m_{ii} = \sum_{k=1}^n m_{ik} m_{ki}.$$

By symmetry of M , we know that $m_{ki} = m_{ik}$ and because we are over \mathbb{F}_2 , we have $m_{ik}^2 = m_{ik}$. So we can restate the i -th diagonal entry of M^2 as

$$m_{ii} = \sum_{k=1}^n m_{ik} = \#N(v_i) \pmod{2}.$$

Recall that in M the sum of every row is 0. Thus the degree of every vertex in Γ must be even. To consider the entries where $i \neq j$, we continue with the assumption that every vertex has even degree. For M to be idempotent, we need

$$\sum_{k=1}^n m_{ik} m_{kj} = m_{ij}.$$

However, by our assumption, we already know that $m_{ii} = m_{jj} = 0$. So we only need

$$\sum_{k \neq i, j} m_{ik} m_{kj} = m_{ij}.$$

Notice that for $k \neq i, j$, the product $m_{ik} m_{kj} = 1$ if and only if the vertex v_k is adjacent to both vertices v_i and v_j . So $m_{ij} = \sum_{k \neq i, j} m_{ik} m_{kj}$ (and therefore M is idempotent) if and only if two vertices are adjacent exactly when they have an odd number of common neighbors. ■

Clearly the idempotency of a Rédei matrix imposes a *sharp* restriction on its associated graph.

Now define K to be the fixed field of $H \subseteq (\mathbb{Z}/p\mathbb{Z})^*$. Since $\pm 1 \in H$,

$$\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\xi)^+ \subseteq \mathbb{Q}(\xi).$$

Let $2 \in G(S)$. Then since $2 \in H$, $b = 1$ (see 1.4.4) and the number, $q_2(K)$, of dyadic primes in K is given by:

$$q_2(K) = \frac{p-1}{\#H} = \begin{cases} r & \text{if } f \equiv 0(2) \\ r/2 & \text{if } f \equiv 1(2) \end{cases}$$

where $r = \frac{p-1}{f}$. Note that for each dyadic prime $\mathcal{P} \subseteq \mathcal{O}_K$ the residue field $\mathcal{O}_K/\mathcal{P}$ is \mathbb{F}_2 . Thus every element in $\mathcal{O}_K/2\mathcal{O}_K$ is idempotent (which agrees with Proposition 1.5.2). From Section 3 (see 1.3.32, 1.3.34), we have

$$\mathcal{S}_*^H \simeq \mathcal{O}_K/2\mathcal{O}_K.$$

If $S \in \mathcal{S}_*^H$, then S is symmetric (since $-1 \in H$) and therefore every element of $\mathcal{O}_K/2\mathcal{O}_K$ has the form γ_S for a unique subset S for which $H \subseteq G(S)$. We now utilize Corollary 1.4.8 to produce a realization theorem.

(1.5.4) **Theorem:** (1) If $f \equiv 0(2)$ then for $0 \leq m \leq r$ there are exactly $\binom{r}{m}$ symmetric subsets $S \subseteq (\mathbb{Z}/p\mathbb{Z})^*$ for which

$$2 \in G(S) \quad \text{and}$$

$$c(\Gamma(S)) = mf.$$

(2) If $f \equiv 1(2)$ then for $0 \leq m \leq r/2$ there are exactly $\binom{r/2}{m}$ symmetric subsets $S \subseteq (\mathbb{Z}/p\mathbb{Z})^*$ for which

$$2 \in G(S) \quad \text{and}$$

$$c(\Gamma(S)) = 2mf.$$

Proof: (1) If $f \equiv 0(2)$ then \mathcal{O}_K contains r distinct dyadic primes, each of degree 1. Each dyadic prime in \mathcal{O}_K is inert in $\mathbb{Q}(\xi)$. Thus if we choose a subset of m distinct dyadic primes in \mathcal{O}_K , there is a unique element, $\gamma_S \in \mathcal{O}_K/2\mathcal{O}_K$, which is mapped to 0 in the residue field at all of the chosen primes, but which is mapped to 1 in the residue field at each of the remaining $r-m$ dyadic primes in \mathcal{O}_K . Since each dyadic prime in K is inert in $\mathbb{Q}(\xi)$, we find by Corollary 1.4.8 that

$$c(\Gamma(S)) = mf.$$

(2) If $f \equiv 1(2)$, then \mathcal{O}_K contains $r/2$ primes, each of which is of degree 2. As above, there is a unique element, $\gamma_S \in \mathcal{O}_K/2\mathcal{O}_K$, which is mapped to 0 in the residue field at all of the chosen primes, but which is mapped to 1 in the residue field at each of the remaining $r/2-m$ dyadic primes. Since each prime is of degree 2, by Corollary 1.4.8 again, we have

$$c(\Gamma(S)) = Nf = 2mf,$$

which proves the theorem. ■

This is, in view of 1.5.2 and 1.5.3, the strongest possible form of realization. We can realize all possible values of $c(\Gamma(S))$ with circulant graphs which have their common neighbors properly described in 1.5.3.

Now we shall examine the complementary graph to a circulant graph. As before, define

$$\tilde{S} = (\mathbb{Z}/p\mathbb{Z})^* \setminus S.$$

Clearly if S is symmetric, then so is \tilde{S} and the circulant graph $\Gamma(\tilde{S})$ is the complementary graph to $\Gamma(S)$. We shall agree that $G(\emptyset) = (\mathbb{Z}/p\mathbb{Z})^*$ so that for every symmetric subset $S \subseteq (\mathbb{Z}/p\mathbb{Z})^*$,

$$(1.5.5) \quad G(\tilde{S}) = G(S).$$

We now restate Lemma 1.4.10 in terms of S .

(1.5.6) **Lemma:** For any symmetric subset $S \subseteq (\mathbb{Z}/p\mathbb{Z})^*$,

$$\gamma_{\tilde{S}} = 1 + \gamma_S.$$

Proof: Follows immediately from Lemma 1.4.10. ■

(1.5.7) **Proposition:** For any symmetric subset $S \subseteq (\mathbb{Z}/p\mathbb{Z})^*$,

$$c(\Gamma(S \nabla 2S)) = c(\Gamma(S)) + c(\Gamma(\tilde{S})).$$

Proof: Since S and $2S$ are symmetric, so is their symmetric difference $S \nabla 2S$.

Then from Theorem 1.3.41 we have,

$$c(\Gamma(S \nabla 2S)) = fN$$

where N is the number of indices with $\eta_i(\gamma_S \nabla 2S) = 0$ in k_i . Now in R we have

$$\gamma_S \nabla 2S = \gamma_S + \gamma_{2S} = \gamma_S + \gamma_S^2 = \gamma_S(1 + \gamma_S) = \gamma_S \cdot \gamma_{\bar{S}}.$$

So,

$$\eta_i(\gamma_S \nabla 2S) = 0 \iff \eta_i(\gamma_S) = 0 \text{ or } \eta_i(\gamma_{\bar{S}}) = 0.$$

Since $\eta_i(\gamma_S)$ and $\eta_i(\gamma_{\bar{S}})$ cannot simultaneously equal 0, we have

$$c(\Gamma(S \nabla 2S)) = c(\Gamma(S)) + c(\Gamma(\bar{S})),$$

which proves the proposition. ■

(1.5.8) **Corollary:** For any symmetric subset $S \subseteq (\mathbf{Z}/p\mathbf{Z})^*$,

$$c(\Gamma(S)) + c(\Gamma(\bar{S})) = p - 1 \iff 2 \in G(S).$$

Proof: By the previous proposition, we have that

$$c(\Gamma(S)) + c(\Gamma(\bar{S})) = c(\Gamma(S \nabla 2S)),$$

and by Remark 1.4.7,

$$c(\Gamma(S \nabla 2S)) = p - 1 \iff S \nabla 2S = \emptyset$$

$$\iff S = 2S$$

$$\iff 2 \in G(S),$$

and hence the corollary is proved. ■

(1.5.9) **Corollary:** If $2 \in G(S)$, then $c(\Gamma(S)) = 0 \iff S = (\mathbf{Z}/p\mathbf{Z})^*$.

Proof: If $S = (\mathbf{Z}/p\mathbf{Z})^*$, then $\Gamma(S)$ is a complete graph on an odd number of vertices, so $c(\Gamma(S)) = 0$. Now if $2 \in G(S)$ and $c(\Gamma(S)) = 0$, then by Corollary

1.5.8, we have $c(\Gamma(\tilde{S})) = p - 1$. But this implies that $\tilde{S} = \emptyset$ which implies that $S = (\mathbb{Z}/p\mathbb{Z})^*$. ■

There is another way to state Corollary 1.5.9 in more generality.

(1.5.10) **Lemma:** For any symmetric subset $S \subseteq (\mathbb{Z}/p\mathbb{Z})^*$, the vertex decomposition

$$\{S, (\tilde{S} \cup \{0\})\}$$

is an EVD of $\Gamma(S)$ if and only if $2 \in G(S)$.

Proof: The given vertex decomposition is an EVD of $\Gamma(S)$ if and only if

$$\gamma_S \cdot \gamma_{\tilde{S}} = 0 \quad (\text{see Lemma 1.4.12}).$$

But recall that $\gamma_S \cdot \gamma_{\tilde{S}} = \gamma_{S \nabla 2S}$ and

$$\gamma_{S \nabla 2S} = 0 \iff S \nabla 2S = \emptyset \iff S = 2S \iff 2 \in G(S),$$

which proves the lemma. ■

There is one other case to mention. We will be interested in those sets $L \in \mathcal{J}_*^{G(S)}$ for which

$$(1.5.11) \quad P(\Gamma(S), L) = L.$$

However, recall that

$$(1.5.12) \quad P(\Gamma(S), L) = L \iff \gamma_S \cdot \gamma_L = \gamma_L \quad (\text{see Lemma 1.4.12}).$$

Since $\gamma_{\tilde{S}} = 1 + \gamma_S$, we have

$$\gamma_S \cdot \gamma_L = \gamma_L \iff (\gamma_S + 1)\gamma_L = 0 \iff \gamma_{\tilde{S}} \cdot \gamma_L = 0.$$

Hence if $L \in \mathcal{J}_*^{G(S)}$, then

$$(1.5.13) \quad P(\Gamma(S), L) = L \iff \gamma_{\tilde{S}} \cdot \gamma_L = 0 \iff P(\Gamma(\tilde{S}), L) = \emptyset.$$

(1.5.14) **Proposition:** The vector space of all $L \in \mathcal{J}_*^{G(S)}$ for which

$$P(\Gamma(S), L) = L$$

is an additive subgroup of $\mathcal{J}_*^{G(S)}$ which has dimension over \mathbb{F}_2 is given by

$$\frac{c(\Gamma(\tilde{S}))}{\#G(S)}.$$

Proof: By 1.5.13, $P(\Gamma(S), L) = L \iff P(\Gamma(\tilde{S}), L) = \emptyset$. So $\{L, (\tilde{L} \cup \{0\})\}$ will be a $G(S)$ -invariant EVD of $\Gamma(\tilde{S})$. Applying Proposition 1.4.14 to $\Gamma(\tilde{S})$ and using the fact that $\#G(\tilde{S}) = \#G(S)$, the proposition is proved. ■

Section 6: The Automorphism Group of a Circulant Graph

Let p be an odd prime and let S be a symmetric subset of $(\mathbb{Z}/p\mathbb{Z})^*$. In this section we will determine the automorphism group $\text{Aut}(\Gamma(S))$ for any circulant graph $\Gamma(S)$. Let us first dispose of the extreme cases.

(1.6.1) **Proposition:** If $S = \emptyset$ or $S = (\mathbb{Z}/p\mathbb{Z})^*$, then $\text{Aut}(\Gamma(S)) = S_p$, the symmetric group on p elements.

Proof: If $S = \emptyset$, then $\Gamma(S)$ is the totally disconnected graph, and if $S = (\mathbb{Z}/p\mathbb{Z})^*$, then $\Gamma(S)$ is the complete graph. In either case, every permutation of the set of vertices yields a graph automorphism. ■

We are now left with the determination of the automorphism group for non-empty, proper symmetric subsets S of $(\mathbb{Z}/p\mathbb{Z})^*$.

(1.6.2) **Proposition:** If $S = \{\pm i\}$, then $\text{Aut}(\Gamma(S)) = D_p$, the dihedral group of order $2p$.

Proof: For $S = \{\pm i\}$ for any $i \in (\mathbb{Z}/p\mathbb{Z})^*$, then the resulting circulant graph $\Gamma(S)$ will be a p -cycle. Therefore $\Gamma(S)$ can be represented by a regular polygon on p vertices and the automorphism group will be the familiar dihedral group of order $2p$. ■

(1.6.3) **Examples:**

(1) Let $p = 3$. There are no non-empty, proper symmetric subsets of $(\mathbb{Z}/3\mathbb{Z})^*$. So for this case $\text{Aut}(\Gamma(S)) = S_3$ for any symmetric subset S .

(2) Let $p = 5$. The only non-empty, proper subsets of $(\mathbb{Z}/5\mathbb{Z})^*$ are $S_1 = \{\pm 1\}$ and $S_2 = \{\pm 2\}$. The corresponding circulant graphs $\Gamma(S_1)$ and $\Gamma(S_2)$ are:



both of which are 5-cycles with automorphism group D_5 .

Let us describe the **affine group** $\text{Aff}(\mathbb{Z}/p\mathbb{Z})$ of the field $\mathbb{Z}/p\mathbb{Z}$. It is a subgroup of S_p consisting of all permutations

$$(a, b): \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \text{ given by}$$

$$x \longmapsto ax + b.$$

(1.6.4) **Lemma:** Let $a, a_1 \in (\mathbb{Z}/p\mathbb{Z})^*$ and $b, b_1 \in \mathbb{Z}/p\mathbb{Z}$. Then

(1) $(a, b) = (a_1, b_1)$ in S_p if and only if $a = a_1$ and $b = b_1$.

(2) multiplication is defined by $(a, b)(a_1, b_1) = (aa_1, ab_1 + b)$.

(3) $(1, 0)$ is the identity and the inverse of (a, b) is $(a^{-1}, -a^{-1}b)$.

(4) $(a, b)(1, b_1)(a, b)^{-1} = (1, ab_1)$.

Proof: Statements (1), (2) and (3) can be verified easily. Let us check the conjugation formula. For $x \in \mathbb{Z}/p\mathbb{Z}$ we have:

$$\begin{aligned}
 (a, b)(1, b_1)(a, b)^{-1}x &= (a, b)(1, b_1)(a^{-1}, -a^{-1}b)x \\
 &= (a, b)(1, b_1)[a^{-1}x - a^{-1}b] \\
 &= (a, b)[a^{-1}x - a^{-1}b + b_1] \\
 &= a[a^{-1}x - a^{-1}b + b_1] + b \\
 &= x - b + ab_1 + b \\
 &= x + ab_1 \\
 &= (1, ab_1)x
 \end{aligned}$$

thus proving the lemma. ■

The above tells us that we have embeddings

$$(\mathbb{Z}/p\mathbb{Z})^* \longrightarrow \text{Aff}(\mathbb{Z}/p\mathbb{Z}) \text{ given by}$$

$$a \longmapsto [(a, 0): x \mapsto ax] \text{ and}$$

$$\mathbb{Z}/p\mathbb{Z} \longrightarrow \text{Aff}(\mathbb{Z}/p\mathbb{Z}) \text{ given by}$$

$$b \longmapsto [(1, b): x \mapsto x + b].$$

In this way we regard the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$ and the additive group $\mathbb{Z}/p\mathbb{Z}$ as subgroups of $\text{Aff}(\mathbb{Z}/p\mathbb{Z})$, and the affine group as being given by the *semi-direct product* of $(\mathbb{Z}/p\mathbb{Z})^*$ and $\mathbb{Z}/p\mathbb{Z}$ with natural divisor $\mathbb{Z}/p\mathbb{Z}$. In notation, we

have,

$$(1.6.5) \quad \text{Aff}(\mathbf{Z}/p\mathbf{Z}) = (\mathbf{Z}/p\mathbf{Z})^* \rtimes \mathbf{Z}/p\mathbf{Z}.$$

We will now check which permutations in $\text{Aff}(\mathbf{Z}/p\mathbf{Z})$ provide us with graph automorphisms of $\Gamma(S)$. This will result in exhibiting “large” subgroups of $\text{Aut}(\Gamma(S))$.

For a symmetric subset $S \subseteq (\mathbf{Z}/p\mathbf{Z})^*$ recall the subgroup of $(\mathbf{Z}/p\mathbf{Z})^*$ defined by

$$(1.6.6) \quad G(S) = \{a \in (\mathbf{Z}/p\mathbf{Z})^* : aS = S\}.$$

Given $i, j \in \mathbf{Z}/p\mathbf{Z}$, we know that if $i - j \in S$, then $a(i - j) \in S$ for every $a \in G(S)$.

So every permutation $(a, 0): x \mapsto ax$ with $a \in G(S)$ is in $\text{Aut}(\Gamma(S))$. Thus we have,

$$(1.6.7) \quad G(S) \subseteq \text{Aut}(\Gamma(S)).$$

Analogously,

$$(1.6.8) \quad \mathbf{Z}/p\mathbf{Z} \subseteq \text{Aut}(\Gamma(S)),$$

since if $i - j \in S$, then $(i + b) - (j + b) \in S$ for every $b \in \mathbf{Z}/p\mathbf{Z}$. Therefore every permutation $(1, b): x \mapsto x + b$ with $b \in \mathbf{Z}/p\mathbf{Z}$ is in $\text{Aut}(\Gamma(S))$. In particular, this means that $\text{Aut}(\Gamma(S))$ is transitive. In view of 1.6.5, these last two inclusions (1.6.7, 1.6.8) tell us that the subgroup of the affine group given by the semi-direct product $G(S) \rtimes \mathbf{Z}/p\mathbf{Z}$ is a subgroup of $\text{Aut}(\Gamma(S))$.

(1.6.9) **Proposition:** The semi-direct product $G(S) \rtimes \mathbf{Z}/p\mathbf{Z}$ is a subgroup of $\text{Aut}(\Gamma(S))$. In fact we have the inclusions,

$$\mathbf{Z}/p\mathbf{Z} \subseteq D_p \subseteq G(S) \rtimes \mathbf{Z}/p\mathbf{Z} \subseteq \text{Aff}(\mathbf{Z}/p\mathbf{Z}) \subseteq S_p \quad \text{and}$$

$$\mathbb{Z}/p\mathbb{Z} \subseteq D_p \subseteq G(S) \rtimes \mathbb{Z}/p\mathbb{Z} \subseteq \text{Aut}(\Gamma(S)) \subseteq S_p.$$

Proof: The inclusion $G(S) \rtimes \mathbb{Z}/p\mathbb{Z} \subseteq \text{Aut}(\Gamma(S))$ was established in 1.6.7 and 1.6.8. Also note that all groups listed in Proposition 1.6.9 are subgroups of S_p . Since $G(S) \subseteq (\mathbb{Z}/p\mathbb{Z})^*$, the inclusion $G(S) \rtimes \mathbb{Z}/p\mathbb{Z} \subseteq \text{Aff}(\mathbb{Z}/p\mathbb{Z})$ is also clear. Since S is symmetric, $\{\pm 1\} \subseteq G(S)$ and therefore the dihedral group $D_p = \{\pm 1\} \rtimes \mathbb{Z}/p\mathbb{Z}$ is a subgroup of $G(S) \rtimes \mathbb{Z}/p\mathbb{Z}$ which clearly contains $\mathbb{Z}/p\mathbb{Z}$. ■

In Proposition 1.6.2, we considered $S = G(S) = \{\pm 1\}$ and found that in this case, the inclusion $G(S) \rtimes \mathbb{Z}/p\mathbb{Z} \subseteq \text{Aut}(\Gamma(S))$ from Proposition 1.6.9 is in fact an equality

$$D_p = \{\pm 1\} \rtimes \mathbb{Z}/p\mathbb{Z} = \text{Aut}(\Gamma(S)).$$

In the special case of Paley graphs $\Gamma(S)$, the analogous equality has been established in the literature (see [Bi2]).

(1.6.10) **Example:** If $p \equiv 1 \pmod{4}$ and $S = G(S) = (\mathbb{Z}/p\mathbb{Z})^{*2}$, then

$$\text{Aut}(\Gamma(S)) = (\mathbb{Z}/p\mathbb{Z})^{*2} \rtimes \mathbb{Z}/p\mathbb{Z}.$$

What about the general case? Are there primes p and symmetric subsets S such that we have not yet exhibited all automorphisms of $\Gamma(S)$? In the remainder of this section, we will prove that for *all* circulant graphs $\Gamma(S)$ (not considered in 1.6.1), the full automorphism group is in fact given by $G(S) \rtimes \mathbb{Z}/p\mathbb{Z}$ (see Theorem 1.6.16). So for the remainder of this section, we will consider circulant graphs $\Gamma(S)$ where $S \neq \emptyset$ and $S \neq (\mathbb{Z}/p\mathbb{Z})^*$. Therefore, the automorphism group $\text{Aut}(\Gamma(S))$ will be a proper subgroup of S_p . In fact, since we saw in 1.6.8 that $\mathbb{Z}/p\mathbb{Z} \subseteq \text{Aut}(\Gamma(S))$, then $\text{Aut}(\Gamma(S))$ is a transitive subgroup of S_p .

(1.6.11) **Proposition:** If $S \neq \emptyset, (\mathbb{Z}/p\mathbb{Z})^*$, then $\text{Aut}(\Gamma(S))$ is not doubly transitive.

Proof: Let $M = \{(i, j) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} : i \neq j\}$ with diagonal action of S_p and let $E = \{(i, j) \in M : i - j \in S\}$. Since $S \neq \emptyset$, we have $E \neq \emptyset$ and since $S \neq (\mathbb{Z}/p\mathbb{Z})^*$, we have $E \neq M$. We can view $\text{Aut}(\Gamma(S))$ as the subgroup of all $\sigma \in S_p$ with $\sigma E = E$. Hence, if $(i, j) \in E$ and $(k, l) \in M \setminus E$, then there is no $\sigma \in \text{Aut}(\Gamma(S))$ with $(\sigma(i), \sigma(j)) = (k, l)$; that is, $\text{Aut}(\Gamma(S))$ is not doubly transitive. ■

Now we are in a position to apply classical results on permutations groups.

(1.6.12) **Theorem:** If $S \neq \emptyset, (\mathbb{Z}/p\mathbb{Z})^*$, then

(1) $\text{Aut}(\Gamma(S))$ is solvable; and

(2) $\text{Aut}(\Gamma(S))$ is conjugate in S_p to a subgroup of $\text{Aff}(\mathbb{Z}/p\mathbb{Z})$.

Proof: (1) By Proposition 1.6.11, $\text{Aut}(\Gamma(S))$ is a permutation group of prime degree p that is not doubly transitive. It is a theorem of Burnside [Bu1] that such groups are solvable.

(2) By 1.6.8 and part (1), $\text{Aut}(\Gamma(S))$ is a transitive subgroup of S_p which is solvable. Galois showed that such groups are conjugate in S_p to a subgroup of $\text{Aff}(\mathbb{Z}/p\mathbb{Z})$. ■

(1.6.13) **Lemma:** If $S \neq \emptyset, (\mathbb{Z}/p\mathbb{Z})^*$, then

(1) The centralizer of $\mathbb{Z}/p\mathbb{Z}$ in S_p is $\mathbb{Z}/p\mathbb{Z}$ itself.

(2) The normalizer of $\mathbb{Z}/p\mathbb{Z}$ in S_p is $\text{Aff}(\mathbb{Z}/p\mathbb{Z})$.

Proof: (1) We denote by $T = (1, 1)$ the permutation $T: x \mapsto x + 1$ for $x \in \mathbb{Z}/p\mathbb{Z}$. Thus T is a generator of the cyclic subgroup $\mathbb{Z}/p\mathbb{Z}$ of S_p . Let $\sigma \in S_p$ be in the centralizer of $\mathbb{Z}/p\mathbb{Z}$, that is $\sigma T = T\sigma$. If σ has a fixed point $x_0 \in \mathbb{Z}/p\mathbb{Z}$, then for

any $b \in \mathbf{Z}/p\mathbf{Z}$, $(1, b)x_0$ is also a fixed point of σ since

$$\sigma((1, b)x_0) = \sigma(T^b x_0) = T^b \sigma(x_0) = T^b x_0 = (1, b)x_0.$$

Clearly, $\{(1, b)x_0 : b \in \mathbf{Z}/p\mathbf{Z}\} = \mathbf{Z}/p\mathbf{Z}$. So if σ has a fixed point, then it is the identity. If σ has no fixed points, then $\sigma(0) = b$ for a unique $b \in (\mathbf{Z}/p\mathbf{Z})^*$. Then $T^{-b}\sigma = (1, -b)\sigma$ fixes $0 \in \mathbf{Z}/p\mathbf{Z}$ and still commutes with T . Therefore by the above, $T^{-b}\sigma$ is the identity, which implies that $\sigma = T^b \in \mathbf{Z}/p\mathbf{Z}$. Hence in either case, the centralizer of $\mathbf{Z}/p\mathbf{Z}$ in S_p is contained in $\mathbf{Z}/p\mathbf{Z}$, that is, $\mathbf{Z}/p\mathbf{Z}$ is its own centralizer in S_p .

(2) Let $(a, b) \in \text{Aff}(\mathbf{Z}/p\mathbf{Z})$ with $a \in (\mathbf{Z}/p\mathbf{Z})^*$ and $b \in \mathbf{Z}/p\mathbf{Z}$. Then for every $c \in \mathbf{Z}/p\mathbf{Z}$, by Lemma 1.6.4 we have

$$(a, b)T^c(a, b)^{-1} = T^{ac} \in \mathbf{Z}/p\mathbf{Z}.$$

Thus the affine group $\text{Aff}(\mathbf{Z}/p\mathbf{Z})$ is contained in the normalizer, $N(\mathbf{Z}/p\mathbf{Z})$ of $\mathbf{Z}/p\mathbf{Z}$ in S_p . Since $\text{Aff}(\mathbf{Z}/p\mathbf{Z}) = (\mathbf{Z}/p\mathbf{Z})^* \rtimes \mathbf{Z}/p\mathbf{Z}$ has $(p-1)p$ elements, it is enough for us to show that $\#N(\mathbf{Z}/p\mathbf{Z}) = (p-1)p$.

There is a short exact sequence

$$1 \longrightarrow \mathbf{Z}/p\mathbf{Z} \longrightarrow N(\mathbf{Z}/p\mathbf{Z}) \longrightarrow \text{Aut}(\mathbf{Z}/p\mathbf{Z}) \longrightarrow 1$$

where the surjection is given by mapping the element σ of the normalizer $N(\mathbf{Z}/p\mathbf{Z})$ to the automorphism of $\mathbf{Z}/p\mathbf{Z}$ given by $T^c \rightarrow \sigma T^c \sigma^{-1}$ for $c \in \mathbf{Z}/p\mathbf{Z}$. This is onto since $\text{Aff}(\mathbf{Z}/p\mathbf{Z}) \subseteq N(\mathbf{Z}/p\mathbf{Z})$ and $\sigma = (a, b)$ gets mapped to the automorphism $T^c \rightarrow T^{ac}$ as noted. Clearly the kernel of this mapping is the centralizer of

$\mathbb{Z}/p\mathbb{Z}$ in S_p which as shown in part (1) is simply $\mathbb{Z}/p\mathbb{Z}$ itself. Thus $\#N(\mathbb{Z}/p\mathbb{Z}) = \#Aut(\mathbb{Z}/p\mathbb{Z}) \cdot \#(\mathbb{Z}/p\mathbb{Z}) = (p-1) \cdot p$ and hence $N(\mathbb{Z}/p\mathbb{Z}) = Aff(\mathbb{Z}/p\mathbb{Z})$. ■

We are going to improve on the statement in Theorem 1.6.12(2).

(1.6.14) **Proposition:** If $S \neq \emptyset, (\mathbb{Z}/p\mathbb{Z})^*$, then

$$Aut(\Gamma(S)) \subseteq Aff(\mathbb{Z}/p\mathbb{Z}).$$

Proof: We know by Proposition 1.6.9 and Theorem 1.6.12(2) that the automorphism group $Aut(\mathbb{Z}/p\mathbb{Z})$ is a subgroup of S_p that contains $\mathbb{Z}/p\mathbb{Z}$ and is conjugate in S_p to a subgroup of $Aff(\mathbb{Z}/p\mathbb{Z})$. Choose an element $\sigma \in S_p$ for which

$$(1.6.15) \quad \sigma Aut(\Gamma(S)) \sigma^{-1} \subseteq Aff(\mathbb{Z}/p\mathbb{Z}).$$

Then $\sigma(\mathbb{Z}/p\mathbb{Z})\sigma^{-1}$ is a p -Sylow subgroup of $Aff(\mathbb{Z}/p\mathbb{Z})$. But since

$$Aff(\mathbb{Z}/p\mathbb{Z}) = (\mathbb{Z}/p\mathbb{Z})^* \rtimes \mathbb{Z}/p\mathbb{Z},$$

we see that $\mathbb{Z}/p\mathbb{Z}$ is normal in $Aff(\mathbb{Z}/p\mathbb{Z})$ (compare to 1.6.5) and $Aff(\mathbb{Z}/p\mathbb{Z})$ has a unique p -Sylow subgroup. We conclude that

$$\sigma(\mathbb{Z}/p\mathbb{Z})\sigma^{-1} = \mathbb{Z}/p\mathbb{Z}.$$

Therefore, $\sigma \in N(\mathbb{Z}/p\mathbb{Z})$. By Theorem 1.6.13(2), we already know that this normalizer is equal to $Aut(\mathbb{Z}/p\mathbb{Z})$. So $\sigma \in Aut(\mathbb{Z}/p\mathbb{Z})$ and by 1.6.15, we obtain that $Aut(\Gamma(S))$ is contained in $Aut(\mathbb{Z}/p\mathbb{Z})$. ■

Notice how the inclusions of Proposition 1.6.9 can be made more precise if one excludes the totally disconnected and the complete graphs from consideration.

Now we can finish the determination of the automorphism group of all circulant graphs $\Gamma(S)$ with $S \neq \emptyset, (\mathbb{Z}/p\mathbb{Z})^*$.

(1.6.16) **Theorem:** If $S \neq \emptyset, (\mathbb{Z}/p\mathbb{Z})^*$, then

$$\text{Aut}(\Gamma(S)) = G(S) \rtimes \mathbb{Z}/p\mathbb{Z}.$$

Proof: By Theorem 1.6.14 we know that

$$\text{Aut}(\Gamma(S)) \subseteq \text{Aff}(\mathbb{Z}/p\mathbb{Z}).$$

In other words, we know that any element of $\text{Aut}(\Gamma(S))$ has the form (a, b) for some $a \in (\mathbb{Z}/p\mathbb{Z})^*$ and $b \in \mathbb{Z}/p\mathbb{Z}$ (see 1.6.5). Since $\mathbb{Z}/p\mathbb{Z}$ is contained in $\text{Aut}(\Gamma(S))$ (see 1.6.8), we have $(1, -b) \in \text{Aut}(\Gamma(S))$, hence (compare to Lemma 1.6.4(2)) $(1, -b)(a, b) = (a, 0)$ lies in $\text{Aut}(\Gamma(S))$. In other words, $x \mapsto ax$ for any $x \in \mathbb{Z}/p\mathbb{Z}$ is an automorphism of $\Gamma(S)$. Thus, if $i, j \in \mathbb{Z}/p\mathbb{Z}$ are two vertices with $i - j \in S$, then $ai - aj = a(i - j) \in S$ also. So $aS = S$ and therefore $a \in G(S)$.

So every element of $\text{Aut}(\Gamma(S))$ is of the form (a, b) for some $a \in G(S)$ and $b \in \mathbb{Z}/p\mathbb{Z}$. Thus

$$\text{Aut}(\Gamma(S)) \subseteq G(S) \rtimes \mathbb{Z}/p\mathbb{Z}.$$

However, again from Theorem 1.6.9, we already knew that

$$G(S) \rtimes \mathbb{Z}/p\mathbb{Z} \subseteq \text{Aut}(\Gamma(S)),$$

which then proves the theorem. ■

This completes the determination of $\text{Aut}(\Gamma(S))$ for all circulant graphs $\Gamma(S)$.

The main theorem can be restated as follows:

If $\text{Aut}(\Gamma(S)) \neq S_p$, then all automorphisms of $\Gamma(S)$ are affine ones.

(1.6.17) **Summary:** Let p be an odd prime, S a symmetric subset of $(\mathbb{Z}/p\mathbb{Z})^*$ and consider the circulant graph $\Gamma(S)$. If $\Gamma(S)$ is the totally disconnected graph or the complete graph, then $\text{Aut}(\Gamma(S)) = S_p$. Otherwise, $\text{Aut}(\Gamma(S)) = G(S) \rtimes \mathbb{Z}/p\mathbb{Z}$.

Specifically, if $S \neq \emptyset, (\mathbb{Z}/p\mathbb{Z})^*$, then $\text{Aut}(\Gamma(S))$ is a subgroup of the normalizer $\text{Aff}(\mathbb{Z}/p\mathbb{Z})$ of the p -Sylow subgroup $\mathbb{Z}/p\mathbb{Z}$ in S_p , and the order of $\text{Aut}(\Gamma(S))$ is the multiple of $2p$ and a proper divisor of $(p-1)p$.

Based on the above investigations, it is possible to add a simple characterization of isomorphisms of circulant graphs.

If $\Gamma(S)$ and $\Gamma(S')$ are isomorphic circulant graphs, then they have the same number, p , of vertices and S and S' are both symmetric subsets of $(\mathbb{Z}/p\mathbb{Z})^*$. As we know

$\Gamma(S)$ is the totally disconnected graph if and only if $S = \emptyset$, and

$\Gamma(S)$ is the complete graph if and only if $S = (\mathbb{Z}/p\mathbb{Z})^*$.

In general we have,

(1.6.18) **Theorem:** $\Gamma(S)$ and $\Gamma(S')$ are isomorphic if and only if

$$aS = S' \text{ for some } a \in (\mathbb{Z}/p\mathbb{Z})^*.$$

Proof: This is clearly true if S or S' is equal to \emptyset or $(\mathbb{Z}/p\mathbb{Z})^*$. Thus we may assume that both S and S' are non-empty, proper symmetric subsets of $(\mathbb{Z}/p\mathbb{Z})^*$.

Suppose that $\Gamma(S)$ and $\Gamma(S')$ are isomorphic. Let σ be such an isomorphism, that is, $\sigma: \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$ is a permutation satisfying

$$i - j \in S \text{ if and only if } \sigma i - \sigma j \in S', \text{ and}$$

$$i - j \in S' \text{ if and only if } \sigma^{-1}i - \sigma^{-1}j \in S$$

for any two vertices $i, j \in \mathbb{Z}/p\mathbb{Z}$.

Let α be an automorphism of $\Gamma(S)$, that is, $\alpha: \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$ is a permutation satisfying

$$i - j \in S \text{ if and only if } \alpha i - \alpha j \in S.$$

We then have

$$\begin{aligned} i - j \in S' &\iff \sigma^{-1}i - \sigma^{-1}j \in S \\ &\iff \alpha\sigma^{-1}i - \alpha\sigma^{-1}j \in S \\ &\iff \sigma\alpha\sigma^{-1}i - \sigma\alpha\sigma^{-1}j \in S' \end{aligned}$$

Thus, if $\alpha \in \text{Aut}(G)$, then $\sigma\alpha\sigma^{-1} \in \text{Aut}(\Gamma(S'))$. In other words,

$$\sigma\text{Aut}(\Gamma(S))\sigma \subseteq \text{Aut}(\Gamma(S')).$$

We conclude that $\text{Aut}(\Gamma(S))$ and $\text{Aut}(\Gamma(S'))$ are conjugate in S_p :

$$\sigma\text{Aut}(\Gamma(S))\sigma = \text{Aut}(\Gamma(S')).$$

By 1.6.8 and Theorem 1.6.14, we know

$$\mathbb{Z}/p\mathbb{Z} \subseteq \text{Aut}(\Gamma(S)) \subseteq \text{Aff}(\mathbb{Z}/p\mathbb{Z}),$$

$$\mathbb{Z}/p\mathbb{Z} \subseteq \text{Aut}(\Gamma(S')) \subseteq \text{Aff}(\mathbb{Z}/p\mathbb{Z}),$$

and since $\mathbb{Z}/p\mathbb{Z}$ is the unique p -Sylow subgroup of the groups $\text{Aut}(\Gamma(S))$ and $\text{Aut}(\Gamma(S'))$, we obtain as in the proof of Theorem 1.6.14,

$$\sigma\mathbb{Z}/p\mathbb{Z}\sigma^{-1} = \mathbb{Z}/p\mathbb{Z}.$$

So, σ lies in the normalizer $N(\mathbf{Z}/p\mathbf{Z})$ of $\mathbf{Z}/p\mathbf{Z}$ in S_p . By Lemma 1.6.13(2), this means

$$\sigma \in \text{Aff}(\mathbf{Z}/p\mathbf{Z}).$$

Hence, $\sigma = (a, b)$ for unique $a \in (\mathbf{Z}/p\mathbf{Z})^*$ and $b \in \mathbf{Z}/p\mathbf{Z}$ (see Lemma 1.6.4), and we have for $i, j \in \mathbf{Z}/p\mathbf{Z}$:

$$\begin{aligned} i - j \in S &\iff (a, b)i - (a, b)j \in S' \\ &\iff (ai + b) - (aj + b) \in S' \\ &\iff a(i - j) \in S'. \end{aligned}$$

We therefore conclude that

$$aS = S'.$$

The converse is clear: if $aS = S'$ for some $a \in (\mathbf{Z}/p\mathbf{Z})^*$, then the permutation $\sigma = (a, b): \mathbf{Z}/p\mathbf{Z} \rightarrow \mathbf{Z}/p\mathbf{Z}$ yields an isomorphism between $\Gamma(S)$ and $\Gamma(S')$. ■

Now we can count the number of circulant graphs in an isomorphism class.

(1.6.19) **Corollary:** Let S be a symmetric subset of $(\mathbf{Z}/p\mathbf{Z})^*$. Then the number of circulant graphs $\Gamma(S')$ that are isomorphic to $\Gamma(S)$ is equal to the index $[(\mathbf{Z}/p\mathbf{Z})^* : G(S)]$.

Proof: This follows from Theorem 1.6.18, since an element $a \in (\mathbf{Z}/p\mathbf{Z})^*$ is in $G(S)$ if and only if $aS = S$. ■

We will now exhibit non-isomorphic circulant graphs with the same automorphism group. Notice that we always have for complementary symmetric subsets $S, \tilde{S} \subseteq (\mathbf{Z}/p\mathbf{Z})^*$, $\text{Aut}(\Gamma(S)) = \text{Aut}(\Gamma(\tilde{S}))$.

(1.6.20) **Example:** Let $S = \{\pm 1\} \subseteq (\mathbb{Z}/p\mathbb{Z})^*$ and let $\tilde{S} = (\mathbb{Z}/p\mathbb{Z})^* \setminus S$. Then $\Gamma(S)$ is a p -cycle, $\Gamma(\tilde{S})$ is regular of degree $p - 3$ and

$$\text{Aut}(\Gamma(S)) = \text{Aut}(\Gamma(\tilde{S})) = D_p.$$

For all odd primes $p \neq 5$, this provides us with examples of non-isomorphic circulant graphs whose automorphism groups are the dihedral group of order $2p$.

CHAPTER 2: QUOTIENT GRAPHS

Section 1: The Deleted Graph and the Quotient Graph

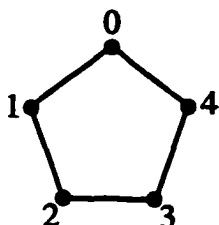
We now focus our attention on the case $S = G(S)$. Recall this means that S is the subgroup of n -th powers in $(\mathbb{Z}/p\mathbb{Z})^*$ for some n dividing $p - 1$ (see 1.3.28). Since S is symmetric, $\#S \equiv 0(2)$. Also, $\#S = \frac{p-1}{n}$. Therefore, we must require that $p \equiv 1(2n)$.

(2.1.1) **Definition:** Let $D(S)$ be the subgraph of $\Gamma(S)$ obtained by deleting the vertex 0. We call $D(S)$ the **deleted graph**.

(2.1.2) **Examples:**

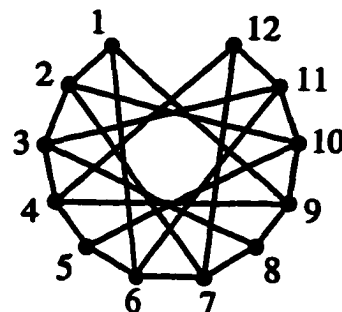
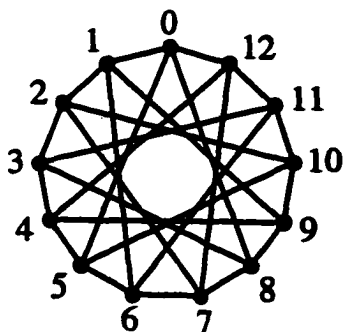
(1) Let $n = 2$ and $p = 5$. Then $S = (\mathbb{Z}/5\mathbb{Z})^{*2} = \{\pm 1\}$.

Then the circulant graph $\Gamma(S)$ is and the deleted graph $D(S)$ is



(2) Let $n = 3$ and $p = 13$. Then $S = (\mathbb{Z}/13\mathbb{Z})^{*3} = \{\pm 1, \pm 5\}$.

Then the circulant graph $\Gamma(S)$ is and the deleted graph $D(S)$ is



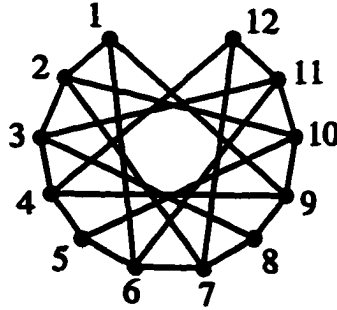
Since the only vertex deleted was 0, two distinct vertices of $D(S)$ are adjacent if and only if they are also adjacent in the circulant graph $\Gamma(S)$. The basic example is $n = 2$. With $p \equiv 1(4)$, $S = (\mathbb{Z}/p\mathbb{Z})^{*2}$ is the subgroup of squares and $\Gamma(S)$ is the **Paley Graph** (see [Bi2]). Now we will use the quotient map

$$(2.1.3) \quad q: (\mathbb{Z}/p\mathbb{Z})^* \rightarrow (\mathbb{Z}/p\mathbb{Z})^*/S = \Pi.$$

Recall that since $S = G(S) = (\mathbb{Z}/p\mathbb{Z})^{*n}$, Π is a cyclic group of order n . We will regard the elements of Π as the cosets of S in $(\mathbb{Z}/p\mathbb{Z})^*$. For example if $S = (\mathbb{Z}/5\mathbb{Z})^{*2}$ as in Example 2.1.2(1), $\Pi = \{S, 2S\}$ and if $S = (\mathbb{Z}/13\mathbb{Z})^{*3}$ as in Example 2.1.2(2), $\Pi = \{S, 2S, 4S\}$.

(2.1.4) **Definition:** For $v, w \in (\mathbb{Z}/p\mathbb{Z})^*$ and $vS \neq wS$, we define $N(v, wS)$ to be the number of vertices of the deleted graph $D(S)$ which are elements of wS and adjacent to v .

(2.1.5) **Example:** Consider Example 2.1.2(2). The deleted graph $D(S)$ is



Then $S = \{\pm 1, \pm 5\}$, $2S = \{\pm 2, \pm 3\}$ and $4S = \{\pm 4, \pm 6\}$. So simply by looking at the deleted graph and counting, we see that

$$N(1, 2S) = 1$$

$$N(1, 4S) = 2$$

$$N(2, 4S) = 1.$$

We wish to see that $N(v, wS)$ depends only on the coset of v in Π . Suppose that ws_0 is adjacent to v . Then for any s in S , $(ws_0)s = w(s_0s)$ is adjacent to vs . So $N(v, wS) \leq N(vs, wS)$ for every $s \in S$. Now suppose that ws_0 is adjacent to vs . If we write $s_0 = s_1s$, then we can see that ws_1 is adjacent to s . So $N(v, wS) \geq N(vs, wS)$ for every $s \in S$. Therefore, $N(v, wS) = N(vs, wS)$ for every $s \in S$. In particular

$$\sum_{s \in S} N(vs, wS) = N(v, wS) \# S.$$

Notice that since $\sum_{s \in S} N(vs, wS)$ is just the number of edges of $D(S)$ with one endpoint in vS and the other in wS , we have

$$N(v, wS) \# S = \sum_{s \in S} N(vs, wS) = \sum_{s \in S} N(ws, vS) = N(w, vS) \# S.$$

Hence for $vS \neq wS$,

$$(2.1.6) \quad N(v, wS) = N(w, vS).$$

(2.1.7) **Definition:** We define the **quotient graph** $Q(S)$ to be the graph with vertex set Π and edges defined by the following condition: distinct vertices $vS \neq wS$ are adjacent if and only if

$$N(v, wS) \equiv 1 \pmod{2}.$$

By 2.1.6 this is a well-defined graph. Notice that since Π is the set of vertices, $Q(S)$ has only n vertices. Therefore, as long as n is “small”, the quotient graph will be a graph on a small number of vertices regardless of which $p \equiv 1(2n)$ is chosen.

(2.1.8) **Examples:**

(1) Let $n = 2$ and $p = 5$. Then

$$S = \{\pm 1\} \text{ and}$$

$$2S = \{\pm 2\}.$$

Since $N(1, 2S) = 1 \equiv 1(2)$, the quotient graph $Q(S)$ is



(2) Let $n = 3$ and $p = 31$. Then

$$S = \{\pm 1, \pm 2, \pm 4, \pm 8, \pm 16\},$$

$$3S = \{\pm 3, \pm 6, \pm 7, \pm 12, \pm 14\} \text{ and}$$

$$5S = \{\pm 5, \pm 9, \pm 10, \pm 11, \pm 13\}.$$

Since $N(1, 3S) = 4 \equiv 0(2)$, $N(1, 5S) = 2 \equiv 0(2)$ and $N(3, 5S) = 4 \equiv 0(2)$, the quotient graph $Q(S)$ is



Recall from Section 1 of Chapter 1 that a vertex decomposition of $Q(S)$ is an unordered pair of subsets $\{U_1, U_2\}$ of Π such that:

$$U_1 \cup U_2 = \Pi \text{ and } U_1 \cap U_2 = \emptyset.$$

In our numbering, we will always choose U_2 to be the subset of Π containing the identity element S . Then $P(Q(S), U_1) = P(Q(S), U_2) \subseteq \Pi$ is the set of special points of $Q(S)$ with respect to the vertex decomposition $\{U_1, U_2\}$. Again we will be interested in determining the number of EVD's of $Q(S)$.

For any subset $X \subseteq \Pi$, $q^{-1}(X) \subseteq (\mathbb{Z}/p\mathbb{Z})^*$ lies in \mathcal{S}_*^S (see 1.3.29). Given a vertex decomposition $\{U_1, U_2\}$ of $Q(S)$, let

$$L = q^{-1}(U_1) \text{ and } \tilde{L} = q^{-1}(U_2).$$

Then $\{L, \tilde{L}\}$ is an S -invariant vertex decomposition of the deleted graph $D(S)$.

Since $S \in U_2$, we see that the set S is contained in \tilde{L} , and therefore $L \cap S = \emptyset$.

(2.1.9) **Lemma:** Let $\{U_1, U_2\}$ be a vertex decomposition of $Q(S)$, with $S \in U_2$ and $L = q^{-1}(U_1)$. Then

$$P(D(S), L) = q^{-1}(P(Q(S), U_1)).$$

Proof: We first note that if $U_1 = \emptyset$, then $L = q^{-1}(U_1) = \emptyset$ and therefore both $P(D(S), L) = \emptyset$ and $q^{-1}(P(Q(S), U_1)) = \emptyset$. So the lemma holds.

Now we assume $U_1 \neq \emptyset$. Since $S \in U_2$, we also know that $U_2 \neq \emptyset$. Let $\#U_2 = k$. Now we choose distinct coset representatives w_1, w_2, \dots, w_k of $(\mathbb{Z}/p\mathbb{Z})^*$ so that $U_2 = \{w_1S, w_2S, \dots, w_kS\} \subseteq \Pi$. Then

$$\tilde{L} = q^{-1}(U_2) = \text{disjoint union of } w_1S, \dots, w_kS = \bigsqcup_{i=1}^k w_iS \subseteq (\mathbb{Z}/p\mathbb{Z})^*.$$

Now for any $v \in L$, $v \in P(D(S), L)$ if and only if v is joined to an odd number of vertices in $\tilde{L} = \bigsqcup_{i=1}^k w_iS$. So

$$(2.1.10) \quad v \in P(D(S), L) \iff \sum_{i=1}^k N(v, w_iS) \equiv 1 \pmod{2} \quad (\text{see 2.1.4}).$$

Clearly there must be an odd number of the w_i for which $N(v, w_iS)$ is odd. From our definition of $Q(S)$, this means vS is adjacent to an odd number of vertices in U_2 . So

$$v \in P(D(S), L) \iff vS \in P(Q(S), U_1) \iff v \in q^{-1}(P(Q(S), U_1))$$

which proves the lemma. ■

Note: With $q^{-1}(U_1) = L$ and $q^{-1}(U_2) = \tilde{L}$ we also have that

$$\{L, (\tilde{L} \cup \{0\})\}$$

is an S -invariant vertex decomposition of the original circulant graph $\Gamma(S)$. So we can generalize the previous lemma to the circulant graph $\Gamma(S)$.

(2.1.11) **Lemma:** Let $\{U_1, U_2\}$ be a vertex decomposition of $Q(S)$ with $S \in U_2$ and $L = q^{-1}(U_1)$. Then $\{L, (\tilde{L} \cup \{0\})\}$ is an S -invariant vertex decomposition of $\Gamma(S)$ and

$$P(\Gamma(S), L) = q^{-1}(P(Q(S), U_1)).$$

Proof: We were careful to arrange it so that $S \subseteq (\tilde{L} \cup \{0\})$. Recall that in $\Gamma(S)$, the vertices which are adjacent to 0 (and thus affected by its deletion) are exactly the elements of S . Since S and 0 lie in the same subset of the vertex decomposition, deleting 0 will not affect whether any vertex is special or not. Consequently,

$$P(\Gamma(S), L) = P(D(S), L),$$

and the conclusion follows from the previous lemma. ■

(2.1.12) **Lemma:** If $L \in \mathcal{S}_*$ and $\{L, (\tilde{L} \cup \{0\})\}$ is an EVD of $\Gamma(S)$, then $L \cap S = \emptyset$.

Proof: If $\{L, (\tilde{L} \cup \{0\})\}$ is an EVD of $\Gamma(S)$ (in other words, $P(\Gamma(S), L) = \emptyset$), then

$$\gamma_S \cdot \gamma_L = 0.$$

Therefore $\gamma_S \cdot \gamma_{\tilde{L}} = \gamma_S$. Thus $P(\Gamma(S), \tilde{L}) = S$.

Suppose that $L \cap S \neq \emptyset$. Then $S \subseteq L$ and $S \cap \tilde{L} = \emptyset$. Then we have a vertex decomposition of the quotient graph $Q(S)$ given by $\{U_1, U_2\}$ where $U_1 = q(\tilde{L})$ and $U_2 = q(L)$. Then by Lemma 2.1.11,

$$q^{-1}(P(Q(S), U_1)) = P(\Gamma(S), \tilde{L}) = S.$$

Hence the vertex S is the unique special vertex with respect to this vertex decomposition. This contradicts Lemma 1.1.6 which says that the number of special vertices is always even. Therefore our assumption that $L \cap S \neq \emptyset$ is incorrect, and the lemma follows. ■

What this lemma tells us is that we have a one-to-one correspondence, given by $q^{-1}(U_1) = L$, between the EVD's $\{U_1, U_2\}$ of the quotient graph $Q(S)$ and the subsets $L \in \mathcal{S}_*^S$ for which $S \cap L = \emptyset$ and $\{L, (\tilde{L} \cup \{0\})\}$ is an S -invariant EVD of the circulant graph $\Gamma(S)$. In Section 4 of Chapter 1 we investigated the set of all subsets $L \in \mathcal{S}_*^S$ with these properties. Therefore we will utilize those results to describe the invariant $c(Q(S))$ in terms of $c(\Gamma(S))$.

(2.1.13) **Theorem:** If $n > 1$, $p \equiv 1(2n)$ and $S = G(S) = (\mathbb{Z}/p\mathbb{Z})^{*n}$, then for the quotient graph $Q(S)$,

$$c(Q(S)) = \frac{c(\Gamma(S))}{\#S}.$$

Proof: By Lemmas 2.1.11 and 2.1.12, the vertex decomposition $\{U_1, U_2\}$ of $Q(S)$ is an EVD if and only if $\{L, (\tilde{L} \cup \{0\})\}$ is an S -invariant EVD of $\Gamma(S)$ where $q^{-1}(U_1) = L \in \mathcal{S}_*^S$. So as vector spaces over \mathbb{F}_2 , the space of all EVD's of $Q(S)$ and the space of all $L \in \mathcal{S}_*^S$ with $\{L, (\tilde{L} \cup \{0\})\}$ an EVD of $\Gamma(S)$ have the same dimension. But in Proposition 1.4.14, we found that the latter dimension is

exactly equal to

$$\frac{c(\Gamma(S))}{\#G(S)} = \frac{c(\Gamma(S))}{\#S},$$

so the theorem is proved. ■

(2.1.14) **Corollary:** For the quotient graph $Q(S)$,

$$c(Q(S)) = 0 \iff c(\Gamma(S)) = 0.$$

Proof: Clear by the previous theorem. ■

Note: For the quotient graph $Q(S)$,

$$(2.1.15) \quad c(Q(S)) = \frac{c(\Gamma(S))}{\#S} = \frac{c(\Gamma(S))}{\#G(S)} = \frac{ab\#G(S)}{\#G(S)} = ab,$$

hence b always divides $c(Q(S))$.

Section 2: The Quotient Graph $Q(S)$

For a fixed rational integer $n \geq 1$, there are infinitely many primes $p \equiv 1(2n)$. Corresponding to each such prime there is a quotient graph $Q(S)$ on a set of n vertices (with $S = (\mathbf{Z}/p\mathbf{Z})^{*n}$). The graph will depend on p , but with the number of vertices fixed, there are only finitely many possibilities, up to isomorphism. Therefore, if n is “small”, we might be able to explain the quotient graphs completely. First we have a characterization of the quotient graph in terms of the arithmetic of the finite field $\mathbf{Z}/p\mathbf{Z}$.

(2.2.1) **Proposition:** Let $v, w \in (\mathbf{Z}/p\mathbf{Z})^*$ with $vS \neq wS$. Then vS and wS are adjacent in $Q(S)$ if and only if there are an odd number of pairs $(X^n, Y^n) \in S \times S$ for which

$$vX^n + wY^n = 1.$$

Proof: From our definition of $Q(S)$ (see 2.1.7), vS and wS are adjacent if and only if there are an odd number of elements in the coset wS which are adjacent to v in the deleted graph $D(S)$. Since every element in wS can be uniquely expressed as wA^n for some $A^n \in S$, we have wS is adjacent to vS if and only if there exists an odd number of $A^n \in S$ with $v - wA^n \in S$ (see 2.1.1), or in other words

$$v - wA^n = B^n \text{ for some } B^n \in S.$$

But this is equivalent to

$$vB^{-n} - wA^nB^{-n} = 1.$$

So we let $X^n = (B^{-1})^n \in S$ and $Y^n = -(AB^{-1})^n \in S$ (since $-1 \in S$). Therefore we have

$$v - wA^n = B^n \iff vB^{-n} - wA^nB^{-n} = 1 \iff vX^n + wY^n = 1,$$

which proves the proposition. ■

(2.2.2) **Remark:** We can therefore consider $N(v, wS)$ as the number of solutions to the equation $vX^n + wY^n = 1$.

We must emphasize that although the vertex set Π of $Q(S)$ is a cyclic group of order n , $Q(S)$ is not a Cayley Graph. In fact, for any $S \neq \emptyset$, the circulant graph $\Gamma(S)$ will be connected and regular (see 1.3.3), but $Q(S)$ need *not* be connected and is seldom regular. In fact $Q(S)$ can be totally disconnected. As might be expected, the element 2 plays a major role.

(2.2.3) **Lemma:** Let $v \in (\mathbb{Z}/p\mathbb{Z})^*$ with $vS \neq S$. Then vS is adjacent to S in $Q(S)$ if and only if $vS = 2S$.

Proof: By the previous proposition, vS is adjacent to S if and only if there are an odd number of pairs $(X^n, Y^n) \in S \times S$ with

$$X^n + vY^n = 1.$$

However,

$$X^n + vY^n = 1 \iff (XY^{-1})^n + v = (Y^{-1})^n \iff A^n + B^n = v$$

if we let $A^n = -(XY^{-1})^n$ and $B^n = (Y^{-1})^n$. So we must have an odd number of pairs (A^n, B^n) with

$$v = A^n + B^n.$$

But note that if (A^n, B^n) is such a pair, then so is (B^n, A^n) . So the only way we can have an *odd* number of pairs (A^n, B^n) is if there exists an $A^n \in S$ such that $v = A^n + A^n = 2A^n$, which is true exactly when $vS = 2S$. ■

What this lemma tells us is that the only vertex which can be adjacent to S in the quotient graph $Q(S)$ is $2S$, and in fact they will be adjacent provided they are distinct.

(2.2.4) Proposition (S-2S Rule): If $b = 1$ then S is an isolated vertex in the quotient graph $Q(S)$. If $b > 1$ then the only vertex which is adjacent to the vertex S in $Q(S)$ is $2S$.

Proof: As noted above, the previous lemma implies that the vertices S and $2S$ will be adjacent provided they are distinct and no other vertices can be adjacent to the vertex S . Since $2S = S$ if and only if $2 \in S$ if and only if $b = 1$ (see 1.4.4), the proposition is proved. ■

Now there is a way to describe edges in $Q(S)$ in terms of the ring $\mathcal{O}_F/2\mathcal{O}_F$. Recall from Section 4 of Chapter 1 that F is the fixed field of the subgroup S and

$$\gamma_S = \sum_{i=1}^{p-1} \chi_S(i) \xi^i \in \mathcal{O}_F/2\mathcal{O}_F.$$

Since $\text{Gal}(\mathbf{Q}(\xi)|\mathbf{Q}) = (\mathbf{Z}/p\mathbf{Z})^*$ and $\text{Gal}(\mathbf{Q}(\xi)|F) = S$, we have

$$\gamma_S = \text{tr}_{\mathbf{Q}(\xi)|F}(\xi) \in \mathcal{O}_F.$$

So $\gamma_S \in \mathcal{O}_F/2\mathcal{O}_F$ is the reduction mod 2 of $\text{tr}_{\mathbf{Q}(\xi)|F}(\xi) \in \mathcal{O}_F$. Hilbert points out (see [Hi]) that the conjugates of $\gamma_S = \text{tr}_{\mathbf{Q}(\xi)|F}(\xi)$ over \mathbf{Q} form a normal \mathbf{Z} -basis of \mathcal{O}_F . Reducing into \mathcal{O}_F , we find γ_S is a basis of \mathcal{O}_F as a free $\mathbf{F}_2[\Pi]$ -module of rank 1.

For $w \in S$ the Galois automorphism σ_w of \mathcal{O}_F depends only on the coset $wS \in \Pi$ since $\text{Gal}(F|\mathbf{Q}) = \Pi$. As seen in Lemma 1.3.30, the cosets of S in \mathcal{S}_*^S are a basis for \mathcal{S}_*^S over \mathbf{F}_2 . Thus for $vS \neq S$, we can express the product $\gamma_S \cdot \gamma_{vS}$ as

$$(2.2.5) \quad \gamma_S \cdot \gamma_{vS} = \sum_{wS \in \Pi} A_w \gamma_{wS}$$

for unique $A_w \in \mathbf{F}_2$.

(2.2.6) **Proposition:** Let vS and wS be distinct vertices of $Q(S)$. Then vS is adjacent to wS if and only if (in the formula 2.2.5) $A_w = 1$. Furthermore, vS will have odd degree in $Q(S)$ if and only if $A_v = 1$.

Proof: Recall the quotient map

$$q : (\mathbf{Z}/p\mathbf{Z})^* \longrightarrow \Pi = (\mathbf{Z}/p\mathbf{Z})^*/S.$$

We will use the vertex decomposition $\{U_1, U_2\}$ of $Q(S)$ where U_1 is the coset $\{vS\}$.

So $q^{-1}(U_1) = vS$. Then by Lemma 2.1.9 we have

$$P(D(S), vS) = q^{-1}(P(Q(S), \{vS\})).$$

Note that for $vS \neq wS$ we have

$$vS \text{ is adjacent to } wS \text{ in } Q(S) \iff wS \in P(Q(S), \{vS\}).$$

Furthermore,

$$vS \text{ has odd degree in } Q(S) \iff vS \in P(Q(S), \{vS\}).$$

Now recall that in \mathcal{O}_F

$$\gamma_{P(D(S), vS)} = \gamma_S \cdot \gamma_{vS} \quad (\text{see 1.3.37, 1.3.39}).$$

So if we write

$$\sum_{wS \in \Pi} A_w \gamma_{wS} = \gamma_S \cdot \gamma_{vS} = \gamma_{P(D(S), vS)} = \sum_{i=1}^{p-1} \chi_{P(D(S), vS)}(i) \xi^i$$

then since $P(D(S), vS)$ is S -invariant, we see that

$$A_w = 1 \iff wS \subseteq P(D(S), vS) \iff wS \in P(Q(S), \{vS\})$$

which as we noted earlier is true if and only if wS is adjacent to vS .

Similarly with $vS = wS$, we have $vS \in P(Q(S), \{vS\})$ (and therefore vS has odd degree) if and only if $A_v = 1$. ■

As a consequence of this proposition, we see that in equation 2.2.5

(2.2.7) the number of coefficients $A_w = 1$ is even.

(2.2.8) **Corollary:** Every vertex of the quotient graph $Q(S)$ has even degree if and only if $b = 1$. If $b > 1$ then $Q(S)$ has exactly two vertices of odd degree, namely S and $2^{b-1}S$.

Proof: Suppose $vS \neq S$ and suppose that the degree of vS is odd. By the previous proposition, this is true if and only if $A_v = 1$. In other words

$$\gamma_S \cdot \gamma_{vS} = \gamma_{vS} + \sum_{wS \neq vS} A_w \gamma_{wS}.$$

We apply $\sigma_{v^{-1}}: \mathcal{O}_F \xrightarrow{\cong} \mathcal{O}_F$ to both sides of this equation and we get

$$\gamma_S \cdot \gamma_{v^{-1}S} = \gamma_S + \sum_{wS \neq vS} A_w \gamma_{v^{-1}wS}.$$

Since $v^{-1}S \neq S$, this implies that $v^{-1}S$ is adjacent to S in $Q(S)$. Hence, for $vS \neq S$, vS has odd degree in $Q(S)$ if and only if $v^{-1}S$ is adjacent to S in $Q(S)$.

Now by Proposition 2.2.4, $b = 1$ if and only if S is isolated. So $b = 1$ if and only if no vertices $v^{-1}S$ are adjacent to S , which means no vertices vS have odd degree. Therefore, $b = 1$ if and only if every vertex has even degree. If $b > 1$, then S is adjacent only to $2S$. So clearly S has odd degree, and again by the above discussion, the only other vertex with odd degree is $2^{-1}S = 2^{b-1}S$. Therefore $2^{b-1}S$ and S are the only vertices with odd degree in $Q(S)$. ■

(2.2.9) **Lemma:** The trace of the product of two distinct conjugates of γ_S is 0.

Proof: Let the Galois group $\text{Gal}(F|\mathbb{Q}) = \Pi$ be generated by wS . Consider $\gamma_S^{w^i}$ and $\gamma_S^{w^j}$, two distinct conjugates of γ_S . Clearly $\text{tr}(\gamma_S^{w^i} \cdot \gamma_S^{w^j}) = \text{tr}(\gamma_S^{w^i + w^j})$.

Without loss of generality, suppose $i < j$. Then

$$\begin{aligned}
 \text{tr}(\gamma_S^{w^i} \cdot \gamma_S^{w^j}) &= \text{tr}(\gamma_S^{w^i(1+w^{j-i})}) \\
 &= \text{tr}(\gamma_S^{1+w^{j-i}}) \\
 &= \text{tr}(\gamma_S \cdot \gamma_{w^{j-i}S}) \\
 &= \text{tr}\left(\sum_{k=0}^{n-1} A_k \gamma_{w^k S}\right).
 \end{aligned}$$

In 2.2.7, we noted that an even number of the A_k 's must be 1. So,

$$\begin{aligned}
 \text{tr}(\gamma_S^{w^i} \cdot \gamma_S^{w^j}) &= \text{tr}\left(\sum_{k=0}^{n-1} A_k \gamma_{w^k S}\right) \\
 &= \sum_{k=0}^{n-1} A_k \text{tr}(\gamma_{w^k S}) \\
 &= \sum_{k=0}^{n-1} A_k \text{tr}(\gamma_S^{w^k}) \\
 &= \sum_{k=0}^{n-1} A_k \text{tr}(\gamma_S) \\
 &= 0
 \end{aligned}$$

which proves the lemma. ■

This lemma will prove quite useful when the concept of quotient graphs is generalized in Chapter 3.

Section 3: Idempotence and the Quotient Graph

We can decide exactly when the Rédei matrix M of the quotient graph $Q(S)$ is idempotent. From Proposition 1.5.3 we know that a necessary condition is that every vertex of $Q(S)$ must have even degree. In fact we will show that this is also sufficient. Recall from Lemma 1.2.19 that for a Rédei matrix M ,

$$(2.3.1) \quad M \text{ is idempotent if and only if } c(Q(S)) + d(Q(S)) = n - 1,$$

where $d(Q(S))$ is the dimension of $\text{Ker}(T + I)$ (see 1.2.18). By Corollary 1.2.8, $d(Q(S))$ is also the dimension of the vector space of all subsets $U_1 \subseteq \Pi$ with $S \notin U_1$ and

$$P(Q(S), U_1) = U_1.$$

(2.3.2) **Lemma:** For the quotient graph $Q(S)$,

$$2 \in S \iff d(Q(S)) = \frac{c(\Gamma(\tilde{S}))}{\#S} - 1.$$

Proof: We know that

$$P(Q(S), U_1) = U_1 \iff P(\Gamma(S), L) = L \text{ where } L = q^{-1}(U_1)$$

$$\iff P(\Gamma(\tilde{S}), L) = \emptyset \quad (\text{see 1.5.13})$$

$$\iff \{L, (\tilde{L} \cup \{0\})\} \text{ is an EVD of } \Gamma(\tilde{S}) \text{ and } S \cap L = \emptyset.$$

So to compute $d(Q(S))$, we will compute the dimension of the vector space of all $L \in \mathcal{S}_*^S$ for which $\{L, (\tilde{L} \cup \{0\})\}$ is an EVD of $\Gamma(\tilde{S})$ and $L \cap S = \emptyset$.

However, $2 \in S$ if and only if

$$\gamma_{\tilde{S}} \cdot \gamma_S = (1 + \gamma_S) \cdot \gamma_S = \gamma_S + \gamma_S^2 = \gamma_S + \gamma_{2S} = \gamma_S + \gamma_S = 0.$$

By Lemma 1.4.12, this means that S is a set with $\{S, (\tilde{S} \cup \{0\})\}$ an EVD of $\Gamma(\tilde{S})$ but clearly $S \cap S \neq \emptyset$. In Section 5 of Chapter 1 (see 1.5.14), we showed that those sets $L \in \mathcal{S}_*^S$ for which $\{L, (\tilde{L} \cup \{0\})\}$ is an EVD of $\Gamma(\tilde{S})$ form a subspace of \mathcal{S}_*^S of dimension $\frac{c(\Gamma(\tilde{S}))}{\#S}$. So if we only consider those $L \in \mathcal{S}_*^S$ for which $\{L, (\tilde{L} \cup \{0\})\}$ is an EVD of $\Gamma(\tilde{S})$ and $L \cap S = \emptyset$, this must have dimension $\frac{c(\Gamma(\tilde{S}))}{\#S} - 1$ which proves the lemma. ■

(2.3.3) **Theorem:** Given $p \equiv 1(2n)$ and $S = G(S) = (\mathbb{Z}/p\mathbb{Z})^{\bullet n}$. Then the Rédei matrix M associated to the quotient graph $Q(S)$ is idempotent if and only if $2 \in S$.

Proof: First notice from Proposition 1.5.3, that M idempotent implies $2 \in S$.

Conversely, assume $2 \in S$. By the previous lemma this implies $d(Q(S)) = \frac{c(\Gamma(\tilde{S}))}{\#S} - 1$. So we have

$$\begin{aligned} c(Q(S)) + d(Q(S)) &= \frac{c(\Gamma(S))}{\#S} + \left(\frac{c(\Gamma(\tilde{S}))}{\#S} - 1 \right) \\ &= \frac{c(\Gamma(S)) + c(\Gamma(\tilde{S}))}{\#S} - 1 \quad (\text{see 1.5.8}) \\ &= \frac{p-1}{\#S} - 1 \\ &= n - 1. \end{aligned}$$

So by 2.3.1, M is idempotent which proves the proposition. ■

As noted in Section 5 of Chapter 1, the idempotency of M imposes a very restrictive condition on the quotient graph $Q(S)$.

(2.3.4) **Proposition:** If $2 \in S$, then $c(Q(S)) \equiv n - 1(2)$.

Proof: Since $2 \in S$, we have $b = 1$. So there are n dyadic prime ideals \mathcal{P}_i , and for each one the residue field $\mathcal{O}_F/\mathcal{P}_i \simeq \mathbb{F}_2$. Also, we know that if ℓ is the number of dyadic primes \mathcal{P}_i for which $\eta_i(\gamma_S) = 1$ where $\eta_i : \mathcal{O}_F/2\mathcal{O}_F \rightarrow \mathbb{F}_2$ is the residue map, then from 2.1.15 and 1.4.6,

$$c(Q(S)) = n - \ell.$$

So we must show that ℓ is odd. Recall that $\gamma_S = \text{tr}_{Q(\xi)/F}(\xi) \in \mathcal{O}_F/2\mathcal{O}_F$. So we have

$$(2.3.5) \quad \text{tr}_{F|Q}(\gamma_S) = \text{tr}_{F|Q}(\text{tr}_{Q(\xi)/F}(\xi)) = \text{tr}_{Q(\xi)|Q}(\xi) = -1.$$

Then in \mathbb{F}_2 we must have that

$$\sum_{i=1}^n \eta_i(\gamma_S) = 1.$$

Hence, ℓ is odd and the proposition is proved. ■

(2.3.6) **Lemma:** Let Γ be a graph with n vertices and Rédei matrix M . If M is idempotent of rank 2, then the number of isolated vertices in Γ is congruent to $n - 1 \pmod{2}$.

Proof: Since an isolated vertex of Γ corresponds to a column of zeroes in M , we wish to determine the number of zero columns in M . With the rank $M = 2$, the linear operator defined in 1.2.1

$$T : W \longrightarrow W$$

is actually a projection onto a 2-dimensional subspace of W , call it W_0 . Choose a basis of 2 vectors $\tilde{\beta}_1, \tilde{\beta}_2$ of W_0 such that

$$\tilde{\beta}_1 \cdot \tilde{\beta}_2 = 1.$$

Then T can be described as follows: for any vector $\tilde{z} \in W$,

$$(2.3.7) \quad T(\tilde{z}) = (\tilde{z} \cdot \tilde{\beta}_2) \tilde{\beta}_1 + (\tilde{z} \cdot \tilde{\beta}_1) \tilde{\beta}_2.$$

We can verify this by checking it on the basis vectors. Recall from Lemma 1.2.2 that for any vector $\tilde{x} \in W_0$, $\tilde{x} \cdot \tilde{x} = 0$. So we have,

$$T(\tilde{\beta}_1) = (\tilde{\beta}_1 \cdot \tilde{\beta}_2) \tilde{\beta}_1 + (\tilde{\beta}_1 \cdot \tilde{\beta}_1) \tilde{\beta}_2 = \tilde{\beta}_1 + \bar{0} = \tilde{\beta}_1, \text{ and}$$

$$T(\tilde{\beta}_2) = (\tilde{\beta}_2 \cdot \tilde{\beta}_2) \tilde{\beta}_1 + (\tilde{\beta}_2 \cdot \tilde{\beta}_1) \tilde{\beta}_2 = \bar{0} + \tilde{\beta}_2 = \tilde{\beta}_2.$$

Let $\bar{\beta}_1 = (x_i)$ and $\bar{\beta}_2 = (y_i)$. Then notice for a standard basis vector \bar{e}_j of W ,

$$\begin{aligned} T(\bar{e}_j) &= (\bar{e}_j \cdot \bar{\beta}_2)\bar{\beta}_1 + (\bar{e}_j \cdot \bar{\beta}_1)\bar{\beta}_2 \\ &= y_j\bar{\beta}_1 + x_j\bar{\beta}_2. \end{aligned}$$

This is the j -th column of the matrix M . We have four possibilities.

- (1) $T(\bar{e}_j) = \bar{0}$ which implies $x_j = 0, y_j = 0$.
- (2) $T(\bar{e}_j) = \bar{\beta}_1$ which implies $x_j = 0, y_j = 1$.
- (3) $T(\bar{e}_j) = \bar{\beta}_2$ which implies $x_j = 1, y_j = 0$.
- (4) $T(\bar{e}_j) = \bar{\beta}_1 + \bar{\beta}_2$ which implies $x_j = 1, y_j = 1$.

First we will consider cases (2) and (3). The number of columns of M equal to either $\bar{\beta}_1$ or $\bar{\beta}_2$ is therefore equal to the number of nonzero entries in the vector $\bar{\beta}_1 + \bar{\beta}_2$. Recall the vector $\bar{w} = \sum_{j=1}^n \bar{e}_j$. For any vector $\bar{z} \in W$,

$$\bar{z} \cdot \bar{w} = \bar{z} \cdot \bar{z}.$$

So

$$\begin{aligned} (\bar{\beta}_1 + \bar{\beta}_2) \cdot \bar{w} &= (\bar{\beta}_1 + \bar{\beta}_2) \cdot (\bar{\beta}_1 + \bar{\beta}_2) \\ &= \bar{\beta}_1 \cdot \bar{\beta}_1 + \bar{\beta}_1 \cdot \bar{\beta}_2 + \bar{\beta}_2 \cdot \bar{\beta}_1 + \bar{\beta}_2 \cdot \bar{\beta}_2 \\ &= 0 + 1 + 1 + 0 \\ &= 0. \end{aligned}$$

So by the definition of \bar{w} , that means that there are an even number of nonzero entries in $\bar{\beta}_1 + \bar{\beta}_2$. So there are an even number of columns in M equal to $\bar{\beta}_1$ or $\bar{\beta}_2$ (and thus nonzero).

Now case (4). The number of columns of M equal to $\bar{\beta}_1 + \bar{\beta}_2$ is equal to the number of indices for which $x_j = y_j = 1$. Since $\bar{\beta}_1 \cdot \bar{\beta}_2 = 1$, this number is odd. So there are an odd number of columns of M equal to $\bar{\beta}_1 + \bar{\beta}_2$ (and thus nonzero).

The rest of the columns of M (from case (1)) are zero columns. Since M has n columns and from the above discussion, M has an odd number of nonzero columns, the number of zero columns of M is congruent to $n - 1$ modulo 2. Since a zero column in M corresponds to an isolated vertex in the graph, the lemma follows. ■

Now let us discuss how “frequently” idempotent quotient graphs occur. We shall do this by analyzing the density of the primes with the required properties in the set of all primes.

Let ϕ denote the Euler phi function. For a given $n > 1$, the set of all primes p which satisfy the condition

$$p \equiv 1(2n)$$

has density

$$\frac{1}{\phi(2n)}$$

in the set of all primes. However, if we choose $n \not\equiv 0(4)$ and if m is a positive divisor of n , then the set of all primes p which satisfy the conditions

$$p \equiv 1(2n) \text{ and } b = n/m$$

has density

$$\frac{\phi(b)}{n\phi(2n)}$$

in the set of all primes. If $n \equiv 0(4)$ and if m is a positive even divisor of n , then the set of all primes p which satisfy the conditions

$$p \equiv 1(2n) \text{ and } b = n/m$$

has density

$$\frac{2\phi(b)}{n\phi(2n)}$$

in the set of all primes.

Thus for a fixed n , the set of all primes $p \equiv 1(2n)$ for which the Rédei matrix of the associated quotient graph is idempotent (in other words, for which $b = 1$) has density

$$\begin{aligned} & \frac{1}{n\phi(2n)} \quad \text{if } n \not\equiv 0(4) \quad \text{or} \\ & \frac{2}{n\phi(2n)} \quad \text{if } n \equiv 0(4) \end{aligned}$$

in the set of all primes.

At the other extreme, when $b = n$ and $n \not\equiv 0(4)$, then the set of all primes $p \equiv 1(2n)$ has density

$$\frac{\phi(b)}{n\phi(2n)} = \frac{\phi(n)}{n\phi(2n)} = \begin{cases} 1/n & n \equiv 1(2) \\ 1/2n & n \equiv 2(4) \end{cases}$$

in the set of all primes.

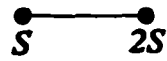
Section 4: The Modified Quotient Graph

In a quotient graph, we know that the vertex S is isolated if and only if $2 \in S$. Otherwise, S is adjacent *only* to the vertex $2S$. Thus we are tempted to delete this one vertex which we understand completely and concentrate on the remaining portion of the graph.

(2.4.1) **Definition:** Let $Q(S)$ be a quotient graph with vertex set Π . Then the **modified quotient graph** $MQ(S)$ is the graph obtained from $Q(S)$ by deleting the vertex S .

(2.4.2) **Examples:** (1) If $n = 2$ and $p = 5$, then

$Q(S)$ is

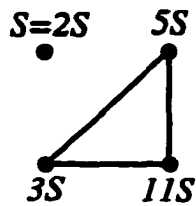


and $MQ(S)$ is

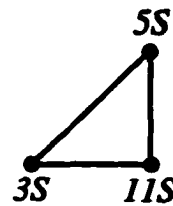


(2) If $n = 4$ and $p = 73$, then

$Q(S)$ is



and $MQ(S)$ is



Two vertices in $MQ(S)$ are adjacent if and only if they are adjacent in the original quotient graph $Q(S)$. Therefore, if $2 \in S$, then the quotient graph $Q(S)$ is a disjoint union of $MQ(S)$ and the isolated vertex S . If $2 \notin S$, then $Q(S)$ is obtained from $MQ(S)$ by adding a “whisker” at the vertex $2S$. This modified quotient graph will prove to be quite useful. One example is the following lemma relating the invariant c for both graphs. Recall that for any graph Γ ,

$$\# \text{ of EVD's of } \Gamma = 2^{c(\Gamma)} \quad (\text{see 1.2.15}).$$

(2.4.3) **Lemma:** If $2 \notin S$, then $c(Q(S)) = c(MQ(S))$. If $2 \in S$, then $c(Q(S)) = c(MQ(S)) + 1$.

Proof: If $2 \notin S$, then the vertices S and $2S$ must lie in the same subset of any EVD since S is only adjacent to $2S$. Hence any EVD of $MQ(S)$ is made into an EVD of $Q(S)$ simply by adding the vertex S to the subset containing $2S$. Thus $c(Q(S)) = c(MQ(S))$.

If $2 \in S$, this implies that the vertex S is isolated. Therefore, it cannot be a special vertex of any vertex decomposition. So given any EVD of $MQ(S)$, we can make an EVD of $Q(S)$ by adding the vertex S to either subset. Therefore, for each EVD of $MQ(S)$ we have 2 EVD's of $Q(S)$, which proves the lemma. ■

(2.4.4) **Proposition (Degree Rule):** If $vS \neq S$, then in the modified quotient graph,

$$\deg(vS) = \deg(v^{-1}S).$$

Also, every vertex of the modified quotient graph will have even degree if and only if $b = 1$ or 2 . If $b > 2$ then $MQ(S)$ has exactly 2 vertices, $2S$ and $2^{-1}S$, of odd degree.

Proof: Suppose that vS and wS are distinct vertices neither of which is S . Then clearly $v^{-1}S$ and $v^{-1}wS$ are also distinct and not S . We want to show that vS is adjacent to wS if and only if $v^{-1}S$ is adjacent to $v^{-1}wS$.

Recall that vS is adjacent to wS if and only if there are an odd number of pairs $(X^n, Y^n) \in S \times S$ with

$$vX^n + wY^n = 1 \quad (\text{see 2.2.1}).$$

This is equivalent to $X^n + v^{-1}wY^n = v^{-1}$. Now using the fact that $-1 \in S$ and letting $A^n = (X^{-1})^n$ and $B^n = -(X^{-1}Y)^n$, we see that this is equivalent to

$$v^{-1}A^n + v^{-1}wB^n = 1,$$

which as just noted is true if and only if the vertices $v^{-1}S$ and $v^{-1}wS$ are adjacent.

Therefore, for every neighbor of vS we have a distinct vertex adjacent to $v^{-1}S$, so $\deg(vS) = \deg(v^{-1}S)$.

If $b = 1$, then every vertex of the quotient graph $Q(S)$ has even degree and since the vertex S is isolated, this will hold in the modified quotient graph $MQ(S)$ as well. If $b = 2$, then we saw that the only vertices of $Q(S)$ with odd degree are S and $2^{b-1}S = 2S$ (see Corollary 2.2.7). But when S is deleted to create $MQ(S)$, the degree of $2S$ will be reduced by one, and thus $2S$ will have even degree in $MQ(S)$. Since all other vertices of $Q(S)$ had even degree and were not affected by the deletion of S , we see that in either case ($b = 1$ or 2), the proposition holds.

If $b > 2$, then again from Corollary 2.2.7, we know that the only two vertices of odd degree in $Q(S)$ are the vertices S (which is adjacent only to $2S$) and $2^{b-1}S = 2^{-1}S$. However, if $b > 2$ then $2^{-1}S \neq 2S$. So when the vertex S is deleted, the degree of $2^{-1}S$ will remain odd, and the degree of $2S$ (which had been even) will now also be odd. The degree of all other vertices will remain unchanged. Therefore $2S$ and $2^{-1}S$ are the only two vertices in $MQ(S)$ with odd degree. ■

Recall that if $2 \in S$, then the Rédei matrix of $Q(S)$ is idempotent. We point out that in this case the Rédei matrix of the modified quotient graph is idempotent as well.

Now, if $2 \in S$, we know that

$$1 \leq c(Q(S)) \leq n - 1 \text{ and}$$

$$c(Q(S)) \equiv n - 1(2).$$

As noted earlier, the possibility that $c(Q(S)) = n - 1$ does occur. It means that $Q(S)$ is totally disconnected. Here is an added observation.

(2.4.5) **Corollary:** If n is odd and if $2 \in S$, then $c(Q(S)) \neq n - 3$.

Proof: Let M be the Rédei matrix of the quotient graph $Q(S)$. Then we know that

$$c(Q(S)) + 1 = \text{corank}(M) \quad (\text{see 1.2.14}).$$

Suppose that $c(Q(S)) = n - 3$. Then the $\text{rank}(M) = 2$. Recall that in our discussion of idempotent Rédei matrices (see Lemma 2.3.6), we showed that if an idempotent Rédei matrix has rank 2, then the number of isolated vertices in the graph is congruent to $n - 1$ modulo 2. Since n is odd, this means that the number of isolated vertices in $Q(S)$ is even. So after the deletion of S (which we know to be isolated), we have an odd number of isolated vertices in $MQ(S)$. This is a contradiction, since from the last proposition, we know that a vertex vS is isolated in $MQ(S)$ if and only if $v^{-1}S$ is isolated as well. This implies that there are an even number of isolated vertices in $MQ(S)$ (since for n odd, $v^{-1}S \neq vS$ for any vertex vS). So $\text{rank}(M)$ cannot equal 2, and therefore the corollary is proved. ■

We now come to a geometric property of the modified quotient graph $MQ(S)$ which we call the triples rule.

(2.4.6) **Lemma (Triples Rule):** If $vS \neq wS$ and neither is S , then in $MQ(S)$ the following are equivalent:

- (1) vS is adjacent to wS .
- (2) $v^{-1}S$ is adjacent to $v^{-1}wS$.
- (3) $w^{-1}S$ is adjacent to $w^{-1}vS$.

Proof: We have already shown the equivalence of (1) and (2) by comparing the equations

$$vX^n + wY^n = 1 \text{ and}$$

$$v^{-1}A^n + v^{-1}wB^n = 1$$

with $A^n = (X^{-1})^n$ and $B^n = -(X^{-1}Y)^n$. However, the parity of the number of solutions of these equations is also equivalent to the parity of the number of solutions of

$$w^{-1}C^n + w^{-1}vD^n = 1$$

which can be seen by letting $C^n = (Y^{-1})^n$ and $D^n = -(XY^{-1})^n$, and thus proves the lemma. ■

The following two corollaries are proven in [M]. They are direct consequences of the Degree Rule (2.4.4) and the Triples Rule (2.4.6).

(2.4.7) **Corollary:** If $n \not\equiv 0(3)$ and $p \equiv 1(2n)$, then the number of edges in $MQ(S)$ is a multiple of 3. Namely if wS generates Π , then

$$N(w^i, w^j S) = N(w^{-i}, w^{j-i} S) = N(w^{-j}, w^{i-j} S).$$

In other words,

$$w^i S, w^j S \text{ are adjacent}$$

$$\iff w^{-i} S, w^{j-i} S \text{ are adjacent}$$

$$\iff w^{-j} S, w^{i-j} S \text{ are adjacent.}$$

(2.4.8) **Corollary:** Let n be odd, and $p \equiv 1(2)$. Let k be the number of triples in $MQ(S)$. Then k is even if and only if $2 \in S$.

These results along with Section 5 will enable us to determine which graphs are possible quotient graphs for many values of n .

Section 5: The Characteristic Polynomial of $Q(S)$

For any quotient graph $Q(S)$ we have a polynomial $\alpha(x)$ associated to it called the characteristic polynomial of $Q(S)$. In this section we will define $\alpha(x)$ and show that $\alpha(x)$ and $Q(S)$ uniquely determine each other (see 2.5.9). Throughout this section we will assume $b = n$ (see 1.4.4). In other words, $2S$ generates the quotient group $\Pi = (\mathbb{Z}/p\mathbb{Z})^*/S$.

Recall from Section 4 of Chapter 1 the general situation. We are considering the p -th cyclotomic extension $\mathbb{Q}(\xi)$ of \mathbb{Q} whose Galois group $\text{Gal}(\mathbb{Q}(\xi)|\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^*$. Then associated to the subgroup $S \subseteq (\mathbb{Z}/p\mathbb{Z})^*$ is the fixed field F ,

$$\mathbb{Q} \subseteq F \subseteq \mathbb{Q}(\xi)$$

where $\text{Gal}(\mathbb{Q}(\xi)|F) = S$ and $\text{Gal}(F|\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^*/S = \Pi$. Then

$$(2.5.1) \quad \text{tr}_{\mathbb{Q}(\xi)|F}(\xi) = \sum_{i \in S} \xi^i = \gamma_S.$$

The conjugates of γ_S in F over \mathbb{Q} are $\{\sigma_i(\gamma_S)\}_{i=1}^n$ for $\sigma_i \in \text{Gal}(F|\mathbb{Q}) = \Pi$. Since Π is generated by $2S$, we have

$$\Pi = \{S, 2S, 2^2S, \dots, 2^{n-1}S\}$$

so the conjugates of γ_S are:

$$(2.5.2) \quad \gamma_S, \sigma_2(\gamma_S), \sigma_{2^2}(\gamma_S), \dots, \sigma_{2^{n-1}}(\gamma_S).$$

Now recall Hilbert's observation (see 1.3.33): As a $\mathbf{Z}[\Pi]$ -module, \mathcal{O}_F is also free of rank 1 and $\text{tr}_{\mathbf{Q}(\xi)|F}(\xi) \in \mathcal{O}_F$ is a module basis. A consequence of this is that these conjugates of $\text{tr}_{\mathbf{Q}(\xi)|F}(\xi) = \gamma_S$ form a normal basis of F which is a \mathbf{Z} -basis of \mathcal{O}_F . Consider the ideal $2\mathcal{O}_F$ in \mathcal{O}_F . Recall that when we reduce modulo 2, we saw that

$$\sigma_{2^i-1}(\gamma_S) = (\gamma_S)^{2^{i-1}} = \gamma_{2^i-1S} \quad (\text{see 1.3.27}).$$

In Section 4 of Chapter 1 it was determined that the number of dyadic primes in \mathcal{O}_F is $\frac{n}{b}$. So with the assumption that $b = n$, we see that $2\mathcal{O}_F$ is a prime ideal of \mathcal{O}_F . Therefore $\mathcal{O}_F/2\mathcal{O}_F = k$ is a field extension of \mathbf{F}_2 of degree n . So from 1.3.27 and 2.5.2 we see that $\{\gamma_S, (\gamma_S)^2, (\gamma_S)^4, \dots, (\gamma_S)^{2^{n-1}}\}$ is a basis for k over \mathbf{F}_2 . Therefore $\text{Irr}(\gamma_S)$, the irreducible polynomial of γ_S over \mathbf{F}_2 , is a polynomial of degree n in $\mathbf{F}_2[x]$. Recall from 2.3.5

$$\begin{aligned} \text{tr}_{F|\mathbf{Q}}(\gamma_S) &= \text{tr}_{F|\mathbf{Q}}(\text{tr}_{\mathbf{Q}(\xi)|F}(\xi)) \\ &= \text{tr}_{\mathbf{Q}(\xi)|\mathbf{Q}}(\xi) = -1. \end{aligned}$$

So the coefficient of x^{n-1} in $\text{Irr}(\gamma_S) \in \mathbf{F}_2[x]$ is 1. Since both $\text{Irr}(\gamma_S)$ and the quotient graph $Q(S)$ are based on the subgroup $S \subseteq (\mathbf{Z}/p\mathbf{Z})^*$, we would like to see their relation to each other.

Let $L : k \longrightarrow k$ be an operator defined by multiplication by γ_S , namely

$$(2.5.3) \quad L(x) = \gamma_S \cdot x \quad \text{for all } x \in k.$$

We can represent L by an $n \times n$ matrix $A = (a_{ij})$ by using the basis

$$\{\gamma_S, \gamma_S^2, \gamma_S^4, \dots, \gamma_S^{2^{n-1}}\}$$

as follows: For each basis element $(\gamma_S)^{2^{j-1}}$, $L((\gamma_S)^{2^{j-1}}) \in k$ and as such can be written using the basis. The coefficients are precisely the entries of A , namely if

$$(2.5.4) \quad L((\gamma_S)^{2^{j-1}}) = \sum_{i=1}^n a_{ij} (\gamma_S)^{2^{i-1}} \quad \text{then}$$

$$A = (a_{ij}).$$

Since in $\mathcal{O}_F/2\mathcal{O}_F$ we have $L(\gamma_S) = \gamma_S \cdot \gamma_S = (\gamma_S)^2 = \gamma_{2S}$, we see that

$$a_{i1} = 1 \iff i = 2.$$

So the first column of A is given by:

$$\begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Now consider $j > 1$. From 2.2.4 we have,

$$(2.5.5) \quad L((\gamma_S)^{2^{j-1}}) = \gamma_S \cdot (\gamma_S)^{2^{j-1}} = \gamma_S \cdot \gamma_{2^{j-1}S} = \sum_{i=1}^n A_i \gamma_{2^i S}.$$

Using this we saw (see 2.2.5) that for

(a) $i \neq j-1$, $A_i = 1 \iff 2^i S$ and $2^{j-1}S$ are adjacent vertices in $Q(S)$.

(b) $i = j-1$, $A_i = A_{j-1} = 1 \iff 2^i S = 2^{j-1}S$ has odd degree in $Q(S)$.

So by comparing 2.5.4 and 2.5.5, we see that the matrix A is equal to the Rédei matrix $M = (m_{ij})$ of $Q(S)$ with the one exception: $m_{11} = 1$ while $a_{11} = 0$. There is a correlation between this matrix A and $\text{Irr}(\gamma_S)$.

(2.5.6) **Definition:** Let $\alpha(x) \in \mathbb{F}_2[x]$ be the characteristic polynomial of the matrix A . In other words, $\alpha(x) = \det(A - xI)$.

(2.5.7) **Theorem:** If $Q(S)$ is a quotient graph with $b = n$, then

$$\alpha(x) = \text{Irr}(\gamma_S).$$

In particular, the polynomial $\alpha(x) \in \mathbb{F}_2[x]$ is irreducible.

Proof: Since A is an $n \times n$ matrix,

$$\begin{aligned}\alpha(x) &= \det(A - xI) \\ &= c_n x^n + c_{n-1} x^{n-1} + \dots + c_1 x + c_0 \quad \text{for } c_i \in \mathbb{F}_2.\end{aligned}$$

We will now show that γ_S is a root of $\alpha(x)$. To see this we'll use the fact that $\alpha(x)$ annihilates A . So we have

$$c_n(A)^n + c_{n-1}(A)^{n-1} + \dots + c_1(A) + c_0 = 0.$$

By the definition of A , we know that $A \cdot v = \gamma_S \cdot v$ for all $v \in k$. So

$$\begin{aligned}0 &= 0 \cdot v \\ &= (c_n(A)^n + c_{n-1}(A)^{n-1} + \dots + c_1(A) + c_0)v \quad \text{for all } v \in k \\ &= c_n A^n v + c_{n-1} A^{n-1} v + \dots + c_1 A v + c_0 v \\ &= c_n \gamma_S^n v + c_{n-1} \gamma_S^{n-1} v + \dots + c_1 \gamma_S v + c_0 v \\ &= (c_n \gamma_S^n + c_{n-1} \gamma_S^{n-1} + \dots + c_1 \gamma_S + c_0)v \quad \text{for all } v \in k \\ &\implies c_n \gamma_S^n + c_{n-1} \gamma_S^{n-1} + \dots + c_1 \gamma_S + c_0 = 0.\end{aligned}$$

So γ_S is a root of $\alpha(x)$. Therefore $\text{Irr}(\gamma_S)$ is a factor of $\alpha(x)$. However, since both polynomials are degree n polynomials in $\mathbb{F}_2[x]$ they must be equal, so the theorem is proved. ■

As noted above, the matrix A is identical to the Rédei matrix M except at the top left entry. So we can produce A from M and then the fact that

the characteristic polynomial $\alpha(x)$ of A is irreducible greatly helps us reduce the number of possible quotient graphs.

(2.5.8) **Corollary:** If $Q(S)$ is a quotient graph with $b = n$, then it is a connected graph.

Proof: If $Q(S)$ were disconnected, then its Rédei matrix M would be a block matrix

$$M = \begin{pmatrix} M_1 & 0 \\ 0 & M_2 \end{pmatrix}$$

So A would be a block matrix also,

$$A = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$$

(Note: $A_2 = M_2$, since the only different entry is $a_{11} \neq m_{11}$.) Therefore

$$\alpha(x) = \det(A - xI) = \det(A_1 - xI) \cdot \det(A_2 - xI)$$

would *not* be irreducible, which contradicts Theorem 2.5.7. Therefore, $Q(S)$ must be connected. ■

(2.5.9) **Theorem:** The quotient graph $Q(S)$ with $b = n$ and the polynomial $\alpha(x)$ uniquely determine each other.

Proof: The fact that $Q(S)$ uniquely determines $\alpha(x)$ is clear by the definition of $\alpha(x)$. So now we will show that in fact $\alpha(x)$ determines $Q(S)$ also. Recall the operator $L : k \rightarrow k$ defined by multiplication by γ_S . We'll represent it as an $n \times n$ matrix again, but this time use the basis $\{1, \gamma_S, \gamma_S^2, \gamma_S^3, \dots, \gamma_S^{n-1}\}$ of k .

Then

$$L(\gamma_S^{j-1}) = \sum_{i=1}^n c_{ij} \gamma_S^{i-1}.$$

Then the matrix $C = (c_{ij})$ is just the companion matrix of $\alpha(x)$. So clearly C and $\alpha(x)$ uniquely determine each other. Now we wish to consider a third matrix $B = (b_{ij})$, the change of basis matrix, defined by expressing the members of the first basis $\{\gamma_S, (\gamma_S)^2, (\gamma_S)^4, \dots, (\gamma_S)^{2^{n-1}}\}$ in terms of the second basis $\{1, \gamma_S, (\gamma_S)^2, (\gamma_S)^3, \dots, (\gamma_S)^{n-1}\}$. In other words, $B = (b_{ij})$ is given by

$$(\gamma_S)^{2^{j-1}} = \sum_{i=1}^n b_{ij} (\gamma_S)^{i-1}.$$

We note that $L^{2^{j-1}-1}(\gamma_S) = (\gamma_S)^{2^{j-1}}$ for any $j = 1, \dots, n$. Also $L^{2^{j-1}-1}$ is representable by the matrix $C^{2^{j-1}-1}$. Therefore, column j of matrix B equals column 2 of matrix $C^{2^{j-1}-1}$. Hence B and C uniquely determine each other.

Lastly notice that

$$A = B^{-1}CB$$

so that the matrix A is determined by B and C and therefore by $\alpha(x)$. Since A , M and $Q(S)$ clearly all determine each other, we see that $\alpha(x)$ uniquely determines $Q(S)$. ■

(2.5.10) **Remark:** We call $\alpha(x)$ the **characteristic polynomial of the quotient graph $Q(S)$** .

Section 6: Examples


We are now in a position to determine quotient graphs for several values of n . Recall that since the number of vertices is determined by n (not p), for many “small” values of n , we will be able to determine all possible quotient graphs. Also notice that we will primarily consider only prime values of n , which reduces the possibilities for b to just 1 and n , however the theory applies to composite values

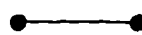
as well. In fact, we will determine all the quotient graphs for the case $n = 4$ in this section along with the prime values $n = 2, 3, 5, 7$. For $n = 11$ we will exhibit several different quotient graphs, but we will leave the proof that these are *all* the possible quotient graphs to Chapter 3.

(2.6.1) Example: $n = 2$

Recall Proposition 2.2.4 (the $S - 2S$ Rule) which states that the vertex S is isolated if $2 \in S$ and adjacent to only $2S$ if $2 \notin S$. For this case, this is all the information we need.

There are only two distinct graphs on 2 vertices:



 the totally
disconnected graph


 the line graph

So $Q(S)$ is completely determined by whether $2 \in S$ or not. With $n = 2$, this amounts to whether or not 2 is a square modulo p . From quadratic reciprocity, we know that this occurs exactly when $p \equiv \pm 1(8)$. So with $n = 2$ and $p \equiv 1(4)$, we can quickly and easily determine $Q(S)$.

(2.6.2) Example: $n = 2, p = 17$

Since $p = 17 \equiv 1(8)$, we know that $2 \in S$. So $Q(S)$ is


 the totally
disconnected graph

Let us also determine this by more elementary methods. We have

$$(\mathbb{Z}/17\mathbb{Z})^* = \{\pm 1, \pm 2, \pm 3, \dots, \pm 8\}.$$

So

$$S = (\mathbb{Z}/17\mathbb{Z})^{*2} = \{\pm 1, \pm 2, \pm 4, \pm 8\} \text{ and}$$

$$3S = \{\pm 3, \pm 5, \pm 6, \pm 7\}.$$

It can then be checked that

$$N(1, 3S) = 4 \equiv 0(2)$$

and therefore by the definition of $Q(S)$, S and $3S$ are not adjacent.

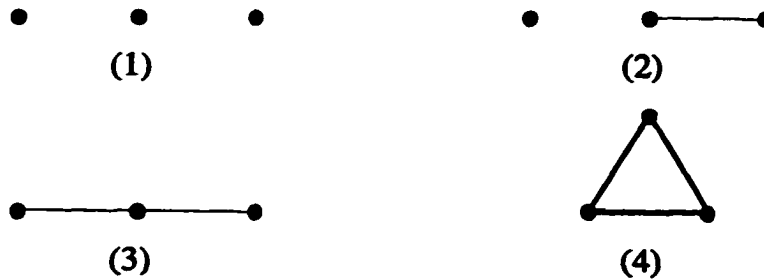
(2.6.3) **Example:** $n = 2, p = 8429$

With $p = 8429 = (1053)(8) + 5 \not\equiv \pm 1(8)$, we see that $2 \notin S$ and so $Q(S)$ is



(2.6.4) **Example:** $n = 3$

There are 4 distinct graphs on three vertices.

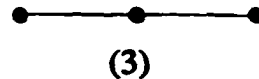


Graph (4) cannot be a quotient graph because we know that the degree of the vertex S is always either 0 or 1, and every vertex in that graph has degree 2. Considering graph (2) recall that the degree rule tells us that if the vertex S is isolated, then every vertex has even degree. So if this graph is to be a quotient graph, S and $2S$ must be the two vertices which are adjacent (which implies that $b = 3$). However, the degree rule also states that if S is not isolated, then S and $2^{b-1}S$ are the only two vertices of odd degree, which is a contradiction. Therefore, the only two possible quotient graphs on three vertices are graphs (1) and (3), the totally disconnected graph and the line graph.

So again $Q(S)$ is completely determined by whether or not 2 is an element of S . With $n = 3$, we only need to determine if 2 is a cube modulo p . From number theory, we know that 2 is a cube modulo p if and only if $p = x^2 + 27y^2$ for some integers x and y . So the smallest prime number with $2 \in S$ (and thus generates the totally disconnected graph on 3 vertices) is $p = 31 = (2)^2 + 27(1)^2$.

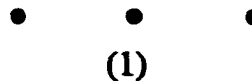
(2.6.5) **Example:** $n = 3, p = 7$.

Clearly $p \neq x^2 + 27y^2$ for any integers x and y . Therefore $2 \notin S$ and so $Q(S)$ is graph (3), the line graph.



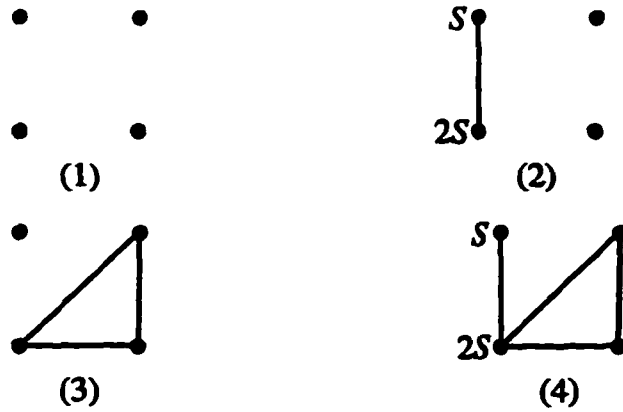
(2.6.6) **Example:** $n = 3, p = 739$.

Since $p = 739 = (8)^2 + 27(5)^2$, we see that $2 \in S$ and hence $Q(S)$ is graph (1), the totally disconnected graph.



(2.6.7) **Example:** $n = 4$

This is the first case which will fully utilize the information we get from the modified quotient graph. By Corollary 2.4.7, we know that the number of edges in any modified quotient graph (where $n = 4$) is a multiple of 3. For $n = 4$, the modified quotient graph has 3 vertices, so it must have either 0 or 3 edges. Therefore, the only possible modified quotient graphs are the totally disconnected graph and the triangle. Using this we see that there are 4 possible quotient graphs on 4 vertices:



Determining if $2 \in S$ or not is simply a matter of determining whether 2 is a 4th power modulo p or not, which happens if and only if $p = x^2 + 64y^2$ for some integers x and y . So all that is left is the determination of the modified quotient graph.

Label the vertices of $Q(S)$ with S, wS, w^2S, w^3S . Note that since $n = 4$, we have $p \equiv 1(8)$. So 2 is a square modulo p , which means that $b = 1$ or 2. Therefore 2 cannot generate Π . Let $\alpha = N(w, w^2S)$. Corollary 2.4.7 tells us that

$$N(w, w^2S) = N(w, w^3S) = N(w^2, w^3S).$$

Clearly in the circulant graph $\Gamma(S)$, the degree of any vertex, for example w^2 , is given by

$$(2.6.8) \quad \deg w^2 = \sum_{i=0}^3 N(w^2, w^iS).$$

But recall that $\Gamma(S)$ is a regular graph of degree $\#S = \frac{p-1}{4}$. So

$$(2.6.9) \quad \frac{p-1}{4} = N(w^2, S) + N(w^2, wS) + N(w^2, w^2S) + N(w^2, w^3S).$$

We now need a lemma, which could have appeared in Section 2.

(2.6.10) **Lemma:** For any vertex v in the circulant graph $\Gamma(S)$,

$$N(v, vS) = N(1, v^{-1}S).$$

Proof: Recall that $N(v, wS)$ is simply the number of solutions to the equation $vX^n + wY^n = 1$ (see 2.2.2). Then since

$$\begin{aligned} vX^n + vY^n &= 1 \\ \iff X^n + Y^n &= v^{-1} \\ \iff -(XY)^n + v^{-1}Y^n &= 1 \end{aligned}$$

we see that $N(v, vS) = N(1, v^{-1}S)$. ■

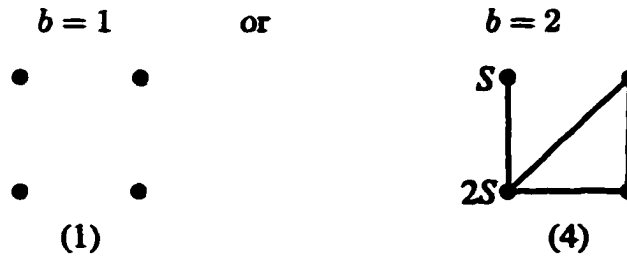
Let $\beta = N(w^2, w^2S) = N(1, w^{-2}S) = N(1, w^2S)$. Then substituting α and β into equation 2.6.9, we get

$$\begin{aligned} \frac{p-1}{4} &= \beta + \alpha + \beta + \alpha \\ (2.6.11) \quad \frac{p-1}{4} &= 2(\alpha + \beta) \\ p-1 &= 8(\alpha + \beta). \end{aligned}$$

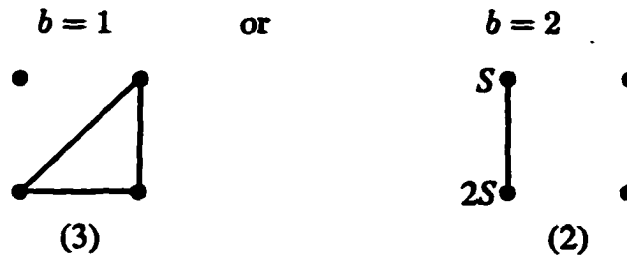
Recall that we know $b = 1$ or 2 . Suppose $b = 1$. Then the vertex S is isolated, which implies β is even. If α is also even, then $MQ(S)$ is the totally disconnected graph and $p \equiv 1(16)$. If α is odd, then $MQ(S)$ is K_3 , the complete graph on 3 vertices, and $p \equiv 9(16)$.

Now suppose $b = 2$. Then $2 \in w^2S$. So S is adjacent to $w^2S = 2S$. Thus β must be odd. If α is also odd, then $MQ(S)$ is K_3 and $p \equiv 1(16)$. If α is even, then $MQ(S)$ is totally disconnected and $p \equiv 9(16)$. This completes every possible case. So for $n = 4$, $Q(S)$ is one of the following 4 graphs.

(2.6.12) if $p \equiv 1(16)$ and

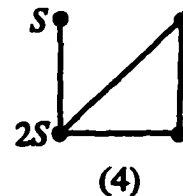


(2.6.13) if $p \equiv 9(16)$ and



(2.6.14) **Example:** $n = 4, p = 17$.

Since $p = 17 \equiv 1(16)$, we simply need to check whether or not p can be written as $x^2 + 64y^2$ for some integers x and y . Since this cannot be done (which implies that $2 \notin S$ and hence $b = 2$), $Q(S)$ is the following graph:



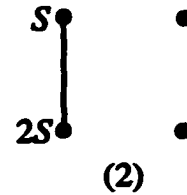
(2.6.15) **Example:** $n = 4, p = 113$.

Since $p = 113 \equiv 1(16)$ and $113 = 7^2 + 64(1)^2$ (which implies that $2 \in S$ and hence $b = 1$), $Q(S)$ is the following graph:



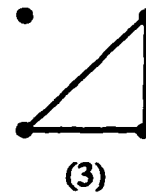
(2.6.16) **Example:** $n = 4, p = 41$.

Since $p = 41 \equiv 9(16)$ and $41 \neq x^2 + 64y^2$ for any integers x and y (which implies that $2 \notin S$ and hence $b = 2$), $Q(S)$ is the following graph:



(2.6.17) **Example:** $n = 4, p = 73$.

Since $p = 73 \equiv 9(16)$ and $73 = 3^2 + 64(1)^2$ (which implies that $2 \in S$ and hence $b = 1$), $Q(S)$ is the following graph:



The remainder of the cases we will consider will be where n is an odd prime. Therefore, in each case, b will either be 1 or n .

(2.6.18) **Example:** $n = 5$

We will now apply the full power of the Triples Rule (2.4.6) and the Degree Rule (2.4.4) to decide which graphs are quotient graphs. The Triples Rule tells us that for a given generator wS of the vertex set Π ,

$$w^i S, w^j S \text{ are adjacent}$$

$$\iff w^{-i} S, w^{j-i} S \text{ are adjacent}$$

$$\iff w^{-j} S, w^{i-j} S \text{ are adjacent.}$$

If we let $i = 1$ and $j = 2$, this implies

wS, w^2S are adjacent

$\iff wS, w^4S$ are adjacent

$\iff w^3S, w^4S$ are adjacent.

If we let $i = 1$ and $j = 3$, we get

wS, w^3S are adjacent

$\iff w^2S, w^4S$ are adjacent

$\iff w^2S, w^3S$ are adjacent.

So notice that the edges come in triples. We denote an edge adjoining w^iS to w^jS by (i, j) . Therefore the two triples are denoted by

$$T_{1,2} = \{(1, 2), (1, 4), (3, 4)\} \text{ and}$$

$$T_{1,3} = \{(1, 3), (2, 4), (2, 3)\}.$$

Notice that every potential edge of the modified quotient graph is in one of the two triples. Now if $2 \in S$, then by Corollary 2.4.8 the number of triples present in $MQ(S)$ is even. So either they are both present or neither are. If both triples are present, then every vertex of the modified quotient graph will have degree 3, which contradicts Proposition 2.4.4 (which states that if $b = 1$, then every vertex of the modified quotient graph has even degree). So if $2 \in S$, then neither triple must be present and therefore $Q(S)$ will be the totally disconnected graph:



If $2 \notin S$, then the number of triples present in $MQ(S)$ is odd. So exactly one triple will be present. As usual, we choose $w = 2$. If the triple present is

$T_{1,2}$, then the vertices 2^2S and 2^3S will have odd degree, which again contradicts Proposition 2.4.4. Therefore the triple present in this case must be $T_{1,3}$. So $Q(S)$ is the line graph:



So for a given $p \equiv 1(10)$ again all that is necessary to determine is if 2 is an element of S or not.

(2.6.19) **Example:** $n = 5, p = 11$.

Simply by computing the 5th powers modulo p , we see that in this case $2 \notin S$. So $Q(S)$ is the line graph:



(2.6.20) **Example:** $n = 5, p = 151$.

Since $2 \equiv 25^5(151)$, we see that $2 \in S$. So $Q(S)$ is the totally disconnected graph.



(2.6.21) **Example:** $n = 7$

For this case there are 5 possible triples in the modified quotient graph:

$$T_{1,2} = \{(1, 2), (1, 6), (5, 6)\}$$

$$T_{1,3} = \{(1, 3), (2, 6), (4, 5)\}$$

$$T_{1,4} = \{(1, 4), (3, 6), (3, 4)\}$$

$$T_{1,5} = \{(1, 5), (4, 6), (2, 3)\}$$

$$T_{2,4} = \{(2, 4), (2, 5), (3, 5)\}.$$

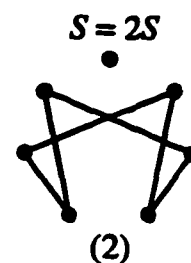
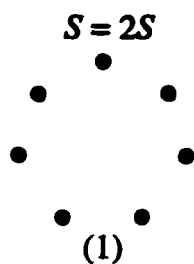
Suppose $b = 1$. Let k be the number of triples present. By Corollary 2.4.8, $k = 0, 2$ or 4 . We consider each possibility.

Case (1): Suppose $k = 0$. This implies that there are no triples present, so the modified quotient graph will be the totally disconnected graph. This does not create any contradictions to the Triples Rule or the Degree Rule, so this is a possibility. Notice that with $b = 1$, $Q(S)$ is formed from $MQ(S)$ by simply adding the isolated vertex S , so $Q(S)$ will be totally disconnected as well.

Case (2): Suppose $k = 2$. Considering every possible combination of 2 triples, we discover that the only possible pair of triples is $T_{1,3}$ and $T_{1,5}$. Every other pair results in at least one vertex of $MQ(S)$ having odd degree, which contradicts the Degree Rule.

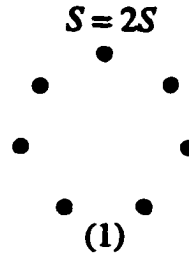
Case (3): Suppose $k = 4$. If 4 triples are included, then exactly one triple is *excluded*. In order to leave every vertex in $MQ(S)$ with even degree, the triple we must exclude must be either $T_{1,3}$ or $T_{1,5}$. Any other triple when excluded leaves at least one vertex of odd degree.

Therefore, we have 4 possible idempotent quotient graphs:





To further reduce this list, we will utilize the idempotency condition on the Rédei matrix. Recall from Theorem 2.3.3 that if $2 \in S$, then the Rédei matrix associated to the quotient graph is idempotent. Considering our list of 4 possible quotient graphs, we determine that only graph (1), the totally disconnected graph has an idempotent Rédei matrix. Therefore, if $b = 1$, the quotient graph $Q(S)$ must be the totally disconnected graph.



Now suppose $b = 7$. In this case, we can choose $2S$ as a generator of the vertex set Π . Again using Corollary 2.4.8, we determine that the number of triples present must be odd. So $k = 1, 3$ or 5 .

Case (1): Suppose $k = 1$. The Degree Rule states that for $b > 2$ the only two vertices of odd degree are $2S$ and $2^{-1}S$. The only possibility which agrees with this is for the triple present to be $T_{1,4}$. All others produce other vertices of odd degree.

Case (2): Suppose $k = 3$. First we will consider $T_{1,2}$. If $T_{1,2}$ is present then in order for $2S$ to have odd degree in $MQ(S)$ (which it must), the other 2 triples

cannot both come from $T_{1,3}, T_{1,4}$ and $T_{1,5}$. So the triple $T_{2,4}$ must be present. So we now have 2 of the 3 triples. If the third triple is $T_{1,4}$, then the vertex 2^2S will have odd degree, which contradicts the Degree Rule. However, including either triple $T_{1,3}$ or triple $T_{1,5}$ does not produce a contradiction.

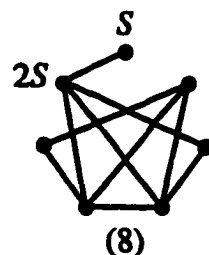
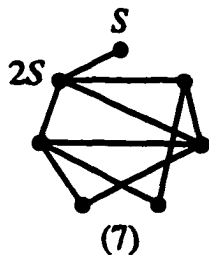
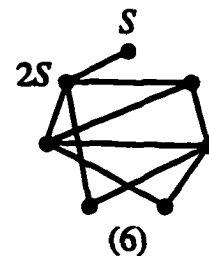
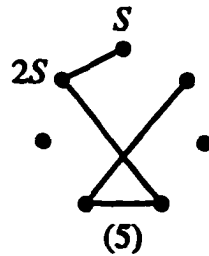
Suppose now that $T_{1,2}$ is not present. Then if triple $T_{2,4}$ is present, vertex $2S$ will have even degree, which is a contradiction. So $T_{2,4}$ must also be excluded (along with $T_{1,2}$), and therefore the 3 triples present must be $T_{1,3}, T_{1,4}$ and $T_{1,5}$.

So with 3 triples present, we have 3 possibilities for the edge set of $MQ(S)$:

$$\{T_{1,2}, T_{2,4}, T_{1,3}\}, \{T_{1,2}, T_{2,4}, T_{1,5}\} \text{ or } \{T_{1,3}, T_{1,4}, T_{1,5}\}.$$

Case (3): Suppose $k = 5$. In this case, every combination of 5 triples leaves every vertex with odd degree, which contradicts the Degree Rule. So there are no possible modified quotient graphs with 5 triples.

Therefore, with $b = 7$ we have 4 possible quotient graphs:



We now utilize the results from Section 5 of Chapter 2 to reduce this list.

From Corollary 2.5.8, we know that with $b = 7$, $Q(S)$ must be connected. So graph

(5) cannot be a quotient graph. Now consider the characteristic polynomial, $\alpha(x)$, of graph (8). For this graph,

$$\alpha(x) = x^7 + x^6 + x^4 + 1 = (x+1)(x^2+x+1)(x^4+x^3+1)$$

which is clearly not irreducible. Therefore, by Theorem 2.5.7, graph (8) also cannot be a quotient graph.

The characteristic polynomials of graphs (6) and (7) are both irreducible, however they in fact are the same polynomial. For both of these graphs,

$$\alpha(x) = x^7 + x^6 + x^4 + x + 1.$$

Since a quotient graph and its characteristic polynomial uniquely determine each other, these cannot both be quotient graphs. To determine which graph is a quotient graph, we only need to exhibit an example where one of these graphs is realized.

(2.6.22) **Example:** $n = 7, p = 29$.

We have $(\mathbb{Z}/29\mathbb{Z})^* = \{\pm 1, \pm 2, \dots, \pm 14\}$. So

$$S = (\mathbb{Z}/29\mathbb{Z})^{*7} = \{\pm 1, \pm 12\}$$

$$2S = \{\pm 2, \pm 5\}$$

$$2^2S = \{\pm 4, \pm 10\}$$

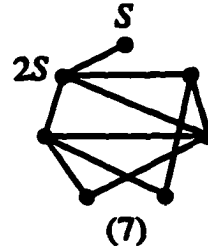
$$2^3S = \{\pm 8, \pm 9\}$$

$$2^4S = \{\pm 11, \pm 13\}$$

$$2^5S = \{\pm 3, \pm 7\}$$

$$2^6S = \{\pm 6, \pm 14\}.$$

Consider $N(2, 2^3S) = 0$. By the definition of $Q(S)$, this means that the vertices $2S$ and 2^3S are not adjacent. So $Q(S)$ must be graph (7):



Hence graph (6) cannot be a quotient graph. Therefore, we have shown that for $n = 7$, there are only two quotient graphs, and again we can determine for a given prime $p \equiv 1(14)$ which quotient graph it generates simply by determining whether $2 \in S$ or not.

(2.6.23) **Example:** $n = 7, p = 631$.

Notice that $2 \equiv 11^7(631)$. So $2 \in S$ and thus $Q(S)$ is totally disconnected.

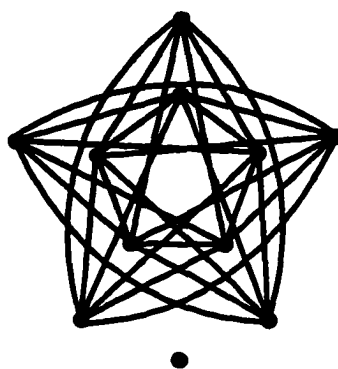
(2.6.24) **Example:** $n = 11$

For this case, we will exhibit examples of 5 distinct quotient graphs on 11 vertices (2 idempotent and 3 non-idempotent). In Chapter 3 we will prove that in fact these are all possible quotient graphs on 11 vertices. For the prime numbers in these examples, we utilized a computer to aid in determining if 2 is an element of S or not.

We begin with $b = 1$. It was determined in [M] that there are at most two idempotent quotient graphs on 11 vertices. The totally disconnected graph on 11 vertices was known to be a *possible* quotient graph. We will exhibit here a prime which generates that graph as well as the other known idempotent graph on 11 vertices, which we call the Myers-Turner Graph.

(2.6.25) **Example:** $n = 11, p = 331$.

The quotient graph generated by this prime is the graph we called the Myers-Turner Graph. Notice that the modified quotient graph associated to it is the edge complement to the Petersen Graph:



the Myers - Turner Graph

(2.6.26) **Example:** $n = 11, p = 6337$.

This is the smallest prime number $p \equiv 1(22)$ with $b = 1$ which generates the totally disconnected graph:



the totally disconnected graph

Now we turn our attention to the case $b = 11$. In [M], the following three graphs were realized, and we reproduce those examples here. In that dissertation however, it could only be shown that there were at most 12 non-idempotent quotient graphs on 11 vertices. In the next chapter (see 3.3.2), we will demonstrate that these three are the *only* non-idempotent quotient graphs on 11 vertices.

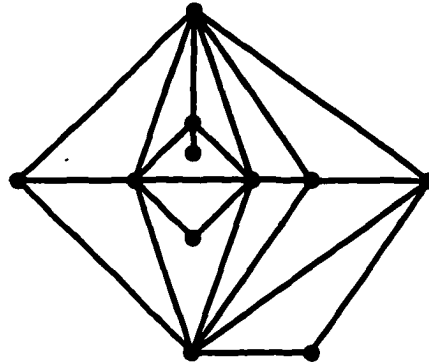
(2.6.27) **Example:** $n = 11, p = 23$

This prime generates the familiar line graph:



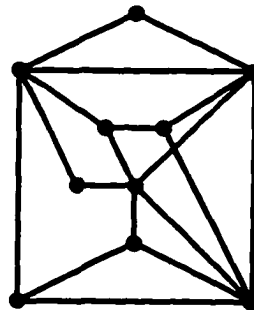
(2.6.28) **Example:** $n = 11, p = 67$.

The graph generated by this prime number is the following:



(2.6.29) **Example:** $n = 11, p = 199$.

The graph produced by this prime is quite complicated with vertex degrees of 4, 6, 7, and 8 (and of course 0 since the vertex S is isolated). Because of the complexity of this graph, we will only exhibit the edge complement of the modified quotient graph generated by this prime:



CHAPTER 3: FORMAL QUOTIENT GRAPHS

Section 1: The General Situation

In order to further understand and determine quotient graphs, we need to generalize the situation. Let k be an arbitrary field extension of F_2 of odd degree n .

(3.1.1) **Definition:** A **graph generator** is an element $\theta \in k^*$ for which the following two conditions hold:

- (1) The conjugates of θ over F_2 form a normal basis of k , and
- (2) The trace of the product of any two distinct conjugates of θ is 0.

We will see in Definition 3.1.7 why these elements are called “graph generators”. First we wish to verify that our discussion of quotient graphs from Chapter 2 is in fact generalized by this situation.

(3.1.2) **Example:** Recall the quotient graph situation. We begin with a fixed integer n and a p -th cyclotomic extension $Q(\xi)$ of Q where ξ is a p -th root of unity and $p \equiv 1(2n)$. The Galois group $\text{Gal}(Q(\xi)|Q) = (\mathbb{Z}/p\mathbb{Z})^*$. Associated to the subgroup $S \subseteq (\mathbb{Z}/p\mathbb{Z})^*$ is a fixed field F . Since $\#S = \frac{p-1}{n}$, F is a degree n extension of Q . If $b = n$, then there is a unique dyadic prime ideal in \mathcal{O}_F . In other words, $\mathcal{O}_F/2\mathcal{O}_F$ is an n -th degree extension field of F_2 . So we let $k = \mathcal{O}_F/2\mathcal{O}_F$. As noted previously (see 1.3.33, 1.4.3), $\gamma_S \in k$ and the conjugates of γ_S form a normal basis of k over F_2 . Also, from Corollary 2.2.9, we know that the trace of the product of any two distinct conjugates of γ_S is 0. So γ_S is a graph generator in the sense of Definition 3.1.1.

Let $\sigma : k \longrightarrow k$ be the Galois automorphism defined by

$$\sigma(x) = x^2 \text{ for all } x \in k.$$

For $1 \leq j \leq n$, let $f_j = \sigma^{j-1}(\theta) = (\theta)^{2^{j-1}}$ where θ is a graph generator. Then $\{f_j\}_{j=1}^n$ is a (naturally) ordered basis of k over \mathbb{F}_2 . For $0 \leq i \leq n-1$,

$$\sigma^i(f_j) = f_{i+j}$$

with the natural clarification that if $i+j > n$, then $\sigma^i(f_j) = f_{i+j-n}$. Since $\{f_j\}_{j=1}^n$ are linearly independent,

$$\text{tr}(\theta) = f_1 + f_2 + \dots + f_n = 1 \in \mathbb{F}_2.$$

Thus for every $1 \leq j \leq n$,

$$(3.1.3) \quad \text{tr}(f_j^2) = \text{tr}(f_j) = 1.$$

We can define an inner product space structure on k . For $x, y \in k$, define

$$b(x, y) = \text{tr}(xy) \in \mathbb{F}_2.$$

Notice that

$$b(\sigma(x), \sigma(y)) = \text{tr}(\sigma(x)\sigma(y)) = \text{tr}(\sigma(xy)) = \text{tr}(xy) = b(x, y).$$

So $\text{Gal}(k|\mathbb{F}_2)$ acts as a group of isometries in this structure.

Let $B = (b_{ij})$ be the matrix representing this trace form (so $b_{ij} = b(f_i, f_j)$).

Note that

$$b_{ij} = b(f_i, f_j) = 0 \text{ if } i \neq j \text{ and}$$

$$b_{ii} = b(f_i, f_i) = 1 \quad (\text{see 3.1.3}).$$

So B is the identity matrix.

If $L : k \longrightarrow k$ is an \mathbb{F}_2 -linear operator, then with respect to the basis $\{f_j\}_{j=1}^n$, L is represented by a matrix $L = (a_{ij})$ in the usual manner:

$$L(f_j) = \sum_{i=1}^n a_{ij} f_i.$$

(3.1.4) **Lemma:** The matrix $L = (a_{ij})$ representing an \mathbb{F}_2 -linear operator $L : k \longrightarrow k$ is symmetric if and only if

$$b(x, L(y)) = b(L(x), y) \quad \text{for all } x, y \in k.$$

Proof: We only need to verify this for the basis elements. Notice that for a fixed i and j ,

$$\begin{aligned} b(f_i, L(f_j)) &= \text{tr}(f_i \cdot L(f_j)) = \text{tr}\left(f_i \cdot \sum_{k=1}^n a_{kj} f_k\right) \\ &= \text{tr}\left(\sum_{k=1}^n a_{kj} f_i f_k\right) \\ &= \sum_{k=1}^n a_{kj} b(f_i, f_k) \\ &= a_{ji}. \end{aligned}$$

Similarly,

$$b(L(f_i), f_j) = a_{ji}.$$

So L is symmetric if and only if $b(f_i, L(f_j)) = b(L(f_i), f_j)$. ■

Now we consider a specific linear operator

$T : k \longrightarrow k$ defined by

$$(3.1.5) \quad T(x) = \theta \cdot x = f_1 \cdot x \text{ for all } x \in k.$$

(3.1.6) **Lemma:** Let $A = (a_{ij})$ be the matrix representing the linear operator T (defined above) with respect to the basis $\{f_j\}_{j=1}^n$. Then

(1) A is symmetric.

(2) $a_{11} = 0$, $a_{21} = 1$ and $a_{i1} = 0$ for $2 < i \leq n$.

(3) $\sum_{i=1}^n a_{ij} = 0$ for $1 < j \leq n$.

Proof: Notice first that

$$b(x, T(y)) = \text{tr}(x\theta y) = \text{tr}(\theta xy) = b(T(x), y)$$

so (1) follows from the previous lemma. Since

$$T(f_1) = f_1^2 = f_2,$$

statement (2) is clear as well. We now show (3) holds. By the definition of A ,

$$T(f_j) = \sum_{i=1}^n a_{ij} f_i.$$

By 3.1.3, the trace of this is $\sum_{i=1}^n a_{ij}$. However, we can also express $T(f_j)$ using the definition of T ,

$$T(f_j) = f_1 \cdot f_j.$$

By 3.1.1, the trace of this is 0 (for $1 < j \leq n$), which proves the lemma. ■

If we form a matrix $M = (m_{ij})$ from A by changing $a_{11} = 0$ to $m_{11} = 1$, then the result will be a symmetric matrix in which *every* column sums to 0. By denoting the elements of $\mathbb{Z}/n\mathbb{Z}$ by v_j (so $v_j = j - 1 \in \mathbb{Z}/n\mathbb{Z}$), we see that M is the Rédei matrix of a unique graph on the ordered set of vertices $V = \{v_1, v_2, \dots, v_n\}$.

(3.1.7) **Definition:** A graph whose Rédei matrix M is formed in this manner is called a **formal quotient graph**, denoted by FQ . Note the absence of a set S in the notation.

(3.1.8) **Remark:** From Example 3.1.2 we see that every (honest) quotient graph (with $b = n$) is a formal quotient graph.

A consequence of Lemma 3.1.6 is that the first column of M is $\begin{pmatrix} 1 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, so we see that the vertex v_1 of FQ is adjacent to only vertex v_2 as expected.

We would now like to determine the invariant $c(FQ)$ for non-idempotent formal quotient graphs. To do this we will need a linear operator and a lemma.

Let $\theta \in k^*$ be a graph generator. We have a linear operator over F_2

$M : k \longrightarrow k$ given by

$$M(x) = b(x, \theta) \cdot \theta + x \cdot \theta.$$

(3.1.9) **Lemma:** The matrix which represents this operator with respect to the basis $\{f_i\}_{i=1}^n$ is the Rédei matrix of the formal quotient graph FQ associated to θ .

Proof: Note that for $i \neq 1$,

$$\begin{aligned} M(f_i) &= b(f_i, \theta) \cdot \theta + f_i \cdot \theta \\ &= \text{tr}(f_i \cdot \theta) \cdot \theta + f_i \cdot \theta \\ &= 0 + f_i \cdot f_1 \\ &= f_1 \cdot f_i \\ &= T(f_i). \end{aligned}$$

So all of the rows except possibly the first will agree between the Rédei matrix (which was determined by T) and the matrix determined by the operator M . Now consider the first row ($i = 1$),

$$\begin{aligned}
 M(f_1) &= b(f_1 \cdot \theta) \cdot \theta + f_1 \cdot \theta \\
 &= \text{tr}(f_1 \cdot \theta) \cdot \theta + f_1 \cdot \theta \\
 &= \text{tr}(\theta^2) \cdot \theta + \theta^2 \\
 &= \theta + \theta^2 \\
 &= f_1 + f_2.
 \end{aligned}$$

So in fact, the matrix representing the operator M is the Rédei matrix. ■

(3.1.10) **Proposition:** Let FQ be a non-idempotent formal quotient graph. Then $c(FQ) = 0$.

Proof: By 1.2.14, we know that $c(FQ) = n - \text{rank} M - 1$. So

$$c(FQ) = \dim_{\mathbb{F}_2}(\text{Ker}(M)) - 1.$$

Therefore to compute $c(FQ)$, we only need to compute $\dim(\text{Ker}(M))$. By definition,

$$\begin{aligned}
 M(x) &= b(x, \theta) \cdot \theta + x \cdot \theta \\
 &= \theta(b(x, \theta) + x).
 \end{aligned}$$

So

$$\begin{aligned}
 M(x) = 0 &\iff x = b(x, \theta) = \text{tr}(x \cdot \theta) \\
 &\iff x = 0, 1.
 \end{aligned}$$

Thus $\text{Ker}(M) = \{0, 1\}$. So $\dim(\text{Ker}(M)) = 1$, and hence $c(FQ) = 0$. ■

We will be able to use these formal quotient graphs to aid our discussion of (honest) quotient graphs. However, we must first determine whether or not

conjugate graph generators produce distinct formal quotient graphs. This question is answered in the next lemma.

(3.1.11) **Lemma:** The formal quotient graph FQ depends only on the conjugacy class of the graph generator.

Proof: Let θ be a graph generator and let $\psi = \sigma^r(\theta)$ be any conjugate of θ .

Clearly ψ is also a graph generator, and we define

$$\begin{aligned} e_j &= \sigma^{j-1}(\psi) = \sigma^{j-1}(\sigma^r(\theta)) \\ &= \sigma^r(\sigma^{j-1}(\theta)) \\ &= \sigma^r(f_j). \end{aligned}$$

If as before we write $f_1 \cdot f_j = \sum_{i=1}^n a_{ij} f_i$ then,

$$\sigma^r(f_1 \cdot f_j) = \sigma^r(f_1) \cdot \sigma^r(f_j) = e_1 \cdot e_j \text{ and,}$$

$$\sigma^r\left(\sum_{i=1}^n a_{ij} f_i\right) = \sum_{i=1}^n a_{ij} e_i.$$

So

$$e_1 \cdot e_j = \sum_{i=1}^n a_{ij} e_i,$$

which implies that the graphs generated by θ and ψ are identical. ■

A natural question therefore is: How many graph generators (up to conjugacy) are there in k^* ?

Section 2: How Many Formal Quotient Graphs Are There?

To determine how many distinct conjugacy classes of graph generators there are in k^* , we will need the group ring $F_2[C_n]$. Let $\sigma \in C_n$ be the generator of the cyclic group of order n . Recall that an arbitrary element, α , in $F_2[C_n]$ can be

written in the form

$$\alpha = \sum_{i=0}^{n-1} c_i \sigma^i.$$

We can therefore view the extension field k of \mathbb{F}_2 as an $\mathbb{F}_2[C_n]$ -module with multiplication defined by:

$$(3.2.1) \quad \alpha \cdot x = \sum_{i=0}^{n-1} c_i \sigma^i(x) \text{ for all } x \in k.$$

Clearly k is free of rank 1.

We will also need the canonical involution of the group ring defined as follows:

$$\alpha \mapsto \alpha^* \text{ where}$$

$$\alpha^* = \sum_{i=0}^{n-1} c_i \sigma^{-i} = \sum_{i=0}^{n-1} c_i \sigma^{n-i}.$$

Consider the \mathbb{F}_2 -linear operator defined on k as follows:

$$x \mapsto \alpha \cdot x.$$

Notice that $b(x, \alpha y) = b(\alpha^* x, y)$. Therefore,

$$(3.2.2) \quad b(\alpha x, \alpha y) = b(\alpha^* \alpha x, y).$$

For a given graph generator $\theta \in k^*$ and $\alpha \in \mathbb{F}_2[C_n]$, under what conditions will $\alpha \cdot \theta$ also be a graph generator in k^* ? Clearly we must require that α be a unit in $\mathbb{F}_2[C_n]$, but we also need

$$b(\alpha f_i, \alpha f_j) = b(f_i, f_j)$$

for all basis elements. In other words, multiplication by α must be an isometry of k . By 3.2.2, that means we must require that

$$(3.2.3) \quad b(x, y) = b(\alpha x, \alpha y) = b(\alpha^* \alpha x, y)$$

for all $x, y \in k$. Therefore, we can conclude that for a graph generator θ , $\alpha \cdot \theta$ is again a graph generator if and only if

$$(3.2.4) \quad \alpha^* \cdot \alpha = 1 \in \mathbb{F}_2[C_n].$$

(3.2.5) **Definition:** Let $SU \subseteq \mathbb{F}_2[C_n]$ be the (multiplicative) subgroup of all units of $\mathbb{F}_2[C_n]$ for which $\alpha^* \cdot \alpha = 1$.

Notice that by definition, $\sigma^* = \sigma^{-1}$, so we have $C_n \subseteq SU$. Also, if θ is a graph generator in k and ψ is *another* graph generator in k , then there exists an element $\alpha \in SU$ such that $\psi = \alpha \cdot \theta$. Therefore, we have a 1-1 correspondence between the conjugacy classes of graph generators and the elements of the quotient group

$$SU/C_n.$$

We will compute the order of this group in many cases.

To begin, let us assume $n = q$ is an odd prime and 2 is a generator of $(\mathbb{Z}/q\mathbb{Z})^*$. This means that $f = q - 1$ and therefore $r = 1$. Hence there is a unique dyadic prime in the q -th cyclotomic extension and $k = \mathbb{Z}[\xi]/2\mathbb{Z}[\xi]$ is an extension field of \mathbb{F}_2 of degree $q - 1$.

(3.2.6) **Lemma:** The subgroup $SU \subseteq \mathbb{F}_2[C_q]$ is isomorphic to the subgroup of elements $z \in \mathbb{Z}[\xi]/2\mathbb{Z}[\xi]$ with $z \cdot \bar{z} = 1$, where the bar denotes complex conjugation.

Proof: Recall from 1.3.4 that for $\mathbb{F}_2[C_q]$ we have the augmentation homomorphism

$\epsilon : \mathbb{F}_2[C_q] \longrightarrow \mathbb{F}_2$ defined by

$$\epsilon\left(\sum_{i=0}^{n-1} c_i \sigma^i\right) = \sum_{i=0}^{n-1} c_i.$$

Notice that $\epsilon(\alpha) = \epsilon(\alpha^*)$ for all $\alpha \in \mathbb{F}_2[C_q]$. Also recall the element

$$\Omega = 1 + \sigma + \dots + \sigma^{q-1} \in \mathbb{F}_2[C_q]$$

which has the properties

$$\epsilon(\Omega) = 1 \quad \text{and} \quad \Omega = \Omega^*.$$

There is also another map

$\eta : \mathbb{F}_2[C_q] \longrightarrow \mathbb{Z}[\xi]/2\mathbb{Z}[\xi]$ defined by

$$\eta(\sigma) = \xi.$$

The kernel of η is $(\Omega) = \{0, \Omega\}$, the ideal generated by Ω . Notice that for any $\alpha \in \mathbb{F}_2[C_q]$,

$$\eta(\alpha^*) = \overline{\eta(\alpha)}.$$

Thus $\alpha^* \cdot \alpha = 1 \in \mathbb{F}_2[C_q]$ if and only if

$$(3.2.7) \quad \epsilon(\alpha) = 1 \in \mathbb{F}_2 \quad \text{and}$$

$$\eta(\alpha) \cdot \overline{\eta(\alpha)} = 1.$$

However, suppose that $\beta \in \mathbb{F}_2[C_q]$ with $\epsilon(\beta) = 0$ and $\eta(\beta) \cdot \overline{\eta(\beta)} = 1$. If we define $\alpha = \Omega + \beta$, then $\alpha^* = \Omega + \beta^*$, and now $\epsilon(\alpha) = 1$ and $\eta(\alpha) = \eta(\beta)$. So while $\beta \notin SU$, $\alpha \in SU$, and hence the lemma is proved. ■

(3.2.8) **Lemma:** If $n = q$ is an odd prime and 2 is a generator of $(\mathbb{Z}/q\mathbb{Z})^*$, then

$$\#(SU/C_q) = \frac{2^{f/2} + 1}{q}.$$

Proof: By the previous lemma, SU is isomorphic to the subgroup of elements $z \in \mathbb{Z}[\xi]/2\mathbb{Z}[\xi]$ with $z \cdot \bar{z} = 1$. Recall that complex conjugation in $k = \mathbb{Z}[\xi]/2\mathbb{Z}[\xi]$ is given by the map

$$z \mapsto z^{2^{q-1}} = z^{2^f}.$$

Thus if $k_1 \subseteq k$ is the fixed field of this map, then what we seek is the kernel of the norm map

$$N : k^* \longrightarrow k_1^*.$$

Since $\#k^* = 2^f - 1$ and $\#k_1^* = 2^{f/2} - 1$, we have

$$\#SU = \frac{2^f - 1}{2^{f/2} - 1} = 2^{f/2} + 1,$$

and the lemma follows. ■

(3.2.9) **Example:** Let $n = q = 3$ or 5. Then $f = 2$ or 4 respectively and therefore in either case,

$$\#(SU/C_q) = 1.$$

We will now compute the size of this quotient group in general (when 2 is *not* necessarily a generator of $(\mathbb{Z}/q\mathbb{Z})^*$). We will need another lemma. We have

the ring of integers of the q -th cyclotomic extension

$$\mathbb{Z}[\xi] \subseteq \mathbb{Q}(\xi).$$

Complex conjugation is the Galois automorphism of $\mathbb{Q}(\xi)$ induced from the map

$$\xi \mapsto \xi^{-1} = \bar{\xi}.$$

In fact, for $z \in \mathbb{Z}[\xi]$, we write $z \mapsto \bar{z}$. The maximal real subfield

$$\mathbb{Q}(\xi)^+ \subseteq \mathbb{Q}(\xi)$$

is the fixed field of this involution. So $\mathbb{Z}[\xi + \xi^{-1}] \subseteq \mathbb{Z}[\xi]$ is the subring of fixed integers. We denote $\mathbb{Z}[\xi]/2\mathbb{Z}[\xi]$ by R , and we denote the subring of elements of R which are fixed under complex conjugation by R^+ . Namely,

$$R^+ = \mathbb{Z}[\xi + \xi^{-1}]/2\mathbb{Z}[\xi + \xi^{-1}] \subseteq \mathbb{Z}[\xi]/2\mathbb{Z}[\xi].$$

If P_1, P_2, \dots, P_r are the dyadic primes in $\mathbb{Z}[\xi]$, then for each i , $k_i = \mathbb{Z}[\xi]/P_i$ is a degree f extension of \mathbb{F}_2 and we have the maps

$$\eta_i : R \longrightarrow k_i$$

which induce a map with the direct sum

$$\bigoplus_{i=1}^r \eta_i : R \longrightarrow \bigoplus_{i=1}^r k_i.$$

So

$$R^* \simeq \prod_{i=1}^r k_i^*,$$

and therefore,

$$(3.2.10) \quad \#R^* = (2^f - 1)^r.$$

In particular, $\#R^*$ is odd. For the subring R^+ there are 2 cases:

(1) If $f \equiv 0(2)$, then the number of dyadic primes in $\mathbb{Z}[\xi + \xi^{-1}]$ is r and each one has inertia degree $f/2$. Thus

$$(3.2.11) \quad \#R^{+*} = (2^{f/2} - 1)^r.$$

(2) If $f \equiv 1(2)$, then the number of dyadic primes in $\mathbb{Z}[\xi + \xi^{-1}]$ is $r/2$ and each one has inertia degree of f . Thus

$$(3.2.12) \quad \#R^{+*} = (2^f - 1)^{r/2}.$$

On R^{+*} , the involution $z \mapsto \bar{z}$ induced by complex conjugation is an action of the cyclic group, C_2 , of order 2 as a group of automorphisms of the multiplicative abelian group R^* . Since as we saw, R^* has *odd* order,

$$H^2(C_2, R^*) \text{ is trivial.}$$

Since $R^{+*} \subseteq R^*$ is the subgroup of fixed elements under this action, and since the cohomology group is trivial, we see that the map

$$R^* \longrightarrow R^{+*} \text{ given by}$$

$$z \longmapsto z \cdot \bar{z}$$

is onto. So the kernel $K \subseteq R^*$ of this map is

$$K \simeq R^*/R^{+*}.$$

So,

$$(3.2.13) \quad \#K = \#R^* / \#R^{+*}.$$

(3.2.14) **Remark:** This kernel (in other words the subgroup of units for which $z \cdot \bar{z} = 1$) is precisely the group SU we are trying to compute.

(3.2.15) **Lemma:** If $f \equiv 0(2)$, then $\#K = (2^{f/2} + 1)^r$. If $f \equiv 1(2)$, then $\#K = (2^f - 1)^{r/2}$.

Proof: Simply combine 3.2.10 with 3.2.11 or 3.2.12 respectively. ■

(3.2.16) **Theorem:** If $n = q$ is an odd prime, then the number of non-idempotent formal quotient graphs on q vertices is

$$\#(SU/C_q) = \begin{cases} \frac{(2^{f/2}+1)^r}{q} & \text{if } f \equiv 0(2) \text{ or} \\ \frac{(2^f-1)^{r/2}}{q} & \text{if } f \equiv 1(2). \end{cases}$$

Proof: We know that the number of formal quotient graphs is the same as the number of conjugacy classes of graph generators. We saw that the number of conjugacy classes of graph generators is the same as $\#(SU/C_q)$. Then by Remark 3.2.14, we saw that computing $\#SU$ amounted to computing $\#K$ which is done in Lemma 3.2.15. ■

As noted in Example 3.1.2, this will have serious implications in our study of quotient graphs. In the case where $b = n$, we saw that every quotient graph is a formal quotient graph. Therefore, this number computed in Theorem 3.2.16 will be an upper bound for the number of quotient graphs with $b = n$. Since we are only considering prime values for n , the only other case we need to address is when $b = 1$. It has been shown by P. E. Conner that idempotent quotient graphs

(in other words quotient graphs with $b = 1$) are also formal quotient graphs and an analogous discussion produces a formula for the number of idempotent formal quotient graphs. This number will therefore also be an upper bound for the number of idempotent (honest) quotient graphs. We will now state this formula (due to P.E.Conner) for the number of idempotent formal quotient graphs without proof.

(3.2.17) **Theorem (Conner):** Let k be the largest positive integer such that $q - 1 = (2^k)(s)$. For every positive divisor d of s , $1 < d \leq s$, let

$$E(d) = \begin{cases} 2^{\frac{q-1}{2d}} + 1 & \text{if } f = q - 1 \text{ or} \\ 2^{\frac{q-1}{2d}} - 1 & \text{if } f = \frac{q-1}{2} \end{cases}$$

and let $\phi(d)$ denote the usual Euler phi function. Then the number of conjugacy classes of idempotent formal quotient graphs on q vertices is given by

$$\#C(q, q) = \frac{\#(SU/C_q) + (2^k - 1)s + \sum_{d|s} \phi(d)E(d)}{(q - 1)}.$$

In the next section, we will compute these necessary numbers from Theorem 3.2.16 and Theorem 3.2.17 for several values of n . This will give us the number of distinct formal quotient graphs in the two cases $b = n$ and $b = 1$ respectively. We will then be able to use this information, along with our previous results to obtain more precise results for honest quotient graphs.

Section 3: Examples

Let $n = q$ be an odd prime. We begin with the case $b = n = q$. We wish to compute the size of this quotient group SU/C_q in several cases. By Theorem 3.2.16, this will give us the number of formal quotient graphs (with $b = q$) on q vertices.

(3.3.1) Examples:

(1) Let $q = 3$. Then $f = 2$ and $r = 1$. So

$$\#(SU/C_q) = \frac{(2^{2/2} + 1)^1}{3} = \frac{3}{3} = 1.$$

(2) Let $q = 5$. Then $f = 4$ and $r = 1$. So

$$\#(SU/C_q) = \frac{(2^{4/2} + 1)^1}{5} = \frac{5}{5} = 1.$$

(3) Let $q = 7$. Then $f = 3$ and $r = 2$. So

$$\#(SU/C_q) = \frac{(2^3 - 1)^{2/2}}{7} = \frac{7}{7} = 1.$$

(4) Let $q = 11$. Then $f = 10$ and $r = 1$. So

$$\#(SU/C_q) = \frac{(2^{10/2} + 1)^1}{11} = \frac{33}{11} = 3.$$

We would like to indicate the importance of these numbers by utilizing this last example.

(3.3.2) Theorem: There are exactly 3 quotient graphs on 11 vertices with $b = 11$.

Proof: We see from Example 3.3.1(4) that there are *at most* 3 quotient graphs on 11 vertices with $b = 11$. However, in Section 2.6 we demonstrated 3 distinct quotient graphs with this property. Therefore there are *exactly* 3 distinct quotient graphs on 11 vertices with $b = 11$. ■

(3.3.3) Examples: We continue with more examples.

(1) Let $q = 13$. Then $f = 12$ and $r = 1$. So

$$\#(SU/C_q) = \frac{(2^{12/2} + 1)^1}{13} = \frac{65}{13} = 5.$$

(2) Let $q = 17$. Then $f = 8$ and $r = 2$. So

$$\#(SU/C_q) = \frac{(2^{8/2} + 1)^2}{17} = \frac{17^2}{17} = 17.$$

(3) Let $q = 19$. Then $f = 18$ and $r = 1$. So

$$\#(SU/C_q) = \frac{(2^{18/2} + 1)^1}{19} = \frac{513}{19} = 27.$$

(4) Let $q = 23$. Then $f = 11$ and $r = 2$. So

$$\#(SU/C_q) = \frac{(2^{11} - 1)^{2/2}}{23} = \frac{2047}{23} = 89.$$

(5) Let $q = 29$. Then $f = 28$ and $r = 1$. So

$$\#(SU/C_q) = \frac{(2^{28/2} + 1)^1}{29} = \frac{16385}{29} = 565.$$

(6) Let $q = 31$. Then $f = 5$ and $r = 6$. So

$$\#(SU/C_q) = \frac{(2^5 - 1)^{6/2}}{31} = \frac{31^3}{31} = 31^2 = 961.$$

We exhibit one final example to show both the ease of computing the size of this quotient group, and how quickly the size gets extremely large.

(3.3.4) **Example:** Let $q = 83$. Then $f = 82$ and $r = 1$. So

$$\#(SU/C_q) = \frac{(2^{82/2} + 1)^1}{83} = \frac{2199023255553}{83} = 26,494,256,091.$$

Now some examples with $b = 1$. We see from the formula in Theorem 3.2.17 that we will need $\#(SU/C_q)$. We will take this number from these previous examples.

(3.3.5) Examples:

(1) Let $q = 3$. Then $f = 2$, $r = 1$, $k = 1$ and $s = 1$. There are no divisors of s greater than 1. So

$$\#C(3, 3) = \frac{1 + (2^1 - 1) \cdot 1}{2} = \frac{2}{2} = 1.$$

(2) Let $q = 5$. Then $f = 4$, $r = 1$, $k = 2$ and $s = 1$. There are no divisors of s greater than 1. So

$$\#C(5, 5) = \frac{1 + (2^2 - 1) \cdot 1}{4} = \frac{4}{4} = 1.$$

(3) Let $q = 7$. Then $f = 3$, $r = 2$, $k = 1$ and $s = 3$. The only divisor of s greater than 1 is $d = 3$. So

$$\#C(7, 7) = \frac{1 + (2^1 - 1) \cdot 3 + \phi(3)(2^{6/6} - 1)}{6} = \frac{6}{6} = 1.$$

(4) Let $q = 11$. Then $f = 10$, $r = 1$, $k = 1$ and $s = 5$. The only divisor of s greater than 1 is $d = 5$. So

$$\#C(11, 11) = \frac{3 + (2^1 - 1) \cdot 5 + \phi(5)(2^{10/10} + 1)}{10} = \frac{20}{10} = 2.$$

(3.3.6) Remark: Notice that $n = q = 11$ is the first case where we have 2 distinct idempotent formal quotient graphs. As we saw in Section 2.6, both of these graphs are indeed honest quotient graphs. We now continue with more examples.

(3.3.7) Examples:

(1) Let $q = 13$. Then $f = 12$, $r = 1$, $k = 2$ and $s = 3$. The only divisor of s greater than 1 is $d = 3$. So

$$\#C(13, 13) = \frac{5 + (2^2 - 1) \cdot 3 + \phi(3)(2^{12/6} + 1)}{12} = \frac{24}{12} = 2.$$

(2) Let $q = 17$. Then $f = 8$, $r = 2$, $k = 4$ and $s = 1$. There are no divisors of s greater than 1. So

$$\#C(17, 17) = \frac{17 + (2^4 - 1) \cdot 1}{16} = \frac{32}{16} = 2.$$

(3) Let $q = 19$. Then $f = 18$, $r = 1$, $k = 1$ and $s = 9$. The only divisors of s greater than 1 are $d_1 = 3$ and $d_2 = 9$. So

$$\begin{aligned} \#C(19, 19) &= \frac{27 + (2^1 - 1) \cdot 9 + \phi(3)(2^{18/3} + 1) + \phi(9)(2^{18/9} + 1)}{18} \\ &= \frac{72}{18} = 4. \end{aligned}$$

In the following section, we will demonstrate how to generate idempotent formal quotient graphs.

Section 4: Generating Idempotent Formal Quotient Graphs

Fix n and choose $b = 1$. We know that every graph generator is obtained from a given graph generator by multiplying it by a “special unit” $\alpha \in SU$. We wish to arrive at the Rédei matrix M of a idempotent formal quotient graph from these special units. To do this we will produce a “natural” formula for generating the modified Rédei matrix A from the units. Then we will simply change the top right entry of A from a 1 to a zero to obtain M .

Let \mathcal{L} be the linear algebra of all functions

$$\phi : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{F}_2.$$

In particular, there is the special graph generator $E \in \mathcal{L}$ with $E(0) = 1$ and $E(x) = 0$ for every $x \neq 0$.

Let E be such a given graph generator. Then we will denote the formal quotient graph associated to αE by $Q(\alpha E)$. Now consider the element $\alpha \in SU \subset \mathbb{F}_2[C_n]$. If we write

$$(3.4.1) \quad \alpha = \sum_{i=1}^n a_i \sigma^{(i-1)},$$

then we associate to α an $n \times n$ circulant matrix $C = (c_{ij})$ as follows: to create the first column of C , define $c_{i1} = a_i$ and then “circulate” it to produce the remaining columns.

(3.4.2) **Example:** Let $n = 11$. Choose $\alpha = \sigma^4 + \sigma^7 + \sigma^9 + \sigma^{10} + \sigma^{11}$. Then

$$C = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Since $\alpha \in SU$ (in other words $\alpha \cdot \alpha^* = 1$), the circulant matrix C is orthogonal. That is,

$$(3.4.3) \quad C^{\text{tr}} = C^{-1}.$$

Next we will need an auxiliary matrix $D = (d_{ij})$ defined by

$$(3.4.4) \quad d_{ij} = c_{i1} \cdot c_{ij}.$$

(3.4.5) **Example:** Using the same α as Example 3.4.2,

$$D = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Note that $d_{i1} = c_{i1}$ for all i . The matrix D will always have a least one row of 0's.

(3.4.6) **Theorem:** If the matrices C and D are formed as described above from the special unit $\alpha \in SU$, then we can produce a modified Rédei matrix A as follows:

$$A = C^{\text{tr}} \cdot D.$$

Proof: We need a standard ordered basis $\{e_i\}_{i=1}^n$ for the vector space \mathcal{L} . For $1 \leq i \leq n$ define

$$e_i : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{F}_2 \text{ by}$$

$$e_i(x) = 0 \text{ for all } x \neq i-1 \text{ and } e_i(i-1) = 1.$$

In particular, note that $e_1 = E$. Also, we clearly have

$$e_i \cdot e_j = 0 \text{ for } i \neq j \text{ and}$$

$$e_i \cdot e_i = e_i.$$

Again we write

$$\alpha = \sum_{i=1}^n a_i \sigma^{(i-1)}.$$

Then for the scalar product $\alpha \cdot E$ we have for any $x \in \mathbb{Z}/n\mathbb{Z}$,

$$(\alpha \cdot E)(x) = \sum_{i=1}^n a_i (E(x - (i - 1))).$$

But $E(x - (i - 1)) = e_i(x)$ and recall that $a_i = c_{i1}$. Thus

$$\alpha \cdot E = \alpha \cdot e_1 = \sum_{i=1}^n c_{i1} e_i.$$

Using the (invertible) matrix $C = (c_{ij})$ we have a second ordered basis $\{f_j\}_{j=1}^n$ for \mathcal{L} given by

$$f_j = \sum_{i=1}^n c_{ij} e_i.$$

Then $f_1 = \alpha \cdot E = \alpha \cdot e_1 \in \mathcal{G}$ is the graph generator for $Q(\alpha \cdot E)$. By definition, the modified Rédei matrix $A = (a_{ij})$ is given by

$$(3.4.7) \quad f_1 \cdot f_j = \sum_{i=1}^n a_{ij} f_i.$$

If we write

$$\begin{aligned} f_1 &= \sum_{k=1}^n c_{k1} e_k \\ f_j &= \sum_{k=1}^n c_{kj} e_k \end{aligned}$$

and recalling that

$$e_i \cdot e_j = 0 \text{ for } i \neq j \text{ and}$$

$$e_i \cdot e_i = e_i$$

we see that

$$(3.4.8) \quad f_1 \cdot f_j = \sum_{i=1}^n c_{i1} c_{ij} e_i = \sum_{i=1}^n d_{ij} e_i.$$

We need to express each e_k in terms of the basis $\{f_j\}_{j=1}^n$. We'll need the matrix $C^{-1} = C^{\text{tr}}$. For each k ,

$$e_k = \sum_{i=1}^n c_{ki} f_i.$$

Thus

$$f_1 \cdot f_j = \sum_{i=1}^n \left(\sum_{k=1}^n c_{ki} d_{kj} \right) \cdot f_i.$$

Consequently by comparing 3.4.7 and 3.4.8, we get,

$$a_{ij} = \sum_{k=1}^n c_{ki} d_{kj} = \sum_{k=1}^n c_{ik}^{\text{tr}} d_{kj},$$

which proves the lemma. ■

Note: Since $C^{-1} = C^{\text{tr}}$, we have

$$A = C^{-1} D$$

which is equivalent to

$$(3.4.9) \quad D = CA.$$

Then since A is symmetric,

$$A = A^{\text{tr}} = (C^{-1} D)^{\text{tr}} = D^{\text{tr}} C.$$

However, this implies that

$$A = A^2 = C^{-1} D D^{\text{tr}} C$$

which tells us that A is similar to the matrix $D \cdot D^{\text{tr}}$.

Now from 3.4.9, we derive that

$$(3.4.10) \quad D^{\text{tr}} = A^{\text{tr}} C^{\text{tr}} = AC^{-1}.$$

So,

$$(3.4.11) \quad DD^{\text{tr}} = (CA)(AC^{-1}) = CAC^{-1}.$$

By combining 3.4.9 and 3.4.11, we have the identity

$$(3.4.12) \quad DC^{\text{tr}} = DC^{-1} = CAC^{-1} = DD^{\text{tr}}.$$

To investigate DD^{tr} , we will consider DC^{tr} . Let $DC^{\text{tr}} = (x_{ij})$. So

$$(3.4.13) \quad x_{ij} = \sum_{k=1}^n d_{ik} c_{kj}^{\text{tr}}.$$

Now recall from how D was defined that

$$d_{ik} = c_{i1} c_{ik}.$$

So 3.4.13 becomes

$$(3.4.14) \quad x_{ij} = c_{i1} \cdot \sum_{k=1}^n c_{ik} c_{kj}^{\text{tr}}.$$

But since $C^{-1} = C^{\text{tr}}$, we have $CC^{\text{tr}} = I$. Thus the matrix DD^{tr} is a diagonal matrix with entries $c_{11}, c_{21}, \dots, c_{n1}$. However, recall that for $\alpha \in U$ we wrote

$$\alpha = \sum_{i=1}^n a_i \sigma^{(i-1)},$$

and then defined the matrix C by the identification

$$c_{i1} = a_i.$$

Therefore, DD^{tr} is the diagonalization of the modified Rédei matrix A . Now recall from Definition 1.2.14 that for any graph Γ with Rédei matrix M ,

$$c(\Gamma) = \text{corank}_{\mathbb{F}_2} M - 1.$$

Hence, since the corank of a matrix is simply the number of zeros on the diagonal of its diagonalization and since the modification we make to M to create A removes exactly one zero, to compute the invariant c for any graph, we only need to compute the number of zeros on the diagonal of the diagonalization of its modified Rédei matrix A . This leads us to the following theorem.

(3.4.15) **Theorem:** Let $\alpha = \sum_{i=1}^n a_i \sigma^{(i-1)} \in U$ and let $Q(\alpha E)$ be the associated idempotent formal quotient graph. Then

$$c(Q(\alpha E)) = \text{the number of coefficients } a_i \text{ with } a_i = 0.$$

Proof: Recall that

$$DD^{\text{tr}} = \text{diagonal matrix with entries } a_1, a_2, \dots, a_n$$

and as noted in the discussion above

$$c(Q(\alpha E)) = \text{the number of zeros on the diagonal of } DD^{\text{tr}}.$$

The theorem follows. ■

This makes computing the invariant c for an idempotent formal quotient graph quite easy. We were already able to compute the invariant for a particular idempotent formal quotient graph because the totally disconnected graph on n

vertices has invariant $n - 1$, and this is always a formal quotient graph (which is clearly idempotent). Also, we have seen (see Proposition 3.1.10) that for non-idempotent formal quotient graphs, this invariant is always 0. Therefore we can easily determine the invariant $c(FQ)$ for any formal quotient graph FQ .

Section 5: Summary

We now wish to review what we have. For a formal quotient graph on n vertices, we have some results when

$$n = 11, 13, 17, 19.$$

With the help of a computer, we were also able to determine the size of the automorphism group of the following graphs, and for a couple of graphs we were able to determine the automorphism group (up to isomorphism). Note that the totally disconnected graph on n vertices always has automorphism group S_n .

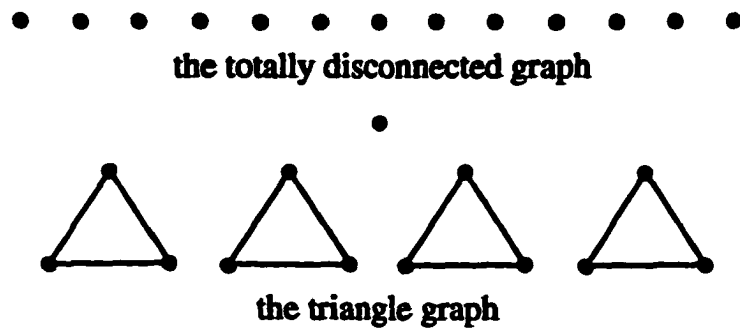
(3.5.1) **Example:** $n = 11$.

For $n = 11$, we have $\#(SU/C_n) = 3$. We found in Example 3.3.1(4) and Example 3.3.5(4) that there are 3 formal quotient graphs with $b = n = 11$ and 2 idempotent formal quotient graphs with $b = 1$. In Section 2.6, we realized all 5 of these graphs. The invariant for the Myers-Turner Graph is 6 and since it is the edge complement to the Petersen Graph (with an additional isolated vertex), we know that its automorphism group is isomorphic to the symmetric group S_5 .

(3.5.2) **Example:** $n = 13$.

For $n = 13$, we have $\#(SU/C_n) = 5$. In Example 3.3.3(1) and Example 3.3.7(1) we found that there are 5 formal quotient graphs with $b = n = 13$ and

2 idempotent formal quotient graphs with $b = 1$. For $b = 1$, the two idempotent formal quotient graphs are the two graphs listed below: the totally disconnected graph on 13 vertices and the graph consisting of 4 triangles and an isolated vertex (called the “triangle graph”).



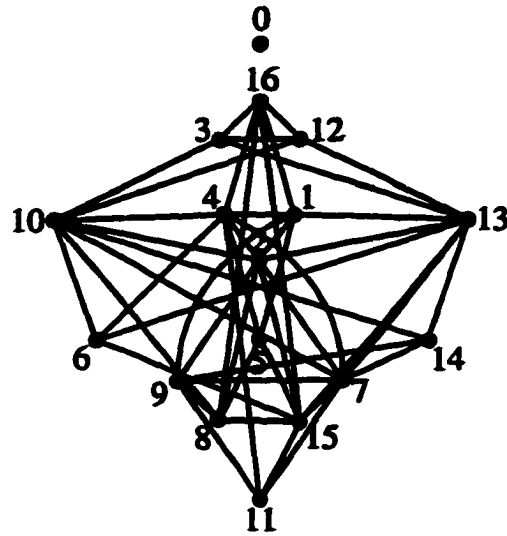
The first prime number $p \equiv 1(26)$ with $b = 1$ is $p = 4421$. This prime generates the triangle graph. The next prime number $p \equiv 1(26)$ with $b = 1$ is $p = 4733$ and was considered in [M]. It also generated the triangle graph. In fact we have checked, with the aid of a computer, the first 900 primes (up to $p = 6997$) and we have yet to find a prime which generates the totally disconnected graph on 13 vertices. So we do not yet know if this formal quotient graph is actually an honest quotient graph. The invariant for the triangle graph is 4. The automorphism group is isomorphic to $S_3 \times S_3 \times S_3 \times S_3 \times S_4$.

(3.5.3) **Example:** $n = 17$.

For $n = 17$, we have $\#(SU/C_n) = 17$. We determined in Example 3.3.3(2) and Example 3.3.7(2) that there are 17 formal quotient graphs with $b = n = 17$ and 2 idempotent formal quotient graphs with $b = 1$. The two idempotent formal quotient graphs are the two graphs listed below: the totally disconnected graph on 17 vertices and the other graph (which we will call the “diamond graph”).



the totally disconnected graph



the diamond graph

The first prime number $p \equiv 1(34)$ with $b = 1$ is $p = 1429$. This prime generates the diamond graph, and again after checking the first 800 primes (up to $p = 6133$), we have not yet found a prime which generates the totally disconnected graph on 17 vertices. So the question as to whether or not the totally disconnected graph on 17 vertices is an honest quotient graph is still unanswered. The invariant for the diamond graph is 8. We do not know what the automorphism group is, but with the aid of a computer, we have determined that it only has 4 elements. Further study is certain to determine which group with 4 elements it is isomorphic to.

(3.5.4) **Example:** $n = 19$.

For $n = 19$, we have $\#(SU/C_n) = 27$. From Example 3.3.3(3) and Example 3.3.7(3) we have that there are 27 formal quotient graphs with $b = n = 19$ and 4

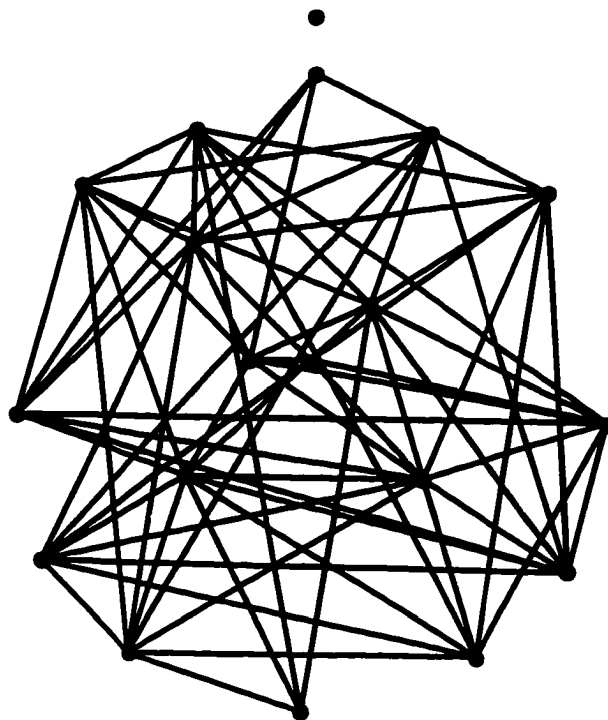
idempotent formal quotient graphs with $b = 1$. The 4 idempotent formal quotient graphs are the following:

(1)

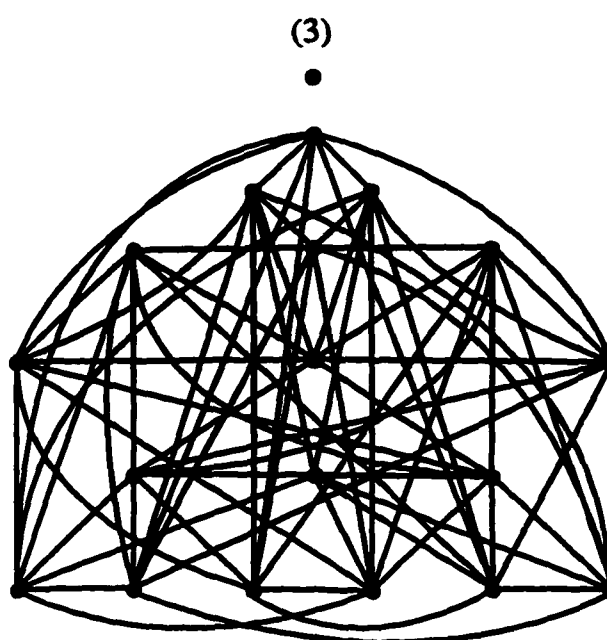


(1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)

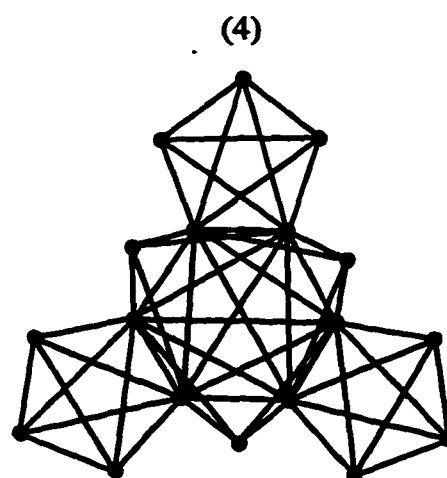
(2)



(1,0,0,0,0,0,0,1,1,0,0,0,1,1,1,1,0,1)



(1,0,0,0,0,1,0,1,0,1,1,1,1,0,0,1,0,0,1)



(1,0,0,0,1,1,0,1,1,1,1,1,1,0,0,1,1,1,1)

Each graph is labeled with the special unit which produced it. To determine the 4 idempotent formal quotient graphs on 19 vertices, we utilized a computer to aid in finding the special units in $F_2[C_{19}]$. Then we determined the 27 distinct conjugacy classes of special units. These are listed in the Appendix. Once we generated the 27 (not necessarily distinct) idempotent formal quotient graphs

from these units, we then used the natural isomorphisms of the group ring to reduce the number of *distinct* graphs to 4. This is the first example with more than 2 distinct idempotent formal quotient graphs.

We know the first prime number $p \equiv 1(38)$ with $b = 1$ is $p = 1103$. This prime generates graph (2). The invariant of each graph again can be easily determined using Theorem 3.4.15. They are respectively: 18, 10, 10, 6. Graphs (3) and (4) have automorphism groups of size 18 and 10,368 (respectively), yet again, we do not know what the groups are. What about graph (2)? As “ugly” as it is, it certainly should not have many automorphisms, and in fact it has only 1, the trivial one.

BIBLIOGRAPHY

- [BW] Beineke, L.W. and Wilson, R.J., *Graph Connections: Relationships Between Graph Theory and other Areas of Mathematics*, Oxford Science Publ., Clarendon Press, Oxford (1997).
- [Bi1] Biggs, N., *Finite Groups of Automorphisms*, Cambridge University Press, London (1971).
- [Bi2] Biggs, N., *Algebraic Graph Theory*, Cambridge University Press, London (1993).
- [Bo] Bollabás, B., *Random Graphs*, Academic Press, London (1985).
- [BM] Bondy, J.A. and Murty, U.S.R., *Graph Theory with Applications*, Macmillan Press, New York (1979).
- [Bu1] Burnside, W., On Simply Transitive Groups of Prime Degree, *Quar. J. Math.* **37** (1906), 215-221.
- [Bu2] Burnside, W., On Some Properties of Groups of Odd Order, *J. London Math. Soc.* **33** (1900), 162-185.
- [CH] Conner, P.E. and Hurrelbrink, J., *Class Number Parity*, Series in Pure Math. Vol. 8, World Scientific Publishing, Singapore (1988).
- [D] Dobson, E., *Some Problems in Algebraic and Extremal Graph Theory*, dissertation, Louisiana State University (1995).
- [FT] Fröhlich, A. and Taylor, M.J., *Algebraic Number Theory*, Cambridge Stud. in Adv. Math. Vol. 27, Cambridge University Press, Cambridge (1991).
- [G] Gauss, C.F., *Disquisitiones Arithmeticae*, Yale University Press, New Haven (1966).
- [H-K] Halter-Koch, F., Über den 4-Rank der Klassengruppe quadratischer Zahlkörper, *J. Number Theory* **19** (1984), 219-227.
- [Hi] Hilbert, D., Über die Zerlegung der Ideale eines Zahlkörpers in Primideale, *Math. Annalen* **44** (1894), 1-8.

- [Ho] Hoffman, W., *Elliptic Curves, Modular Forms and Galois Groups*, notes (1992)
- [HS] Holton, D.A. and Sheehan, J., *The Petersen Graph*, Cambridge University Press, Cambridge (1993).
- [Hun] Hungerford, T., *Algebra*, Graduate Texts in Math. Vol. 73, Springer-Verlag, New York (1989).
- [Hur] Hurrelbrink, J., *Circulant Graphs and 4-Ranks of Ideal Class Groups*, *Can. J. Math.* (1994).
- [IR] Ireland, K. and Rosen, M., *A Classical Introduction to Modern Number Theory*, Graduate Texts in Math. Vol. 84, Springer-Verlag, New York (1990).
- [K] Kingan, R., *Tournaments and Ideal Class Groups*, dissertation, Louisiana State University (1992).
- [Lag] Lagarias, J.C., *On Determining the 4-Rank of the Ideal Class Group of a Quadratic Number Field*, *J. Number Theory* 12 (1980), 191-196.
- [Lan1] Lang, S., *Algebraic Number Theory*, Graduate Texts in Math. Vol. 110, Springer-Verlag, New York (1986).
- [Lan2] Lang, S., *Cyclotomic Fields*, Graduate Texts in Math. Vol. 59, Springer-Verlag, New York (1978).
- [M] Myers, L.A., *Graphs in Number Theory*, dissertation, Louisiana State University (1994).
- [Re1] Rédei, L., *Arithmetischer Beweis des Satzes über die Anzahl der durch 4 teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper*, *J. reine angew. Math.* 171 (1934), 55-60.
- [Re2] Rédei, L., *Eine obere Schranke der Anzahl der durch 4 teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper*, *J. reine angew. Math.* 171 (1934), 61-64.
- [RR] Rédei, L. and Reichardt, H., *Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, *J. reine angew. Math.* 170 (1933), 69-74.

- [Ro] Rose, H.E., *A Course in Number Theory*, Oxford Science Publ., Clarendon Press, Oxford (1988).
- [U] Uehara, T., On the 4-Rank of the Narrow Ideal Class Group of a Quadratic Field, *J. Number Theory* **31** (1989) 167-173.
- [W] Weil, A., Number of Solutions of Equations in a Finite Field, *Bull. Amer. Math. Soc.* **55** (1949), 497-508.

APPENDIX

The following is a list of the coefficients of the 27 non-conjugate special units in $\mathbb{F}_2[C_{19}]$. Elements of the group ring $\mathbb{F}_2[C_{19}]$ can be expressed in the following form:

$$\alpha = \sum_{i=0}^{18} a_i \sigma^i.$$

To express a unit, simply write a sum of powers of the generator of C_{19} , σ to all the powers indicated. For example,

$$\alpha_2 = 1 + \sigma^7 + \sigma^8 + \sigma^{12} + \sigma^{13} + \sigma^{14} + \sigma^{15} + \sigma^{16} + \sigma^{18}$$

Special Units for $n = 19$

$$\alpha_1 = (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$$

$$\alpha_2 = (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$$

$$\alpha_3 = (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$$

$$\alpha_4 = (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$$

$$\alpha_5 = (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$$

$$\alpha_6 = (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$$

$$\alpha_7 = (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$$

$$\alpha_8 = (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$$

$$\alpha_9 = (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$$

$$\alpha_{10} = (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$$

$$\alpha_{11} = (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$$

$$\alpha_{12} = (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$$

$$\alpha_{13} = (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$$

$$\alpha_{14} = (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$$

$$\alpha_{15} = (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$$

$$\alpha_{16} = (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$$

$$\alpha_{17} = (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$$

$$\alpha_{18} = (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$$

$$\alpha_{19} = (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$$

$$\alpha_{20} = (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$$

$$\alpha_{21} = (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$$

$$\alpha_{22} = (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$$

$$\alpha_{23} = (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$$

$$\alpha_{24} = (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$$

$$\alpha_{25} = (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$$

$$\alpha_{26} = (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$$

$$\alpha_{27} = (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$$

By considering the automorphisms of the group ring, we see that these 27 units will yield 4 non-isomorphic idempotent formal quotient graphs. The four classes are represented by the units α_1 , α_2 , α_9 , and α_{22} .

VITA

Brian Heck was born in Boulder, Colorado on December 18, 1967. He graduated in May 1990 from McMurry College with a Bachelor of Science degree in mathematics. He received his Master of Science degree in mathematics from Louisiana State University in May 1994 and is currently a candidate for the doctoral degree in mathematics at Louisiana State University.

DOCTORAL EXAMINATION AND DISSERTATION REPORT

Candidate: Brian Heck

Major Field: Mathematics

Title of Dissertation: Graphs and Number Theory

Approved:

J. Hurrelbrink
Major Professor and Chairman

John W. Larkin
Dean of the Graduate School

EXAMINING COMMITTEE:

Rose E. Conner

Bogdan Oprea

Robert Puri

E. Feneberg

P. Arlin

Matt Field

Date of Examination:

April 3, 1997