A structural approach to the endomorphisms of certain abelian groups

Ben-Eben de Klerk

September 2016

MATM9100
A structural approach to the endomorphisms of certain abelian groups

Ben-Eben de Klerk
2008047041

Dissertation towards the fulfilment of the requirements for the Degree of Doctor of Philosophy.

Faculty of Natural and Agricultural Sciences
Department of Mathematics and Applied Mathematics
University of the Free State
Supervisor: Prof J.H. Meyer
September 2016

Abstract:

Given a set S, and any selfmap $f : S \to S$, the functional graph associated with f can be described as a graph with vertex set S and directed edge set $E = \{(u, v) \in S^2 : f(u) = v\}$. A classification of all functional graphs induced by lattice endomorphisms has recently been done by J. Szigeti ([12]). In this dissertation, we aim to achieve a similar type of classification with respect to functional graphs induced by endomorphisms on certain abelian groups.

A method for finding all functional graphs that can be induced by endomorphisms of a group has been developed for all groups of the form $\mathbb{Z}_p^n$ with p any prime, $n \in \mathbb{N}$, and $\mathbb{Z}^n$ for any $n \in \mathbb{N}$, as well as all cyclic groups.

A deep connection between the functional graphs corresponding to group endomorphisms and the minimal polynomial of the matrix representation of the group endomorphism has been found.

Opsomming:

Gegewe 'n versameling S, en enige selfafbeelding $f : S \to S$, kan die funksionele grafiek geassosieer met f beskryf word as die grafiek met nodus versameling S en gerigte randversameling $E = \{(u, v) \in S^2 : f(u) = v\}$. 'n Klassifikasie van alle funksionele grafieke wat deur tralie endomorfismes geinduseer word, was onlangs deur J. Szigeti gedoen ([12]). In hierdie verhandeling beoog ons om 'n soortgelyke tipe klassifikasie te bekom met betrekking tot die funksionele grafieke wat deur endomorfismes van sekere abelse groepe geinduseer word.

'n Metode vir die bepaling van alle funksionele grafieke wat geïnduseer word deur endomorfismes van 'n groep is ontwikkel vir alle groepe van die vorm $\mathbb{Z}_p^n$ met p enige priem, $n \in \mathbb{N}$, en $\mathbb{Z}^n$ vir enige $n \in \mathbb{N}$, sowel as alle sikliese groepe.

'n Belangrike verband tussen die funksionele grafieke wat ooreenstem met groep endomorfismes en die minimale polinoom van die matriks voorstelling van die endomorfisme is gevind.

Key terms:

Abelian Group, Automorphism, Endomorphism, Conjugacy classes, Finite Field, Functional graph, Cyclotomic Polynomial, Minimal Polynomial, Tree

Declaration:

1. I, Ben-Eben de Klerk (2008047041), declare that the thesis that I herewith submit for the Doctoral Degree in Mathematics at the University of the Free State, is my independent work, and that I have not previously submitted it for a qualification at another institution of higher education.

2. I hereby declare that I am aware that the copyright is vested in the University of the Free State.

3. I declare that all royalties as regards intellectual property that was developed during the course of and/or in connection with the study at the University of the Free State, will accrue to the University.

Signature: .....

Date: .....

Acknowledgements:

Firstly, I would like to thank my supervisor, Prof. Johan Meyer, for the time, guidance and effort that he had put into carefully reading through my dissertation. I am truly thankful for the ideas and suggestions as well as tremendous effort put into improving the readability and clarity of the dissertation.

Thanks to Prof. Leon van Wyk, as well as Prof. Jeno Szigeti, who, together with my supervisor, first introduced me to the ideas which eventually condensed and emerged as this dissertation.

I would also like to thank all the staff members of my department, not only for being excellent teachers throughout my undergraduate degree but also for their support over the past few years as colleagues. Special mention should go to Mr. Renier Jansen, for so many tremendously enjoyable conversations, and not only for those which beared fruit, but also those that didn't.

Also, thank you to my fiancée, Jireh Smit, towards whom I am grateful for all the love, kindness and friendship throughout the past 7 years. You have made my life immeasurably richer. I would also like this opportunity to thank her parents, Sampie and Bea for always being willing to help out and support whenever needed.

I would like to thank my family for their love and encouragement, especially my grandmother, Kitty, my sister, Corli-Mari, my mother, Tiekie and lastly, my late father Eben, who kindled an undying passion for science and mathematics within me. This work is dedicated to you dad.

Contents

Why are numbers beautiful? It's like asking why is Beethoven's Ninth Symphony beautiful. If you don't see why, someone can't tell you. I know numbers are beautiful. If they aren't beautiful, nothing is.

$\sim$ P. Erdös (1913-1996)

1 Introduction

One of the most important concepts in mathematics is undoubtedly that of structure. Sets in general do not possess any structure except for the inclusion of its elements. The introduction of internal structure on a set leads to very rich mathematics. We will briefly name a few examples:

1. The concept of an open set structure gives rise to topology which defines continuity, compactness and eventually even leads to the mathematical backbone of Calculus.

2. The concept of structures defined by binary operations gives rise to group theory, ring theory, field theory which leads to vector spaces and linear algebra.

3. The concept of imposing an order structure on a set naturally leads to the concept of posets, boolean algebras, frames etc.

All of the examples mentioned above motivate why structural embedding on a set is of fundamental importance in mathematics. Through structural embedding we form the class of all sets, all topological spaces, all groups, all graphs etc. It is only through the introduction of a structure on an underlying set that mathematics becomes truly rich.

This dissertation started off as a research project done by JH Meyer, L van Wyk, J Szigeti and myself in 2013, made possible by a joint research grant between the NRF and Hungary.

The question that we investigated back then was: Given a set S and a bijective function $f : S \to S$, when can an abelian group $\hat{S}$ with underlying set S be found such that f is an automorphism?

In this dissertation, a function with this property will be said to possess the **Automorphism property**.

In essence, this amounts to enriching the internal structure of the set S to that of an abelian group, in such a way that f is not only a bijection but actually an automorphism. In [12] a similar question was posed for lattices rather than abelian groups.

Sections 2 and 3 of this dissertation take care of most of the background that will be used throughout this dissertation. Feel free to use it only as reference if you are already familiar with basic algebraic terminology.

Section 4 concentrates on subject specific background needed for this project.

Sections 5 through 8 contain most of our earlier results which centred on structures in which the underlying groups are finite cyclic or have p^2 members for some prime p. Many of these results can be obtained with much greater ease using the high-powered results of the later sections 10 and 11, but we decided to include these sections as not only do they provide an alternative view on the project but, in a sense, the shortcomings of these early attempts formed the drive behind much of what followed after them.

In section 9, we turn our attention towards infinite groups, and in this section the first connection between the automorphism property and minimal polynomials (and in particular cyclotomic polynomials) are glimpsed.

Sections 10 and 11 exploit the connection noted in section 9, which then leads to a complete classification of all functions with the automorphism property, with underlying group $\mathbb{Z}^n$ or $\mathbb{Z}_p^n$, for a natural number n and a prime p.

Sections 12 and 13 expand on the results of sections 10 and 11 by relaxing the bijection restriction, and looking at endomorphisms in general rather than just automorphisms.

The scientist does not study nature because it is useful; he studies it because he delights in it, and he delights in it because it is beautiful.

$\sim$ H. Poincare (1854-1912)

2 Structures

The structures that we will mainly be interested in in this thesis are groups. However in order to prove many of our theorems, we shall see a delicate interplay between groups, rings, modules, vector spaces and graphs. It is truly breath-taking to see how these concepts all interlock and interact with one another.

This section is thus dedicated towards establishing the definitions and concepts that will be required to prove some of our main results later. If you are already familiar with these concepts feel free to skip this section, and refer back to it only if necessary*.

In order to compare different instances of the same type of structure, we shall introduce the notion of an isomorphism:

Definition 2.1: Isomorphism, homomorphism

A bijective function between two elements which preserves the defining properties of the structural class is called an **Isomorphism**. Typically, if the name of the structure class that is being considered is $\mathbb{A}$, it's isomorphisms shall be referred to as $\mathbb{A}$-isomorphisms.

An $\mathbb{A}$-homomorphism is defined in exactly the same way as an isomorphism, but with the requirement of f being a bijection dropped.

To each of the structures that will be discussed, it will be clearly stated what we mean by an isomorphism for the particular structure.

Definition 2.2: Group

A **group** $(G, \cdot_G)$ consists of a set G endowed with a binary operation $\cdot_G$ which satisfies the following group axioms:
For all α, β, γ in G :

1. Closure: $\alpha \cdot_G \beta \in G$.
2. Associativity: $\alpha \cdot_G (\beta \cdot_G \gamma) = (\alpha \cdot_G \beta) \cdot_G \gamma$.
3. Identity: $\exists 1_G \in G$ such that $1_G \cdot_G \alpha = \alpha \cdot_G 1_G = \alpha$. 1_G is called the identity of G.
4. Inverses: $\forall \alpha \in G, \exists \alpha^{-1} \in G$ with $\alpha \cdot_G \alpha^{-1} = \alpha^{-1} \cdot_G \alpha = 1_G$. α^{-1} is called the inverse of α.

*We shall only work with rings with unity and only consider left modules.

5. $(G, \cdot_G)$ is called abelian if $\alpha \cdot_G \beta = \beta \cdot_G \alpha$.

If there is no danger of confusion, the group $(G, \cdot_G)$ will simply be denoted by G, and we will simply say that G is a group. The binary operation $\cdot_G$ will dropped in favour of juxtaposition, meaning $\alpha \cdot_G \beta$ will simply be denoted by $\alpha\beta$.

For abelian groups we will often denote the binary operation using a + symbol, denote the identity by 0, as well as referring to the inverse of each element as it's negative.

$(N, \cdot_N)$ is called a **subgroup** of $(G, \cdot_G)$ if $N \subseteq G$, $\cdot_N$ is the restriction of $\cdot_G$ to N and $1_G = 1_N$.

A *group isomorphism* is defined by:

Definition 2.3: **Group isomorphism**

For groups A, B and bijective $f : A \to B$, f is called a **group isomorphism** if

$$f(a \cdot_A b) = f(a) \cdot_B f(b)$$

for all $a, b \in A$, with $\cdot_X$ the binary operation on group X. Two groups are said to be isomorphic if there exists an isomorphism between them.

Note that throughout this essay, the $\cdot_X$ will be dropped in favour of juxtaposition, meaning the equation above would simply be written as

$$f(ab) = f(a)f(b)$$

where it should be understood that ab is the invocation of the binary operator of A on (a, b) and $f(a)f(b)$ is the invocation of the binary operator of B on $(f(a), f(b))$.

Example 2.4: The integers with the usual addition operator is an abelian group, $(\mathbb{Z}, +)$, with identity 0. The negative of each element a in this group is simply $-a$ in the usual sense.

Example 2.5: The set of integers modulo n under modular addition is a group, $(Z_n, +)$, with identity 0.

Definition 2.6: **Group (endo)auto-morphism**

Given any group G, a group homomorphism from G into itself is called an **Endomorphism**. An isomorphism from G to itself is called an **Automorphism**. For any abelian group G, the collection of all automorphisms of G forms a group under function composition, called the **Automorphism group** of G, denoted by $Aut(G)$. The identity element of this group is the identity map on G, and the inverse of any automorphism is simply it's map inverse on the underlying set.

Definition 2.7: **Direct product of groups**

Given a collection of groups $S = \{G_i\}_{i \in I}$ indexed by a set I, the **direct product** of S, denoted by

$$\prod_{i \in I} G_i$$

is the Cartesian product of S, with the binary operator acting component-wise, meaning for each $x, y \in \prod_{i \in I} G_i$, with components x_j and y_j in G_j for each $j \in I$, xy is defined by $(xy)_j = x_j y_j$. The identity of the direct product group is simply the element in the Cartesian product with $j-th$ component the identity of G_j for each $j \in I$.

For finite index sets $I = \{1, 2, \ldots, n\}$, the direct product of $\{G_i\}_{i \in I}$ could also be denoted by $G_1 \times G_2 \times \ldots \times G_n$.

Example 2.8: The direct product of $\{\mathbb{Z}_2, \mathbb{Z}_3\}$, denoted by $Z_2 \times Z_3$, consists of the elements $\{(0,0); (0,1); (0,2); (1,0); (1,1); (1,2)\}$ together with component-wise modular addition, for example $(1,2) + (0,2) = (1,1)$. It can easily be verified that the homomorphism $\phi : \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$ with $\phi : 1 \mapsto (1,1)$ is indeed a group isomorphism.

A ring is in some sense an extension of the concept of a group, with two interacting binary operators. The one operator endows the ring with the structure of an abelian group, and the other being a generalized type of multiplication.

Definition 2.9: **Ring**

A **Ring**, $(R, +, \cdot)$ with $+$ and $\cdot$ binary operators on R, is a structure for which $(R, +)$ is an abelian group, but additionally satisfies the following axioms for all $a, b, c \in R$:

1. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
2. $\exists 1 \in R$ such that $1 \cdot a = a \cdot 1 = a$.
3. $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$.

For rings, the $+$ operation will be called the ring addition operator, and the $\cdot$ operation will be referred to as the multiplication operator. If there is no danger of confusion, the $\cdot$ will be left out. The first axiom simply states that the multiplication operator is associative. The second states the existence of a multiplicative unity. Some authors do not demand the existence of a multiplicative unity (or identity), yet in this thesis it shall be a very convenient property to retain. The third axiom states that the multiplicative operator distributes over the addition operator from the left as well as from the right.

If it is clear from the context, the ring $(R, +, \cdot)$ will simply be denoted by R.

A **subring** S, of a ring R, is a subset of R which is closed under the operations of R, closed under additive inverses, as well as containing the identity element

of R.

Definition 2.10: Endomorphism ring

The set of all endomorphisms on an abelian group $(G, +)$ forms a ring under the operators of addition and composition, called the **endomorphism ring** of G. This group is denoted by $End(G)$.

Since a ring has two defining binary operations, it is natural to expect ring homomorphisms to preserve them, as well as preserving the multiplicative identity:

Definition 2.11: Ring isomorphisms

For rings A, B and bijective $f : A \to B$, f is called a **Ring isomorphism** if

$$f(a + b) = f(a) + f(b)$$
$$f(ab) = f(a)f(b)$$

for all $a, b \in A$, and

$$f(1_A) = 1_B.$$

Two rings are called isomorphic if there exists an isomorphism between them.

Example 2.12: The set of integers endowed with normal addition and multiplication is a ring, denoted by $(\mathbb{Z}, +, \cdot)$. The additive group structure is clearly the same as discussed in Example 2.4, and the multiplicative identity is 1.

One particular property that is easily taken for granted because of our familiarity with it in $\mathbb{R}$ is the assumption that for any two $a, b \in R$, $ab = 0 \Rightarrow a = 0$ or $b = 0$. General rings however do not have this property, and it is important to make distinctions between rings that do and those that do not.

Definition 2.13: Zero divisor

An element a of a ring R is called a **zero divisor** of R if $\exists b \in R - \{0\}$ such that $ab = 0$ or $ba = 0$.

Definition 2.14: Integral domain

A commutative ring with $0 \neq 1$ and with no zero divisors is called an **integral domain**.

Definition 2.15: Field

A commutative ring with $0 \neq 1$ and in which all non-zero elements have multiplicative inverses, is called a **field**.

All fields are clearly integral domains.

Example 2.16: The integers modulo n endowed with the usual modular addition and multiplication (denoted by $\mathbb{Z}_n$) is clearly a ring with additive identity 0 and unity 1. For composite n however, each $d \neq 1$, dividing n is clearly a zero divisor, as $d\frac{n}{d} = 0$. If n is prime, an application of Fermat's little Theorem shows that for any non-zero $a \in \mathbb{Z}_n$, a^{n-2} is the multiplicative inverse of a. It consequently follows that $\mathbb{Z}_n$ is a field iff n is prime.

Example 2.17: The two by two matrices with entries from $\mathbb{Z}$ with binary operators matrix addition and multiplication is a ring with additive identity $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and multiplicative identity $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.
Since $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ it follows that $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ is a zero divisor.
The set $\left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} : a \in \mathbb{Z} \right\}$ is a subset of the set of all two by two matrices with entries from $\mathbb{Z}$ which does form a ring with the same binary operations. However, the multiplicative identity of this ring is $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, meaning that it is not a subring of the ring of all two by two matrices over $\mathbb{Z}$ even though it is a ring strictly contained in it.

Example 2.18: The set of all $n \times n$ matrices over any ring R with usual matrix addition and multiplication is a ring, called the **n × n matrix ring over** R and is denoted by $M_n(R)$. The additive identity is called the zero matrix ($\mathbf{0}$) which is the $n \times n$ matrix with all entries equal to 0, and the multiplicative identity ($\mathbf{I}$) is simply called the $n \times n$ identity matrix, which has all its entries equal to zero, except for those along the main diagonal which are equal to 1.

Given any matrix M, we shall denote the entry located in the i-th row and j-th column by $[M]_{ij}$.

Later in this thesis we shall devote quite a bit of our attention to groups of the form X^n for some group X and positive integer n. It will become clear that a very natural way of handling these groups is via the notion of a module;

Definition 2.19: Module

Given a ring R and an abelian group $(M, +)$. M is called an **R-module** if there exists a scalar multiplication $\mu : R \times M \to M$, simply denoted by $\mu(r, m) = rm$ for all $r \in R$ and $m \in M$, such that for all $r, r_1, r_2 \in R$ and all $m, m_1, m_2 \in M$ the following axioms hold:

1. $r(m_1 + m_2) = rm_1 + rm_2$
2. $(r_1 + r_2)m = r_1m + r_2m$
3. $r_1(r_2m) = (r_1r_2)m$

4. $1_R m = m$

The R-module M will be denoted by ${}_R M$. Technically a module defined in this manner is called a left R-module as the action of R on the elements of M is exclusively from the left. It is possible to define a similar notion with R acting on M from the right, which will constitute a right $R-$ module. In this thesis we shall only work with left $R-$ modules which means that when we refer to an R-module, we mean left R-module.

Definition 2.20: Module isomorphisms

Given R-modules ${}_R M$ and ${}_R N$. A bijective function $f : {}_R M \to {}_R N$ is called an **R-module isomorphism** if for all $r \in R$ and $m, m_1, m_2 \in M$ the equalities

1. $f(rm) = rf(m)$
2. $f(m_1 + m_2) = f(m_1) + f(m_2)$

hold.

Definition 2.21: Free module

A R-module M is called a free module if there exists a subset $X \subseteq M$ such that each element $m \in M$ can be expressed uniquely as a finite sum $m = \sum_{i=1}^{n} a_i x_i$, with $a_i \in R$ and distinct $x_i \in X$ for all $i \in \{1, 2, \ldots, n\}$. The set X is called a base of ${}_R M$

Example 2.22: For any integers m, n, the group $\mathbb{Z}_m^n$ is a free $\mathbb{Z}_m$-module with scalar multiplication given by $\alpha(x_1, x_2, \ldots, x_n) = (\alpha x_1, \alpha x_2, \ldots, \alpha x_n)$. We define $e_i = (0, 0, \ldots, 0, 1, 0, \ldots, 0)$ with the 1 in the $i-$th component. It is clear that the set $\{e_1, e_2, \ldots, e_n\}$ forms a base of ${}_{\mathbb{Z}_m}\mathbb{Z}_m^n$.

Definition 2.23: Vector space, linear transformation

A module over a field F is called a **vector space** over F. An F-module homomorphism $f : {}_F M \to {}_F N$ is called a **linear transformation** from ${}_F M$ to ${}_F N$.

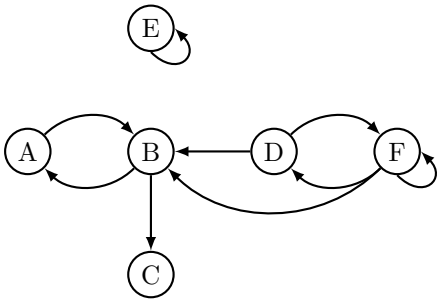
Example 2.24: We know from Example 2.16 that $\mathbb{Z}_p$ is a field iff p is prime, and from Example 2.22 it follows that Z_p^n is a vector space over Z_p .

The next type of structure that we will consider is a *graph*:

Definition 2.25: (Directed-)graph

A **directed-graph** $\mathcal{G} = (V, E)$ consists of a set V, called the vertices, and E, called the edges, which is a binary relation on V. We say that vertex $a \in V$ is connected to $b \in V$ by an edge iff $(a, b) \in E$. $\mathcal{G}$ is called a **graph**, or undirected graph, if E is symmetric, meaning if a is connected to b, then b is connected to a.

Example 2.26: Suppose $V = \{A, B, C, D, E, F\}$, and $E = \{(A, B), (B, A), (B, C), (D, B), (D, F), (F, D), (F, F), (E, E), (F, B)\}$ is a relation on V. We can graphically depict the directed graph $\mathcal{G} = (V, E)$, by:



A *graph isomorphism* is defined as:

Definition 2.27: **Graph isomorphism**

For any two graphs $\mathcal{G} = (V_1, E_1), \mathcal{H} = (V_2, E_2)$ and bijective $f : V_1 \to V_2$, f is called a **graph isomorphism** if

$$(a, b) \in E_1 \Leftrightarrow (f(a), f(b)) \in E_2.$$

Two graphs are called isomorphic if there exists a graph isomorphism between them.

Mathematics, rightly viewed, possesses not only truth, but supreme beauty - a beauty cold and austere, like that of sculpture, without appeal to any part of our weaker nature, without the gorgeous trappings of paintings or music, yet sublimely pure and capable of a stern perfection such as only the greatest art can show.

$\sim$ B. Russell (1872-1970)

3 Number theoretic functions

During our investigations in the subsequent sections, we shall often encounter functions defined from the set of natural numbers to the reals, for which $f(n)$ expresses some arithmetical property of n. These are called **number theoretic functions**. In this section we shall look at some number theoretic functions which are of use later on in this thesis as well as some results related to them.

Definition 3.1: **Multiplicative**

A number theoretic function f is called **multiplicative** if for all relatively prime * a, b, $f(ab) = f(a)f(b)$.

For any multiplicative function f and distinct primes $p_1, p_2, \ldots, p_k$, it is clear that $f\left(\prod_{i=1}^{k} p_i^{\alpha_i}\right) = \prod_{i=1}^{k} f(p_i^{\alpha_i})$ for all non-negative integers α_i. This allows for a quick evaluation of f at any integer n, if the value of f is known at all powers of primes.

Definition 3.2: **Euler totient function**

The **Euler totient function**, denoted by $\varphi(n)$ is the number of positive integers not greater than n, which are relatively prime to n.

Example 3.3: The only integer not greater than 1 which is relatively prime to 1 is 1, so $\varphi(1) = 1$. The set of all positive integers not greater than 15 that are relatively prime to 15 is $\{1, 2, 4, 7, 8, 11, 13, 14\}$, and thus $\varphi(15) = 8$. For any prime p, $\varphi(p) = p - 1$.

Example 3.4: The **Möbius function**, denoted by μ, is defined by:

$$\mu(n) = \begin{cases} 1 \text{ if } n = 1 \\ 0 \text{ if } p^2 | n \text{ for some prime } p. \\ (-1)^r \text{ if } n = p_1 p_2 \ldots p_r \text{ for distinct primes } p_1, p_2, \ldots, p_r. \end{cases}$$

*meaning $\gcd(a, b) = 1$

Lemma 3.5: ([6], Theorem 7.2) φ is multiplicative.

Proof:
Given any two relatively prime integers m and n, we can list the numbers $1, 2, \ldots, mn$ into an $n \times m$ array as follows:

$$\begin{array}{ccccccc} 1 & 2 & \ldots & r & \ldots & m \\ m+1 & m+2 & \ldots & m+r & \ldots & 2m \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ (n-1)m+1 & (n-1)m+2 & \ldots & (n-1)m+r & \ldots & mn \end{array}$$

$\varphi(mn)$ is the number of positive integers not larger than mn which are relatively prime to mn. These are precisely the positive integers which are relatively prime to both m and n. Since $\gcd(mk+r, m) = \gcd(r, m)$, it follows that $mk+r$ is relatively prime to m iff r is relatively prime to m, from which it follows that all positive integers not larger than mn which are relatively prime to m are those be found in any of the $\varphi(m)$ columns with top element r with $\gcd(r, m) = 1$. The set of all integers in the $r-$th column is $\{r, m+r, 2m+r, \ldots, (n-1)m+r\}$. Suppose two of these integers, say $mi + r$ and $mj + r, i \neq j$, were congruent modulo n, then $mi \equiv_n mj$, but since $\gcd(m, n) = 1$, it follows that $i \equiv_n j$, which is clearly a contradiction. Hence the integers in the $r-$th column is a rearrangement of $\{0, 1, 2, \ldots, n-1\}$ modulo n, from which it follows that there are $\varphi(n)$ of them relatively prime to n. There are thus $\varphi(n)$ integers in each of $\varphi(m)$ rows which are relatively prime to mn, from which it follows that $\varphi(mn) = \varphi(m)\varphi(n)$. □

Lemma 3.6: ([6], Theorem 7.3) For any integer n with prime factorization $\prod_{i=1}^{k} p_i^{\alpha_i}, \alpha_i > 0$,

$$\varphi(n) = \prod_{i=1}^{k} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right)$$

Proof:
For any prime p, the positive integers less than or equal to p^α which are not relatively prime to p^α are exactly the multiples of p less than or equal to p^α. There are $\frac{p^\alpha}{p} = p^{\alpha-1}$ of these, thus $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$. From Lemma 3.5 it follows that $\varphi(n) = \prod_{i=1}^{k} \left(p_i^{\alpha_i} - p_i^{\alpha-1}\right)$. □

Theorem 3.7: ([6], Theorem 6.8) For any multiplicative number theoretic function f, the function S_f, defined by $S_f(n) = \sum_{d|n} f(d)$ is multiplicative.

Proof:
For any relatively prime positive integers m and n,

$$\begin{aligned} S_f(mn) &= \sum_{d|mn} f(d) \\ &= \sum_{d_1|m, d_2|n} f(d_1 d_2) \\ &= \sum_{d_1|m, d_2|n} f(d_1) f(d_2) \\ &= \sum_{d_1|m} f(d_1) \sum_{d_2|m} f(d_2) \\ &= S_f(m) S_f(n). \end{aligned}$$

The second step uses the fact that each d dividing mn can be uniquely expressed as a product of d_1 dividing m and d_2 dividing n. □

A useful consequence of this was found by the great German mathematician C.F. Gauss:

Lemma 3.8: For any integer n,

$$\sum_{d|n} \varphi(d) = n.$$

Proof:
Since φ is multiplicative, so is S_φ, so it is sufficient to prove the result for all powers of primes. For any prime p,

$$\begin{aligned} S_\varphi(p^\alpha) &= \sum_{d|p^\alpha} \varphi(d) \\ &= \varphi(1) + \sum_{i=1}^{\alpha} \left(p^i - p^{i-1}\right) \\ &= 1 + (p-1) + \left(p^2 - p\right) + \ldots + \left(p^\alpha - p^{\alpha-1}\right) \\ &= p^\alpha. \end{aligned}$$

□

The Möbius inversion formula provides us with a method to recover f from S_f. The proof of this Theorem is quite elementary, and can be found in almost any introductory textbook on number theory. Since the proof itself is not of much importance in this thesis, the result will only be stated here. The interested reader may find a proof in [6].

Theorem 3.9: The Möbius inversion formula

For any number theoretic function f,

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) S_f(d)$$

with μ the Möbius function as defined in Example 3.4. □

One generalization of the Euler totient function is the Jordan totient function:

Definition 3.10: Jordan totient function

For any positive integers a and n, the **Jordan totient function**, denoted by $J_n(a)$, is the number of positive integer n-tuples $(m_1, m_2, \ldots, m_n)$, with all $m_i \leq a$, and $\gcd(m_1, m_2, \ldots, m_n, a) = 1$. $J_1(n)$ corresponds to the Euler totient function.

Lemma 3.11: ([13]) For any positive integers n, a, and $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ the prime factorization of a, with each p_i a prime,

$$J_n(a) = a^n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i^n}\right).$$

Proof:
We partition the set of all n-tuples $(m_1, m_2, \ldots, m_n)$ with each m_i a positive integer not greater than a into equivalence classes defined by the relation $(m_1, m_2, \ldots, m_n) \sim (m'_1, m'_2, \ldots, m'_n)$ iff $\gcd(m_1, \ldots, m_n, a) = \gcd(m'_1, \ldots, m'_n, a)$. For each $d|a$, $\gcd(m_1, \ldots, m_n, a) = d$ iff $\gcd\left(\frac{m_1}{d}, \ldots, \frac{m_n}{d}, \frac{a}{d}\right) = 1$. Since all of the a^n tuples must be in one of these classes, it follows that

$$a^n = \sum_{d|a} J_n\left(\frac{a}{d}\right) = \sum_{d|a} J_n\left(d\right).$$

Applying the Möbius inversion formula yields

$$J_n(a) = \sum_{d|a} \mu\left(\frac{n}{d}\right) d^n.$$

The term $\mu\left(\frac{n}{d}\right)$ is non-zero iff $\frac{n}{d}$ is square-free, which is equivalent to

$$d = \frac{\prod_{i=1}^{k} p_i^{\alpha_i}}{\prod_{t \in T} p_t}$$

for some $T \subset \{1, 2, \ldots, k\}$. Clearly for any such d, $\mu\left(\frac{n}{d}\right) = (-1)^{|T|}$. It follows that

$$\begin{aligned} J_n(a) &= \sum_{T \subset \{1,\ldots,k\}} (-1)^{|T|} \left(\frac{a}{\prod_{t \in T} p_t}\right)^n \\ &= a^n \sum_{T \subset \{1,\ldots,k\}} (-1)^{|T|} \left(\frac{1}{\prod_{t \in T} p_t^n}\right) \end{aligned}$$

By the expansion of $\prod_{i=1}^{k} \left(1 - \frac{1}{p_i^n}\right)$, it is immediate that for any $T \subset \{1, 2, \ldots, k\}$, the coefficient of the term $\frac{1}{\prod_{t \in T} p_t^n}$ is $(-1)^{|T|}$, from which the result follows.

□

A immediate consequence of Lemma 3.11 is

Corollary 3.12: J_n is multiplicative. □

By Theorem 3.7 and Corollary 3.12, we get

Corollary 3.13: For any positive integers n, m

$$\sum_{d|m} J_n(d) = m^n.$$

Proof:
Since J_n is multiplicative, it follows from Theorem 3.7 that S_{J_n} is also multiplicative.

Given any prime p and positive integer α,

$$\begin{aligned}\sum_{d|p^\alpha} J_n(d) &= \sum_{d|p^\alpha} d^n \left(1 - \frac{1}{p^n}\right) \\ &= 1 + \sum_{i=1}^{\alpha} p^{in} \left(1 - \frac{1}{p^n}\right) \\ &= 1 + \sum_{i=1}^{\alpha} p^{in} - p^{(i-1)n} \\ &= p^{\alpha n} \\ &= (p^\alpha)^n\end{aligned}$$

The result now follows by the multiplicity of S_{J_n}. □

Example 3.14: Another interesting number theoretic function, denoted by κ, is defined by $\kappa(d) = \sum_{lcm(a,b)=d} \varphi(a)\varphi(b)$. For example, $\kappa(6) = \varphi(1)\varphi(6) + \varphi(2)\varphi(6) + \varphi(3)\varphi(6) + \varphi(6)\varphi(6) + \varphi(2)\varphi(3) + \varphi(6)\varphi(3) + \varphi(3)\varphi(2) + \varphi(6)\varphi(2) + \varphi(6)\varphi(1)$, which is equal to 24.

Even though κ was defined purely in terms of the φ function, we can ask ourselves what exactly does it count, if anything? As $\varphi(n)$ is the number of positive integers no greater than n which are relatively prime to n, it follows that $\varphi(a)\varphi(b)$ is the number of pairs of integers (s, t) with $s \leq a$ and $t \leq b$ and $\gcd(s, a) = \gcd(t, b) = 1$. Since we are summing over all (a, b) with $lcm(a, b) = d$, it is clear that $\kappa(d)$ is the number of positive integer quadruples (a, b, s, t) with $lcm(a, b) = d$ and $\gcd(a, s) = \gcd(b, t) = 1$, and $s \leq a$ and $t \leq b$. Denote the set of all such quadruples by U_d. We will now see that the κ function is nothing else but the function $J_2(n)$ in disguise.

Proposition 3.15: For any positive integer d, $J_2(d) = \kappa(d)$.

Proof:
Recall that $J_2(d)$ is the number of pairs (u, v) with $1 \leq u, v \leq d$ with $\gcd(u, v, d) = 1$. Denote the set of all these pairs by V_d. We will now prove that $|U_d| = |V_d|$, by constructing an injection $\phi : U_d \to V_d$, as well as an injection $\psi : V_d \to U_d$. The result then follows trivially.

1. Define ϕ to be a function on U_d defined by $\phi(a, b, s, t) = \left(\frac{sd}{a}, \frac{td}{b}\right)$. We first verify that the image of ϕ is contained in V_d. Suppose, for the sake of contradiction, that there was an element $(a, b, s, t) \in U_d$ which did not map into V_d, meaning that $\gcd\left(\frac{sd}{a}, \frac{td}{b}, d\right) = c \neq 1$. For any prime $p|c$, denote the highest power of p that divides d by p^η. Note that as $d = lcm(a, b)$, if follows that p^η cannot divide both $\frac{d}{a}$ and $\frac{d}{b}$, so w.l.o.g assume that it does not divide $\frac{d}{a}$. The fact that $p|d$ necessarily means that $p|a$. Since p divides $\frac{sd}{a}$, it is clear that $p|s$, contradicting $\gcd(a, s) = 1$. The codomain of ϕ can consequently be taken as V_d.

   Now suppose that $\phi(a, b, s, t) = \phi(\alpha, \beta, \sigma, \tau)$. Then $\left(\frac{sd}{a}, \frac{td}{b}\right) = \left(\frac{\sigma d}{\alpha}, \frac{\tau d}{\beta}\right)$. By equating components it follows that

$$\frac{s}{a} = \frac{\sigma}{\alpha}$$
$$\frac{t}{b} = \frac{\tau}{\beta}$$

   i.e.,

$$\alpha s = \sigma a$$
$$\beta t = \tau b.$$

   Since $\gcd(a, s) = \gcd(b, t) = \gcd(\alpha, \sigma) = \gcd(\beta, \tau) = 1$, it follows that $a|\alpha$ and $\alpha|a$, with similar relations holding for b, s and t. Since all of the terms are positive, $\alpha = a, \beta = b, \sigma = s, \tau = t$, showing that ϕ is injective.

2. Define the function ψ on V_d by $\psi(u, v) = (a, b, s, t)$ with $\frac{s}{a} = \frac{u}{d}, \gcd(a, s) = 1$ and $\frac{t}{b} = \frac{v}{d}, \gcd(b, t) = 1$. We shall now show that the image of V_d under ψ is contained in U_d, which means that the codomain of ψ can be taken as U_d. Note that ψ is well defined as the representation of a positive fraction as the ratio of two positive relatively prime integers is unique. Since a and b are obtained from d by the cancellation of common factors with u and v respectively, it is immediately clear that $a|d$ and $b|d$, from which it follows that $lcm(a, b)|d$.

   Now suppose that d does not divide $lcm(a, b)$. Then there must exist a prime power p^γ which divides d but neither a nor b. Now since $ua = sd$, and p^γ divides d, p must divide u and similarly p divides v, which means

that $p|\gcd(u,v,d)$, which is clearly a contradiction. Hence $d|lcm(a,b)$, which gives $lcm(a,b) = d$. By definition $\gcd(a,s) = \gcd(b,t) = 1$, from which it now follows that the image of V_p under ψ is indeed contained in U_d. Now suppose $\psi(u,v) = \psi(u',v')$. Then $\frac{u}{d} = \frac{u'}{d}$ and $\frac{v}{d} = \frac{v'}{d}$, from which it is immediately clear that $(u,v) = (u',v')$ and consequently ψ is injective.

Since we have found an injective function ϕ from U_d to V_d and an injective function ψ from V_d to U_d, it is now clear that $|U_d| = |V_d|$, and thus $J_2(d) = \kappa(d)$ for all positive integers d.

□

Well, as you know, there are 24 hours in every day.
And if that's not enough, you've always got the nights!

$\sim$ Ronald Graham (1935-)

4 Automorphism structures

In order to compare functions on a set to automorphisms on a group we define a *structural graph* of a function:

Definition 4.1: **Structural graph**

Given a function $\phi : S \to S$ from a set S into itself. Let $\mathcal{G} = (V, E)$ be a directed graph with $|V| = |S|$, and $\rho : S \to V$ a bijection. $\mathcal{G}$ is called a **structural graph** of ϕ if

$$(u, v) \in E \Leftrightarrow (\exists s \in S : u = \rho(s) \wedge v = \rho(\phi(s))).$$

In this case, we call ρ a graph projection of ϕ.

The following theorem gives a necessary and sufficient condition for a function to posses the automorphism property:

Theorem 4.2: For any set S and any bijective $f : S \to S$, if there exists some group automorphism $h : G \to G$ for some abelian group G such that the structural graph of f is graph isomorphic to that of h then S can be endowed with an abelian group structure such that f is a group automorphism.

To be precise, let ρ_f and ρ_h be graph projections of f and h respectively, and ψ the graph isomorphism from the codomain of ρ_f to the codomain of ρ_h. Define $\eta : S \to G$ by $\eta = \rho_h^{-1}\psi\rho_f$. For each α, β in S define

$$\alpha \cdot_S \beta = \eta^{-1}(\eta(\alpha) \cdot_G \eta(\beta)).$$

Then:

1. S together with this binary operation is an abelian group with identity $1_S = \eta^{-1}(1_G)$ and $\alpha^{-1} = \eta^{-1}(\eta(\alpha)^{-1})$.
2. f is an automorphism.

Proof:
Since ρ_f, ρ_h, ψ are all bijective, η, being the composition of bijective functions is also bijective, hence η^{-1} exists. Let α, β, γ be elements of S. Define $1_S = \eta^{-1}(1_G)$ and $\alpha^{-1} = \eta^{-1}(\eta(\alpha)^{-1})$.

1. S has an abelian group structure:

(a) The binary operation on S is associative:

$$\begin{aligned}(\alpha\beta)\gamma &= \eta^{-1}(\eta(\alpha\beta)\eta(\gamma)) \\ &= \eta^{-1}(\eta(\eta^{-1}(\eta(\alpha)\eta(\beta)))\eta(\gamma)) \\ &= \eta^{-1}(\eta(\alpha)\eta(\beta)\eta(\gamma)) \\ &= \eta^{-1}(\eta(\alpha)\eta(\eta^{-1}(\eta(\beta)\eta(\gamma)))) \\ &= \alpha(\eta^{-1}(\eta(\beta)\eta(\gamma))) \\ &= \alpha(\beta\gamma)\end{aligned}$$

(b) The binary operation defined on S is commutative:

$$\begin{aligned}\alpha\beta &= \eta^{-1}(\eta(\alpha)\eta(\beta)) \\ &= \eta^{-1}(\eta(\beta)\eta(\alpha)) \\ &= \beta\alpha\end{aligned}$$

(c) S has an identity element 1_S:

$$\begin{aligned}1_S\alpha &= \eta^{-1}(\eta(1_S)\eta(\alpha)) \\ &= \eta^{-1}(\eta(\eta^{-1}(1_G))\eta(\alpha)) \\ &= \eta^{-1}(1_G\eta(\alpha)) \\ &= \eta^{-1}(\eta(\alpha)) \\ &= \alpha\end{aligned}$$

From commutativity $\alpha 1_S = \alpha$, from which it follows that S has identity 1_S.

(d) Each element of S has an inverse:

$$\begin{aligned}\alpha\alpha^{-1} &= \eta^{-1}(\eta(\alpha)\eta(\eta^{-1}(\eta(\alpha)^{-1}))) \\ &= \eta^{-1}(\eta(\alpha)\eta(\alpha)^{-1}) \\ &= \eta^{-1}(1_G) \\ &= 1_S\end{aligned}$$

Consequently S, together with the defined binary operation, is an abelian group.

2. f is an isomorphism: First we note that $\eta(\alpha\beta) = \eta(\eta^{-1}(\eta(\alpha)\eta(\beta))) = \eta(\alpha)\eta(\beta)$. Also note that $(\rho_f(\alpha), \rho_f(f(\alpha)))$ is an edge in the structural graph of f, and since ψ is a graph isomorphism from the structural graph of f to that of h it follows that $(\psi\rho_f(\alpha), \psi\rho_f(f(\alpha)))$ is an edge in the structural graph of h, meaning $h(\rho_h^{-1}\psi\rho_f(\alpha)) = \rho_h^{-1}\psi\rho_f(f(\alpha))$ or $h(\eta(\alpha)) = \eta(f(\alpha))$ thus $h\eta = \eta f$.

It now follows that

$$\begin{aligned}\eta f(\alpha\beta) &= h(\eta(\alpha\beta)) \\ &= h(\eta(\alpha)\eta(\beta)) \\ &= h(\eta(\alpha))h(\eta(\beta)) \\ &= \eta f(\alpha)\eta f(\beta) \\ &= \eta(f(\alpha)f(\beta)).\end{aligned}$$

Since η is injective if follows that $f(\alpha\beta) = f(\alpha)f(\beta)$.

□

With Theorem 4.2 in mind, it is clear that given a bijective function $f : S \to S$, it is sufficient to find the structural graphs of all automorphisms on abelian groups of the same order as S and then simply determine if the structural graph of f is graph isomorphic to one of these. If this is indeed the case, then S can be made into an abelian group with f an automorphism as described in Theorem 4.2. If, however, no such automorphism was found, then S cannot be made into an abelian group with f an automorphism.

We will now proceed to define a few graph theoretic terms that will be needed in discussing the structural graphs of functions.

Definition 4.3: Path, component, cycle, chain

Given a graph $\mathcal{G}$. A finite sequence of edges from $\mathcal{G}$, $P_i = (v_i, w_i), i \in \{1, 2, \ldots, n-1\}$, is called a **path from vertex** a **to vertex** b if $w_i = v_{i+1}$, $v_1 = a$ and $w_{n-1} = b$. a and b are called the terminal vertices of the path. A path is called **simple** if each vertex that the path passes through is only passed through once.

For any vertex a of $\mathcal{G}$, the **component** of a, denoted by $\mathcal{C}(a)$ is the subgraph of $\mathcal{G}$ consisting of all vertices b for which there is a path from a to b, and all the edges occurring in a path from a to b.

In the literature it is common to define a (simple-)cycle as a (simple-)path with terminal vertices coinciding. In this thesis however, we will use the term **cycle** to refer to a component (rather than a sequence of edges) of which the set of edges can be ordered into a sequence being a simple path with terminal vertices coinciding. The cardinality of the vertex set of a cycle is called the **cycle length**. We will often say that a function f has a cycle of length k, with which it should be understood that the structural graph of f has a cycle with cycle length equal to k.

For a vertex v in a graph $G = (V, E)$, the cardinality of the set of members of E with second component v is called the in-degree of v, and the cardinality of the set of members of E with v as first component is referred to as the out-degree of v. In the case of an undirected graph, these two numbers coincide, and will simply be referred to as the degree of vertex v.

A subgraph $\mathcal{H}$ of $\mathcal{G}$ is called a **chain** if the degree of each vertex of $\mathcal{H}$ is exactly two, and there is a path between any two of the vertices, and the set of vertices

is infinite.

We can now immediately place a few basic restrictions on functions that possess the automorphism property:

Proposition 4.4: Suppose $f : S \to S$ has the automorphism property. Then

1. each component of the structural graph of f is either a cycle or a chain.
2. if S is finite then each component of the structural graph of f is a cycle.
3. the structural graph of f has at least one cycle of length 1 (which will be called the zero cycle) which corresponds to the action of the automorphism on the zero element of the group.

Proof:
Let $\mathcal{G}$ be the structural graph of f, and ρ_f a graph projection of f. For any vertex of $\mathcal{G}$, say v, there is an $a \in S$ such that $\rho_f(a) = v$.

1. The edges containing v are exactly $(v, \rho_f(f(a)))$ and $(\rho_f(b), v)$ with $f(b) = a$ (Note, such a b exists, as f is surjective and it is unique since f is injective). The degree of each of $\mathcal{G}$'s vertices is thus at most two. In the case where $f(a) = a$ the component of $\rho_f(a)$ is simply the graph with vertex set $\{\rho_f(a)\}$ and edge set $\{(\rho_f(a), \rho_f(a))\}$ which is a cycle of length 1. If $\mathcal{C}(v)$ is infinite, then it is by definition a chain, so suppose $\mathcal{C}(v)$ is finite with at least two elements. Consider the set $\{\rho_f(f^k(a)) : k \in \mathbb{N}_0\}$. From the finiteness of $\mathcal{C}(v)$ it follows that $f^x(a) = f^y(a)$ for some integers $x < y$ and thus $f^{y-x}(a) = a$ from the injectivity of f. Since each vertex of $\mathcal{C}(v)$ has a degree of two, it follows that $\mathcal{C}(v)$ is a cycle.
2. If S is finite, it can clearly not contain any chains, the result then follows from 1.
3. $f(1_S) = 1_S$, meaning $\mathcal{C}(\rho_f(1_S))$ is a cycle of length 1.

□

Proposition 4.4 enables us to conveniently classify the structures of automorphisms on finite groups in terms of their cycles:

Definition 4.5: **Cyclic structure**

If the structural graph of $f : S \to S$ has c_i cycles of length $t_i (1 \leq i \leq k)$ then we say f has **cyclic structure** represented by the array $\begin{bmatrix} c_1 & c_2 & \dots & c_k \\ t_1 & t_2 & \dots & t_k \end{bmatrix}$, where we take $t_1 > t_2 > \ldots > t_k$. In the case of any of the c_i's being 0, we can simply omit their columns from the array. We also note that $\sum_{i=1}^{k} c_i t_i = |S|$, and the identity mapping has cyclic structure $\begin{bmatrix} |S| \\ 1 \end{bmatrix}$.

In the case of f having a finite domain, we can appeal to the Fundamental Theorem of finitely generated abelian groups ([1, p. 336]).

Theorem 4.6: The Fundamental Theorem of finitely generated abelian groups

Any finitely generated abelian group G is isomorphic to

$$\prod_{i=1}^{k} \mathbb{Z}_{d(i)} \times \mathbb{Z}^n$$

for some non-negative integers k and n *, with each $d(i)$ some power of a prime. □

From Theorems 4.2 and 4.6 it is clear that if S is finite, we can list structural graphs of all isomorphisms of all abelian groups of the form $\prod_{i=1}^{k} \mathbb{Z}_{d(i)}$ with $\prod_{i=1}^{k} d(i) = |S|$. f will have the automorphism property exactly when it's structural graph is isomorphic to one of the graphs on the list. As the number of automorphisms is finite, as well as the number of abelian groups that we need to check, the list is finite, and can be exhausted by computer computation.

*if k or n is 0, the corresponding term is omitted from the product.

Reason is immortal, all else mortal.

$\sim$ Pythagoras (c.570 BC - c.495 BC)

5 The cyclic groups

We shall first investigate the cyclic structures of the automorphisms of cyclic groups $\mathbb{Z}_n$, $n \in \mathbb{N}$. The complete classification of the cyclic structures of the automorphisms of cyclic groups was one of the results published in the paper on functions realising as abelian group automorphisms ([11]). We shall thus stick to the notation used in this paper.

Denote the group of units of the ring $\mathbb{Z}_n$ by $U_n = \{k_1, k_2, \ldots, k_{\varphi(n)}\} = \{k \in \mathbb{Z}_n : \gcd(k,n) = 1\}$, where we take $k_1 = 1$. Let $T_n = (\mathbb{Z}_n \setminus U_n) \setminus \{0\}$, and for any $z \in T_n$ put $z' = \frac{n}{\gcd(z,n)}$. For each $i, 2 \leq i \leq \varphi(n)$, put $l_i = \mathrm{ord}_n(k_i)$ (the least $x \in \mathbb{N}$ such that $k_i^x \equiv_n 1$), and for each divisor λ of l_i, put $L_{i,\lambda} = \frac{1}{\lambda}|\{z \in T_n : \mathrm{ord}_{z'}(k_i) = \lambda\}|$.

It is evident that if we want to investigate the conditions $f : S \to S$ has to satisfy to have the automorphism property, then by Theorem 4.2 it suffices to find the cyclic structures of all possible automorphisms on all abelian groups of order $|S|$. In the following theorem we do it for finite cyclic groups.

Theorem 5.1: Let $|S| = n$ and let $f : S \to S$ be a bijection. Then there exists a binary operation $\star$ on S (as defined by Theorem 4.2) such that $(S, \star)$ is a cyclic group and $f \in Aut(S)$ iff either f is the identity map or there is an $i, 2 \leq i \leq \varphi(n)$, such that f has the cyclic structure

$$\begin{bmatrix} [U_n : \langle k_i \rangle] + L_{i,l_i} & L_{i,\lambda_1} & \ldots & L_{i,\lambda_t} & L_{i,1} + 1 \\ l_i & \lambda_1 & \ldots & \lambda_t & 1 \end{bmatrix}$$

where $l_i > \lambda_1 > \ldots > \lambda_t > 1$ denotes the complete list of (positive) divisors of l_i.

Proof:
It suffices to determine all possible cyclic structures of automorphisms $f : \mathbb{Z}_n \to \mathbb{Z}_n$ for the additive cyclic group $Z_n = \{0, 1, \ldots, n-1\}$.

Let $f : \mathbb{Z}_n \to \mathbb{Z}_n$ be an automorphism. Then $f(1) \in U_n$ otherwise if $f(1) = z \in T_n$, then $f(z') = 0 = f(0)$, a contradiction. If $f(1) = 1 = k_1$, then f is the identity map. Let $2 \leq i \leq \varphi(n)$, and assume $f(1) = k_i$. Then 1 lies in the cycle $(1, k_i, k_i^2, \ldots, k_i^{l_i - 1})$ (of length l_i), which consists exactly of the elements of the subgroup $\langle k_i \rangle$ of U_n. If $\langle k_i \rangle \neq U_n$, choose any $k_j \in U_n \setminus \langle k_i \rangle$, then $(k_j, k_j k_i, k_j k_i^2, \ldots, k_j k_i^{l_i - 1})$ is another cycle of length l_i, and is exactly the coset $k_j \langle k_i \rangle$ of $\langle k_i \rangle$ in U_n. Continuing in this manner, we obtain $[U_n : \langle k_i \rangle]$ cycles of length l_i, exhausting all the elements of U_n.

Consider any $z \in T_n$. The cycle $(z, zk_i, zk_i^2, \ldots, zk_i^{\lambda - 1})$ is obtained where the length of the cycle is the least $\lambda \in \mathbb{N}$ such that $n | z(k_i^{\lambda - 1} - 1)$. This means that $\lambda = \mathrm{ord}_{z'}(k_i)$. Note that $\lambda | l_i$. Also note that each member of this cycle is in T_n. Other elements of T_n, not in this cycle, might give rise to cycles of

the same length (λ), hence the total number of cycles of length λ is given by $\frac{1}{\lambda}|\{z \in T_n : \mathrm{ord}_{z'}(k_i) = \lambda\}|$. Finally, cycles of length 1 obtained in this way excludes the zero-cycle, so there are $|\{z \in T_n : \mathrm{ord}_{z'}(k_i) = 1\}| + 1$ cycles of length 1. □

Corollary 5.2: If $|S| = n$, then there are at most $\varphi(n)$ cyclic structures for a bijection $f : S \to S$ that will turn S into a cyclic group, with $f \in Aut(S)$.

Proof:
Apart from the identity map, the possible cyclic structures of automorphisms are determined by $2 \leq i \leq \phi(n)$, but note that different i could give rise to the same cyclic structures of an automorphism. □

Example 5.3: If $|S| = p$, where p is prime, then $f : S \to S$ has the automorphism property iff it has the cyclic structure $\begin{bmatrix} d & 1 \\ \frac{p-1}{d} & 1 \end{bmatrix}$ for some divisor d of $p-1$. (Keep in mind that a group of prime order is abelian iff it is cyclic.)

Example 5.4: Let $|S| = 12$, then $U_{12} = \{1, 5, 7, 11\}$, so that $(k_1, k_2, k_3, k_4) = (1, 5, 7, 11)$. Then we have $l_2 = \mathrm{ord}_{12}(5) = 2$, $L_{2,1} = |\{3, 6, 9\}| = 3, L_{2,2} = \frac{1}{2}|\{2, 4, 8, 10\}| = 2$, which gives the cyclic structure $\begin{bmatrix} [U_{12} : \langle 5 \rangle] + L_{2,2} & L_{2,1} + 1 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 4 & 4 \\ 2 & 1 \end{bmatrix}$.
Similarly for $l_3 = 2$ we obtain the cyclic structure $\begin{bmatrix} 3 & 6 \\ 2 & 1 \end{bmatrix}$ and for $l_4 = l_{\varphi(12)} = 2$ we obtain the cyclic structure $\begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix}$. Hence S can be endowed with a cyclic group structure in such a way that $f \in Aut(S)$ iff f is the identity map or f has one of the three cyclic structures above.

Example 5.5: Let $|S| = p^2$, with p a prime. Then $z' = p$ for all $z \in T_{p^2} = \{p, 2p, \ldots, (p-1)p\}$. This implies that

$$L_{i,\lambda} = \frac{1}{\lambda}|\{z \in T_{p^2} : \mathrm{ord}_p(k_i) = \lambda\}| = \begin{cases} \frac{p-1}{\lambda} \text{ if } \mathrm{ord}_p(k_i) = \lambda \\ 0 \text{ otherwise} \end{cases}$$

for each divisor λ of $l_i = \mathrm{ord}_{p^2}(k_i)$, where $2 \leq i \leq p^2 - p$.

For instance, if $p = 3$, then $(k_1, k_2, \ldots, k_6) = (1, 2, 4, 5, 7, 8)$. For $i = 2$, we have $l_2 = \mathrm{ord}_9(2) = 6$, and since $\mathrm{ord}_3(2) = 2$, it follows that $L_{2,2} = \frac{2}{2} = 1$ and $L_{2,1} = L_{2,3} = L_{2,6} = 0$. Also since $k_2 = 2$ is a generator of the group U_9, $[U_9 : \langle 2 \rangle] = [U_9 : U_9] = 1$. So (for the case $i = 2$) we obtain by Theorem 5.1, the cyclic structure $\begin{bmatrix} 1 & 0 & 1 & 1 \\ 6 & 3 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 6 & 2 & 1 \end{bmatrix}$. Similarly for $i = 3$ we get the cyclic structure $\begin{bmatrix} 2 & 3 \\ 3 & 1 \end{bmatrix}$, for $i = 4$ we get $\begin{bmatrix} 1 & 1 & 1 \\ 6 & 2 & 1 \end{bmatrix}$, for $i = 5$ we get $\begin{bmatrix} 2 & 3 \\ 3 & 1 \end{bmatrix}$, and finally for $i = 6 = \varphi(9)$ we get $\begin{bmatrix} 4 & 1 \\ 2 & 1 \end{bmatrix}$. Consequently, if $|A| = 9$, it can be endowed with a cyclic group structure with $f \in Aut(A)$ iff f has one of the cyclic structures $\begin{bmatrix} 1 & 1 & 1 \\ 6 & 2 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 3 \\ 3 & 1 \end{bmatrix}, \begin{bmatrix} 4 & 1 \\ 2 & 1 \end{bmatrix}$ or $\begin{bmatrix} 9 \\ 1 \end{bmatrix}$ (the identity).

There are proofs that date back to the Greeks that are still valid today.

$\sim$ A. Wiles (1953-)

6 Automorphisms and the general linear group

Given any ring R and positive integer n, let $\bar{R}$ be the underlying abelian group of R. $\bar{R}^n$ is a left R-module with group addition componentwise and R-multiplication defined by $r(x_1, x_2, \ldots, x_n) = (rx_1, rx_2, \ldots, rx_n)$ for all $(x_1, \ldots, , x_n) \in \bar{R}^n$, and $r \in R$. Let $B = \{e_1, \ldots, e_n\}$ with $e_i = (0, 0, \ldots, 0, 1, 0, \ldots, 0) \in \bar{R}^n$ with 1 in the i-th component and zeros elsewhere. It is clear any element $x = (x_1, x_2, \ldots, x_n) \in \bar{R}^n$ can be written uniquely as $x = \sum_{i=1}^{n} x_i e_i$ from which it follows that ${}_R\bar{R}^n$ is a free module with base B.

For now we shall focus our attention towards the ring $End(\bar{R}^n)$. The next Theorem states that any endomorphism on a module with a base is in fact uniquely determined by its action on the base, as well as showing that all functions from the base of the module to the module determines a unique endomorphism. We shall actually prove a stronger result which holds for R-homomorphisms in general, however the results stated above follows from it if the domain of the R-homomorphism is taken to be the same as the co-domain.

Proposition 6.1: ([14], Proposition 2.2.5) Given any basis $B = \{b_i\}_{i \in I}$ of ${}_RM$, the following statements hold:

1. Any R-homomorphism $f : {}_RM \to {}_RN$ is determined by its action on B;

2. Given any function $\xi : B \to {}_RN$, there exists a unique R-homomorphism $f : {}_RM \to {}_RN$ such that $f(b_i) = \xi(b_i)$ for all $b_i \in B$.

Proof:
1) Any $x \in {}_RM$ can be expressed uniquely in the form $x = \sum_{i \in S} \alpha_i b_i$, with S a finite subset of I and $\alpha_i \in R$. Since f is an $R-$homomorphism, it is clear that

$$\begin{aligned} f(x) &= f\left(\sum_{i \in S} \alpha_i b_i\right) \\ &= \sum_{i \in S} f(\alpha_i b_i) \\ &= \sum_{i \in S} \alpha_i f(b_i) \end{aligned}$$

which shows that f is determined by its action on the elements of B.

2) Given any $\xi : B \to {}_RN$, define $f : {}_RM \to {}_RN$ by $f(x) = f(\sum_{i \in S} \alpha_i b_i) = \sum_{i \in S} \alpha_i \xi(b_i)$. From the uniqueness of base representation, it follows that f is well defined. For any two elements $x = \sum_{i \in S} \alpha_i b_i, y = \sum_{i \in S} \beta_i b_i$ * in ${}_RM$, and

*Even though x and y could be composed out of different base elements, we can take the sum to be indexed over a common set S by allowing some of the coefficients in R to be equal to 0.

$r \in R$ it follows that

$$\begin{aligned} f(x+y) &= \sum_{i\in S}(\alpha_i+\beta_i)\xi(b_i) \\ &= \sum_{i\in S}\alpha_i\xi(b_i) + \sum_{i\in S}\beta_i\xi(b_i) \\ &= f(x)+f(y). \end{aligned}$$

Since $rx = r\left(\sum_{i\in S}\alpha_i b_i\right) = \sum_{i\in S} r\alpha_i b_i$ it follows that

$$\begin{aligned} f(rx) &= \sum_{i\in S} r\alpha_i\xi(b_i) \\ &= r\sum_{i\in S}\alpha_i\xi(b_i) \\ &= rf(x). \end{aligned}$$

It is now clear that f is indeed an R-homomorphism, and by 1) it is unique. □

Let $X = (z_1, z_2, \ldots, z_n)$ be an ordered n-tuple with each component z_i an element of $\bar{R}^n$. We shall denote the $n \times n$ matrix with its i-th column equal to z_i, by $[z_1|z_2|\ldots|z_n]$.

Example 6.2: Suppose $X = \{z_1 = (1,1,2), z_2 = (1,4,5), z_3 = (1,3,3)\}$, with $z_i \in \bar{\mathbb{Z}}_7^3$, then $[z_1|z_2|z_3]$ denotes the matrix

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 4 & 3 \\ 2 & 5 & 3 \end{bmatrix}.$$

Even though $M_n(R)$ (as defined in example 2.18) is defined completely differently from $End(\bar{R}^n)$, our next Theorem tells us that with regards to structure they are actually the same ring.

Theorem 6.3: **(([15], p. 210)Matrix representation of endomorphism rings**

The map $\tau : End(\bar{R}^n) \to M_n(R)$ defined by

$$\tau(f) = [f(e_1)|f(e_2)|\ldots|f(e_n)], \forall f \in End(\bar{R}^n)$$

is a ring isomorphism for all commutative rings R.

Proof:
First it needs to be established that τ is a ring homomorphism. Let $f, g \in End(\bar{R}^n)$. Note that

$$\tau(f+g) = [(f+g)(e_1)|(f+g)(e_2)|\ldots|(f+g)(e_n)],$$

from which it follows that

$$\tau(f+g) = [f(e_1)|f(e_2)|\ldots|f(e_n)] + [g(e_1)|g(e_2)|\ldots|g(e_n)] = \tau(f)+\tau(g).$$

Since $B = \{e_j : j \in \{1, 2, \ldots, n\}\}$ is a base of ${}_R\bar{R}^n$, we can find unique $\alpha_{ji}, \beta_{ji} \in R, i, j \in \{1, 2 \ldots, n\}$ such that $f(e_i) = \sum_{j=1}^{n} \alpha_{ji} e_j$ and $g(e_i) = \sum_{j=1}^{n} \beta_{ji} e_j$, thus

$$\tau(f) = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \cdots & \alpha_{nn} \end{bmatrix}$$

and

$$\tau(g) = \begin{bmatrix} \beta_{11} & \beta_{12} & \cdots & \beta_{1n} \\ \beta_{21} & \beta_{22} & \cdots & \beta_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{n1} & \beta_{n2} & \cdots & \beta_{nn} \end{bmatrix}.$$

Consequently

$$\forall s, t \in \{1, 2, \ldots, n\}, [\tau(f)\tau(g)]_{st} = \sum_{j=1}^{n} \alpha_{sj} \beta_{jt}.$$

However,

$$\begin{aligned} f(g(e_i)) &= \sum_{j=1}^{n} \beta_{ji} f(e_j) \\ &= \sum_{j=1}^{n} \beta_{ji} \sum_{k=1}^{n} \alpha_{kj} e_k \\ &= \sum_{j=1}^{n} \sum_{k=1}^{n} \beta_{ji} \alpha_{kj} e_k \\ &= \sum_{k=1}^{n} \left(\sum_{j=1}^{n} \beta_{ji} \alpha_{kj} \right) e_k \end{aligned}$$

and thus $[\tau(fg)]_{st} = \sum_{j=1}^{n} \beta_{jt} \alpha_{sj}$, giving $\tau(f)\tau(g) = \tau(fg)$ by the commutativity of R.

τ is injective, because any two endomorphisms mapping to the same matrix will have the same action on the base B, making them equal to one another by Proposition 6.1 1. To see that τ is surjective; to any matrix $M \in M_n(R)$, define a function $h : B \to \bar{R}^n$ by mapping e_i to the i-th column of M (seen as an element of $\bar{R}^n$). It follows from 6.1 that h induces an endomorphism $f : \bar{R}^n \to \bar{R}^n$ with $\tau(f) = M$. Consequently $M_n(R)$ is isomorphic to $End(\bar{R}^n)$. □

Proposition 6.4: The group of units of the ring $End(\bar{R}^n)$ is isomorphic to the multiplicative group consisting of the invertible matrices in $M_n(R)$.

Proof:
Let f be any automorphism of $\bar{R}^n$. Since f is surjective, $\tau(f)$ is right invertible, and since f is injective, $\tau(f)$ is left invertible, meaning $\exists A, B \in M_n(R)$ such that $A\tau(f) = \tau(f)B = \mathbf{I}$. But this means that $(A\tau(f))B = \mathbf{I}B$, giving $A(\tau(f)B) = A = B$, proving that $\tau(f)$ is invertible.

Starting with an invertible matrix M, from Theorem 6.3, we can find an endomorphism f of $\bar{R}^n$ such that $\tau(f) = M$. From the invertibility of M, $\forall y \in \bar{R}^n$, defining $x = M^{-1}y$ we have that $Mx = y$, showing that f is surjective. Since $Mx = My \Rightarrow x = y$ (by multiplying by M^{-1} on the left), we see that f is injective and thus an automorphism. □

Definition 6.5: **General linear group**

For any commutative ring R, the **general linear group**, denoted by $GL(R, n)$, is the multiplicative group of all invertible $n \times n$ matrices over R.

Corollary 6.6: $Aut(\bar{R}^n)$ is isomorphic to $GL(R, n)$. □

Corollary 6.6 allows us to investigate the automorphism groups of $\bar{R}^n$ via $GL(R, n)$. We can decompose the elements of the group $\bar{R}^n$ into their components with respect to the base $B = \{e_1, e_2, \ldots, e_n\}$, allowing the elements to be represented as $n \times 1$ column vectors and the automorphisms as $n \times n$ matrices. Instead of applying the automorphisms directly, we can multiply the column representation of the element on the left by the matrix representation of the automorphism.

In the case of R being a finite field, the exact size of $GL(R, n)$ can be determined.

Theorem 6.7: ([16]) Let $\mathbb{F}_q$ be a field of order q, then

$$|GL(\mathbb{F}_q, n)| = \prod_{i=1}^{n} \left(q^n - q^{i-1}\right).$$

Proof:
Let $A = [C_1|C_2|\ldots|C_n] \in GL(\mathbb{F}_q, n)$. We will now count the number of possible automorphisms by noticing that C_1 can be any non-zero column vector. C_2 can then be any non-zero column vector which is linearly independent of C_1; and in general C_i can be any non-zero column vector which is linearly independent of all the elements in $\{C_j : j < i\}$. In order to count the number of linearly independent vectors, we shall rather count the number of linearly dependent and subtract it from the total number of possible vectors.

Since C_1 can be any non zero vector, there are $q^n - 1$ possibilities for C_1.

If D is linearly dependent on C_1, it means $\exists k \in \mathbb{F}_p$ such that $D = kC_1$, from which it follows that D can be any one of q possibilities, and C_2 any of $q^n - q$. In general, if D is linearly dependent on the set $\{C_1, C_2, \ldots, C_{i-1}\}$, it follows that there exists $a \neq 0, \alpha_j \in \mathbb{F}_q$, $j \in \{1, 2, \ldots, i-1\}$ such that

$$aD + \sum_{j=1}^{i-1} \alpha_j C_j = 0,$$

which can be expressed as

$$D = \sum_{j=1}^{i-1} \left(\frac{-\alpha_j}{a} \right) C_j.$$

Now each of the coefficients $\left(\frac{-\alpha_j}{a}\right)$ can be any of the elements of $\mathbb{F}_q$, from which it is clear that D can be any one of q^{i-1} different vectors and C_i any of $q^n - q^{i-1}$. Since this holds for all $i \in \{1, 2, \ldots, n\}$ it follows that

$$|GL(\mathbb{F}_q, n)| = \prod_{i=1}^{n} \left(q^n - q^{i-1} \right).$$

□

Definition 6.8: Jordan block, Jordan matrix

An $n \times n$ **Jordan block**, denoted by $J(n, \lambda)$ is an upper triangular matrix with all entries equal to 0, except those on the diagonal all equal to λ, and those immediately above the diagonal (called the super-diagonal) all equal to 1. A **Jordan matrix** is a square diagonal block matrix with all its block matrices being Jordan blocks (not necessarily of the same size).

Theorem 6.9: Jordan normal form

Every $n \times n$ matrix M over an algebraically closed field $\mathbb{F}$ is similar to some unique(up to the order of the blocks on the main diagonal) $n \times n$ Jordan matrix (called the Jordan normal form of M) over $\mathbb{F}$([3, p. 69]).

Every block of stone has a statue inside it and it is the task of the sculptor to discover it.

$\sim$ Michelangelo (1475-1564)

7 The conjugacy classes of $GL(\mathbb{Z}_p, 2)$

We shall now consider the automorphisms of groups of the form $\mathbb{Z}_p^2$ for any prime p. Corollary 6.6 assures us that every automorphism of $\mathbb{Z}_p^2$ can be represented by a 2×2 invertible matrix over the ring $\mathbb{Z}_p$, and all of these describes the automorphisms of $\mathbb{Z}_p^2$. If we want to know what the action of an automorphism f is on some element $x \in \mathbb{Z}_p^2$, we simply represent the element x as a column of length 2, and multiply it from the left by the matrix, A, which is the matrix representation of f. For any x we can write down the cycle of, say, length k containing x as $(x, Ax, A^2x, \ldots, A^{k-1}x)$, with $A^k x = x$.

Lemma 7.1: If F is a finite field, and $A, B \in GL(F, n)$ are similar, then they determine the same cyclic structure on the group F^n.

Proof:
Let $B = QAQ^{-1}$ for some $Q \in GL(F, n)$. Consider an arbitrary cycle $(v_1, v_2, \ldots, v_t)$ of A in F^n (meaning $Av_i = v_{i+1}$ for all $1 \leq i \leq t-1$ and $Av_t = v_1$). Then $v_i = Q^{-1}w_i$ for (uniquely determined) $w_i \in F^n, 1 \leq i \leq t$. So, for $1 \leq i \leq t$, we have $QAv_i = QAQ^{-1}w_i = Bw_i$, i.e. $w_{i+1} = Bw_i$ (indices taken modulo t), and the cycle $(w_1, w_2, \ldots, w_t)$ is established for B. From the bijectivity of Q (and Q^{-1}), it is clear that disjoint cycles $(v_1, v_2, \ldots, v_t)$ and $(v'_1, v'_2, \ldots, v'_s)$ of A will establish disjoint cycles $(w_1, w_2, \ldots, w_t)$ and $(w'_1, w'_2, \ldots, w'_s)$ of B. $\square$
We will partition the general linear group $GL(\mathbb{Z}_p, 2)$ into equivalence classes of similar matrices, after which Lemma 7.1 allows us to choose only one representative from each equivalence class and only investigate it's cyclic structure instead of having to look at the cyclic structures of all the elements of the general linear group individually. The conjugacy classes of $GL(\mathbb{Z}_p, 2)$ under matrix multiplication are exactly the classes of similar matrices in $GL(\mathbb{Z}_p, 2)$.

Definition 7.2: **Conjugate, conjugacy class**

Given any group G and $x, y \in G$, y is called a **conjugate** of x iff $y = gxg^{-1}$ for some $g \in G$. The set of all elements from G which are conjugate to x is called the **conjugacy class*** of x, denoted by C_x.

*Conjugacy classes can be defined in the somewhat broader setting of group actions([1, p. 328]), however we use a somewhat restricted version in which the sets which are acted on are the groups themselves.

Definition 7.3: Stabilizer

For any x in a group G, the set of all $g \in G$ for which $gxg^{-1} = x$ is called the **stabilizer** of x, denoted by $Z(x)$.

Theorem 7.4: The Orbit-Stabilizer Theorem([1, p. 158])

For any finite group G and $x \in G$

$$|G| = |C_x||Z(x)|.$$

□

In the context of $GL(\mathbb{Z}_p, 2)$, we shall invoke Theorem 7.4 with the group operation taken to be matrix multiplication.

Theorem 6.9 guarantees the existence of a matrix in Jordan normal form (possibly over a quadratic extension of $\mathbb{Z}_p$) in each conjugacy class of $GL(\mathbb{Z}_p, 2)$. If all the eigenvalues of $M \in GL(\mathbb{Z}_p, 2)$ are in $\mathbb{Z}_p$, the Jordan normal form of M is once again a matrix over $\mathbb{Z}_p$, which means we need to consider all Jordan normal matrices of the forms $\begin{bmatrix}\lambda & 0\\ 0 & \lambda\end{bmatrix}$, $\begin{bmatrix}\lambda_1 & 0\\ 0 & \lambda_2\end{bmatrix}$ and $\begin{bmatrix}\lambda & 1\\ 0 & \lambda\end{bmatrix}$ with non-zero $\lambda, \lambda_1, \lambda_2 \in \mathbb{Z}_p, \lambda_1 \neq \lambda_2$. If the eigenvalues of M however do not lie in $\mathbb{Z}_p$, they must lie in the quadratic field extension $\mathbb{Z}_p(\alpha)$ of $\mathbb{Z}_p$, a root of the (irreducible over $\mathbb{Z}_p$) characteristic polynomial of M. Since α is an eigenvalue of M, so is $\bar{\alpha}$ (the conjugate of α). But as $\alpha \neq \bar{\alpha}$ (both being outside $\mathbb{Z}_p$), the Jordan form of M is $\begin{bmatrix}\alpha & 0\\ 0 & \bar{\alpha}\end{bmatrix}$. We shall now investigate the conjugacy classes by looking at their representatives in Jordan normal form.

1. **Diagonalizable matrices, repeated eigenvalue:** These are all the matrices A which are conjugate to Jordan normal matrices of the form $R_A = \begin{bmatrix}\lambda & 0\\ 0 & \lambda\end{bmatrix}$, $\lambda \in \mathbb{Z}_p - \{0\}$.

   If $B = \begin{bmatrix}r & s\\ v & u\end{bmatrix} \in Z(R_A)$, then $\begin{bmatrix}r & s\\ v & u\end{bmatrix} \cdot \begin{bmatrix}\lambda & 0\\ 0 & \lambda\end{bmatrix} = \begin{bmatrix}\lambda & 0\\ 0 & \lambda\end{bmatrix} \cdot \begin{bmatrix}r & s\\ v & u\end{bmatrix}$. Thus $\begin{bmatrix}r\lambda & s\lambda\\ v\lambda & u\lambda\end{bmatrix} = \begin{bmatrix}r\lambda & s\lambda\\ v\lambda & u\lambda\end{bmatrix}$ which holds for all matrices $B \in GL(\mathbb{Z}_p, 2)$. Consequently, $|Z(R_A)| = |Z(A)| = |GL(\mathbb{Z}_p, 2)|$ and by Theorem 7.4, $|C_A| = 1$. The conjugacy class of A is the singleton class consisting of only A.

   It follows from Fermat's Little Theorem ([5, p. 63]) that $\begin{bmatrix}\lambda & 0\\ 0 & \lambda\end{bmatrix}^{p-1} = \begin{bmatrix}\lambda^{p-1} & 0\\ 0 & \lambda^{p-1}\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$. We shall denote the multiplicative order of λ by $\text{ord}(\lambda)$. Also note that $\text{ord}(\lambda)|p-1$. Let r be a primitive root modulo p ([6, p. 154]).

   For each $d|p-1$, $\begin{bmatrix}r^{\frac{(p-1)i}{d}} & 0\\ 0 & r^{\frac{(p-1)i}{d}}\end{bmatrix}$ has order d for all $i < d$, relatively prime with d. Consequently, there are $\varphi(d)$ distinct conjugacy classes of

diagonalizable matrices with repeated eigenvalues, all of which has order d for any $d|p-1$, each containing one member.

2. **Diagonalizable matrices, distinct eigenvalues:** These are all matrices A conjugate to a matrix of the form $R_A = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}$, with $\lambda_1, \lambda_2 \in \mathbb{Z}_p - \{0\}, \lambda_1 \neq \lambda_2$. $B = \begin{bmatrix} r & s \\ v & u \end{bmatrix} \in Z(R_A)$ iff $\begin{bmatrix} r & s \\ v & u \end{bmatrix} \cdot \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} \cdot \begin{bmatrix} r & s \\ v & u \end{bmatrix}$ which is equivalent to

$$\begin{bmatrix} r\lambda_1 & s\lambda_2 \\ v\lambda_1 & u\lambda_2 \end{bmatrix} = \begin{bmatrix} r\lambda_1 & s\lambda_1 \\ v\lambda_2 & u\lambda_2 \end{bmatrix}.$$

This holds iff $v = s = 0$, meaning $Z(R_A)$ is the set of all diagonal matrices with nonzero entries on the diagonal, hence $|Z(A)| = |Z(R_A)| = (p-1)^2$. By Theorems 7.4 and 6.7 it follows that

$$|C_A| = \frac{\left(p^2-1\right)\left(p^2-p\right)}{(p-1)^2} = p\left(p+1\right).$$

Once again we have that $\begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}^{p-1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, and $\text{ord}(A)|p-1$. Let r denote a primitive root modulo p.

For any $d_1|p-1$ and $d_2|p-1$, the matrix $\begin{bmatrix} r^{\frac{(p-1)i}{d_1}} & 0 \\ 0 & r^{\frac{(p-1)j}{d_2}} \end{bmatrix}$ with $\gcd(i, d_1) = \gcd(j, d_2) = 1, \text{lcm}(d_1, d_2) = d$, has order d. The number of distinct matrices of this form is

$$\kappa(d) = \sum_{lcm(a,b)=d} \varphi(a)\varphi(b),$$

which is equal to $J_2(d)$ by Proposition 3.15. We note though that we have now also counted the matrices with repeated eigenvalues, of which there are $\phi(d)$ (corresponding to $\text{lcm}(a, b) = d, i = j$), and each other conjugacy class represented by a diagonalizable matrix with two distinct eigenvalues (over $\mathbb{Z}_p$) has exactly two representatives in this set (if the one is $\begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}$, then the other is $\begin{bmatrix} \lambda_2 & 0 \\ 0 & \lambda_1 \end{bmatrix}$). The number of distinct classes represented by diagonalizable matrices of order d for each $d|p-1$ with two distinct eigenvalues in $\mathbb{Z}_p$, is accordingly given by $\frac{J_2(d)-\phi(d)}{2}$. Each of these classes has $p(p+1)$ elements.

3. **2×2 Jordan block matrices:** Denote the representative matrix by $R_A = \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}$, $\lambda \in \mathbb{Z}_p - \{0\}$. Now $B = \begin{bmatrix} r & s \\ v & u \end{bmatrix} \in Z(R_A)$ iff $\begin{bmatrix} r & s \\ v & u \end{bmatrix} \cdot \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix} = \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix} \cdot \begin{bmatrix} r & s \\ v & u \end{bmatrix}$ which is equivalent to

$$\begin{bmatrix} r\lambda & r+s\lambda \\ v\lambda & v+u\lambda \end{bmatrix} = \begin{bmatrix} r\lambda+v & u+s\lambda \\ v\lambda & u\lambda \end{bmatrix}.$$

Equality holds iff $v = 0$ and $r = u$, from which it follows that $B = \begin{bmatrix} u & s \\ 0 & u \end{bmatrix}$. B is invertible iff $\det(B) \neq 0$, which holds iff $u \neq 0$. It is now clear that u can be any one of $p-1$ possibilities and s any one of p, meaning $|Z(R_A)| = p(p-1)$. By Theorems 7.4 and 6.7 it follows that

$$|C_A| = \frac{\left(p^2-1\right)\left(p^2-p\right)}{p\,(p-1)} = p^2 - 1.$$

Now note that for any positive integer k, $\begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}^k = \begin{bmatrix} \lambda^k & k\lambda^{k-1} \\ 0 & \lambda^k \end{bmatrix}$, from which it is clear that if $\mathrm{ord}(\lambda) = d$,(of course $d|p-1$), then $\mathrm{ord}(R_A) = pd$. Furthermore, for any $d|p-1$ and primitive root r modulo p, the matrix $\begin{bmatrix} r^{\frac{(p-1)i}{d}} & 1 \\ 0 & r^{\frac{(p-1)i}{d}} \end{bmatrix}$ has order pd for each $i < d$, relatively prime to d. In conclusion, there are $\varphi(d)$ conjugacy classes of matrices conjugate to 2×2 Jordan block matrices of order pd, and each class contains p^2-1 members.

4. **Matrices without a Jordan Normal form in $\mathbb{Z}_p$:** Instead of attempting to investigate these conjugacy classes using the Jordan normal form over some field extension of $\mathbb{Z}_p$, we shall use their rational canonical forms ([10, p. 332]). Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ have characteristic equation $k(\lambda) = \lambda^2 + a_1\lambda + a_0, a_0, a_1 \in \mathbb{Z}_p$. Since A does not have a Jordan normal form over $\mathbb{Z}_p$, it follows that k is irreducible over $\mathbb{Z}_p$, as otherwise it would have decomposed into linear factors with roots (and hence eigenvalues of A) in $\mathbb{Z}_p$. This immediately implies that k is also the minimal polynomial of A, making A conjugate to the matrix $\hat{C}_A = \begin{bmatrix} 0 & -a_0 \\ 1 & -a_1 \end{bmatrix}$, being the rational canonical form of A.

If $G = \begin{bmatrix} s & t \\ u & v \end{bmatrix} \in Z(\hat{C}_A)$, then $\begin{bmatrix} s & t \\ u & v \end{bmatrix} \cdot \begin{bmatrix} 0 & -a_0 \\ 1 & -a_1 \end{bmatrix} = \begin{bmatrix} 0 & -a_0 \\ 1 & -a_1 \end{bmatrix} \cdot \begin{bmatrix} s & t \\ u & v \end{bmatrix}$ which is equivalent to

$$\begin{bmatrix} t & -a_0 s - a_1 t \\ v & -a_0 u - a_1 v \end{bmatrix} = \begin{bmatrix} -a_0 u & -a_0 v \\ s - a_1 u & t - a_1 v \end{bmatrix}$$

from which it follows that $t = -a_0 u$, $-a_0 s + a_1 a_0 u - a_0 v$ and $s = v + a_1 u$, and thus $G = \begin{bmatrix} v + a_1 u & -a_0 u \\ u & v \end{bmatrix}$, with $\det(G) = v(v + a_1 u) + a_0 u^2 = v^2 + a_1 uv + a_0 u^2$. We now claim that for any $(u, v) \neq (0, 0)$, $\det(G) \neq 0$, meaning that $G \in GL(\mathbb{Z}_p, 2)$. To see this, first note that if $(u, v) = (0, 0)$ then $\det(G) = 0$, and $G \notin GL(\mathbb{Z}_p, 2)$.

If $(u, v) = (0, v), v \neq 0$, then $\det(G) = v^2 \neq 0$.

Now consider the case $u \neq 0$. Suppose for the sake of contradiction that $\det(G) = 0$. then $v^2 + a_1uv + a_0u^2 = 0$, from which it follows that $\left(vu^{-1}\right)^2 + a_1\left(vu^{-1}\right) + a_0 = 0$, making $vu^{-1} \in \mathbb{Z}_p$ a root of k. This is clearly a contradiction, as k is irreducible over $\mathbb{Z}_p$. Since all non-zero pairs $(u, v) \in \mathbb{Z}_p^2$ leads to G being invertible, we have that $|Z(A)| = |Z(\hat{C}_A)| = p^2 - 1$. By invoking Theorem 7.4 yet again, it follows that $|C_A| = p(p-1)$.

Even though these matrices do not have Jordan normal forms over $\mathbb{Z}_p$, we know that they are indeed conjugate to matrices of the form $\begin{bmatrix}\alpha & 0\\ 0 & \bar{\alpha}\end{bmatrix}$ in some quadratic field extension $\mathbb{Z}_p(\beta)$ of $\mathbb{Z}_p$. By the Primitive Root Theorem, we note that $\alpha = \beta^k$ for some $k \in \mathbb{N}$, and $\text{ord}(\beta) = p^2 - 1$, and $\text{ord}(\alpha)|p^2 - 1$. Note however that since $\mathbb{Z}_p(\beta)$ is a finite field with p^2 elements, it is ring isomorphic to the Galois field $GF(p^2)$. The Galois field $GF(p^2)$ contains exactly $\varphi(d)$ elements each of order $d|p^2 - 1$, and since the diagonalizable matrices with repeated eigenvalue in $\mathbb{Z}_p$ of order $d|p - 1$ already amounts to $\varphi(d)$ matrices, there are no additional matrices with the mentioned Jordan normal form over $\mathbb{Z}_p(\beta)$ with order d, where $d|p-1$. Consequently all of the matrices considered here have orders dividing $p^2 - 1$ but not $p - 1$. For each d and relatively prime $j < d$, the matrix $\begin{bmatrix}\beta^{\frac{(p^2-1)j}{d}} & 0\\ 0 & \bar{\beta}^{\frac{(p^2-1)j}{d}}\end{bmatrix}$ has order d. Consequently, for all d dividing $p^2 - 1$ but not $p - 1$, there are $\frac{\varphi(d)}{2}$ disjoint conjugacy classes in $GL(\mathbb{Z}_p(\beta), 2)$, each of size $p(p-1)$. The factor $\frac{1}{2}$ is once again a compensation for over counting each class twice, once represented by $\begin{bmatrix}\alpha & 0\\ 0 & \bar{\alpha}\end{bmatrix}$ and then again by $\begin{bmatrix}\bar{\alpha} & 0\\ 0 & \alpha\end{bmatrix}$. We now remind ourselves that we want to find the number of conjugacy classes of order d in $GL(\mathbb{Z}_p, 2)$, not $GL(\mathbb{Z}_p(\beta), 2)$! It might be possible that some of these conjugacy classes do not at all have representatives as matrices over $\mathbb{Z}_p$, which means that they should be discarded. This (fortunately!) does not occur, meaning, for every $d|p^2 - 1$ not dividing $p - 1$, there is always a matrix of the form discussed here, of order d.

To see this, suppose that some of the conjugacy classes found do not have representatives in $GL(\mathbb{Z}_p, 2)$. If we then count the number of matrices classified, there would be strictly more than the size of $GL(\mathbb{Z}_p, 2)$, as we would have counted all elements within the general linear group as well as a few extra classes of matrices diagonalizable over $\mathbb{Z}_p(\beta)$. We will see that counting all of the matrices classified so far gives us exactly the size of $GL(\mathbb{Z}_p, 2)$ as stated by Theorem 6.7. Hence no conjugacy class in part (4) should thus be discarded.

So far we saw that the diagonalizable matrices with repeated eigenvalue contributes $\varphi(d)$ matrices to $GL(\mathbb{Z}_p, 2)$ for each $d|p - 1$. The diagonaliz-

able matrices with distinct eigenvalues contributes $p(p+1)\left(\frac{J_2(d)-\phi(d)}{2}\right)$ matrices for each $d|p-1$, and the 2×2 Jordan block matrices contributes $(p^2-1)\varphi(d)$ matrices for each $d|p-1$. The maximum number of possible matrices in $GL(\mathbb{Z}_p,2)$ without Jordan normal form (over $\mathbb{Z}_p$) is $\frac{\varphi(d)p(p-1)}{2}$ for each $d|p^2-1$ not dividing $p-1$.

Counting the number of matrices which have classified so far, we get

$$\sum_{d|p-1}\left(\varphi(d)+p(p+1)\left(\tfrac{J_2(d)-\varphi(d)}{2}\right)+(p^2-1)\varphi(d)\right)+\tfrac{p(p-1)}{2}\sum_{d|p^2-1,d\nmid p-1}\varphi(d),$$

which simplifies to

$$\sum_{d|p-1}\left(p(p+1)\left(\tfrac{J_2(d)-\varphi(d)}{2}\right)+p^2\varphi(d)\right)+\tfrac{p(p-1)}{2}\sum_{d|p^2-1}\varphi(d)-\sum_{d|p-1}\varphi(d).$$

We know from Lemma 3.8 that $\sum_{d|n}\varphi(d)=n$, and from Corollary 3.13 that $\sum_{d|n}J_2(d)=n^2$. Which means that the previous expression can be simplified to

$$\frac{p(p+1)}{2}\left((p-1)^2-(p-1)\right)+p^2(p-1)+p(p-1)\left((p^2-1)-(p-1)\right).$$

After expansion, simplification and factorization this expression reduces to

$$(p^2-p)(p^2-1),$$

which is exactly the size of $GL(\mathbb{Z}_p,2)$, meaning that no conjugacy class should be discarded, completing our classification of all conjugacy classes of $GL(\mathbb{Z}_p,2)$. We summarize our findings in a table:

Theorem 7.5: **Full classification of all conjugacy classes of $GL(\mathbb{Z}_p,2)$**

Type \ Order	$d, d\|p-1$	$d, d\|p^2-1, d\nmid p-1$	$pd, d\|p-1$
$\begin{bmatrix}\lambda & 0\\ 0 & \lambda\end{bmatrix}$	$\varphi(d)$ [1]	0 [0]	0 [0]
$\begin{bmatrix}\lambda_1 & 0\\ 0 & \lambda_2\end{bmatrix}$, $\lambda_1\neq\lambda_2$	$\frac{J_2(d)-\varphi(d)}{2}$ $[p(p+1)]$	0 [0]	0 [0]
$\begin{bmatrix}\lambda & 1\\ 0 & \lambda\end{bmatrix}$	0 [0]	0 [0]	$\varphi(d)$ $[p^2-1]$
$\begin{bmatrix}\alpha & 0\\ 0 & \bar{\alpha}\end{bmatrix}$	0 [0]	$\frac{\varphi(d)}{2}$ $[p(p-1)]$	0 [0]

Each cell in the table shows the number of distinct conjugacy classes of order and representation type, followed by the size of the corresponding conjugacy class in square brackets. □

A table of all conjugacy classes similar to this one, was found on the internet at [17], however at the date of this writing, it contained an error as well as no proof for the obtained results. The author thus took it upon himself to locate and fix the error by manufacturing the proof above.

The art of doing mathematics consists in finding that special case which contains all the germs of generality.

$\sim$ D. Hilbert (1862-1943)

8 Structural classification of all automorphisms on groups of order p^2

We shall now investigate the cyclic structures of automorphisms of abelian groups of order p^2, with p a prime. Theorem 4.6 implies that any abelian group of order p^2 must be isomorphic to either $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p^2$. Theorem 5.1 already gave a complete description of the $\mathbb{Z}_{p^2}$ case. Hence, if we can find the cyclic structures of all the automorphisms of $\mathbb{Z}_p^2$, we will have a complete description of all bijections from a set of order p^2 to itself, which has the automorphism property.

Corollary 6.6 shows that any automorphism acting on $\mathbb{Z}_p^2$ can be naturally represented by an element of $GL(\mathbb{Z}_p, 2)$. It follows from Lemma 7.1 that we only need to consider one element from every conjugacy class in order to find all the possible cyclic structures, and Theorem 7.5 provides us with a representative (in Jordan normal form) from every conjugacy class in $GL(\mathbb{Z}_p, 2)$. We shall now proceed by finding the cyclic structure of a Jordan normal form representative from each conjugacy class.

In the discussion that follows, for any α in the finite field F, we shall use the notation $o^+(\alpha)$ for the additive order of α, and $o^\cdot(\alpha)$ for the multiplicative order of α.

1. We shall first consider the matrices which has a Jordan normal form $A = \begin{bmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{bmatrix}$, where $\alpha_1, \alpha_2 \in U_p$.* The order of such an A is a divisor of $p-1$ (by Theorem 7.5). Let $o^\cdot(\alpha_1) = d_1$ and $o^\cdot(\alpha_2) = d_2$, where d_1 and d_2 are divisors of $p-1$. The automorphism represented by A has $\frac{p-1}{d_1}$ cycles of the form
$$\left(\begin{bmatrix} x \\ 0 \end{bmatrix}, \begin{bmatrix} \alpha_1 x \\ 0 \end{bmatrix}, \ldots, \begin{bmatrix} \alpha_1^{d_1-1} x \\ 0 \end{bmatrix} \right),$$
each of length d_1, where $x \in U_p$;
$\frac{p-1}{d_2}$ cycles of the form
$$\left(\begin{bmatrix} 0 \\ y \end{bmatrix}, \begin{bmatrix} 0 \\ \alpha_2 y \end{bmatrix}, \ldots, \begin{bmatrix} 0 \\ \alpha_2^{d_2-1} y \end{bmatrix} \right),$$
each of length d_2, where $y \in U_p$;
$\frac{(p-1)^2}{\mathrm{lcm}(d_1,d_2)}$ cycles of the form
$$\left(\begin{bmatrix} x \\ y \end{bmatrix}, \begin{bmatrix} \alpha_1 x \\ \alpha_2 y \end{bmatrix}, \ldots, \begin{bmatrix} \alpha_1^{K-1} x \\ \alpha_2^{K-1} y \end{bmatrix} \right),$$

*Recall that U_p is the group of all units (i.e. invertible elements) of the ring $\mathbb{Z}_p$.

each of length $K = \text{lcm}(d_1, d_2)$, where $x, y \in U_p$.

In the event that $\alpha_1 = \alpha_2 = \alpha$ (say), with $o^{\cdot}(\alpha) = d$, then the automorphism represented by $A = \begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix}$ has $\frac{p^2-1}{d}$ cycles of the form

$$\left(\begin{bmatrix} x \\ y \end{bmatrix}, \begin{bmatrix} \alpha_1 x \\ \alpha_2 y \end{bmatrix}, \ldots, \begin{bmatrix} \alpha_1^{d-1} x \\ \alpha_2^{d-1} y \end{bmatrix} \right),$$

each of length d, where $x, y \in \mathbb{Z}_p$, not both 0.

2. Now we consider the matrices with Jordan normal form $A = \begin{bmatrix} \alpha & 1 \\ 0 & \alpha \end{bmatrix}$, where $\alpha \in U_p$. Using Theorem 7.5, we conclude that these all have order pd, with $d = o^{\cdot}(\alpha)$ a divisor of $p-1$. Since the conjugacy classes are all non-empty, there is such an A for any $d|p-1$. The automorphism represented by A, has $\frac{p-1}{d}$ cycles of the form

$$\left(\begin{bmatrix} x \\ 0 \end{bmatrix}, \begin{bmatrix} \alpha x \\ 0 \end{bmatrix}, \ldots, \begin{bmatrix} \alpha^{d-1} x \\ 0 \end{bmatrix} \right),$$

each of length d, where $x \in U_p$;
A has $\frac{p-1}{d}$ cycles of the form

$$\left(\begin{bmatrix} x \\ y \end{bmatrix}, \begin{bmatrix} \alpha x + y \\ \alpha y \end{bmatrix}, \ldots, \begin{bmatrix} \alpha^k x + k\alpha^{k-1} y \\ \alpha^k y \end{bmatrix}, \ldots \begin{bmatrix} \alpha^{pd-1} x + (pd-1)\alpha^{pd-2} y \\ \alpha^{pd-1} y \end{bmatrix} \right),$$

each of length pd, where $x, y \in \mathbb{Z}_p$, with $y \neq 0$. (Note that $o^{+}(d\alpha^{pd-1} y) = p$.)

3. The only remaining case is the Jordan normal form $\tilde{A} = \begin{bmatrix} \beta & 0 \\ 0 & \bar{\beta} \end{bmatrix}$, where $\beta, \bar{\beta} \in \mathbb{Z}_p(\beta)$, a quadratic field extension of $\mathbb{Z}_p$ (β and $\bar{\beta}$ are conjugate roots of an irreducible quadratic polynomial over $\mathbb{Z}_p$). Theorem 7.5 demonstrates the existence of a matrix $A \in GL(\mathbb{Z}_p, 2)$ similar to $\tilde{A}$ of any order d, dividing $p^2 - 1$ but not $p - 1$. For all $x, y \in \mathbb{Z}_p(\beta)$, not both 0, the cycle

$$\left(\begin{bmatrix} x \\ y \end{bmatrix}, \begin{bmatrix} \beta x \\ \bar{\beta} y \end{bmatrix}, \begin{bmatrix} \beta^2 x \\ \bar{\beta}^2 y \end{bmatrix}, \ldots, \begin{bmatrix} \beta^{d-1} x \\ \bar{\beta}^{d-1} y \end{bmatrix} \right),$$

has length d, since $o^{\cdot}(\beta) = o^{\cdot}(\bar{\beta})$. It follows from Lemma 7.1 that all of the cycles of A in $\mathbb{Z}_p(\beta)^2$ must have length d, so by restricting the action of A to $\mathbb{Z}_p^2$, all the non-zero cycles are of length d.

Since we have investigated all possible Jordan forms of 2×2 matrices over $\mathbb{Z}_p$, we now have all the cyclic structures of the group automorphisms of $\mathbb{Z}_p^2$. We summarise our findings as a Theorem:

Theorem 8.1: Let $|A| = p^2$ where p is prime, and let $f : A \to A$ be a bijection. Then f has the automorphism property iff f has one of the following cyclic structures:

1. $\begin{bmatrix} \frac{p^2-1}{d} & 1 \\ d & 1 \end{bmatrix}$ for some divisor d of $p^2 - 1$;
2. $\begin{bmatrix} \frac{p-1}{d} & \frac{p-1}{d} & 1 \\ pd & d & 1 \end{bmatrix}$ for some divisor d of $p - 1$;
3. $\begin{bmatrix} \frac{(p-1)^2}{\mathrm{lcm}(d_1,d_2)} & \frac{p-1}{d_1} & \frac{p-1}{d_2} & 1 \\ \mathrm{lcm}(d_1, d_2) & d_1 & d_2 & 1 \end{bmatrix}$ for divisors d_1, d_2 of $p - 1$.

□

Example 8.2: Let $p = 7$. Then case (1) of Theorem 8.1 that does not coincide with case (3) comes from the divisors of $p^2 - 1 = 48$, that are not divisors of 6, namely $d \in \{4, 8, 12, 16, 24, 48\}$. For these divisors we obtain the following corresponding cyclic structures

$$\begin{bmatrix} 12 & 1 \\ 4 & 1 \end{bmatrix}, \begin{bmatrix} 6 & 1 \\ 8 & 1 \end{bmatrix}, \begin{bmatrix} 4 & 1 \\ 12 & 1 \end{bmatrix}, \begin{bmatrix} 3 & 1 \\ 16 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 24 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 48 & 1 \end{bmatrix}.$$

The divisors of $p - 1 = 6$ are $d \in \{1, 2, 3, 6\}$, so Theorem 8.1(2) gives the corresponding cyclic structures

$$\begin{bmatrix} 6 & 6 & 1 \\ 7 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 6 & 7 \\ 7 & 1 \end{bmatrix}, \begin{bmatrix} 3 & 3 & 1 \\ 14 & 2 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 2 & 1 \\ 21 & 3 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 \\ 42 & 6 & 1 \end{bmatrix}.$$

Finally, for the remaining cases, we consider Theorem 8.1(3), where we take $d_1, d_2 \in \{1, 2, 3, 6\}$ and we may assume $1 \leq d_1 \leq d_2 \leq 6$. We obtain the cyclic structures

$$\begin{bmatrix} 36 & 6 & 6 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 49 \\ 1 \end{bmatrix}, \begin{bmatrix} 18 & 6 & 3 & 1 \\ 2 & 1 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 21 & 7 \\ 2 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 12 & 6 & 2 & 1 \\ 3 & 1 & 3 & 1 \end{bmatrix} = \begin{bmatrix} 14 & 7 \\ 3 & 1 \end{bmatrix}, \begin{bmatrix} 6 & 6 & 1 & 1 \\ 6 & 1 & 6 & 1 \end{bmatrix} = \begin{bmatrix} 7 & 7 \\ 6 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 18 & 3 & 4 & 1 \\ 2 & 2 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 24 & 1 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 6 & 3 & 2 & 1 \\ 6 & 2 & 3 & 1 \end{bmatrix} = \begin{bmatrix} 6 & 2 & 3 & 1 \\ 6 & 3 & 2 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 6 & 3 & 1 & 1 \\ 6 & 2 & 6 & 1 \end{bmatrix} = \begin{bmatrix} 7 & 3 & 1 \\ 6 & 2 & 1 \end{bmatrix}, \begin{bmatrix} 12 & 2 & 2 & 1 \\ 3 & 3 & 3 & 1 \end{bmatrix} = \begin{bmatrix} 16 & 1 \\ 3 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 6 & 2 & 1 & 1 \\ 6 & 3 & 6 & 1 \end{bmatrix} = \begin{bmatrix} 7 & 2 & 1 \\ 6 & 3 & 1 \end{bmatrix}, \begin{bmatrix} 6 & 1 & 1 & 1 \\ 6 & 6 & 6 & 1 \end{bmatrix} = \begin{bmatrix} 8 & 1 \\ 6 & 1 \end{bmatrix}$$

Consequently, if $|A| = 49$ and $f : A \to A$ is a bijection then A can be made into a group isomorphic to $\mathbb{Z}_7^2$ with $f \in Aut(\mathbb{Z}_7^2)$ iff f has one of the 20 cyclic structures shown here.

One immediately raises the question on how the cyclic structures of automorphisms on $\mathbb{Z}_{p^2}$ relate to the cyclic structures of automorphisms on $\mathbb{Z}_p^2$. It turns out that the former forms a subset of the latter.

Proposition 8.3: Let $|A| = p^2$, with p prime, and let $f : A \to A$ be a bijection. Then f has the automorphism property iff f has one of the cyclic structures of an automorphism of $\mathbb{Z}_p^2$, given by Theorem 8.1.

Proof:
It suffices to show that every cyclic structure that appears in example 5.5, also appears in Theorem 8.1. According to the analysis in Example 5.5, there are two possibilities for the parameters $l_i = \mathrm{ord}_{p^2}(k_i), 2 \leq i \leq p^2 - p$ and $\lambda = \mathrm{ord}_p(k_i)$, namely

1. $l_i = \lambda$. This gives the cyclic structure $\begin{bmatrix} \frac{p^2-p}{\lambda} + \frac{p-1}{\lambda} & 1 \\ \lambda & 1 \end{bmatrix} = \begin{bmatrix} \frac{p^2-1}{\lambda} & 1 \\ \lambda & 1 \end{bmatrix}$, which agrees with the cyclic structure of Theorem 8.1.3 with $d_1 = d_2 = \lambda$. (Recall that $\lambda | p - 1$.)

2. $l_i = p\lambda$. This gives the cyclic structure $\begin{bmatrix} \frac{p^2-p}{p\lambda} & \frac{p-1}{\lambda} & 1 \\ p\lambda & \lambda & 1 \end{bmatrix} = \begin{bmatrix} \frac{p-1}{\lambda} & \frac{p-1}{\lambda} & 1 \\ p\lambda & \lambda & 1 \end{bmatrix}$, which agrees with the cyclic structure of Theorem 8.1.2 with $d = \lambda$.

□

Proposition 8.3 is in itself a truly remarkable result, and it is very natural to ask whether it might be generalized. For example, if you want to know if a bijective function f has the automorphism property if the domain of f is say a set with 32 elements, it would be very useful if we could only search through the automorphisms of $\mathbb{Z}_2^5$ rather than having to look at all the automorphisms of all the groups $\mathbb{Z}_{2^5}, \mathbb{Z}_2 \times \mathbb{Z}_{2^4}, \mathbb{Z}_2^2 \times \mathbb{Z}_{2^3}, \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^3}, \mathbb{Z}_2^3 \times \mathbb{Z}_{2^2}, \mathbb{Z}_2 \times \mathbb{Z}_2^2, \mathbb{Z}_2^5$, and be assured that we have indeed found all cyclic structures. Our next result however completely shatters any hope of this, by providing a counter example.

Example 8.4: The group $\mathbb{Z}_8$ has an automorphism of which the cyclic structure is different from that of all automorphisms of $\mathbb{Z}_2^3$.

Proof:
Consider $f : \mathbb{Z}_8 \to \mathbb{Z}_8$ defined by $f(x) = -x$. The cyclic structure of f is $\begin{bmatrix} 3 & 2 \\ 2 & 1 \end{bmatrix}$.
Now suppose for the sake of contradiction that there is an automorphism, g, of $\mathbb{Z}_2^3$ which has the same cyclic structure. We know from Corollary 6.6 that g can be represented by a matrix $A \in GL(\mathbb{Z}_2, 3)$. Suppose

$$A = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{bmatrix}.$$

Since the cyclic structure of g has two cycles of length 1, there must be some non-zero element $\begin{bmatrix} \alpha \\ \beta \\ \gamma \end{bmatrix} \in \mathbb{Z}_2^3$ that maps to itself.

Note that for all $x \in \mathbb{Z}_2^3$, $Ax+x$ has cycle length 1, hence $Ax+x \in \left\{ \begin{bmatrix}0\\0\\0\end{bmatrix}, \begin{bmatrix}\alpha\\\beta\\\gamma\end{bmatrix} \right\}$.

Now suppose that $Ax + x = \begin{bmatrix}0\\0\\0\end{bmatrix}$. Then $x = -Ax = Ax$ (for all $x \in \mathbb{Z}_2^3$, $x = -x$), placing x in a cycle of length 1. Thus for all elements $x \in \mathbb{Z}_2^3$ not in a cycle of length 1, we have $Ax + x = \begin{bmatrix}\alpha\\\beta\\\gamma\end{bmatrix}$. If $\begin{bmatrix}\alpha\\\beta\\\gamma\end{bmatrix} = \begin{bmatrix}1\\0\\0\end{bmatrix}$, then

$$A\begin{bmatrix}0\\1\\0\end{bmatrix} + \begin{bmatrix}0\\1\\0\end{bmatrix} = \begin{bmatrix}\alpha_{12}\\\alpha_{22}+1\\\alpha_{32}\end{bmatrix} = \begin{bmatrix}1\\0\\0\end{bmatrix}, A\begin{bmatrix}0\\0\\1\end{bmatrix} + \begin{bmatrix}0\\0\\1\end{bmatrix} = \begin{bmatrix}\alpha_{13}\\\alpha_{23}\\\alpha_{33}+1\end{bmatrix} = \begin{bmatrix}1\\0\\0\end{bmatrix}$$

giving $A = \begin{bmatrix}1&1&1\\0&1&0\\0&0&1\end{bmatrix}$, which has cyclic structure $\begin{bmatrix}4&2\\1&2\end{bmatrix}$, which is a contradiction, hence

$$A\begin{bmatrix}1\\0\\0\end{bmatrix} \neq \begin{bmatrix}1\\0\\0\end{bmatrix} \text{ and similarly } A\begin{bmatrix}0\\1\\0\end{bmatrix} \neq \begin{bmatrix}0\\1\\0\end{bmatrix}, A\begin{bmatrix}0\\0\\1\end{bmatrix} \neq \begin{bmatrix}0\\0\\1\end{bmatrix}.$$

meaning that these three elements must be in cycles of length 2, so

$$\begin{bmatrix}1+\alpha_{11}\\\alpha_{21}\\\alpha_{31}\end{bmatrix} = \begin{bmatrix}\alpha_{12}\\\alpha_{22}+1\\\alpha_{32}\end{bmatrix} = \begin{bmatrix}\alpha_{13}\\\alpha_{23}\\\alpha_{33}+1\end{bmatrix} = \begin{bmatrix}\alpha\\\beta\\\gamma\end{bmatrix}.$$

Thus

$$A = \begin{bmatrix}\alpha+1&\alpha&\alpha\\\beta&\beta+1&\beta\\\gamma&\gamma&\gamma+1\end{bmatrix}.$$

However, since $A\begin{bmatrix}\alpha\\\beta\\\gamma\end{bmatrix} = \begin{bmatrix}\alpha\\\beta\\\gamma\end{bmatrix}$, we have that $\alpha(\alpha+1) + \alpha\beta + \alpha\gamma = \alpha$, which means that

$$\alpha(\alpha+\beta+\gamma) = 0$$

and similarly

$$\beta(\alpha+\beta+\gamma) = 0$$
$$\gamma(\alpha+\beta+\gamma) = 0.$$

If $\alpha + \beta + \gamma \neq 0$, then $\alpha = \beta = \gamma = 0$, which is clearly a contradiction, so $\alpha + \beta + \gamma = 0$. As α, β, γ cannot all be equal to 0, the only way that this can be is if two of the three are equal to 1, and the other one equal to 0, so w.l.o.g. assume that $\begin{bmatrix} \alpha \\ \beta \\ \gamma \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$. Consequently $A = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}$, which has cyclic structure $\begin{bmatrix} 4 & 2 \\ 1 & 2 \end{bmatrix}$, which is once again a contradiction.

Hence the cyclic structure $\begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}$ is not associated with any of the group automorphisms of $\mathbb{Z}_2^3$, even though it does occur as the cyclic structure of an automorphism of $\mathbb{Z}_8$.

□

The infinite! No other question has ever moved so profoundly the spirit of man.

$\sim$ D. Hilbert (1862-1943)

9 The automorphisms of $\mathbb{Z}^n$ with variable n

We will now investigate the cyclic structures of the automorphisms of all groups of the form $\mathbb{Z}^n$. Once again Proposition 4.4 tells us that there must be a zero cycle. Since $\mathbb{Z}$ is infinite there is the possibility of not only having cycles such as with the $\mathbb{Z}_p$ cases, but also chains. One of the major tools that we used to investigate the automorphisms of the finite groups was the fact that the elements of the general linear group were much more than just matrices over rings, but they were actually matrices over fields, which allowed us to use the Jordan normal form to form conjugacy classes which partitioned the general linear group. In the case of matrices over $\mathbb{Z}$ this cannot be done, as $\mathbb{Z}$ is not a field. Even though we have lost the Jordan normal forms, we still have that the Automorphism group is isomorphic to $GL(\mathbb{Z}, n)$ by Corollary 6.6. These are clearly all the $n \times n$ integer matrices with determinant equal to ± 1 ([2, p. 12]).

Proposition 9.1: Suppose $f : X \to X$ has the automorphism property with underlying group $\mathbb{Z}^n$ for some positive integer n. Then the following conditions must hold:

1. If there is any cycle apart from the zero cycle, of any length k, then there are infinitely many cycles of length k.
2. If there is a chain, there are infinitely many chains.
3. If all the base elements $e_i, i \in \{1, 2, \ldots, n\}$ are in cycles, then all elements are in cycles.

Proof:

1. Let the matrix representation of f be A, and represent the elements of the group $\mathbb{Z}^n$ as columns as usual. Now consider any non-zero cycle $T = (x, Ax, A^2x, \ldots, A^{k-1}x)$ of length k. Let S_T be the set of all the absolute values of the non-zero components of T. From the well-ordering principle on $\mathbb{N}$, we can find a (non-zero) minimum element in S_T. Now for any positive integer n, we see that $nT = (nx, A(nx), A^2(nx), \ldots, A^{k-1}(nx)) = (nx, nAx, nA^2x, \ldots, nA^{k-1}x)$ is a cycle of length k, with $S_{nT} = nS_T$, from which it follows that the cycles nT are disjoint for different $n \in \mathbb{N}$ as the minimum components are all distinct from one another. Consequently there are infinitely many cycles of length k.
2. The proof is roughly the same as that of 1. The cycle $T = (x, Ax, \ldots, A^{k-1}x)$ is just replaced by the chain $T = (\ldots, A^{-2}x, A^{-1}x, x, Ax, A^2x, \ldots)$.
3. Suppose all the base elements e_i are in cycles with the cycle containing e_i of length k_i. Any $x \in \mathbb{Z}^n$ can be represented as $x = \sum_{i=1}^{n} \alpha_i e_i, \alpha_i \in \mathbb{Z}$.

Denote the least common multiple of the set $\{k_j, j \in \{1, 2, \ldots, n\}\}$ by M, and define $q_i = \frac{M}{k_i}$. Now we notice that

$$\begin{aligned} A^M x &= \sum_{i=1}^{n} \alpha_i A^M e_i \\ &= \sum_{i=1}^{n} \alpha_i A^{(q_i-1)k_i} A^{k_i} e_i \\ &= \sum_{i=1}^{n} \alpha_i A^{(q_i-1)k_i} e_i \end{aligned}$$

as $A^{k_i} e_i = e_i$. Repeating this process of removing a A^{k_i} factor another $q_i - 1$ times we see that

$$\begin{aligned} A^M x &= \sum_{i=1}^{n} \alpha_i e_i \\ &= x \end{aligned}$$

which means that x lies in a cycle of length dividing M.

□

Proposition 9.1 tells us that if the structural graph of an automorphism only consists of cycles, then there is only a finite number of possible cycle lengths, as all cycles must be of length diving the lowest common multiple of the lengths of the cycles of the e_i's. In principle it is still possible for the structural graph to have an infinite number of distinct cycle lengths, however Proposition 9.1 tells us that the only way in which this can occur is when one of the e_i's lies in a chain.

Proposition 9.2: A structural graph with chains can have at most finitely many different cycle lengths.

Proof:
Suppose the structural graph of f has cycles of infinitely many different lengths. Suppose the matrix representation of f is an $n \times n$ matrix denoted by A.

If $n = 1$, as $\det(A) = \pm 1$, it follows that $f(1) = 1$ or $f(1) = -1$. The first case is simply the identity mapping, and the second has a cyclic structure consisting of only cycles of length two and the zero-cycle.

Assume $n \geq 2$. Let

$$x_1 = \begin{bmatrix} x_{11} \\ x_{21} \\ \vdots \\ x_{n1} \end{bmatrix}; \quad x_2 = \begin{bmatrix} x_{12} \\ x_{22} \\ \vdots \\ x_{n2} \end{bmatrix}; \quad \ldots; \quad x_i = \begin{bmatrix} x_{1i} \\ x_{2i} \\ \vdots \\ x_{ni} \end{bmatrix}; \quad \ldots; \quad x_n = \begin{bmatrix} x_{1n} \\ x_{2n} \\ \vdots \\ x_{nn} \end{bmatrix}$$

be any n distinct non-zero elements occurring in cycles. For each i, let the cycle length of x_i be s_i. Let $M = [x_1|x_2|\dots|x_n]$. From Proposition 9.1 it follows that at least one of the e_i's must lie in a chain, w.l.o.g. assume it to be e_1. Let $M(r,c)$ denote the (r,c)-minor of M.* We now form

$$y = \sum_{i=1}^{n} (-1)^{i-1} M(1,i) x_i$$

For each $i \in \{2,\dots,n\}$, the entry in the i-th row of y is clearly the determinant of the matrix

$$\begin{bmatrix} x_{i1} & x_{i2} & \dots & x_{in} \\ x_{21} & x_{22} & \dots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{i1} & x_{i2} & \dots & x_{in} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \dots & x_{nn} \end{bmatrix}$$

which is zero, as the i-th row is identical to the first row. This means all the components of y except perhaps the first, are equal to zero.
In the same way we see that the first component of y is simply the determinant of M. By denoting the least common multiple of $\{s_i, i \in \{1,2,\dots,n\}\}$ by l it is clear that

$$\begin{aligned} A^l y &= \sum_{i=1}^{n} (-1)^{i-1} M(1,i) A^l x_i \\ &= \sum_{i=1}^{n} (-1)^{i-1} M(1,i) x_i \\ &= y, \end{aligned}$$

which means that y lies in a cycle. However, the element e_1 lies in a chain, implying that all non-zero elements with only their first coefficients non-zero lie in a chain. Consequently, y must be 0 from which it follows that $\det(M) = 0$. This means that the columns of M are not linearly independent, and for fixed $x_1, x_2, \dots, x_{n-1}$, all other elements,z, that lies in some cycle can be expressed as $z = \sum_{i=1}^{n-1} \gamma_i x_i$, with $\gamma_i \in \mathbb{Q}$. It is now clear that z must have a cycle length dividing the least common multiple of the set $\{s_1, s_2, \dots, s_{n-1}\}$. Since this holds for all z occurring in cycles, it follows that a structural graph of any automorphism with a chain can have only finitely many distinct cycle lengths. □

Example 9.3: The structural graph of the automorphism represented by $A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ does not have any non-zero cycles, hence it consists only of the zero cycle, and infinitely

*The (r,c)-minor is simply the determinant of the matrix obtained by deleting the r-th row and c-th column. A comprehensive introduction to similar terms can be found in any introductory text on linear algebra, for example [9].

many chains.

Proof:
First we notice that for any positive integer n, $A^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}$ with F_n the n-th number in the Fibonacci sequence.

The proof of this is a straightforward induction on n, The result trivially holds for $n = 1$, by defining $F_0 = 0$ which is perfectly in order as it does not disturb the recursion relation of the Fibonacci sequence. Now suppose the result holds for some integer m, then

$$\begin{aligned} A^{m+1} &= \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} F_{m+1} & F_m \\ F_m & F_{m-1} \end{bmatrix} \\ &= \begin{bmatrix} F_{m+1} + F_m & F_m + F_{m-1} \\ F_{m+1} & F_m \end{bmatrix} \\ &= \begin{bmatrix} F_{m+2} & F_{m+1} \\ F_{m+1} & F_m \end{bmatrix}. \end{aligned}$$

It follows that $A^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}$ for all $n \geq 1$.

Now suppose for the sake of contradiction that the structural graph contains a non-zero cycle of length $n \in \mathbb{N}$. Then there exist $a, b \in \mathbb{Z}$ such that

$$\begin{aligned} aF_{n+1} + bF_n &= a \\ aF_n + bF_{n-1} &= b \end{aligned}$$

This can be written as

$$\begin{aligned} (F_{n+1} - 1)a + F_n b &= 0 \\ F_n a + (F_{n-1} - 1)b &= 0. \end{aligned}$$

The determinant of this system is $(F_{n+1}-1)(F_{n-1}-1)-F_n^2$, which after expansion and simplification reduces to $(F_{n+1}^2 - F_{n+1}F_n - F_n^2) + 1 - (F_{n+1} - F_{n-1})$. Cassini's identity ([4]) states that $F_{n+1}^2 - F_{n+1}F_n - F_n^2 = (-1)^n$, from which it follows that the system has a non-zero determinant, so $\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$ is the only solution.

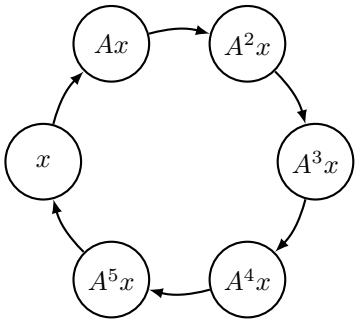
□

Definition 9.4: Primitive cycle

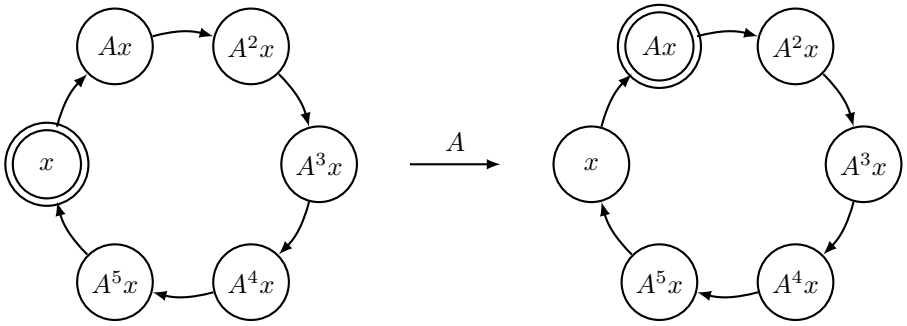
A cycle of length n is called a **primitive cycle** of a structural graph if for any d properly dividing n, there are no non-zero cycles of length d present in the structural graph. If this is the case, we shall call n a **primitive cycle length** of the structural graph.

We shall now investigate whether for any natural number n, there exists an automorphism for which all the non-zero cycles are of length n. In order to do

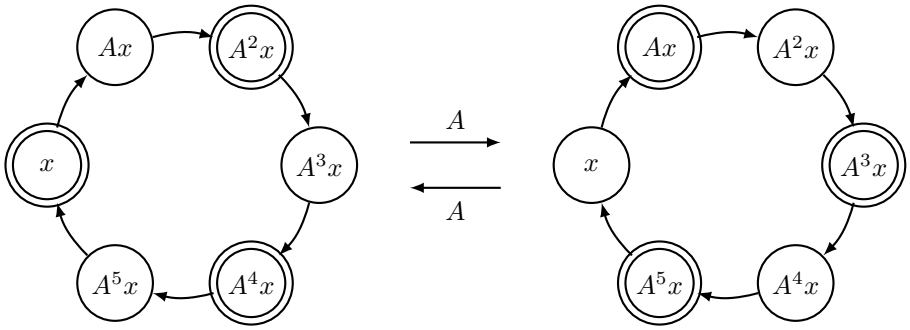
so we shall first take some inspiration on the construction of cycles from larger ones. Suppose we have some cycle $(x, Ax, A^2x, \ldots, A^5x)$ of length 6. We can represent it as



Now note how the cycle changes as we invoke A on it (we have marked the progress of x for the sake of clarity):



We will need to repeat this process another 5 times in order for x to be restored to it's initial position, however note what happens if we use $x + A^2x + A^4x$ rather than x.



The exact same term is achieved after only applying A twice, which means that $x + A^2x + A^4x$ must have a cycle length diving two. A similar result is obtained for $x + A^3x$ which must have a cycle length which divides 3. It is important to note that the cycle lengths are not necessarily of lengths 2 and 3, they could also be of length 1. At first this seems that this could severely restrict the possibilities on the numbers which could be primitive cycle lengths, however surprisingly, this result does not eventually restrict the numbers which

are primitive cycle lengths but rather tells us how to construct automorphisms with exactly those primitive cycle lengths! The idea is simple, for our 6 cycle case for example, if we can somehow get an invertible integer matrix A such that $I + A^2 + A^4 = 0$ as well as $I + A^3 = 0$, the constructed elements which could have cycle lengths of 2 and 3, will actually be the zero element, and the cycle reduces to the zero-cycle!

Example 9.5: The automorphism with matrix representation $A = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}$ has all of its non-zero cycle lengths equal to 6.

Proof:
It can be easily verified that $I + A^2 + A^4 = 0$ and $I + A^3 = 0$ and also that $A^6 = I$, which means that all cycles are of length dividing 6. Now for explicit verification, consider any $\begin{bmatrix} x \\ y \end{bmatrix}$. We have the following cyclic structure:

$$\left(\begin{bmatrix} x \\ y \end{bmatrix}, \begin{bmatrix} y \\ y-x \end{bmatrix}, \begin{bmatrix} y-x \\ -x \end{bmatrix}, \begin{bmatrix} -x \\ -y \end{bmatrix}, \begin{bmatrix} -y \\ x-y \end{bmatrix}, \begin{bmatrix} x-y \\ x \end{bmatrix} \right).$$

This is an explicit example of an automorphism of which the structural graph consists of the zero cycle, no chains and all cycles of length 6, implying that 6 is a primitive length with respect to this structural graph. □

This example paves the way towards establishing a technique that will allow us for any positive integer n, the construction of a automorphism with a structural graph having all of it's non-zero cycles of length n. The next Theorem is the first step towards this goal:

Theorem 9.6: For any $n > 1$, let $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ be the prime factorization of n, where we assume that $p_1 > p_2 > \cdots > p_k$. Define, for each $i \in \{1, \ldots, k\}$ the polynomial Q_i by

$$Q_i(\lambda) = \sum_{j=0}^{p_i - 1} \lambda^{\frac{n \cdot j}{p_i}}.$$

Then the n-th cyclotomic polynomial Φ_n divides Q_i for all $i \in \{1, 2, \ldots, k\}$. Moreover, Φ_n is the only non-constant polynomial that divides all the Q_i.
Proof:
First we notice that $\lambda^n - 1 = (\lambda^{\frac{n}{p_i}} - 1)Q_i$ for any $i \in \{1, 2, \ldots, k\}$. Let ζ be a primitive n-th root of unity. From $(\zeta^{\frac{n}{p_i}} - 1)Q_i(\zeta) = 0$ and $\zeta^{\frac{n}{p_i}} - 1 \neq 0$ it follows that $Q_i(\zeta) = 0$. An immediate consequence is that $\lambda - \zeta$ is a factor of Q_i for all primitive roots ζ of unity, so the n-th cyclotomic polynomial Φ_n divides all of the Q_i.

Now suppose that there is another non-constant polynomial R which is a factor of all the Q_i's but with a root η which is not a primitive n-th root of unity. As the roots of R must all be n-th roots of unity, it follows that $\eta = \zeta^m$ for some $m \in \{1, 2, \ldots, n\}$ and such that $\gcd(m, n) \neq 1$. However, then there exists an i such that $\eta^{\frac{n}{p_i}} - 1 = 0$, and as $Q_i(\eta) = 0$, it follows that η is a root of $\lambda^n - 1$ of multiplicity at least two. This is a contradiction, as all roots of $\lambda^n - 1$ have

multiplicity 1. □

We now proceed to a matrix theoretic Lemma, which will be of immediate use.

Lemma 9.7: Let R be a commutative ring and n a positive integer. Define the Adjoint of the $n \times n$ matrix M, denoted $\mathrm{Adj}(M)$, by $[\mathrm{Adj}(M)]_{ij} = (-1)^{i+j} M(j,i)$ with $M(j,i)$ once again denoting the (j,i)-minor. For any $M \in M_n(R)$ there holds

$$\det(M)I = M\mathrm{Adj}(M).$$

Note, $\det(M)I$ should be understood as left scalar multiplication of I by the ring element $\det(M)$.

Proof:

The left hand side is a matrix with all its diagonal entries equal to $\det(M)$ and all other entries equal to 0. We shall now expand the right hand side term by term.

Let us denote $[M]_{ij}$ by a_{ij} and $[\mathrm{Adj}(M)]_{ij}$ by b_{ij}. For all diagonal entries

$$\begin{aligned}
[M\mathrm{Adj}(M)]_{ii} &= \sum_{k=1}^{n} a_{ik} b_{ki} \\
&= \sum_{k=1}^{n} a_{ik} (-1)^{k+i} M(i,k) \\
&= \det(M).
\end{aligned}$$

For $i \neq j$,

$$\begin{aligned}
[M\mathrm{Adj}(M)]_{ij} &= \sum_{k=1}^{n} a_{ik} b_{kj} \\
&= \sum_{k=1}^{n} a_{ik} (-1)^{k+j} M(j,k),
\end{aligned}$$

which is the determinant of the matrix which is exactly the same as M, except for having row i replaced by a copy of row j, meaning that the rows are linearly dependent, and the determinant equal to 0. □

Theorem 9.8: **The Cayley-Hamilton Theorem**

For any field F, and matrix $M \in M_n(F)$, M is a root of its own characteristic polynomial.

Proof:
The proof that follows is from [7, p. 250].

Given any matrix $M \in M_n(F)$, denote the characteristic polynomial of M by $p(X) = X^n + \sum_{i=0}^{n-1} a_i X^i$.

We now form the matrix $XI - M$, with X an indeterminate which commutes with elements from F. From Lemma 9.7, we know that $\det(XI - M)I = (XI - M)\text{Adj}(XI - M)$, where $\det(XI - M)$ is simply $p(X)$, and the entries in $\text{Adj}(M)$ are polynomials in X of degree at most $n - 1$.

We can now write $\text{Adj}(XI - M)$ as $\sum_{i=1}^{n} X^i B_{n-i}$ with each $B_{n-i} \in M_n(F)$. From Lemma 9.7 we know that

$$\det(XI - M) = (XI - M)\left(\sum_{i=1}^{n} X_i B_{n-i}\right)$$

which, by equating corresponding powers of X, leads to the system

$$\begin{aligned} B_1 &= I \\ B_2 - MB_1 &= a_{n-1}I \\ B_3 - MB_2 &= a_{n-2}I \\ &\vdots \\ B_n - MB_{n-1} &= a_1 I \\ -MB_n &= a_0 I. \end{aligned}$$

For each $h \in \{1, 2, \ldots, n\}$, multiplying the h-th equation above by M^{n+1-h} from the left and then summing them all up, leads to $0 = p(M)$. □

Even though for any matrix M over a field F, is always a root of it's own characteristic equation, there often exist polynomials over F of smaller degree which also have M as a root. The smallest of these (ordered by degree) is called the **Minimal polynomial of** M, and denoted by $Min(M)$.

Combining Theorems 9.6 and 9.8, it is clear that Φ_n divides all the Q_i's of Theorem 9.6 and if we can find a matrix A with characteristic polynomial Φ_n, by the Cayley-Hamilton Theorem, it will be a root of Φ_n, and thus of all the Q_i's!

Definition 9.9: Companion matrix

For each monic polynomial $p(\lambda) = \lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_0$, the $n \times n$ matrix

$$C_p = \begin{bmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_2 & -a_3 & \cdots & -a_{n-1} \end{bmatrix}$$

is called the **companion matrix** of p.

Proposition 9.10: The characteristic polynomial of the companion matrix of p is p.

Proof:
We shall prove this result by induction on deg p. The base case for the induction is deg $p = 2$. Let $p(\lambda) = \lambda^2 + a_1\lambda + a_0$, then $C_p = \begin{bmatrix} 0 & 1 \\ -a_0 & -a_1 \end{bmatrix}$. The characteristic polynomial of C_p is $\det(\lambda I - C_p) = \lambda(a_1 + \lambda) - (-a_0) = \lambda^2 + a_1\lambda + a_0 = p(\lambda)$, which concludes the base case.

Suppose the result holds for all monic polynomials of degree up to n. Now consider the companion matrix of $q(\lambda) = \lambda^{n+1} + a_n\lambda^n + \cdots + a_0$:

$$C_q = \begin{bmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_2 & -a_3 & \cdots & -a_n \end{bmatrix}$$

The characteristic equation of C_q is given by

$$\det\left(\begin{bmatrix} \lambda & -1 & 0 & 0 & \cdots & 0 \\ 0 & \lambda & -1 & 0 & \cdots & 0 \\ 0 & 0 & \lambda & -1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & -1 \\ a_0 & a_1 & a_2 & a_3 & \cdots & \lambda + a_n \end{bmatrix}\right) = 0$$

which is equivalent to

$$\lambda \det\left(\begin{bmatrix} \lambda & -1 & 0 & 0 & \dots & 0 \\ 0 & \lambda & -1 & 0 & \dots & 0 \\ 0 & 0 & \lambda & -1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & -1 \\ a_1 & a_2 & a_3 & a_4 & \dots & \lambda + a_n \end{bmatrix}\right) - (-1)^{n+1} a_0 \det\left(\begin{bmatrix} -1 & 0 & 0 & 0 & \dots & 0 \\ \lambda & -1 & 0 & 0 & \dots & 0 \\ 0 & \lambda & -1 & 0 & \dots & 0 \\ 0 & 0 & \lambda & -1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & -1 \end{bmatrix}\right) = 0$$

The second matrix is clearly a lower $n \times n$ triangular matrix, so it's determinant is equal to $(-1)^n$. The first determinant is the characteristic polynomial of C_s with $s(\lambda) = a_1 + a_2\lambda + \ldots + a_n\lambda^{n-1} + \lambda^n$, which is equal s by the inductive hypothesis as $\deg(s) = n$. It now follows that the characteristic polynomial of C_q is $a_0 + a_1\lambda + \ldots + a_n\lambda^n + \lambda^{n+1}$, and the result follows by induction.

□

Corollary 9.11: For each natural number n, there exists an automorphism $f_n : \mathbb{Z}^{\varphi(n)} \to \mathbb{Z}^{\varphi(n)}$ such that the structural graph of f_n consists of only the zero cycle and infinitely many cycles of length n. We shall call such an automorphism a pure n-cyclic automorphism and denote its matrix representation by P_n.

Proof:

As the constant term of Φ_n is either 1 or -1, it is clear that $\det C_{\Phi_n} = \pm 1$, hence C_{Φ_n} is invertible, making it the matrix representation of an automorphism. Theorem 9.8 tells us that C_{Φ_n} is a root of Φ_n, and since Φ_n divides all the Q_i's, C_{Φ_n} is a root of all the Q_i's.

Since all the Q_i's divide $\lambda^n - 1$, all cycles associated with C_{Φ_n} have lengths dividing n. Any cycle length d properly dividing n, would have to divide $\frac{n}{p_i}$ for some p_i. By letting $v \in \mathbb{Z}^{\varphi(n)}$ be a non-zero element in any cycle of length d, we note that

$$\begin{aligned} Q_i(C_{\Phi_n})v &= \sum_{j=0}^{p_i-1} C_{\Phi_n}^{\frac{nj}{p_i}} v \\ &= \sum_{j=0}^{p_i-1} v \\ &= p_i v \\ &\neq 0 \end{aligned}$$

which clearly cannot hold since $Q_i(C_{\Phi_n}) = 0$. The automorphism of which C_{Φ_n} is the matrix representation consequently has a structural graph consisting of the zero-cycle, no chains, and only cycles of length n. Note, we cannot use Theorem 9.6 if $n = 1$, but if we would like to have an automorphism with all its cycles of length 1, we can simply use the identity mapping on the group $\mathbb{Z}$.

□

Since we are now capable of constructing automorphisms of which the structural graph has all non-zero cycles of any length n, we proceed to investigate how cycles of different lengths interact.

Theorem 9.12: Suppose the structural graph of an automorphism has non-zero cycles of length α and β, then the structural graph will also have a cycle of length $[\alpha, \beta]$ (the least common multiple of α and β).

Proof:

Let A be the matrix representation of the particular automorphism. Suppose x lies in a cycle of length α and y in a cycle of length β. It is clear that for each positive integer k,

$$\begin{aligned} A^{[\alpha,\beta]}(x + ky) &= A^{[\alpha,\beta]}x + kA^{[\alpha,\beta]}y \\ &= x + ky \end{aligned}$$

as $\alpha | [\alpha, \beta]$ and $\beta | [\alpha, \beta]$. Now denote the cycle length of $x + ky$ by γ_k for all $k \in \mathbb{N}$. Clearly $\gamma_k | [\alpha, \beta]$, so there exist distinct $k, j \in \mathbb{N}$ with $\gamma_k = \gamma_j$. We shall denote this common value simply by γ. Consider the two cycles $(x + ky, A(x + ky), \ldots, A^{\gamma-1}(x + ky))$ and $(x + jy, A(x + jy), \ldots, A^{\gamma-1}(x + jy))$. Since matrix multiplication is distributive over matrix summation we can subtract these two

cycles term by term to give a new cycle $((j-k)y, A(j-k)y, \ldots, A^{\gamma-1}(j-k)y)$. Note though, the cycle length of y need not be γ, it is possible that the newly formed cycle actually fully traverses the cycle containing $(j-k)y$ a couple of times. However the cycle length of $(j-k)y$ must divide γ. Since $k \neq j$ and $A(j-k)y = (j-k)Ay$ it is clear that $(j-k)y$ must be in a cycle of the same length as y, and thus $\beta|\gamma$.

By the Quotient-remainder Theorem, let $\gamma = q\alpha + r, 0 \leq r < \alpha$. We now have

$$\begin{aligned} A^{\gamma}(x+ky) &= A^{r}x + kA^{\gamma}y \\ &= A^{r}x + ky \\ &= x + ky. \end{aligned}$$

Thus $A^r x = x$, but since the cycle containing x is of length α, $r = 0$, so $\alpha|\gamma$. It follows that $[\alpha, \beta]|\gamma$, and thus $\gamma = [\alpha, \beta]$. □

We can now give a complete structural characterization of all functions having the automorphism property with underlying group $\mathbb{Z}^n$.

Theorem 9.13: Structural classification of all automorphisms of the groups $\mathbb{Z}^n$

A function $f : X \to X$ possesses the automorphism property with underlying group structure $\mathbb{Z}^n$ iff the structural graph satisfies all of the following:

1. Contains only chains and cycles, and at least one cycle of length 1, called the zero cycle.
2. The number of distinct cycle lengths is finite.
3. If it contains a non-zero cycle then it contains infinitely many cycles of the same length.
4. If it contains a chain, it contains infinitely many chains.
5. If it contains non-zero cycles of length α and β, then it contains a cycle of length $[\alpha, \beta]$.

Proof:

Propositions 9.1, 9.2 and Theorem 9.12 shows that the conditions listed above are necessary.

Let f be a function on a countably infinite set satisfying all the conditions listed in the Theorem. We shall now show that f has the automorphism property by constructing a invertible integer matrix representing f. Condition (2) allows the construction of a finite set $\mathcal{L} = \{n_1, n_2, \ldots, n_s\}$ consisting of the distinct cycle lengths occurring in the structural graph of f. For each $n_i \in \mathcal{L}$, Corollary 9.11 shows the existence of a pure n_i-cyclic automorphism. If f has no chains, construct the integer matrix

$$M = \begin{bmatrix} P_{n_1} & 0 & 0 & \cdots & 0 \\ 0 & P_{n_2} & 0 & \cdots & 0 \\ 0 & 0 & P_{n_3} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & P_{n_s} \end{bmatrix}$$

which is a diagonal block matrix obtained by placing the matrices P_{n_i}, as defined in 9.11 (as blocks) along the diagonal of M and equating all other entries to 0. If f has chains, simply append the matrix $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ along the diagonal of M in a similar fashion, say at the bottom on the right.

Since all of the P_{n_i}'s are along the diagonal, it follows that $\det(M) = \det(P_{n_1})$ $\det(P_{n_2}) \cdots \det(P_{n_s})$ is either 1 or -1, as all the P_{n_i}'s are invertible. This shows that M is invertible, and represents an automorphism $f_M : \mathbb{Z}^m \to \mathbb{Z}^m$ for some positive integer m. Let the number of rows of P_{n_i} be denoted by x_i. For n_i, it is clear that the cycle of the element $e_{x_1+\ldots+x_{i-1}+1}$ is of length n_i in the structural graph of f_M as the cycle of e_1 is of length n_i in the structural graph of the pure n_i-cycle represented by the matrix P_{n_i}. The structural graph of f_M thus contains cycles of length n_i for each $n_i \in \mathcal{L}$. If f contains a chain, the last matrix embedded on the diagonal of M is $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$. Example 9.3 demonstrates that $e_{x_1+\ldots+x_s+1}$ then lies in a chain. It is now clear that a nonzero cycle of length n_i (or chain) occurs in the structural graph of f only if one also occurs in that of f_M.

Given any element $z \in \mathbb{Z}^m$, represented as a column, we can decompose z as the sum $z = z_1 + z_2 + \cdots + z_s + \hat{z}$ with each z_n being a column of length m, with it's j-th entry equal to that of z for all $j \in \left\{ \left(\sum_{k=1}^{n-1} x_i \right) + 1, \ldots, \left(\sum_{k=1}^{n-1} x_i \right) + x_n \right\}$ and zero otherwise. If f has chains, $\hat{z}$ is a column of length m with all entries equal to zero[†], except for the last two which are equal to the corresponding entries of z, otherwise put $\hat{z}$ equal to the zero column of length m. We will refer to z_i as the n_i-cycle component of z, and to $\hat{z}$ as the chain component of z. Since $M^i z = \sum_{j=1}^{s} M^i z_j + M^i \hat{z}$, and each z_i is in a cycle of length dividing n_i. It is clear that z is in a chain iff $\hat{z}$ is in a chain, which is the case for exactly all non-zero $\hat{z}$, by example 9.3. Consequently if f_M has a chain, then f must also have had one (as otherwise $\hat{z} = 0$ for all $z \in \mathbb{Z}^m$). Now take any z in a non-zero cycle of f_M. As just discussed above, it is clear that $\hat{z}$ must be the zero column. However since M acts on z_i in the same way as the pure n_i-cycle would on a column consisting of the $\left(\left(\sum_{i=1}^{k-1} x_i \right) + 1 \right)$'th up to $\left(\left(\sum_{i=1}^{k-1} x_i \right) + x_k \right)$'th entries of z_k, it follows that the cycle of z_i is either the zero-cycle or of length n_i. Since the z_i's are linearly independent, the cycle length of z is equal to the least common multiple of the n_i's for which the corresponding z_i's are not zero columns. It now follows that any non-zero cycle of f_M has length $[n_{\sigma(1)}, n_{\sigma(2)}, \ldots, n_{\sigma(k)}]$ for some permutation σ of $(1, 2, \ldots, s), k \leq s$, and by condition 5 of the same length as some cycle of f. Consequently, a cycle of length n (or a chain) occurs in the structural graph of f_M only if one also occurs in that of f. We now

[†]A column with all entries equal to 0 will be referred to as a **zero column**.

have that the structural graphs of f and f_M have cycles of the same distinct lengths (as well as chains) iff the other has, and by conditions (1), (3) and (4) infinitely many of them, as well as a zero-cycle. This is clearly equivalent to having isomorphic structural graphs. By Theorem 4.2 it follows that f has the automorphism property. □

Example 9.14: Suppose we want to construct a matrix which represents an automorphism with chains, and cycles of lengths 6 and 15. Since there are cycles of length 6 and 15, there must be a cycle of length 30. We proceed to find P_6, P_{15} and P_{30}.

Pure 6-cycle: $Q_1(\lambda) = 1 + \lambda^2 + \lambda^4$ and $Q_2(\lambda) = 1 + \lambda^3$. The gcd of the Q_i's is $\Phi_6(\lambda) = 1 - \lambda + \lambda^2$. The companion matrix of this polynomial is:

$$P_6 = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}.$$

Pure 15-cycle: $Q_1(\lambda) = 1 + \lambda^3 + \lambda^6 + \lambda^9 + \lambda^{12}$ and $Q_2(\lambda) = 1 + \lambda^5 + \lambda^{10}$. The gcd of the Q_i's is $\Phi_{15}(\lambda) = 1 - \lambda + \lambda^3 - \lambda^4 + \lambda^5 - \lambda^7 + \lambda^8$. The companion matrix of this polynomial is:

$$P_{15} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ -1 & 1 & 0 & -1 & 1 & -1 & 0 & 1 \end{bmatrix}.$$

Pure 30-cycle: $Q_1(\lambda) = 1 + \lambda^6 + \lambda^{12} + \lambda^{18} + \lambda^{24}$, $Q_2(\lambda) = 1 + \lambda^{10} + \lambda^{20}$ and $Q_3(\lambda) = 1 + \lambda^{15}$. The gcd of the Q_i's is $\Phi 30(\lambda) = 1 + \lambda - \lambda^3 - \lambda^4 - \lambda^5 + \lambda^7 + \lambda^8$. The companion matrix of this polynomial is:

$$P_{30} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ -1 & -1 & 0 & 1 & 1 & 1 & 0 & -1 \end{bmatrix}.$$

The matrix which represents the desired automorphism is

$$\begin{bmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & -1 & 1 & 0 & -1 & 1 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & 0 & 1 & 1 & 1 & 0 & -1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
\end{bmatrix}.$$

The study of mathematics, like the Nile, begins in minuteness but ends in magnificence.

$\sim$ C. Colton (1780-1832)

10 The automorphisms of $\mathbb{Z}^n$ for fixed n.

Lemma 10.1: For any $M \in GL(\mathbb{Z}, n)$, the cyclic structure induced by M on $\mathbb{Z}^n$ is the same as that of M induced on $\mathbb{Q}^n$.

Proof:
Clearly every cycle (or chain) induced by M on $\mathbb{Z}^n$ occurs identically as a cycle (or chain) in $\mathbb{Q}^n$. Now consider any $v = (v_i) \in \mathbb{Q}^n$. Denote by L the lowest common multiple of the denominators of the v_i. Clearly Lv lies in $\mathbb{Z}^n$, and lies in a cycle iff v does.
□
From Lemma 10.1, we can prove our results over $\mathbb{Q}$, from which they will follow over $\mathbb{Z}$.

Definition 10.2: **Point annihilator and polynomial annihilator**

Let $M \in GL(F, n)$ and $v \in F^n$. We define the **point annihilator** at v as $\mathcal{P}_v = \{f \in F[X] : f(M)v = 0\}$. Similarly, for any $f \in F[X]$, we define the **polynomial annihilator** at f as $S_f = \{v \in F^n : f(M)v = 0\}$. Note taht $\mathcal{P}_v \subset F[X]$ and $S_f \subset F^n$

Lemma 10.3: $\mathcal{P}_v$ is an ideal of $F[X]$, and hence there exists an $f_v \in F[X]$, such that $\mathcal{P}_v = \langle f_v \rangle$.

Proof:
Let $f, g \in \mathcal{P}_v$ and $h \in F[X]$. Clearly $(f(M) + g(M))v = f(M)v + g(M)v = 0$ and $h(M)f(M)v = h(M)(0) = 0$. Obviously the zero polynomial lies in $\mathcal{P}_v$. As F is a field, $F[X]$ is a principal ideal domain, hence there exists an $f_v \in F[X]$, such that $\mathcal{P}_v = \langle f_v \rangle$. □

Lemma 10.4: S_f is a subspace of F^n.

Proof:
Let $u, v \in S_f$ and $c \in F$, then $f(M)(u + v) = f(M)u + f(M)v = 0$ as $f(M)$ is a linear transformation. Also, $f(M)(cu) = cF(M)u = 0$. □

Theorem 10.5: For any $M \in GL(F, n)$, if $f | Min(M)$ and f is not constant, then S_f is not trivial.

Proof:
Suppose S_f is trivial. It follows that the linear transformation $f(M)$ satisfies $f(M)v \neq 0, \forall v \in F^n - \{0\}$, and is thus injective. By the rank-nullity Theorem it follows that $f(M)$ is surjective, and thus invertible!

Consider the polynomial $h = \frac{Min(M)}{f}$. It follows that $h(M)v = f(M)^{-1}Min(M)v = 0$ for all $v \in F^n$, contradicting the minimality of $Min(M)$. $\square$

Lemma 10.6: For any $M \in GL(F, n)$, if $f|Min(M)$,and $h|f$ with h not constant nor equal to f, then S_h is a proper subspace of S_f.

Proof:
That S_h is a subspace of S_f is obvious, We just need to show that it is indeed a proper subset.
Suppose $S_h = S_f$, i.e. $f(M)x = 0 \Rightarrow h(M)x = 0$. As $h|f$, there exists a non-constant polynomial r, such that $f = hr$. For any $x \in F^n$, $Min(M)(M)x = f(M)\frac{Min(M)}{f}(M)x = f(M)\left(\frac{Min(M)}{f}(M)x\right) = 0$, so $h\frac{Min(M)}{f}(M)x = 0$. As $h\frac{Min(M)}{f} = \frac{Min(M)}{r}$, it follows that $\frac{Min(M)}{r}(M)x = 0$ for all $x \in F^n$, contradicting the minimality of $Min(M)$. $\square$

We will now look at the case where $F = \mathbb{Q}$. One very important thing to keep in mind here is that all cyclotomic polynomials are irreducible over $\mathbb{Q}$.

Definition 10.7: Relatively pure cycle

We shall refer to $m > 1$ as a **relatively pure cycle** length of M if the structural graph of M contains cycles of length m, but there are no cycles of lengths a and b, both less than n, in the structural graph of M with the property $[a, b] = m$.

Theorem 10.8: If M has relatively pure m-cycles then $\Phi_m|Min(M)$.

Proof:
In $\mathbb{Q}^n$, let T_d be the members of $\mathbb{Q}^n$ with cycles of order d induced by M. For any relatively pure m, define

$$K_m = \bigcup_{d|m;d\neq m} T_d.$$

First we note that K_m is a subgroup of $\mathbb{Q}^n$, which can easily be verified. The key to remember is that for any $a, b \in K_m$, the order of $a + b$ divides $[a, b]$ which is strictly a divisor of m, as m is relatively pure. Suppose $x \in T_m$, then $Q_i(M)(x) \in K_m$, $\forall Q_i$. As Φ_m is a linear combination of the Q_i's, it follows that

$$\Phi_m(M)(x) \in K_m.$$

We define $\mathcal{Q}_x$ as the set of all polynomials $f \in \mathbb{Q}[x]$ such that $f(M)(x) \in K_m$, then $\Phi_m \in \mathcal{Q}_x$. We will now show that $\mathcal{Q}_x$ is an ideal in $\mathbb{Q}[x]$. Let $f, g \in \mathcal{Q}_x, h \in \mathbb{Z}[x]$ then

$$f(M)x + g(M)x = (f + g)(M)(x) \in K_m$$

as K_m is a group. Also

$$fg(M)(x) = f(M)g(M)(x)$$

and as $g(M)(x) \in K_m$, the order of $g(M)(x)$ must be a strict divisor of m, and as m is relatively pure it follows that $f(M)g(M)(x) \in K_m$. As $\mathbb{Q}$ is a

field, $\mathbb{Q}[x]$ is a principle ideal domain. Hence there exists a $f \in \mathbb{Q}[x]$ such that $\mathcal{Q}_x = \langle f \rangle$. As $\Phi_m \in \mathcal{Q}_x$, if follows that $f \in \{\Phi_m, \bar{1}\}$, where $\bar{1}(x) = 1$. However, as $I(M)(x) = x$ it follows that $\bar{1} \notin \mathcal{Q}_x$, so $\mathcal{Q}_x = \langle \Phi_m \rangle$. As $Min(M) \in \mathcal{Q}_x$ we have $\Phi_m | Min(M)$. □

We now prove the converse of the above Theorem.

Theorem 10.9: If $\Phi_n | Min(M)$ then the cyclic structure induced by M contains n-cycles.

Proof:
For convenience, denote Φ_n by ρ. We know from Theorem 10.5 that S_ρ is not trivial, so there exists $v \in F^n - \{0\}$ such that $\rho(M)v = 0$. As $\rho | x^n - 1$ it follows that $(M^n - 1)v = 0$, so v lies in a cycle of length dividing n, but as ρ does not divide $x^k - 1$ for any $k < n$, it follows that v lies in a cycle of length n. □
We now turn our attention to chain formation.

Theorem 10.10: If f is an irreducible, non-cyclotomic polynomial over F and $f | Min(M)$ then the cyclic structure induced by M has chains.

Proof:
Let $v \in S_f - \{0\}$, then $\mathcal{P}_v = \langle f \rangle$. If M has no chains, then there exists n such that $M^n v = v$, so $x^n - 1 \in \mathcal{P}$, from which it follows that $f | x^n - 1$. This is a contradiction, as $x^n - 1 = \prod_{d|n} \Phi_d(x)$. □

Theorem 10.11: If $Min(M)$ has no irreducible, non-cyclotomic factors, but a cyclotomic factor of multiplicity greater than 1, then the cyclic structure induced by M has chains.

Proof:
For the sake of contradiction, suppose M induces only cycles, then for any $v \in F^n$, there exists an m such that $x^m - 1 \in \mathcal{P}_v$, thus there exists $m_1, m_2, \ldots, m_k$ such that $\mathcal{P}_v = \left\langle \prod_{i=1}^k \Phi_{m_i} \right\rangle$.
Suppose $Min(M) = \prod_{i=1}^s \Phi_{w_i}^{\alpha_i}$. We now just need to show that $\alpha_i = 1$. But as $\prod_{i=1}^k \Phi_{m_i} | Min(M)$ it follows that

$$\prod_{i=1}^{k} \Phi_{m_i} | \prod_{i=1}^{s} \Phi_{w_i}.$$

So

$$\prod_{i=1}^{s} \Phi_{w_i} \in \mathcal{P}_v, \forall v \in F^n.$$

It follows that $\prod_{i=1}^s \Phi_{w_i}(M) = 0$, and the result follows. □
So far, we have demonstrated two sufficient conditions for chains to occur in the cyclic structure of M. We will now proceed to show that it is necessary for one of these to hold if the cyclic structure induced by M has chains.

Theorem 10.12: If the cyclic structure induced by M has chains then $Min(M)$ either has a non-cyclotomic, irreducible factor or a cyclotomic factor of multiplicity greater than 1.

Proof:
Suppose the result does not hold, then $Min(M) = \prod_{i=1}^{k} \Phi_{m_i}$ with $m_i \neq m_j$ if $i \neq j$. Then $Min(M) | x^{[m_1,m_2,\ldots,m_k]} - 1$. As $Min(M) \in \mathcal{P}_v$ for all $v \in F^n$, it follows that $x^{[m_1,m_2,\ldots,m_k]} - 1 \in \mathcal{P}_v$, meaning all v lies in cycles of lengths dividing $[m_1, m_2, \ldots, m_k]$. $\square$

God used beautiful mathematics in creating the world.

$\sim$ P. Dirac (1902-1984)

11 The automorphisms of $\mathbb{Z}_p^n$

We now turn our attention to the automorphisms of groups of the form $\mathbb{Z}_p^n$, for prime p. We firstly consider the $n \times n$ matrices over $\mathbb{Z}_p^n$ for which the minimal and characteristic polynomials coincide, after which we will use the rational canonical form of any invertible matrix to solve the general case.

Note, these are exactly the matrices M for which the rational canonical from is similar to a companion matrix of a polynomial of degree n. Consider such a matrix C_f, with $f = \prod_{i=1}^{k} f_i^{\alpha_i}$, with f_i irreducible over $\mathbb{Z}_p$. Consider the matrix

$$D_f = \begin{bmatrix} C_{f_1^{\alpha_1}} & 0 & 0 & \cdots & 0 \\ 0 & C_{f_2^{\alpha_2}} & 0 & \cdots & 0 \\ 0 & 0 & C_{f_3^{\alpha_3}} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & C_{f_k^{\alpha_k}} \end{bmatrix}$$

with companion matrices $C_{f_i^{\alpha_i}}$ all along the diagonal. Since the $f_i^{\alpha_i}$'s are relatively prime, $Min(D_f) = f$ and it follows that C_f is the rational canonical form of D_f, so C_f and D_f are similar matrices,implying that the cyclic structures induced by them are identical. The usefulness of this representation is that the effect on the cyclic structure attributed by each companion matrix along the diagonal can be easily isolated.

We now appeal to a few results on polynomials ([8]):

Lemma 11.1: ([8], lemma 3.1)Let $f \in F[X]$ of degree m with $|F| = q$ and $f(0) \neq 0$. There exists a positive integer $e \leq q^m - 1$ such that $f | x^e - 1$.

Proof:
The factor ring $F[x]/\langle f \rangle$ contains $q^m - 1$ non-zero cosets. The q^m cosets $x^j + \langle f \rangle$, $j = 0, 1, \ldots, q^m - 1$, are all nonzero, so there exist integers r and s with $0 \leq r < s \leq q^m - 1$ such that $x^s \equiv x^r \bmod f(x)$, i.e. f divides $x^{s-r} - 1$ and $0 < s - r \leq q^m - 1$. □

Definition 11.2: **Order of polynomial ([8], definition 3.2)**

Given a polynomial f with $f(0) \neq 0$, the least e such that $f | x^e - 1$ is called the **order** of f, denoted by $ord(f)$.

Theorem 11.3: Denote the finite field with q elements by F_q. Let $f \in F_q[x]$ be an irreducible polynomial over F_q of degree m and $f(0) \neq 0$. Then $ord(f)$ is equal to the order of any root of f in the multiplicative group $F_{q^m}^*$.

Proof:
F_{q^m} is the splitting field of f over F_q. The roots of f have the same order in the group $F^*_{q^m}$. Let $\alpha \in F^*_{q^m}$ be any root of f. Then we have $\alpha^e = 1$ if and only if $f(x)$ divides $x^e - 1$. The result follows from the definitions of $ord(f)$ and the order of α in the group $F^*_{q^m}$. □

Corollary 11.4: ([8], corollary 3.4) If $f \in F[x]$ is an irreducible polynomial over a finite field F, of degree m then $ord(f)$ divides $q^m - 1$.

Proof:
If $f(x) = cx$ with $c \in F^*$, then $ord(f) = 1$ and the result is trivial. Otherwise, the result follows from Theorem 11.3 and the fact that F^* is a group of order $q^m - 1$. □

Theorem 11.5: ([8], theorem 3.5) The number of monic irreducible polynomials in $F[x]$ of degree m and order e is equal to

1. $\frac{\phi(e)}{m}$ if $e \geq 2$ and m is the multiplicative order of q modulo e.
2. 2 if $m = e = 1$.
3. 0 otherwise.

In particular, the degree of an irreducible polynomial in $F[x]$ of order e must be equal to the multiplicative order of q modulo e.

Proof:
$ord(f) = e$ if and only if all roots of f are primitive $e - th$ roots of unity over F, in other words, $ord(f) = e$ if and only if f divides the cyclotomic polynomial Φ_e. Any monic irreducible factor of Φ_e has the same degree m, which is the least positive integer such that $q^m \equiv 1 \bmod e$, and the number of such factors is $\phi(e)/m$. For $m = e = 1$, we also have to take into account the monic irreducible polynomial $f(x) = x$. □

Lemma 11.6: ([8], lemma 3.6) Let c be any positive integer, and let $f \in F[x]$ with $f(0) \neq 0$. Then f divides $x^c - 1$ if and only if $ord(f)|c$.

Proof:
If $e = ord(f)$ divides c, then $f(x)$ divides $x^e - 1$ and $x^e - 1$ divides $x^c - 1$, so $f(x)$ divides $x^c - 1$. Conversely, if $f(x)$ divides $x^c - 1$, we have that $c \geq e$, so we can write $c = me + r$ with $m \in \mathbb{N}$ and $0 \leq r < e$. Since $x^e - 1 = (x^{me} - 1)x^r + (x^r - 1)$, it follows that $f(x)$ divides $x^r - 1$ which is only possible if $r = 0$, therefore e divides c. □

Theorem 11.7: ([8], theorem 3.8) Let $g \in F[x]$ be irreducible over F with $g(0) \neq 0$ and $ord(g) = e$, let $f = g^b$ with b a positive integer. Let t be the smallest integer with $p^t \geq b$, with p the characteristic of F. Then $ord(f) = ep^t$.

Proof:
Setting $c = ord(f)$ and noting that the divisibility of $x^c - 1$ by f implies the

divisibility of $x^c - 1$ by g, we obtain that e divides c by Lemma 11.6, and thus f divides $(x^e - 1)^{p^t} = x^{ep^t} - 1$. Thus according to Lemma 11.6, c divides ep^t. It follows that $c = ep^u$ with $0 \leq u \leq t$. We note that $x^e - 1$ only has simple roots, as e is not a multiple of p by Corollary 11.4. Therefore, all roots of $x^{ep^u} - 1 = (x^e - 1)^{p^u}$ have multiplicity p^u. But $g(x)^b$ divides $x^{ep^u} - 1$, hence $p^u \geq b$ by comparing multiplicities of roots, so $u \geq t$ and $c = ep^t$.
□

Theorem 11.8: ([8], theorem 3.9)Let $g_1, g_2, \ldots, g_k$ be pairwise relatively prime nonzero polynomials over F. Let $f = g_1 g_2 \ldots g_k$. Then $ord(f) = lcm(ord(g_1), ord(g_2), \ldots, ord(g_k))$.

Proof:
It is easily seen that it suffices to consider the case where $g_i(0) \neq 0$ for $1 \leq i \leq k$. Set $e = ord(f)$ and $e_i = ord(g_i)$, and let $c = lcm(e_1, e_2, \ldots, e_k)$. Then each g_i divides $x^{e_i} - 1$ and so g_i divides $x^c - 1$. Because of the pairwise relative primality of the polynomials g_i, we obtain that f divides $x^c - 1$, so e divides c. On the other hand, f divides $x^e - 1$, and so each g_i divides $x^e - 1$. It once again follows from 11.6 that e_i divides e and therefore c divides e. We conclude that $e = c$.
□
We now summarize these results in one Theorem,

Theorem 11.9: ([8], theorem 3.11) Let F be a finite field of characteristic p, and let $f \in F[x]$ be a polynomial of positive degree and $f(0) \neq 0$. Let $f = a f_1^{b_1} f_2^{b_2} \ldots f_k^{b_k}$, where $a \in F, b_i \in \mathbb{N}$ and f_i distinct monic irreducible polynomials over F, be the canonical factorization of f in $F[x]$. Then $ord(f) = ep^t$ where $e = lcm(ord(f_1), ord(f_2), \ldots, ord(f_k))$ and t is the smallest integer with $p^t \geq max(b_1, b_2, \ldots, b_k)$.
□

Corollary 11.10: If f is an irreducible polynomial with $deg(f) = m$, then $ord(f) | p^s - 1$ if and only if $m | s$.

Proof:
Immediate consequence of lemma 11.6. □
We now have all of the results on polynomials that we will need for the rest of this section.

For any finite field F, Firstly we consider an automorphism of F^n for which the characteristic polynomial as well as the minimal polynomial is $f = f_1^\alpha$. As $\deg(Char(f)) = n$, it follows that $deg(f_1) = \frac{n}{\alpha}$. Denote the order of f_1 by e.

Consider the sequence $S_{f_1^i}, i \in \{1, 2, \ldots, \alpha\}$ of subspaces of F^n. We know $S_{f_1^{i+1}}$ properly contains $S_{f_1^i}$, and also that S_{f_1} is non-trivial.

Lemma 11.11: Each non-zero member of S_{f_1} lies in a cycle of length e.

Proof:
Let $y \in S_{f_1} - \{0\}$, clearly $x^{ord(f_1)} - 1 \in \mathcal{P}_y$, from which it follows that the cycle

length of y divides $ord(f_1)$. Suppose s is the least positive integer such that $(x^s-1)(M)y = 0$, then $x^s - 1 \in \mathcal{P}_y$. As $f_1 \in \mathcal{P}_y$, and f_1 is irreducible, it follows that $f_1 | x^s - 1$, so $e|s$, from which $s = e$. Consequently, each $y \in S_{f_1} - \{0\}$ lies in a cycle of length e. □

Lemma 11.12: If $y \in S_{f_1^{i+1}} - S_{f_1^i}$, then y lies in a cycle of length $ord(f_1^{i+1})$.

Proof:
For any such y, $f_1^{i+1} \in \mathcal{P}_y$, and $f_1^i \notin \mathcal{P}_y$, consequently $\mathcal{P}_y$ is generated by f_1^{i+1}. Suppose $x^s - 1 \in \mathcal{P}_y$ for some $s \in \mathbb{N}$, then as f_1^{i+1} is a divisor of $x^s - 1$, it follows that $ord(f_1^{i+1})|s$. As $x^{ord(f_1^{i+1})} - 1 \in \mathcal{P}_y$, it follows that y lies in a cycle of length $ord(f_1^{i+1})$. □

Lemma 11.13: For each $i \in \{1, 2, \ldots, \alpha\}$, $|S_{f_1^i}| = (p^m)^i$, with $m = deg(f_1)$.

Proof:
For each $i \in \{1, 2, \ldots, \alpha\}$, let $|S_{f_1^i}| = p^{t_i}$. From Corollary 11.10, $t_1 = m\delta_1$ for some integer δ_1. From Lemma 11.12, $p^{t_{i+1}} = p^{t_i} + c_{i+1} \cdot ord(f_1^{i+1})$, with c_{i+1} the number of cycles in $S_{f_1^{i+1}} - S_{f_1^i}$. As $e = ord(f_1)$ divides $ord(f_1^{i+1})$ we have $p^{t_{i+1}} \equiv_e p^{t_i}$. Consequently $p^{t_{i+1}-t_i} \equiv_e 1$, so that m divides $t_{i+1} - t_i$. We can thus conclude that $t_{i+1} = t_i + m\delta_{i+1}$, for some integer δ_{i+1}. However, $m\alpha = n = m(\delta_1 + \delta_2 + \ldots + \delta_\alpha)$ and as $S_{f_1^{i+1}}$ strictly contains $S_{f_1^i}$, each $\delta_i \geq 1$, so $m(\delta_1 + \delta_2 + \ldots + \delta_\alpha) \geq m\alpha$. Since equality holds, $\delta_i = 1$ for each i, from which the result follows. □

We summarize our work in the following theorem:

Theorem 11.14: Let M be the matrix representation of an automorphism of $\mathbb{Z}_p^n$, with $Char(M) = Min(M) = C_{f^\alpha}$, for an irreducible polynomial f of degree m. The cyclic structure of the endomorphism induced by M is

$$\begin{bmatrix} 1 & \frac{p^m-1}{ord(f)} & \frac{p^m(p^m-1)}{ord(f^2)} & \frac{p^{2m}(p^m-1)}{ord(f^3)} & \cdots & \frac{p^{m(\alpha-1)}(p^m-1)}{ord(f^\alpha)} \\ 1 & ord(f) & ord(f^2) & ord(f^3) & \ldots & ord(f^\alpha) \end{bmatrix}$$

with $\alpha = \frac{n}{m}$.

As all square matrices over a field have a rational matrix form, which has companion matrices along the diagonal, and all companion matrices are similar to a matrix with companion matrices of factors of the corresponding polynomial, it follows that every matrix is similar to a matrix of the form

$$\begin{bmatrix} C_{f_1^{\alpha_1}} & 0 & 0 & \cdots & 0 \\ 0 & C_{f_2^{\alpha_2}} & 0 & \cdots & 0 \\ 0 & 0 & C_{f_3^{\alpha_3}} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & C_{f_k^{\alpha_k}} \end{bmatrix}$$

with each $C_{f_i^{\alpha_i}}$ a companion matrix (they are not necessary distinct). The important observation is that this form allows for the $C_{f_i^{\alpha_i}}$'s along the diagonal to act on disjoint (excluding 0) subspaces of $\mathbb{Z}_p^n$ independently.
To see what we mean by this, it is perhaps best to look at an enlightening example.

Example 11.15: Consider the automorphism of $\mathbb{Z}_3^3$ which is induced by

$$M = \begin{bmatrix} C_{(x+1)^2} & 0 \\ 0 & C_{x-1} \end{bmatrix} = \begin{bmatrix} 0 & 2 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Looking at the cyclic structure induced by M on the subspace $V_1 = \begin{bmatrix} \alpha \\ \beta \\ 0 \end{bmatrix}, \alpha, \beta \in \mathbb{Z}_3$, Theorem 11.14 gives the cyclic structure

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 6 \end{bmatrix}.$$

Similarly, the cyclic structure induced by M on $V_2 = \begin{bmatrix} 0 \\ 0 \\ \gamma \end{bmatrix}, \gamma \in \mathbb{Z}_3$, is given by

$$\begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 3 \\ 1 \end{bmatrix}.$$

All members of $\mathbb{Z}_3^3$ can be expressed (uniquely) as linear combinations of members of the subspaces mentioned above, say $v = v_1 + v_2, v_i \in V_i$. Furthermore denote the cycle length of v_i by c_i then v lies within a cycle of length $lcm(c_1, c_2)$. By pairing off the members of the annihilator spaces with one another in this fashion, we find $\frac{2\times 2}{2} = 2$ cycles of length 2, and $\frac{2\times 6}{6} = 2$ cycles of length 6. Summing up, we find that the cyclic structure induced by M is

$$\begin{bmatrix} 1+2 & 1+2 & 1+2 \\ 1 & 2 & 6 \end{bmatrix} = \begin{bmatrix} 3 & 3 & 3 \\ 1 & 2 & 6 \end{bmatrix}.$$

Using this, we can now calculate all possible cyclic structures on $\mathbb{Z}_p^n$ for arbitrary prime p and natural number n. We will now calculate all the cyclic structures which are induced by automorphisms on $\mathbb{Z}_p^3$.

Case 1: $Min(M) = l_1 l_2 l_3$, where the l_i are distinct linear polynomials. M is similar to the matrix

$$\begin{bmatrix} C_{l_1} & 0 & 0 \\ 0 & C_{l_2} & 0 \\ 0 & 0 & C_{l_3} \end{bmatrix}.$$

Lemma 11.13 gives $|S_{l_i}| = p$. Let the order of l_i be d_i. Then it follows that there are $\frac{p-1}{d_i}$ cycles of length d_i in S_{l_i}. By accounting for all other members of $\mathbb{Z}_p^3$, as linear combinations of the members of S_{l_i}, we get $\frac{(p-1)^2}{lcm(d_i,d_j)}$ cycles of length

$lcm(d_i, d_j)$ and lastly $\frac{(p-1)^3}{lcm(d_1,d_2,d_3)}$ cycles of length $lcm(d_1, d_2, d_3)$. Summing up, the cyclic structure induced by a matrix with minimal polynomial the product of three distinct linear factors is

$$\begin{bmatrix} 1 & \frac{p-1}{d_1} & \frac{p-1}{d_2} & \frac{p-1}{d_2} & \frac{(p-1)^2}{lcm(d_1,d_2)} & \frac{(p-1)^2}{lcm(d_1,d_3)} & \frac{(p-1)^2}{lcm(d_2,d_3)} & \frac{(p-1)^3}{lcm(d_1,d_2,d_3)} \\ 1 & d_1 & d_2 & d_3 & lcm(d_1,d_2) & lcm(d_1,d_3) & lcm(d_2,d_3) & lcm(d_1,d_2,d_3) \end{bmatrix}.$$

where the d_i are any divisors of $p-1$.

Case 2: $Min(M) = l_1^2 l_2$ where l_i are two distinct linear polynomials. M is similar to the matrix

$$\begin{bmatrix} C_{l_1^2} & 0 \\ 0 & C_{l_2} \end{bmatrix}.$$

The cyclic structure induced by M on the subspace spanned by $\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$ is consequently given by

$$\begin{bmatrix} 1 & \frac{p-1}{ord(l_1)} & \frac{p(p-1)}{ord(l_1^2)} \\ 1 & ord(l_1) & ord(l_1^2) \end{bmatrix} = \begin{bmatrix} 1 & \frac{p-1}{d_1} & \frac{p-1}{d_1} \\ 1 & d_1 & pd_1 \end{bmatrix}.$$

The cyclic structure induced by M on the subspace of $\mathbb{Z}_p^3$ spanned by $\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$ is

$$\begin{bmatrix} 1 & \frac{p-1}{ord(l_2)} \\ 1 & ord(l_2) \end{bmatrix} = \begin{bmatrix} 1 & \frac{p-1}{d_2} \\ 1 & d_2 \end{bmatrix}.$$

The other members of $\mathbb{Z}_p^3$ occur in $\frac{(p-1)^2}{lcm(d_1,d_2)}$ cycles of length $lcm(d_1, d_2)$ and $\frac{p(p-1)^2}{p.lcm(d_1,d_2)}$ cycles of length $p.lcm(d_1, d_2)$. Summarising case 2 we get the cyclic structure

$$\begin{bmatrix} 1 & \frac{p-1}{d_1} & \frac{p-1}{d_1} & \frac{p-1}{d_2} & \frac{(p-1)^2}{lcm(d_1,d_2)} & \frac{(p-1)^2}{lcm(d_1,d_2)} \\ 1 & d_1 & pd_1 & d_2 & lcm(d_1,d_2) & p.lcm(d_1,d_2) \end{bmatrix}$$

Where the d_i are is any divisors of $p-1$.

Case 3: $Min(M) = l_1^3$, with l_1 a linear polynomial. M is thus similar to the matrix

$$C_{l_1^3}$$

The cyclic structure of this matrix is already described by Theorem 11.14, as

$$\begin{bmatrix} 1 & \frac{p-1}{ord(l_1)} & \frac{p(p-1)}{ord(l_1^2)} & \frac{p^2(p-1)}{ord(l_1^3)} \\ 1 & ord(l_1) & ord(l_1^2) & ord(l_1^3) \end{bmatrix}.$$

Theorem 11.7 reveals the order of l_1^2 as $p.d_1$ and that of l_1^3 as $p^2 d_1$ if $p = 2$ and pd_1 otherwise. So summing up, we get that the cyclic structure induced by M is given by

$$\begin{bmatrix} 2 & 1 & 1 \\ 1 & 2 & 4 \end{bmatrix} \text{ if } p = 2$$

or

$$\begin{bmatrix} 1 & \frac{p-1}{d_1} & \frac{p^2-1}{d_1} \\ 1 & d_1 & pd_1 \end{bmatrix}$$

with d_1 any divisor of $p-1$ otherwise.

Case 4: $Min(M) = lq$ with l, q irreducible linear and quadratic polynomials respectively. In this case, M is similar to a matrix of the form

$$\begin{bmatrix} C_q & 0 \\ 0 & C_l \end{bmatrix}.$$

Denote the orders of q and l by d_1 and d_2 respectively. From Theorem 11.5, d_1 can be any divisor of p^2-1 which is not a divisor of $p-1$ and d_2 can be any divisor of $p-1$. The cyclic structure induced by M on the subspace of $\mathbb{Z}_p^3$ spanned by $\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$ is then given by

$$\begin{bmatrix} 1 & \frac{p^2-1}{d_1} \\ 1 & d_1 \end{bmatrix}.$$

The cyclic structure induced by M on the subspace spanned by $\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$ is

$$\begin{bmatrix} 1 & \frac{p-1}{d_2} \\ 1 & d_2 \end{bmatrix}.$$

The remaining members of $\mathbb{Z}_p^3$ lie within $\frac{(p^2-1)(p-1)}{lcm(d_1,d_2)}$ cycles of length $lcm(d_1, d_2)$. Summing up, we find the cyclic structure as

$$\begin{bmatrix} 1 & \frac{p^2-1}{d_1} & \frac{p-1}{d_2} & \frac{(p^2-1)(p-1)}{lcm(d_1,d_2)} \\ 1 & d_1 & d_2 & lcm(d_1, d_2) \end{bmatrix}$$

with d_1 any divisor of p^2-1 which does not divide $p-1$ and d_2 any divisor of $p-1$.

Case 5: $Min(M) = c$, with c any irreducible cubic polynomial. Denote the order of c as d. From Theorem 11.5, d can be any divisor of p^3-1 which does not divide p^2-1. M is then similar to

$$C_c,$$

and the cyclic structure is given by

$$\begin{bmatrix} 1 & \frac{p^3-1}{d} \\ 1 & d \end{bmatrix}$$

for any d which divides p^3-1 but not p^2-1.

Case 6: $Min(M) = l_1 l_2$ with the l_i two distinct linear polynomials. As usual, denote the order of l_i by d_i, which can be any divisor of $p-1$. Without loss of generality, M is similar to

$$\begin{bmatrix} C_{l_1} & 0 & 0 \\ 0 & C_{l_1} & 0 \\ 0 & 0 & C_{l_2} \end{bmatrix}.$$

The cyclic structure that M induces on the space spanned by $\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$, as well as that spanned by $\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$, is

$$\begin{bmatrix} 1 & \frac{p-1}{d_1} \\ 1 & d_1 \end{bmatrix}.$$

Once again, the structure induced by M on the space spanned by $\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$ is

$$\begin{bmatrix} 1 & \frac{p-1}{d_2} \\ 1 & d_2 \end{bmatrix}.$$

The remaining members of $\mathbb{Z}_p^3$ occur in $\frac{(p-1)^2}{d_1}$ cycles of length d_1 and $2\frac{(p-1)^2}{lcm(d_1,d_2)} + \frac{(p-1)^3}{lcm(d_1,d_2)} = \frac{(p+1)(p-1)^2}{lcm(d_1,d_2)}$ cycles of length $lcm(d_1, d_2)$. Summing up, we get the following cyclic structure:

$$\begin{bmatrix} 1 & \frac{p^2-1}{d_1} & \frac{p-1}{d_2} & \frac{(p+1)(p-1)^2}{lcm(d_1,d_2)} \\ 1 & d_1 & d_2 & lcm(d_1, d_2) \end{bmatrix}$$

with d_i any divisor of $p-1$.

Case 7: $Min(M) = q$ with q an irreducible quadratic. The rational canonical form of any 3×3 matrix which has a quadratic companion matrix along its diagonal will also have a linear factor which divides the quadratic. However for this case, the quadratic needs to be irreducible, and hence have no linear factors, meaning that this case cannot occur.

Case 8: $Min(M) = l^2$ with l a linear polynomial of order d. By Theorem 11.5, d can be any divisor of $p-1$ and M is similar to the matrix

$$\begin{bmatrix} C_{l^2} & 0 \\ 0 & C_l \end{bmatrix}.$$

By Theorem 11.14, the cyclic structure induced by M on the space spanned by $\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$ is

$$\begin{bmatrix} 1 & \frac{p-1}{d} & \frac{p-1}{d} \\ 1 & d & pd \end{bmatrix}$$

and the cyclic structure induced by M on the space spanned by $\begin{bmatrix}0\\0\\1\end{bmatrix}$ is given by

$$\begin{bmatrix}1 & \frac{p-1}{d}\\ 1 & d\end{bmatrix}.$$

The remaining members of $\mathbb{Z}_p^3$ lie within $\frac{(p-1)^2}{d}$ cycles of length d and $\frac{p(p-1)^2}{pd}$ cycles of length pd. Summing up we get the following cyclic structure:

$$\begin{bmatrix}1 & \frac{p^2-1}{d} & \frac{p(p-1)}{d}\\ 1 & d & pd\end{bmatrix}$$

for any d which divides $p-1$.

Case 9: $Min(M) = l$ with l a linear polynomial. Denote the degree of l by d, which, by Theorem 11.14, can once again be any divisor of $p-1$. M is similar to a matrix of the form

$$\begin{bmatrix}C_l & 0 & 0\\ 0 & C_l & 0\\ 0 & 0 & C_l\end{bmatrix}.$$

In this case, all non-zero members of $\mathbb{Z}_p^3$ occur in cycles of length d, making the cyclic structure

$$\begin{bmatrix}1 & \frac{p^3-1}{d}\\ 1 & d\end{bmatrix}$$

for any d which divide $p-1$.

After listing all the cases, we see that some of the cyclic structures that arise from different cases might indeed overlap. For example, the cyclic structure found in Case 9 is also found as a special case of a structure found in Case 1, with $d_1 = d_2 = d_3$. Taking care of overlaps, we can list this result as the following Theorem:

Theorem 11.16: Let $|A| = p^3$ where p is prime, and let $f : A \to A$ be a bijection. Then f has the automorphism property with underlying group $\mathbb{Z}_p^3$ if and only if f has one of the following cyclic structures:

1. $\begin{bmatrix}1 & \frac{p-1}{d_1} & \frac{p-1}{d_2} & \frac{p-1}{d_2} & \frac{(p-1)^2}{lcm(d_1,d_2)} & \frac{(p-1)^2}{lcm(d_1,d_3)} & \frac{(p-1)^2}{lcm(d_2,d_3)} & \frac{(p-1)^3}{lcm(d_1,d_2,d_3)}\\ 1 & d_1 & d_2 & d_3 & lcm(d_1,d_2) & lcm(d_1,d_3) & lcm(d_2,d_3) & lcm(d_1,d_2,d_3)\end{bmatrix}$

   where each d_i is any divisor of $p-1$.

2. $\begin{bmatrix}1 & \frac{p-1}{d_1} & \frac{p-1}{d_1} & \frac{p-1}{d_2} & \frac{(p-1)^2}{lcm(d_1,d_2)} & \frac{(p-1)^2}{lcm(d_1,d_2)}\\ 1 & d_1 & pd_1 & d_2 & lcm(d_1,d_2) & plcm(d_1,d_2)\end{bmatrix}$ where d_i is any divisor of $p-1$.

3. $\begin{bmatrix}2 & 1 & 1\\ 1 & 2 & 4\end{bmatrix}$ if $p = 2$ or $\begin{bmatrix}1 & \frac{p-1}{d_1} & \frac{p^2-1}{d_1}\\ 1 & d_1 & pd_1\end{bmatrix}$ with d_1 any divisor of $p-1$ otherwise.

4. $\begin{bmatrix} 1 & \frac{p^2-1}{d_1} & \frac{p-1}{d_2} & \frac{(p^2-1)(p-1)}{lcm(d_1,d_2)} \\ 1 & d_1 & d_2 & lcm(d_1,d_2) \end{bmatrix}$ with d_1 any divisor of p^2-1 and d_2 any divisor of $p-1$.

5. $\begin{bmatrix} 1 & \frac{p^3-1}{d} \\ 1 & d \end{bmatrix}$ for any d which divides p^3-1 but not p^2-1.

6. $\begin{bmatrix} 1 & \frac{p^2-1}{d} & \frac{p(p-1)}{d} \\ 1 & d & pd \end{bmatrix}$ for any d that divides $p-1$.

When you're curious, you find lots of interesting things to do.

∼ W. Disney (1901-1966)

12 Endomorphisms of cyclic groups

When investigating the endomorphisms of a group, the first observation is that each vertex of the functional graph can be one of only two possible types.

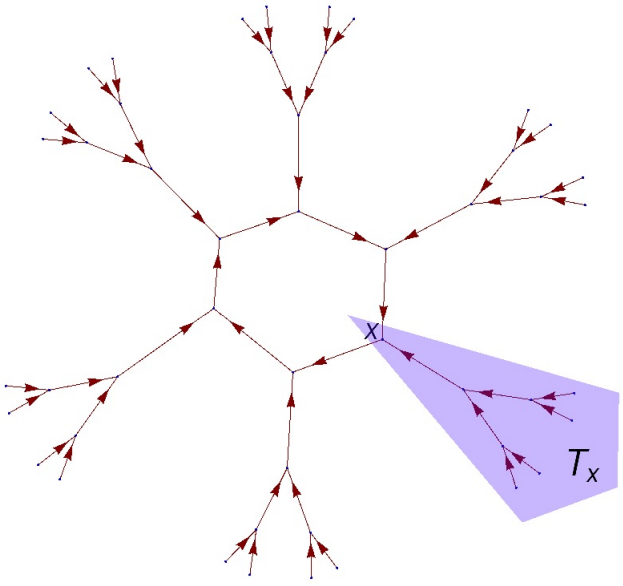
Definition 12.1: **$f-$cyclic and f-acyclic members**

Let G be a group and f an endomorphism on G. Let $g \in G$. We will say that g is **f-cyclic** if there is a $k \in \mathbb{N}$ such that $f^k(g) = g$. Otherwise, g is called **f-acyclic**.

It is important to note that for any finite group G, the sequence $g, f(g), f^2(g), f^3(g), \ldots$ the sequence must eventually settle in a cycle.

Definition 12.2: **Remoteness, acyclic Tree**

This smallest natural number k such that $f^k(y)$ is f-cyclic, will be referred to as the **remoteness** of y. For any f-cyclic $x \in G$, define the **Acyclic tree** of x, denoted by T_x as the structural graph of x together with all acyclic $y \in G$ and $f^{c_y}(y) = x$ where c_y is the remoteness of y.



An Acyclic Tree T_x.

Lemma 12.3: The collection of all f-cyclic members of G is a subgroup of G.

Proof:
If x_1, x_2 are f-cyclic members of G with cycles of length n_1, n_2 respectively, then $f^{lcm(n_1,n_2)}(x_1 + x_2) = x_1 + x_2$, so $x_1 + x_2$ is f-cyclic. 0 is clearly f-cyclic. □

Definition 12.4: **Cycles subgroup**

Define the group consisting of all f-cyclic members of G as the **Cycles subgroup** of G, denoted by C_G.

Lemma 12.5: T_0 is a subgroup of G.

Proof:
If $z_1, z_2 \in T_0$, then there exists $m_1, m_2 \in \mathbb{N}$ such that $f^{m_i}(z_i) = 0$, $i \in \{1, 2\}$. Let $m = max\{m_1, m_2\}$. Then $f^m(z_1 + z_2) = f^m(z_1) + f^m(z_2) = 0$. □

Corollary 12.6: If $G = \mathbb{Z}_p^n$ for a prime p, then T_0 is a subspace of G.

Corollary 12.7: If $G = \mathbb{Z}_p^n$ for a prime p, then $|T_0| = p^k$, for some $k \in \mathbb{N} \cup \{0\}$.

Lemma 12.8: For any f-cyclic $x \in G$, T_x is isomorphic to T_0 (as trees).

Proof:
Define $\bar{f} = f|_{C_G}$. Clearly $\bar{f}$ is an automorphism, meaning the inverse mapping is well defined.
Define the function $m : T_0 \to G$ by $m(u) = \bar{f}^{-k}(x) + u$, with k the remoteness of u.

Note that $f^k(m(u)) = f^k(\bar{f}^{-k}(x)) + f^k(u) = x + 0 = x$. Furthermore, suppose that $f^s(m(u))$ is f-cyclic for some $s < k$, then $\bar{f}^{-k+s}(x) + f^s(u)$ is f-cyclic, but as $\bar{f}^{-k+s}(x)$ is f-cyclic, so is $f^s(u)$. As the only f-cyclic member of T_0 is 0, it follows that $f^s(u) = 0$, which contradicts the minimality of k. It thus follows that the remoteness of $m(u)$ is k, and thus the range of m lies in T_x.

We now proceed to show that m is onto T_x. Given any $v \in T_x$, there exists a minimum $r \in \mathbb{N}$ such that $f^r(v) = x$. Consider $u = v - \bar{f}^{-r}(x)$. $f^r(u) = f^r(v) - f^r(\bar{f}^{-r}(x)) = x - x = 0$, so $u \in T_0$. Also $m(u) = v - \bar{f}^{-r}(x) + \bar{f}^{-r}(x) = v$.

m is also injective, for suppose $m(a) = m(b)$, then there exists natural numbers k_a, k_b such that $\bar{f}^{-k_a}(x) + a = \bar{f}^{-k_b}(x) + b$. Rearranging the terms gives $b - a = f^{-k_a}(x) - f^{-k_b}(x)$. The term on the left hand is in T_0 and the one on the right hand in C_G, it follows that $b - a = 0$, so $a = b$.

In order to show that m is a tree isomorphism, we now just need to show that m preserves and reflects edges.

Suppose $f(u) = v$, then $f(m(u)) = \bar{f}^{-k+1}(x) + f(u)$, with k the minimum natural number such that $f^k(u) = 0$. Clearly the least natural number q such that $f^q(v) = 0$ is $k-1$, so $f(m(u)) = \bar{f}^{-(k-1)}(x) + v = m(v)$.

Also, if $f(m(u)) = m(v)$, then $f(\bar{f}^{-k}(x) + u) = \bar{f}^{-s}(x) + v$ with s the minimum natural number such that $f^s(v) = 0$. It follows that $\bar{f}^{-k+1}(x) - \bar{f}^{-s}(x) = v - f(u)$ and once again, as the left hand side is f-cyclic, $v - f(u) = 0$, so that $f(u) = v$. □

It follows from Lemma 12.8 that if the functional graph of C_G (which is that of an automorphism) is known, as well as that of T_0, then the full functional graph of f can be found by simply attaching a copy of T_0 to each member of C_G. As we have already delved quite deep into the structure of automorphisms, we will thus now turn our focus to the structure of T_0. Note that $f|_{T_0}$ is a nilpotent endomorphism.

Turning our attention to cyclic groups, note that $f(1) = m$ induces a nilpotent endomorphism on $\mathbb{Z}_n$ if and only if every prime factor of n is a prime factor of m as well.

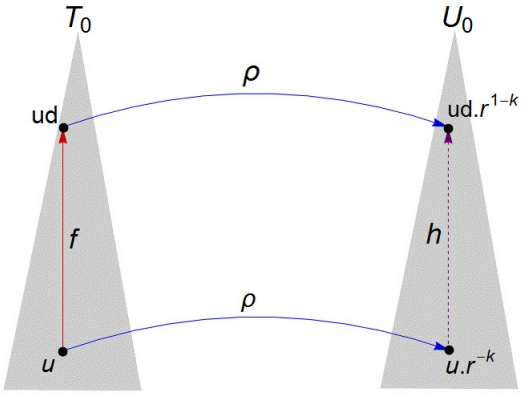
Theorem 12.9: Consider the cyclic group $\mathbb{Z}_n$. For any $d|n$ with the property that each prime factor of n is a prime factor of d, there exists exactly one possible d-regular functional graph induced by a nilpotent endomorphism, and an endomorphism that induces this structure is given by $f(1) = d$.

Proof:
Let r be any integer relatively prime to n. First we show that the functional graph induced by $f(1) = d$ is isomorphic to that induced by $h(1) = rd$.

Let T_0 be the tree induced by f, and U_0 the one induced by h. Define $\rho : T_0 \to U_0$ by $\rho(u) = ur^{-k}$, with k the remoteness of u with respect to f.

We first prove that ρ is injective. Suppose $\rho(u) = \rho(v)$ for some $u, v \in T_0$. Consequently $ur^{-k_u} = vr^{-k_v}$, with k_u, k_v the remoteness of u and v respectively. It now follows that $u = vr^{k_u - k_v}$, from which $f^{k_v}(u) = f^{k_v}(v)r^{k_u - k_v} = 0$. Consequently, $k_v \geq k_u$. Similarly, by exchanging the roles of u and v, one can see that $k_u \geq k_v$, so $k_u = k_v$, and as $ur^{-k_u} = vr^{-k_u}$, $u = v$.

Furthermore, for any $u \in T_0$, $\rho(f(u)) = \rho(ud)$, but as $f(u) = ud$, $f^t(u), t \in \mathbb{N} \cup \{0\}$ is f- cyclic if and only if $f^{t-1}(ud)$ is. The remoteness of ud is consequently one less than that of u and it follows that $\rho(ud) = ud.r^{1-k}$. It is also clear that $h(\rho(u)) = u.r^{-k}.dr = ur^{1-k} = \rho(f(u))$. So if $v = f(u)$ then $\rho(v) = \rho(f(u))$. Consequently, ρ is a tree isomorphism.



Commutativity diagram of ρ.

It is now clear that in order to study the structures induced by nilpotent endomorphisms of $\mathbb{Z}_n$, we only need to consider those of the form $f(1) = d$, with $d|n$ and each prime dividing n divides d. In order to establish the indegree of each vertex, note that $ker(f) = \{g \in G : dg = 0\}$, which is clearly all multiples of $\frac{n}{d}$, of which there are d, so $|ker(f)| = d$. The fact that each such d uniquely determines $|ker(f)|$ is hardly surprising, but the fact that there are no two distinct d's which determine the same cardinality for $ker(f)$ is far more enlightening, as it means that the size of the kernel (and hence the indegree) uniquely determines which endomorphism satisfying $f(1) = d$ induced it! Consequently, for a cyclic group $\mathbb{Z}_n$, for any $d|n$ which contains all prime factors of n, there is one unique functional graph with indegree d, which can be induced by nilpotent endomorphisms. □

This theorem allows one to recursively construct the unique d-regular functional graph of $\mathbb{Z}_n$. using the following procedure:

Procedure: Let $f(1) = d$ in $\mathbb{Z}_n$, Let $m = |ker(f^2)|$, Construct the unique $\frac{m}{d}$-regular tree of $\frac{n}{d}$, and then saturate each of these vertices until they have indegree d.

Proof: Given any tree T, induced by a nilpotent endomorphism, define the set of parents, $P(T)$, in the tree as all vertices with non-zero indegree.*
Note that the set of parents form a subgroup of G, and in the case of a cyclic group, $\mathbb{Z}_n$, the set of parents is once again a cyclic group generated by d. As $f|_{P(T)}$ is once again a group endomorphism, it follows that if we know the structure of the tree induced by $f|_{P(T)}$ then, in order to find the structure of T, we just need to add edges and vertices to $P(T)$ until the indegree of each vertex is d. As $P(T)$ is generated by d, it is clear that the group structure of $P(T)$ is isomorphic to $\mathbb{Z}_{\frac{n}{d}}$. If c is the indegree of $f|_{P(T)}$, then we know that there is a unique c-regular tree structure on $\mathbb{Z}_{\frac{n}{d}}$ that can be induced by an endomorphism.

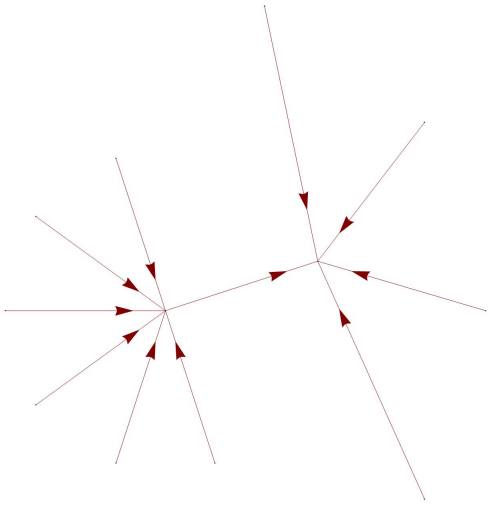
*In this context the author admits that perhaps the term "children" would be more applicable than "parents" due to all the edges being directed to the root vertex rather than to the leaves, but due to well established graph theoretic terminology we will stick to saying the vertices closer to the root are the parents.

In order to find c, we ask ourselves, which members of $\mathbb{Z}_n$ lie in $ker(f^2)$? Clearly all d members of $ker(f)$ lie in $ker(f^2)$, but also so does each child of the $c-1$ non-zero parents in $ker(f)$. As each parent has indegree d, we have $m = |ker(f^2)| = d+(c-1).d = cd$. Consequently $c = \frac{m}{d}$. The structure induced by $f|_{P(T)}$ is thus the $\frac{m}{d}$-regular structure on $\mathbb{Z}_{\frac{n}{d}}$.

Example 12.10: Find all functional graphs of nilpotent endomorphisms of $\mathbb{Z}_{72}$.

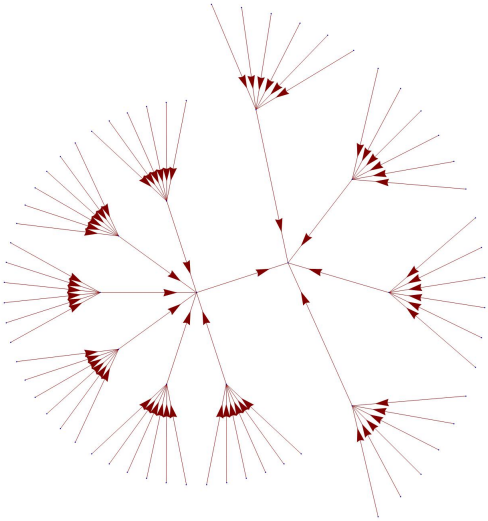
For this group, $d \in \{6, 12, 18, 24, 36, 72\}$. We will consider each of these cases.

Case 1: $d = 6$. $m = |\{x \in \mathbb{Z}_{72} : 36.x = 0\}| = 36$, so we construct the 6-regular tree of $\mathbb{Z}_{12}$. In turn to construct this tree, we have to find the 2-regular tree of $\mathbb{Z}_2$, which is simply the zero map on $\mathbb{Z}_2$, making the functional graph of the 6-regular tree of $\mathbb{Z}_{12}$



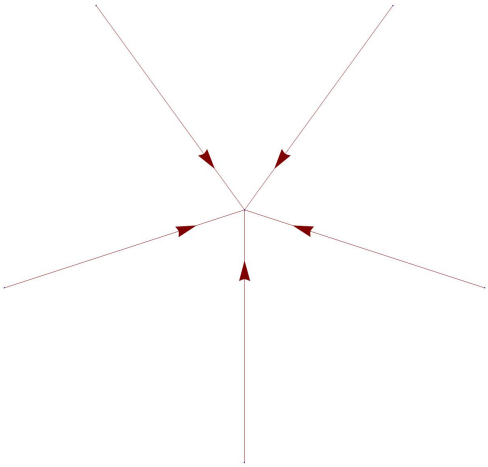
Structure induced by $f(1) = 6$ on $\mathbb{Z}_{12}$.

which in turn makes the 6-regular tree of $\mathbb{Z}_{72}$



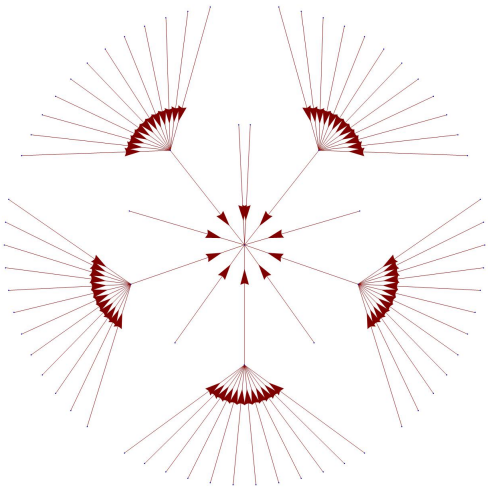
Structure induced by $f(1) = 6$ on $\mathbb{Z}_{72}$.

Case 2: $d = 12$. $m = |\{x \in \mathbb{Z}_{72} : 72.x = 0\}| = 72$, so we need to construct the $\frac{72}{12} = 6$ regular tree of $\mathbb{Z}_6$, which is induced by the zero map on $\mathbb{Z}_6$.



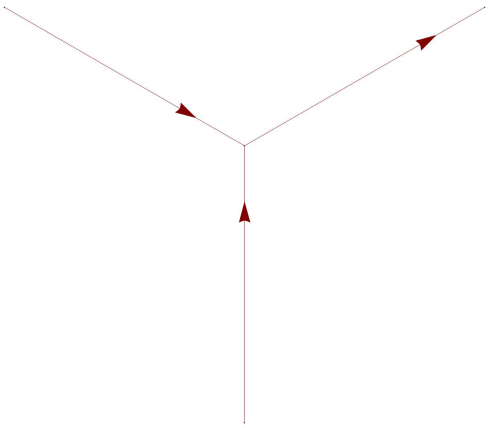
Structure induced by $f(1) = 0$ on $\mathbb{Z}_6$.

By adding and increasing all of the indegrees to 12, we get the following structure:



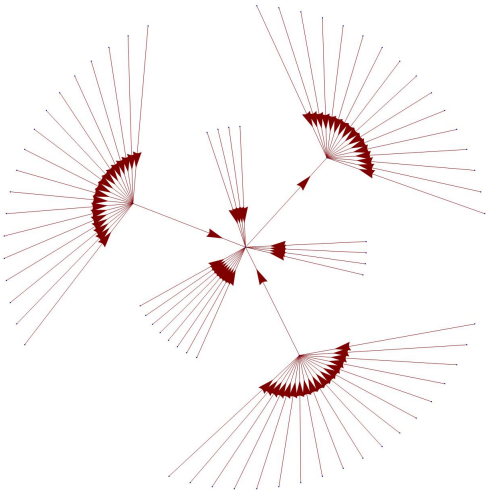
Structure induced by $f(1) = 12$ on $\mathbb{Z}_{72}$.

Case 3: $d = 18$. $m = |\{x \in \mathbb{Z}_{72} : 324.x = 0\}| = |\{x \in \mathbb{Z}_{72} : 36.x = 0\}| = 36$, so we need to construct the $\frac{36}{18} = 2$ regular tree of $\mathbb{Z}_4$, for which we need to find the $\frac{4}{2} = 2$ regular tree of $\mathbb{Z}_2$, which is the zero mapping.



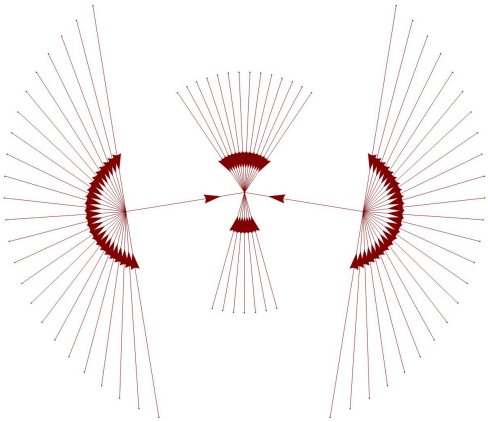
Structure induced by $f(1) = 2$ on $\mathbb{Z}_4$.

And then finally:



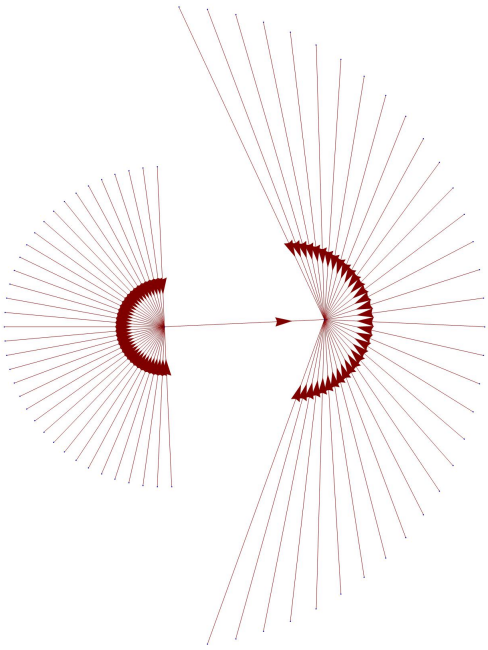
Structure induced by $f(1) = 18$ on $\mathbb{Z}_{72}$.

Case 4: $d = 24$. $m = |\{x \in \mathbb{Z}_{72} : 576.x = 0\}| = |\{x \in \mathbb{Z}_{72} : 72.x = 0\}| = 72$, so we need to construct the $\frac{72}{24} = 3$ regular tree of $\mathbb{Z}_3$, which is simply the zero mapping. Similar to the previous cases, we find the functional graph as



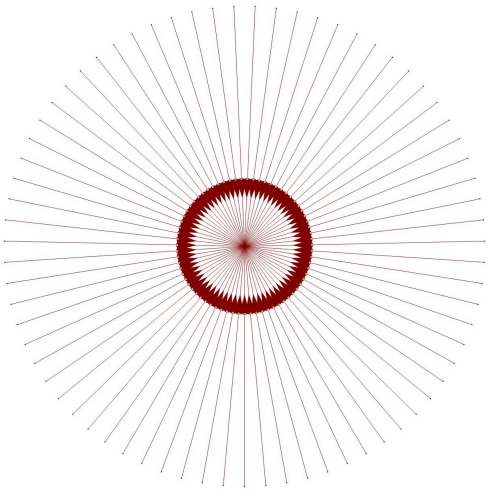
Structure induced by $f(1) = 24$ on $\mathbb{Z}_{72}$.

Case 5: $d = 36$. $m = |\{x \in \mathbb{Z}_{72} : 1296.x = 0\}| = |\{x \in \mathbb{Z}_{72} : 72.x = 0\}| = 72$, so we need to find the $\frac{72}{36} = 2$ regular tree of $\mathbb{Z}_2$, which is once again just the star with indegee 2 with 2 members. By filling up the indegrees we get the last structure as



Structure induced by $f(1) = 36$ on $\mathbb{Z}_{72}$.

Case 6: $d = 72$. Here all members of the group gets mapped to 0, leading to a star with 0 having in degree 72, and all other vertices having in-degree 0.



Structure induced by $f(1) = 0$ on $\mathbb{Z}_{72}$.

Since we are now able to find the functional graphs of each nilpotent endomorphism on a cyclic group, we can turn our attention to the structures of general endomorphisms on cyclic groups. Most of the work has already been done by now. We just need to patch it together. We just need to note that given any endomorphism on $G = \mathbb{Z}_n$, the structure of T_0 and C_G uniquely determine the functional graph, and that $f|_{T_0}$ is nilpotent, and $f|_{C_G}$ is an automorphism.

Lemma 12.11: Let $G = \mathbb{Z}_n$ and f an endomorphism defined by $f(1) = m$. Define w as the greatest factor of n which is relatively prime to m, then T_0 is generated by w and C_G is generated by $\frac{n}{w}$.

Proof:
Let us decompose n and m into prime factors as follows:

$$n = \prod_{i=1}^{j} p_i^{\alpha_i} \prod_{i=1}^{k} q_i^{\beta_i}.$$

$$m = R_m \prod_{i=1}^{j} p_i^{\gamma_{(m,i)}}.$$

Here we have all prime factors distinct, no exponent zero, and R_m relatively prime to n. In fact, every $g \in \mathbb{Z}_n$ can be decomposed into the form

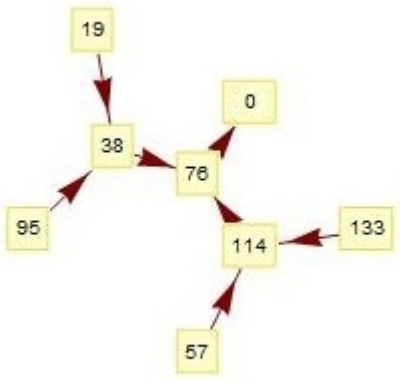
$$g = R_g \prod_{i=1}^{j} p_i^{\gamma_{(g,i)}} \prod_{i=1}^{k} q_i^{\delta_{(g,i)}}$$

with R_g relatively prime to n. It follows that

$$f^a(g) = (R_m)^a R_g \prod_{i=1}^{j} p_i^{\gamma_{(g,i)} + a(\gamma_{(m,i)})} \prod_{i=1}^{k} q_i^{\delta_{(g,i)}}.$$

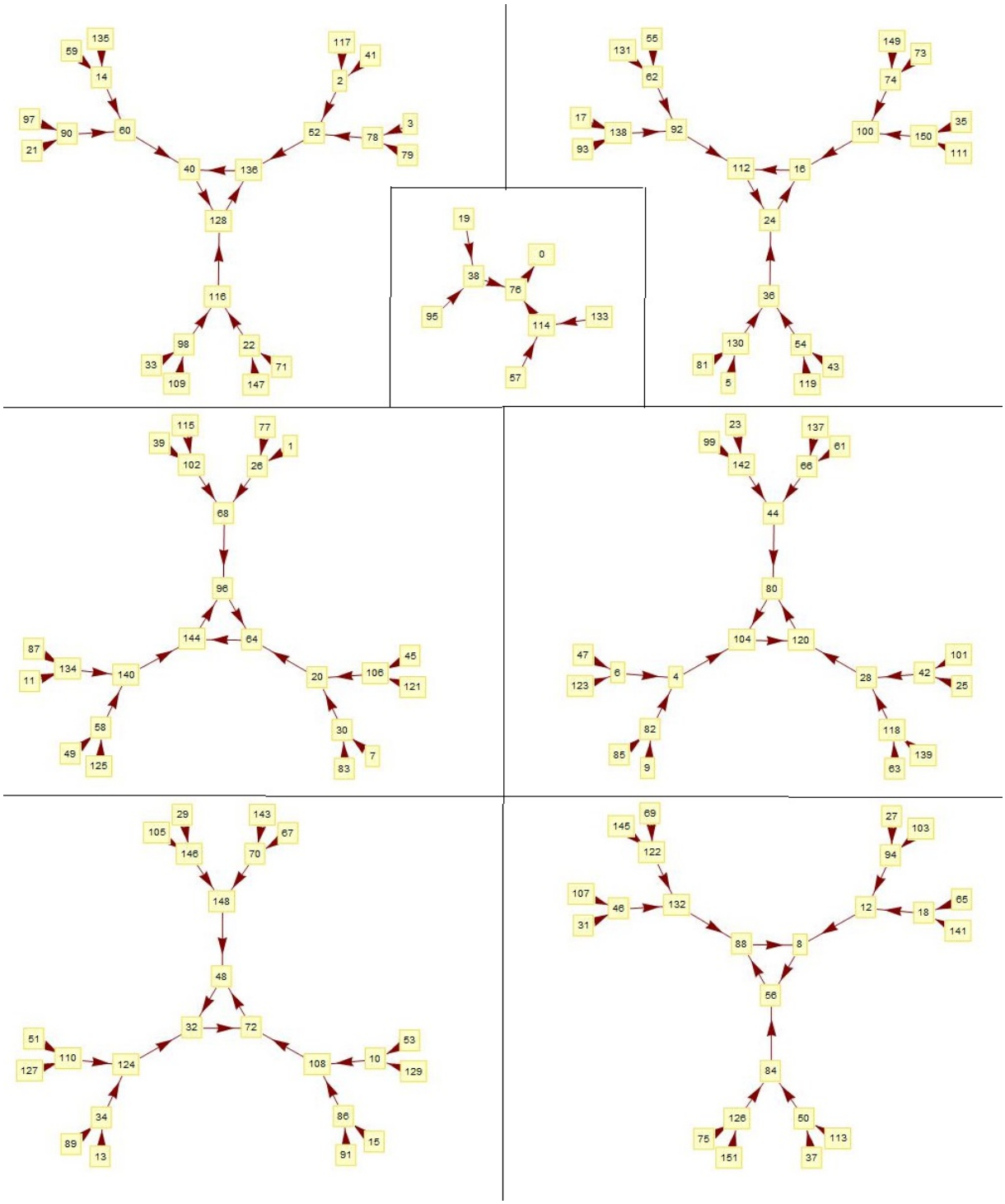
As $\gamma_{(m,i)} > 0$, by repeated evaluation of f at g, eventually $\gamma_{(g,i)} + a(\gamma_{(m,i)}) \geq \alpha_i$, but the exponents of the q_i's stay constant on repeated evaluation of f at g, meaning that there exists a natural number a such that $f^a(g) = 0$ if and only if $\delta_{(g,i)} \geq \beta_i$. The set of all such g is exactly all multiples of $w = \prod_{i=1}^{k} q_i^{\beta_i}$. Consequently $|T_0| = \frac{n}{w}$, and $|C_G||T_0| = n$ (each f-cyclic member x is associated with its own unique acyclic tree T_x), so $|C_G| = \frac{n}{n} w = Q$, implying that C_G is generated by $\frac{n}{w}$. □

Example 12.12: Find the functional graph of the endomorphism $f(1) = 26$ on $G = \mathbb{Z}_{152}$.
We note that T_0 is generated by 19, making T_0 isomorphic to $\mathbb{Z}_8$. As $f(1) \equiv_8 2$, the induced nilpotent endomorphism on $\mathbb{Z}_8$ is given by $f_{T_0}(1) = 2$. Using our established methods, we find the following functional graph for T_0:



T_0 for $f(1) = 26$ on $\mathbb{Z}_{152}$.

C_G is isomorphic to $\mathbb{Z}_{19}$, and as $26 \equiv_{19} 7$, it follows that $f_{C_G}(1) = 7$. Using our results on the automorphisms of cyclic groups, we find that the cyclic structure of C_G is $\begin{bmatrix} 1 & 6 \\ 1 & 3 \end{bmatrix}$. By appending a copy of T_0 at each vertex of C_G, we find the following functional graph:



Structure induced by $f(1) = 26$ on $\mathbb{Z}_{152}$.

Imagination will often carry us to worlds that never were. But without it we go nowhere.

$\sim$ C. Sagan (1934-1996)

13 Endomorphisms of $\mathbb{Z}_p^n$

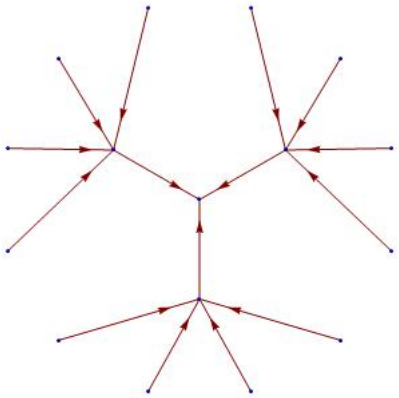
We now turn our attention once again to groups of the form $G = \mathbb{Z}_p^n$, for some prime p. Some of our previous work can easily be extended here, for example knowing the action of an endomorphism f on T_0 and C_G once again allows one to construct the functional graph of f, $f|_{T_0}$ is nilpotent and $f|_{C_G}$ is an automorphism. As we already know the structure of the automorphisms, we will now investigate the structure of T_0 for nilpotent endomorphisms of the group $\mathbb{Z}_p^n$. At this stage one might hope (optimistically) that similar to the cyclic groups, for each $d|p^n$, there is exactly one d-regular tree on $\mathbb{Z}_p^n$, but unfortunately this is not true, as the next example shows.

Example 13.1: Consider the endomorphisms f, h on $\mathbb{Z}_2^4$, with matrix forms

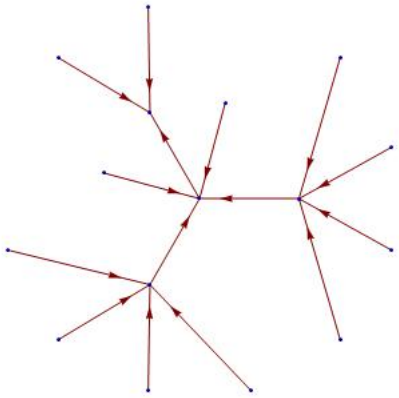
$$f = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$h = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

The associated functional graphs are



Structure induced by f on $\mathbb{Z}_2^4$.



Structure induced by h on $\mathbb{Z}_2^4$.

As can be seen, these two trees are indeed non-isomorphic 4-regular trees, which means that unlike the case with cyclic groups we cannot speak about "The p^k-regular tree of size p^n". We will thus need a new notation to exactly describe the structure of a k-regular tree. The key lies in a process that was glanced at during the iterative construction used for cyclic groups, where we used the notion of a "parent set", as this construction lies central in the way in which we will describe the trees associated with the endomorphisms of $\mathbb{Z}_p^n$, we will give it a formal definition.

Definition 13.2: **Parent tree**

The **parent tree** of a tree T is the induced subgraph of T, of which the vertex set contains exactly all vertices which has non-zero indegree. The parent tree of T will be denoted by $P(T)$.

It should be noted that for any functional graph of a nilpotent endomorphism f, $P(T) = Im(f)$.

Corollary 13.3: $P^k(T_0)$ is a subspace of $\mathbb{Z}_p^n$ for each $k \in \mathbb{N}$, and $f|_{P^k(T_0)}$ is a nilpotent endomorphism.

In order to describe the structure of a k-regular tree, we will look at the trees resulting from successive evaluation of P at T_0, until the only member left in the range is 0. To ease the construction we will now define a construction sequence of a k-regular tree.

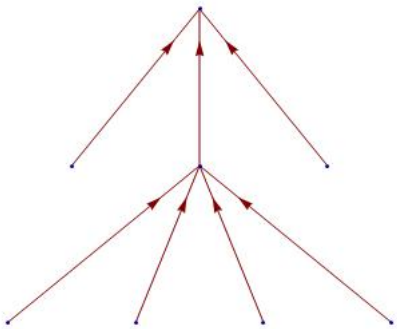
Henceforth, for a given tree T induced by a null-potent endomorphism, f, the sequence $\langle |T|, |P(T)|, |P^2(T)|, \ldots, |P^k(T)| \rangle$, where k is the least natural number such that $|P^k(T)| = 1$, will be referred to as the **construction sequence** of f, and denoted by $\mathcal{C}_f$.

For example, the construction sequences of f and h in example 13.1 are $\mathcal{C}_f =$

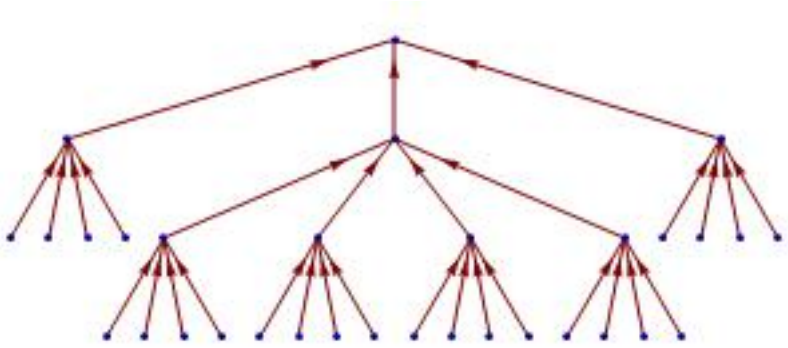
$\langle 16, 4, 1\rangle$ and $\mathcal{C}_h = \langle 16, 4, 2, 1\rangle$.

The important observation is that the structure of the tree can uniquely be constructed from the construction sequence, by reading the terms from the back to the front and saturating the vertices to the required level at each step.

For example, consider the construction sequence $\mathcal{C} = \big\langle |T|, |P(T)|, |P^2(T)|, |P^3(T)|\big\rangle$ $= \langle 32, 8, 2, 1\rangle$. Starting from the right, we have a single vertex (which corresponds to 0). Being the sole parent of every member of $P^2(T)$, we get that $P^2(T)$ is a star with one loop back to 0 and 1 vertex mapping to 0. These are in turn the parents of everything in $P(T)$. As $\frac{|P(T)|}{|P^2(T)|} = 4$, we construct $P(T)$ by saturating each vertex of $P^2(T)$ up to indegree 4.



Lastly, T can be obtained from $P(T)$ by saturating each vertex of $P(T)$ until the indegree is $\frac{|T|}{|P(T)|} = 4$. The resulting graph is shown below.



Remarks:

1. While working with groups of the form $\mathbb{Z}_p^n$, all terms in the sequence must be powers of p, as all subspaces of $\mathbb{Z}_p^n$ have cardinalities a power of p.

2. While working with finite groups, the construction sequence must terminate, and it will always terminate on 1, as all group members are eventually mapped to 0 by nilpotent endomorphisms.

3. For any construction sequence $\mathcal{C} = \langle c_1, c_2, \ldots, 1\rangle$, the sequence $\left\langle \frac{c_i}{c_{i+1}} \right\rangle$ cannot increase. If it were to increase the indegree of $P^{i+1}(T)$ would be greater than that of $P^i(T)$, which would clearly be a contradiction, since, in this case moving over from $P^{i+1}(T)$ to $P^i(T)$ would require the destruction of edges.

It is however delightful that the restrictions mentioned in this remark, are not only necessary for the existence of a null-potent endomorphism induced tree with a given construction sequence, but actually sufficient!

Theorem 13.4: Given any construction sequence $\mathcal{C}$, satisfying the remarks mentioned above, there exists a nilpotent endomorphism on $\mathbb{Z}_p^n$, of which the construction sequence is $\mathcal{C}$.

Proof:
From the construction sequence $\mathcal{C} = \langle c_1, c_2, \ldots, c_s = 1\rangle$ for a tree on $\mathbb{Z}_p^n$, construct the sequence $d_i = \log_p \frac{c_i}{c_{i+1}}$, $i < s$. From the remarks, d_i is a non-increasing sequence of natural numbers. To see the significance of the d_i's, suppose we have a space, V of size c_i. When applying f to V, we are left (by definition) with a space of size c_{i+1}, It follows that d_i is the number of dimensions eliminated from V by f, i.e. $dim(f^i(V)) = dim(f^{i-1}(V)) - d_i$. As $dim(G) = n$, it follows that $\sum_{i=1}^{s-1} d_i = n$ (in other words, every dimension is eventually eliminated by f, which makes sense as f is nilpotent).

Let us construct the following $d_1 \times (s-1)$ table, D, from the sequence d_i:

$$D(r,c) = \begin{cases} 1 \text{ if } r \leq d_c \\ 0 \text{ otherwise} \end{cases}$$

Here is an example for $(d_i) = 4, 3, 3, 2, 1$.

$$D = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Define $\alpha_r = \sum_{i=1}^{s-1} D(r,i)$.

For $t \geq 1$ consider the $t \times t$ matrix, A_t with all subdiagonal terms equal to 1, and all other terms 0:

$$A_t = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix}$$

Now note that applying A_t as an endomorphism of $\mathbb{Z}_p^t$, A_t eliminates one dimension of $\mathbb{Z}_p^t$ after each successive application of A_t to $\mathbb{Z}_p^t$, up to the t'th application after which everything has been mapped to 0.

We can now construct our desired matrix that eliminates d_i dimensions on the i'th application. Let A be obtained by placing copies of A_{α_i} along the diagonal, and making all other entries 0.

$$A = \begin{bmatrix} A_{\alpha_1} & 0 & \cdots & 0 \\ 0 & A_{\alpha_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_{\alpha_{s-1}} \end{bmatrix}$$

This matrix represents an endomorphism on $\mathbb{Z}_p^n$, as $\sum_{i=1}^{s-1} \alpha_i = n$. On the j'th application of A to $\mathbb{Z}_p^n$, The A_k with $k \geq i$ will each eliminate one dimension of $\mathbb{Z}_p^n$, and all the others will no longer eliminate anything. The number of dimensions annihilated is thus $|\{\alpha_i : \alpha_i \geq j\}|$, which is exactly the number of 1's in the j'th column of D, which is d_j. Consequently, the construction sequence associated with the endomorphism induced by A is $\mathcal{C}$. □

Example 13.5: Find a nilpotent endomorphism of $\mathbb{Z}_p^6$ with construction sequence $\langle p^6, p^3, p, 1 \rangle$.

The corresponding d_i sequence is $3, 2, 1$, which gives:

$$D = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

From which $\alpha_1 = 3, \alpha_2 = 2$ and $\alpha_3 = 1$. We can now construct A as

$$A = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Mathematics is a game played according to certain simple rules with meaningless marks on paper.

$\sim$ D. Hilbert (1862-1943)

A Table of symbols

Symbol	Description	Page(s)
$Aut(G)$	Automorphism group	9
C_x	Context dependent: Conjugacy class, Companion matrix of cycles subgroup.	34, 53, 75
$\mathcal{C}_f$	Construction sequence of an endomorphism	87
$End(G)$	Endomorphism ring of a group	9
$GL(F,n)$	The $n \times n$ general linear group over a field	32
$J_n(a)$	Jordan n-totient function.	18
$J(n,\lambda)$	Jordan Block matrix	33
$M_n(R)$	Matrix ring over ring	12
$Min(M)$	Minimal polynomial of M	53
$ord(x)$	Context dependent: order of group member, order of polynomial	27, 64
$\varphi(n)$	Euler totient function	15
Φ_n	$n-th$ Cyclotomic polynomial	51
$\mathcal{P}_v$	point annihilator at v	60
$P(T)$	Parent tree of tree T	87
$Q_i(\lambda)$	Polynomial of form $\sum_{j=0}^{p_i-1} \lambda^{\frac{n \cdot j}{p_i}}$ for some natural number n, and prime p_i dividing it.	51
S_f	Polynomial annihilator at f	60
T_x	Acyclic tree at x	74
$Z(x)$	Stabilizer of x	35
$\mathbb{Z}_n$	Additive cyclic group with n members	9
$\mathbb{Z}$	Additive group of the integers	9

References

[1] J. Fraleigh, *A First course in abstract algebra*, (7^{th}), Pearson, 2002.

[2] IM. Newman, *Integral matrices*, Academic press, London, 1972.

[3] V.V. Prasolov, *Problems and Theorems in Linear Algebra*, Translations of Mathematical Monographs **134**, 68-71.

[4] E. Weisstein, *Cassini's Identity*. http://mathworld.wolfram.com/CassinisIdentity.html.

[5] G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers*, Oxford Science, Clarendon, 1979.

[6] D.M Burton, *Elementary number theory*, Mc Graw Hill, New York, 2007.

[7] JS. Golan, *The linear algebra a beginning graduate ought to know*, (2^{nd}), Springer, Dordrecht, The Netherlands, 2007.

[8] R. and Niederreiter Lidl H, *Finite Fields*, (2^{nd}), Cambridge University Press, Cambridge, 2008.

[9] H. and Rorres Anton C., *Elementary linear algebra*, (10^{th}), Wiley, United States of America, 2010.

[10] R.E. Hartwig, *Roth's removal rule and the rational canonical form*, Amer. Math. Monthly **103** (1996), 332-335.

[11] B. de Klerk and J. Meyer and J. Szigeti and L. Van Wyk, *Functions realising as abelian group automorphisms*, Comm. Algebra. to appear.

[12] J. Szigeti, *Which self maps appear as lattice endomorphisms?*, submitted.

[13] C. Jordan, *Traité des substitutions* (1870).

[14] P.E. Bland, *Rings and their modules*, de Gruyter, Berlin, 2011.

[15] W. Rudin, *Principles of Mathematical Analysis*, 3^{rd}, McGraw-Hill, United States of America, 1976.

[16] *Order of General Linear Group over Finite Field*, `https://proofwiki.org/wiki/Order_of_General_Linear_Group_over_Finite_Field`.

[17] *Element structure of general linear group of degree two over a finite field*, `http://groupprops.subwiki.org/wiki/Element_structure_of_general_linear_group_of_degree_two_over_a_finite_field`.