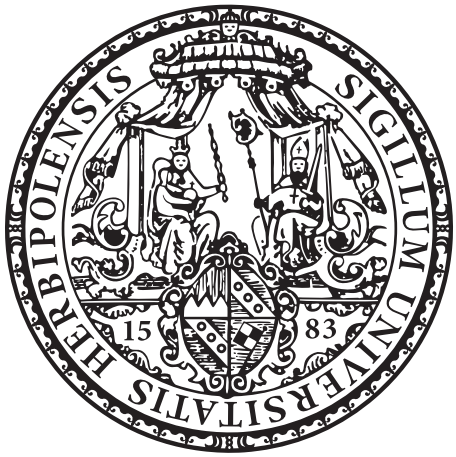
Algebraic and Arithmetic Properties of Graph Spectra

Dissertation zur Erlangung des
naturwissenschaftlichen Doktorgrades
der Bayerischen Julius-Maximilians-Universität
Würzburg



vorgelegt von

Katja Mönius

Würzburg, 2021

2010 *Mathematics Subject Classification.* 05C50, 05C25.
Key words and phrases. Graph spectrum, eigenvalues, integral graph, circulant graph, Cayley graph, Schur ring, graph isomorphism, zero-divisor graph.

Eingereicht am 9. Oktober 2020
bei der Fakultät für Mathematik und Informatik
der Bayerischen Julius-Maximilians-Universität Würzburg.

Erster Gutachter: Prof. Dr. Jörn Steuding
Zweiter Gutachter: Prof. Dr. Wasin So
Dritter Gutachter: Prof. Dr. Jürgen Sander

Tag der mündlichen Prüfung: 3. März 2021

Abstract

In the present thesis we investigate algebraic and arithmetic properties of graph spectra. In particular, we study the *algebraic degree* of a graph, that is the dimension of the splitting field of the characteristic polynomial of the associated adjacency matrix over the rationals, and examine the question whether there is a relation between the algebraic degree of a graph and its structural properties. This generalizes the yet open question "Which graphs have integral spectra?" stated by Harary and Schwenk [42] in 1974.

We provide an overview of graph products since they are useful to study graph spectra and, in particular, to construct families of integral graphs. Moreover, we present a relation between the diameter, the maximum vertex degree and the algebraic degree of a graph, and construct a potential family of graphs of maximum algebraic degree.

Furthermore, we determine precisely the algebraic degree of *circulant graphs* and find new criteria for isospectrality of circulant graphs. Moreover, we solve the *inverse Galois problem for circulant graphs* showing that every finite abelian extension of the rationals is the splitting field of some circulant graph. Those results generalize a theorem of So [92] who characterized all *integral* circulant graphs. For our proofs we exploit the theory of *Schur rings* which was already used in order to solve the isomorphism problem for circulant graphs.

Besides that, we study spectra of *zero-divisor graphs* over finite commutative rings. Given a ring R, the zero-divisor graph over R is defined as the graph with vertex set being the set of non-zero zero-divisors of R where two vertices x, y are adjacent if and only if $xy = 0$. We investigate relations between the eigenvalues of a zero-divisor graph, its structural properties and the algebraic properties of the respective ring.

Acknowledgments

First and foremost, I would like to thank my advisor Jörn Steuding for his consistent support and guidance during the last years, for his encouragement and for always believing in me. I am very grateful that he gave me the chance to elaborate this thesis.

Moreover, I would like to express my sincere gratitude to Wasin So who gave me the chance to come to the U.S. and who hosted me in the kindest possible way. It was an honor and a joy for me to work with him, and I am still very sad that I had to leave early.

At that point, I also thank Peter Müller without whom it would not have been possible for me to take this journey.

I am very grateful to Richard Greiner thanks to whom I was never unemployed, especially not at the time when the Corona pandemic started.

More thanks are due to Dominik Barth who answered several questions of mine and helped me to run some examples in Magma.

Furthermore, I would like to thank all my friends who supported me during the last years. I am especially grateful to Kathi, Felix, Alex, Daniel and my brother Ralph who proofread my thesis and gave me helpful feedback.

Special thanks to Jan Bartsch who always listened to me and encouraged me when I had doubts about myself. I also thank Dmitri Nedrenco for many helpful discussions about teaching and for his excellent coffee, and Michaela Kohmann for driving me around in her car many times.

Last but not least, I would like to thank my family from the bottom of my heart. They always supported me and believed in me, they gave me the chance to move to Würzburg and to study Mathematics. Without the support of my family I certainly would not be where I am today.

Würzburg, October 2020 *Katja Mönius*

Contents

List of Symbols

Graphs

$\mathcal{C}_n$	The cycle graph of order n.
$\mathcal{P}_n$	The path graph of order n.
$\mathcal{K}_n$	The complete graph of order n.
$\mathcal{K}_{n,m}$	The complete bipartite graph with bipartitions of order n and m, respectively.
$\mathrm{Cay}(G, S)$	The Cayley graph with vertex set being the group G and connection set $S \subseteq G$.
$\mathrm{Pal}(n)$	The Paley graph of prime power order n.
$\Gamma(R)$	The zero-divisor graph of the ring R.
$\Gamma_E(R)$	The compressed zero-divisor graph of the ring R.

Groups, rings and fields

$\mathbb{N}$	The positive integers.
$\mathbb{Z}$	The integers.
$\mathbb{Q}$	The rationals.
$\mathbb{R}$	The real numbers.
$\mathbb{C}$	The complex numbers.
$\mathbb{Z}_n$	The ring of integers modulo n.
$\mathbb{Z}_n^*$	The multiplicative group of units of $\mathbb{Z}_n$.
C_n	The multiplicative cyclic group of order n.
$\mathbb{F}_q$	The finite field of order q.
S_n	The symmetric group of order n.
R^*	The group of units of the ring R.
$\mathrm{Aut}(G)$	The automorphism group of a group G.

Sets

$\#S$	Number of elements in the set S.
$\mathcal{P}(S)$	The power set of a set S.
$\{x_1^{[m_1]}, \ldots, x_r^{[m_r]}\}$	Multiset with elements $x_1, \ldots, x_r$ where each element x_i appears with multiplicity m_i.

Matrices

I	The identity matrix.
A^{t}	The transpose of the matrix A.
$\dim A$	The dimension of the domain of the linear transformation associated to the matrix A, i.e. the number of columns of A.
$\det(A)$	The determinant of the matrix A.
$\operatorname{rank}(A)$	The rank of the matrix A, i.e. the maximum number of linearly independent column vectors in A.
$\operatorname{tr}(A)$	The trace of the matrix A, i.e. the sum of the diagonal entries of A.

Graph quantities

$V(\mathcal{G})$	The set of vertices of the graph $\mathcal{G}$.
$E(\mathcal{G})$	The (multi-)set of edges of the graph $\mathcal{G}$.
$A(\mathcal{G})$	The adjacency matrix of the graph $\mathcal{G}$.
$\operatorname{spec}(\mathcal{G})$	The spectrum of the graph $\mathcal{G}$, i.e. the multiset of eigenvalues of $A(\mathcal{G})$.
$\chi_{\mathcal{G}}$	The characteristic polynomial of the graph $\mathcal{G}$, i.e. $\chi_{\mathcal{G}}(x) = \det(xI - A(\mathcal{G}))$.
$\deg(\mathcal{G})$	The algebraic degree of the graph $\mathcal{G}$, i.e. the dimension of the splitting field of the characteristic polynomial of $A(\mathcal{G})$ over the rationals.
$\eta(\mathcal{G})$	The nullity of the graph $\mathcal{G}$, i.e. the multiplicity of 0 in $\operatorname{spec}(\mathcal{G})$.
$\operatorname{diam}(\mathcal{G})$	The diameter of the graph $\mathcal{G}$.

Numbers

$\gcd(x, y)$	The greatest common divisor of $x, y \in \mathbb{Z}$.
$\operatorname{lcm}(x, y)$	The least common multiple of $x, y \in \mathbb{Z}$.
$x \mid y$	x divides y.
$\operatorname{ord}_n(x)$	The order of x in $\mathbb{Z}_n$.

Other symbols

φ	Euler's totient function.
ζ_n	Primitive n-th root of unity $\exp(2\pi i/n)$.
$\mathrm{e}(x)$	Abbreviation for $\exp(2\pi i x)$.

CHAPTER 1

Introduction

From Euler to graphs

Graph theory (as it is known today) has its origins back in the 18th century when Euler answered the famous problem of the *Seven Bridges of Königsberg* (cf. [31]). The question was whether there exists a walk through the city crossing each of the seven bridges in Königsberg once and only once. Euler was the first who reformulated this problem in abstract terms after noticing that lots of information were irrelevant. Every land mass could be replaced with an abstract *vertex* and each bridge with an abstract *edge* recording which pair of land masses is connected by this bridge.

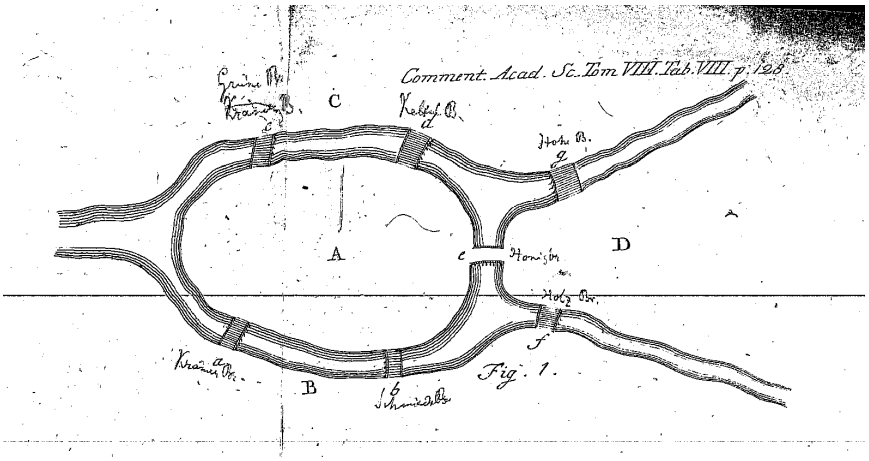


FIGURE 1.1. The seven bridges of Königsberg. From [31].

A *graph* $\mathcal{G}$ consists of a set $V(\mathcal{G})$ of vertices and a (multi-)set $E(\mathcal{G}) \subseteq V(\mathcal{G}) \times V(\mathcal{G})$ of edges. A vertex $v \in V(\mathcal{G})$ is called *adjacent* to the vertex $w \in V(\mathcal{G})$ if $(v, w) \in E(\mathcal{G})$. This is also denoted by $v \sim w$. Furthermore, the number of vertices adjacent to a fixed vertex v is said to be the *degree* of v. We always assume $\mathcal{G}$ to be finite, i.e. $\#V(\mathcal{G}) < \infty$. An edge $e = (v, w) \in E(\mathcal{G})$ is called *directed* if there is an orientation from v to w, and *undirected* otherwise. In the latter case, we also write $e = \{v, w\}$. A graph is called *undirected* if it consists of undirected edges only, and is called *simple* if, in addition, it has no *multiple-edges* (i.e. $E(\mathcal{G})$ is a set) and no *loops* (i.e. no edges of the form (v, v)).

A *path* from v to w of length n is a sequence of n distinct edges $(e_1, e_2, \ldots, e_n)$ which joins a sequence of distinct vertices $(v = v_0, v_1, \ldots, v_n = w)$ such that $e_i = (v_{i-1}, v_i)$ for $i = 1, \ldots, n$. An undirected graph $\mathcal{G}$ is said to be *connected* if for every pair of vertices v, w in $\mathcal{G}$ there is a path from v to w. A directed graph is called *connected* if replacing all of its directed edges with undirected edges produces a connected (undirected) graph. The *distance* $d(v, w)$ between two vertices v,w of a connected graph $\mathcal{G}$ is the minimum length of the paths connecting v and w, and the *diameter* $\operatorname{diam}(\mathcal{G})$ of $\mathcal{G}$ is defined as the length $\max_{v,w} d(v, w)$ of the 'longest shortest path' between any two vertices v, w of $\mathcal{G}$.

The adjacency matrix of a graph

By labeling the vertices $V(\mathcal{G}) = \{1, \ldots, n\}$ of $\mathcal{G}$, we can define the $n \times n$ *adjacency matrix* $A(\mathcal{G}) = \left(a_{i,j}\right)$ of $\mathcal{G}$ as the matrix with entries

$$a_{i,j} = \begin{cases} 1, & \text{if } i \sim j, \\ 0, & else. \end{cases}$$

Note that different labelings lead to different adjacency matrices, but all adjacency matrices of a fixed graph $\mathcal{G}$ are similar. In the following, when we speak of a graph $\mathcal{G}$, we always think of the graph together with a particular labeling of its vertices. Therefore, it is valid, from now on, to speak about *the* adjacency matrix of $\mathcal{G}$.

Two graphs $\mathcal{G}, \mathcal{H}$ are called *isomorphic* if there is a bijection $\sigma : V(\mathcal{G}) \longrightarrow V(\mathcal{H})$ such that two vertices v and w are adjacent in $\mathcal{G}$ if and only if $\sigma(v)$ and $\sigma(w)$ are adjacent in $\mathcal{H}$. This means that $\mathcal{G}$ and $\mathcal{H}$ are basically the same graphs but the chosen vertex labeling of $\mathcal{G}$ may be different from the one of $\mathcal{H}$. The *automorphism group* $\operatorname{Aut}(\mathcal{G})$ of a graph $\mathcal{G}$ is the set of all graph isomorphisms $\sigma : V(\mathcal{G}) \longrightarrow V(\mathcal{G})$ and, in fact, forms a group by composition.

Spectra of graphs

The *eigenvalues* of a graph $\mathcal{G}$ are defined as the eigenvalues of its adjacency matrix $A(\mathcal{G})$. The multiset of eigenvalues is called *spectrum* of $\mathcal{G}$. The first mathematical paper on graph spectra [25] was published in 1957 and was motivated by the so-called membrane vibration problem. The paper [43] from 1931 though is considered to be the first paper where graph spectra appear in an implicit form. Since the adjacency matrices of isomorphic graphs are similar, isomorphic graphs always have the same spectrum. Unfortunately, the converse of this statement is not true in general since, for example, the graphs in Figure 1.2 with

respective adjacency matrices

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

have the same spectrum $\{2, -2, 0, 0, 0\}$ although they are not isomorphic.

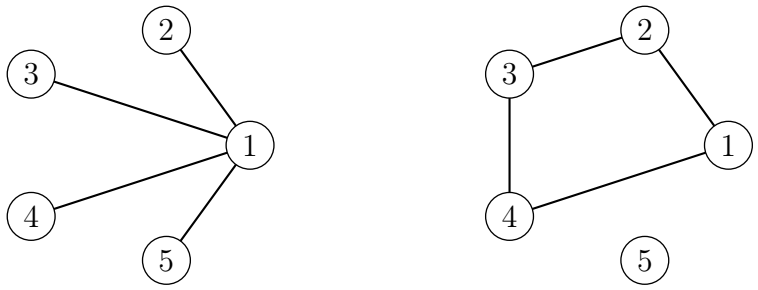


FIGURE 1.2. Non-isomorphic isospectral graphs.

Such pairs of graphs are called *cospectral*. Until now, there is no efficient algorithm known in order to decide whether two (arbitrary) given graphs are isomorphic or not. This problem is referred to as the *graph isomorphism problem*. Surprisingly, it is not known to be solvable in polynomial time nor to be NP-complete. In fact, the fastest known algorithm so far was published by Babai [13] in 2016 who found a quasipolynomial time algorithm.

The main idea of spectral graph theory is to relate important invariants of a graph to its spectrum. Often, such invariants are difficult to compute. Therefore, comparing them with expressions involving eigenvalues turned out to be very useful.

For example, the spectrum of a connected *k-regular* graph $\mathcal{G}$, that is a graph where each vertex has the same degree k, contains the eigenvalue k exactly once, and every other eigenvalue of $\mathcal{G}$ is strictly smaller than k in absolute value. More generally, the eigenvalues of an arbitrary graph $\mathcal{G}$ are all contained in the interval $[-d, d]$ where d denotes the maximum vertex degree of $\mathcal{G}$.

Since the spectrum of a non-connected graph is the union of the spectra of its connected components, graphs are mostly assumed to be connected in spectral graph theory.

The *nullity* $\eta(\mathcal{G})$ of a graph $\mathcal{G}$ is defined as the multiplicity of the eigenvalue 0 of $\mathcal{G}$. Obviously,

$$\eta(\mathcal{G}) = \dim A(\mathcal{G}) - \operatorname{rank} A(\mathcal{G}).$$

Studying the nullity of graphs has its origin in chemistry since it turned out that the chemical compound corresponding to a molecular graph $\mathcal{G}$ with $\eta(\mathcal{G}) > 0$ is highly reactive and unstable, or nonexistent. Further background and results on the nullity of graphs are summarized in [40].

For a good introduction to spectral graph theory we refer to the books [39, 27, 24].

Some graph families and their spectra

In order to gain more insight into the relation between graph invariants and the respective graph spectrum, it is usually helpful to restrict to *families* of graphs. For example, a graph $\mathcal{G}$ is called *bipartite* if its vertex set can be partitioned into two disjoint parts X_1, X_2 such that all edges of $\mathcal{G}$ meet both X_1 and X_2. In fact, a graph is bipartite if and only if its spectrum is symmetric with respect to zero (cf. [24, Proposition 3.4.1]).

Another important family of graphs is the family of *cycle graphs* $\mathcal{C}_n$. Those simple graphs are (as the name suggests) cycles of length n. The spectrum of $\mathcal{C}_n$ consists of the numbers

$$2\cos(2\pi j/n) \quad \text{for } j = 0, \dots, n-1.$$

Furthermore, the *complete graph* $\mathcal{K}_n$ of order n is a simple graph where each vertex is connected to each other vertex. Its spectrum is always given by $\{n-1, -1^{[n-1]}\}$. Conversely, it can be shown that a graph with spectrum $\{n-1, -1^{[n-1]}\}$ must be a complete graph. Therefore, the family $\{\mathcal{K}_n \mid n \in \mathbb{N}\}$ is uniquely determined by its spectrum.

The *complete bipartite graph* $\mathcal{K}_{n,m}$ consists of a vertex set which can be written as a disjoint union $V_n \cup V_m$ of sets of size n and m, respectively, such that every vertex in V_n is connected to every vertex in V_m (and the other way round), but vertices of the same set are never connected. The spectrum of $\mathcal{K}_{n,m}$ is given by

$$\operatorname{spec}(\mathcal{K}_{n,m}) = \{\pm\sqrt{mn}, 0^{[m+n-2]}\}.$$

Cayley graphs and circulant graphs. In fact, the families of complete and cycle graphs are subfamilies of so-called *circulant graphs* or *Cayley graphs*. Cayley graphs were first introduced by Cayley in 1878 in order to depict groups. Let G be a finite (additive) group and $S \subseteq G$. The *Cayley graph* $\operatorname{Cay}(G, S)$ is defined as the graph with vertex set G and edge set $\{(g, h) \mid g - h \in S\}$. Note that $\operatorname{Cay}(G, S)$ is an undirected graph if and only if the set S is symmetric, i.e. $S = -S$, and $\operatorname{Cay}(G, S)$ has loops if and only if $0 \in S$. We call S the *connection set* (also known as *difference set* or *symbol*) of $\operatorname{Cay}(G, S)$. For $S \subseteq \mathbb{Z}_n$, the graph $\operatorname{Cay}(\mathbb{Z}_n, S)$ is called a *circulant graph* (where $\mathbb{Z}_n$ is considered as the additive group of integers modulo n). Therefore, circulant graphs are exactly the Cayley graphs over cyclic groups. The name has its origin in

the fact that circulant graphs have (with a suitable enumeration of its vertices) circulant adjacency matrices. Note that circulant graphs are of great interest in physics since they model the behavior of quantum systems. We refer the reader to the surveys [17] and [94].

Besides that, a remarkable thing about Cayley graphs (from a mathematical point of view) is that we can study algebraic objects (groups) with tools from linear algebra (adjacency matrices).

Moreover, the spectra of Cayley graphs bear abundant structure (cf. [63, 12, 58]): If G is a finite additive group, $\chi_1, \chi_2, \ldots, \chi_h$ denote the irreducible characters of G and $n_1, n_2, \ldots, n_h$ their respective degrees, then the eigenvalues $\lambda_{i,j}$ for $1 \leq i \leq h, 1 \leq j \leq n_i$ of a Cayley graph $\mathrm{Cay}(G, S)$ satisfy

$$\lambda_{i,1}^t + \ldots + \lambda_{i,n_i}^t = \sum_{A \subseteq S, \#A = t} \chi_i\Big(\sum_{g \in A} g\Big)$$

for any positive integer t. In particular, if G is abelian, then $h = n$, $n_1 = n_2 = \ldots = n_h = 1$ and, hence, the eigenvalues of $\mathrm{Cay}(G, S)$ are precisely the values

$$\lambda_i = \sum_{s \in S} \chi_i(s), \quad \text{for } i = 1, 2, \ldots, n.$$

Therefore, in particular, the spectrum of a circulant graph $\mathrm{Cay}(\mathbb{Z}_n, S)$ is given by

$$\mathrm{spec}(\mathrm{Cay}(\mathbb{Z}_n, S)) = \Big\{ \sum_{s \in S} \zeta_n^{sk} \mid k = 0, \ldots, n-1 \Big\},$$

for $\zeta_n = \exp(2\pi i/n)$ (see also [105, Theorem 5.8]).

Paley graphs. Another subfamily of Cayley graphs are so-called *Paley graphs*. They were named after Paley since they are closely related to his construction of Hadamard matrices from quadratic residues (cf. [80]). Let q be a prime power with $q \equiv 1 \bmod 4$. Moreover, let $V := \mathbb{F}_q$ and let

$$E := \{\{x, y\} \mid x - y \in S\},$$

where

$$S := \{x^2 \mid x \in \mathbb{F}_q,\ x \neq 0\}$$

denotes the set of squares in the multiplicative group $\mathbb{F}_q^*$. Then the graph $\mathrm{Pal}(q) := (V, E)$ is called *Paley graph of order* q. Since $q \equiv 1 \bmod 4$, the element -1 is a square modulo q and, therefore, $x - y \in S$ if and only if $-(x - y)$, i.e. $y - x \in S$. Hence, Paley graphs are always simple graphs. The spectrum of a Paley graph $\mathrm{Pal}(q)$ is given by

$$\mathrm{spec}(\mathrm{Pal}(q)) = \left\{ \frac{q-1}{2}, \frac{\sqrt{q}-1}{2}^{[(q-1)/2]}, \frac{-\sqrt{q}-1}{2}^{[(q-1)/2]} \right\}.$$

Note that if q is a prime number, then $\mathrm{Pal}(q) = \mathrm{Cay}(\mathbb{Z}_q, S)$. Figure 1.3 shows the Paley graph Pal(9) writing $\mathbb{F}_9 = \{0, 1, 2, a, 2a, 1+a, 1+2a, 2+a, 2+2a\} \cong \mathbb{Z}_3[x]/(x^2+1)$ for a being a root of x^2+1. For a good survey on Paley graphs we refer to [49].

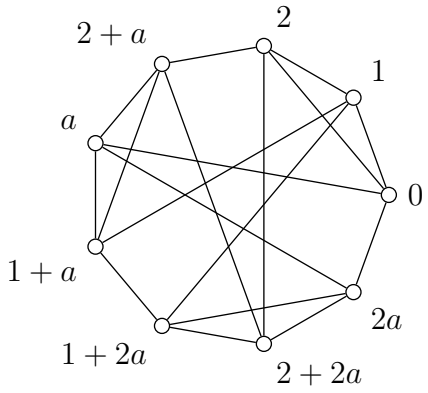


FIGURE 1.3. The Paley graph Pal(9).

Zero-divisor graphs. Another graph family, which was also inaugurated in order to study algebraic objects with tools from linear algebra, are *zero-divisor graphs*. They were first introduced by Anderson and Livingston [11] in 1999 and have received a lot of attention since then. Let R be a finite commutative ring with $1 \neq 0$ and let $Z(R)$ denote its set of zero-divisors. Then, the *zero-divisor graph* $\Gamma(R)$ is defined as the graph with vertex set $Z^*(R) = Z(R)\backslash\{0\}$ where two vertices x, y are adjacent if and only if $xy = 0$. The aim of considering these graphs is to study the interplay between graph theoretic properties of $\Gamma(R)$ and the ring properties of R. In order to simplify the representation of $\Gamma(R)$ it is often useful to consider the so-called *compressed zero-divisor graph* $\Gamma_E(R)$. This graph was first introduced by Mulay [71] and further studied in [93, 101, 10, 82]. For an element $r \in R$ let $[r]_R = \{s \in R \mid \mathrm{ann}_R(r) = \mathrm{ann}_R(s)\}$, where $\mathrm{ann}_R(r) = \{s \in R \mid rs = 0\}$ denotes the annihilator of r, and let $R_E = \{[r]_R \mid r \in R\}$. Then, $\Gamma_E(R)$ is defined as the graph with vertex set R_E where two vertices $[x]_R, [y]_R$ are adjacent if and only if $xy = 0$. Note that $[0]_R = \{0\}, [1]_R = R\backslash Z(R)$ and $[r]_R \subseteq Z(R)\backslash\{0\}$ for every $r \in R\backslash([0]_R \cup [1]_R)$.

By now, surprisingly little is known about the eigenvalues and adjacency matrices of zero-divisor graphs. First research in this direction was done by Sharma et. al. [91] in 2011. They investigated the adjacency matrices and eigenvalues of the graphs $\Gamma(\mathbb{Z}_p \times \mathbb{Z}_p)$ and $\Gamma(\mathbb{Z}_p[i] \times \mathbb{Z}_p[i])$. Further results were found by Young [104] in 2015 who studied the graphs $\Gamma(\mathbb{Z}_n)$ and determined precisely the eigenvalues of $\Gamma(\mathbb{Z}_p), \Gamma(\mathbb{Z}_{p^2}), \Gamma(\mathbb{Z}_{p^3})$ and $\Gamma(\mathbb{Z}_{p^2q})$ for p and q being prime numbers. Other recent papers on this topic are [95, 79].

The isomorphism problem for Cayley graphs

Let G be a finite (additive) group and $S \subseteq G$. We may write

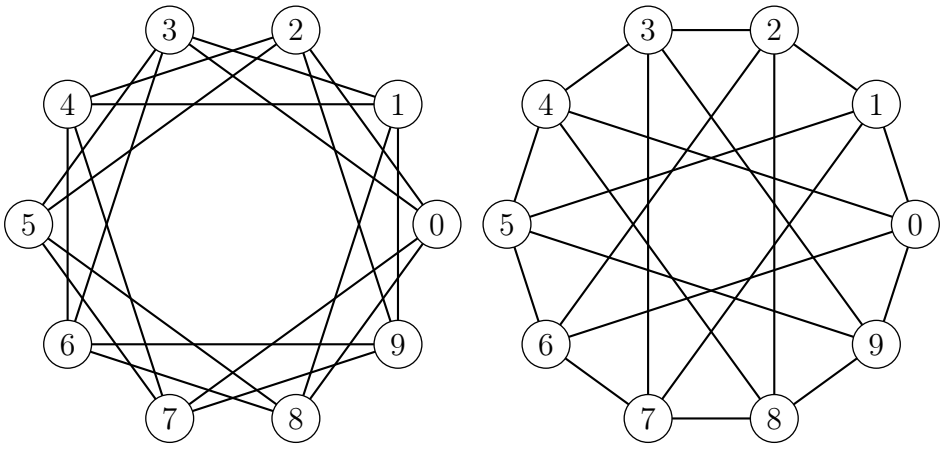
$$\mathrm{Cay}(G, S) = \{(x, y) \in G \times G \mid x - y \in S\}.$$

Therefore, two Cayley graphs $\mathrm{Cay}(G, S)$ and $\mathrm{Cay}(H, T)$ are isomorphic if there exists a bijection $f : G \longrightarrow H$ between the vertex set of $\mathrm{Cay}(G, S)$ and the vertex set of $\mathrm{Cay}(H, T)$ which preserves edges, i.e. $x - y \in S$ if and only if $f(x) - f(y) \in T$. This is equivalent to the condition that $\mathrm{Cay}(G, S)^f = \mathrm{Cay}(H, T)$, where $\mathrm{Cay}(G, S)^f$ is defined as

$$\mathrm{Cay}(G, S)^f := \{(f(x), f(y)) \in H \times H \mid x - y \in S\}.$$

We say that an isomorphism is *normalized* if $f(0_G) = 0_H$, where 0_G and 0_H denote the identity element of G and H, respectively. It is easy to see that if there exists an isomorphism between two Cayley graphs, then there also exists a normalized one. Moreover, if f is a normalized isomorphism between $\mathrm{Cay}(G, S)$ and $\mathrm{Cay}(H, T)$, we have that $f(S) = T$ for $f(S) := \{f(s) \mid s \in S\}$.

Example 1. The two Cayley graphs $\mathrm{Cay}(\mathbb{Z}_{10}, \{2, 3, 7, 8\})$ and $\mathrm{Cay}(\mathbb{Z}_{10}, \{1, 4, 6, 9\})$, shown in Figure 1.4, are isomorphic. For example, the bijection $f : \mathbb{Z}_{10} \longrightarrow \mathbb{Z}_{10}$ defined by the permutation $(2\ 3\ 5\ 4)(7\ 8\ 0\ 9)$ is an isomorphism between those graphs. The graph $\mathrm{Cay}(\mathbb{Z}_{10}, \{2, 3, 7, 8\})^f$ is illustrated in Figure 1.5. Note that f is not normalized since $f(0) = 9 \neq 0$. However, the permutation $(1\ 7\ 4\ 3)(2\ 9\ 8\ 6)$ provides a normalized isomorphism between $\mathrm{Cay}(\mathbb{Z}_{10}, \{2, 3, 7, 8\})$ and $\mathrm{Cay}(\mathbb{Z}_{10}, \{1, 4, 6, 9\})$.



$\mathrm{Cay}(\mathbb{Z}_{10}, \{2, 3, 7, 8\})$ $\mathrm{Cay}(\mathbb{Z}_{10}, \{1, 4, 6, 9\})$

Figure 1.4. Two isomorphic Cayley graphs.

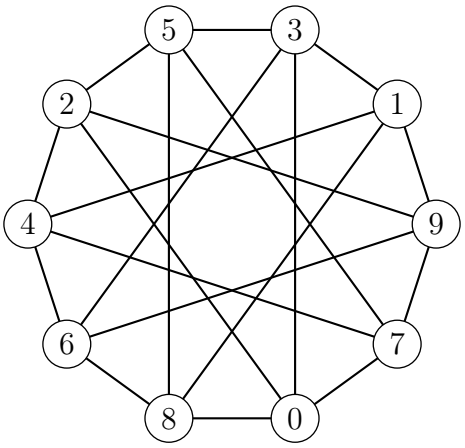


FIGURE 1.5. The graph $\mathrm{Cay}(\mathbb{Z}_{10}, \{2, 3, 7, 8\})^f$ for $f = (2\ 3\ 5\ 4)(7\ 8\ 0\ 9)$.

The *isomorphism problem for Cayley graphs* is stated as follows: Given two Cayley graphs $\mathrm{Cay}(G, S)$ and $\mathrm{Cay}(H, T)$, find an efficient algorithm which recognizes isomorphism between these graphs.

Studying isomorphic circulant graphs (and later Cayley graphs in general) goes back to Ádám [3] in 1967 who conjectured that two circulant graphs $\mathrm{Cay}(\mathbb{Z}_n, S)$, $\mathrm{Cay}(\mathbb{Z}_n, T)$ are isomorphic if and only if $S = mT := \{mt \mid t \in T\}$ for some multiplier $m \in \mathbb{Z}_n^*$. Only three years later, Elspas and Turner [29] gave a simple counterexample showing that the circulant graphs $\mathrm{Cay}(\mathbb{Z}_8, \{1, 2, 5\})$ and $\mathrm{Cay}(\mathbb{Z}_8, \{1, 5, 6\})$ are isomorphic but there is no such multiplier as Ádám expected. Since then, the problem has attracted the attention of many researchers [96, 8, 81, 74, 61, 64].

As already mentioned, the isomorphism problem for graphs in general is yet unsolved. But first Ádám's conjecture and only about ten years later an interesting relation between isomorphisms of Cayley graphs and so-called *Schur rings* gave hope that there might be an efficient (i.e. polynomial time) algorithm deciding whether two Cayley graphs $\mathrm{Cay}(G, S)$ and $\mathrm{Cay}(H, T)$ are isomorphic or not. This was first observed by Klin and Pöschel [56] in 1978. Since then, the structure of Schur rings was studied intensively in order to solve the isomorphism problem for Cayley graphs. Schur rings over a group G are defined as special subalgebras of a group algebra $\mathbb{Q}G$ and can be identified with a partition of G. Two Schur rings $\mathcal{A}$ and $\mathcal{B}$ are called *isomorphic* if there is an isomorphism between the algebras $\mathcal{A}$ and $\mathcal{B}$. The group of automorphisms of a Schur ring $\mathcal{A}$ is denoted by $\mathrm{Aut}(\mathcal{A})$. Now, the key connection between Cayley graphs and Schur rings is that every normalized Cayley graph isomorphism induces a Schur ring isomorphism (cf. [77, 76]). In particular:

THEOREM 2 ([53, Theorem 3.2]). *Let G be a finite group and $S \subseteq G$. Then,*

$$\mathrm{Aut}(\mathrm{Cay}(G, S)) = \mathrm{Aut}(\langle\langle S\rangle\rangle),$$

where $\langle\langle S\rangle\rangle$ denotes the smallest Schur ring which contains the element $\sum_{s\in S} s \in \mathbb{Q}G$.

Therefore, it seems to be a promising approach to study Schur ring isomorphisms and automorphisms in order to solve the isomorphism problem for Cayley graphs.

In fact, in 2004, after an immense study of Schur rings over cyclic groups [55, 54, 73, 77, 76], Muzychuk [75] and, independently, Evdokimov and Ponomarenko [32] finally solved the isomorphism problem for circulant graphs.

Cospectral and isospectral graphs

We have already mentioned that two non-isomorphic graphs which have the same spectrum are called *cospectral*. More generally, two graphs are said to be *isospectral* if they have the same spectrum (not paying attention to whether they are isomorphic or not). Note that in some literature the words *cospectral* and *isospectral* are used identically or exactly the other way round.

In 1966 Kac [50] posted the question "Can one hear the shape of a drum?" as a paradigm example for a class of problems which is of fundamental importance in several physical applications. Shortly afterwards, Fisher [33] formulated the discrete analogue addressing whether one can hear the shape of a graph. That means, given the spectrum of a graph $\mathcal{G}$, is $\mathcal{G}$ uniquely determined? Of course, this is not true, as we have already seen in an example above. At least, it is true for some families of graphs like the complete graphs. It is still a present quest to characterize graph families which are determined by their spectra.

Another motivation for constructing isospectral or cospectral graphs comes from chemistry. Therein, the aim is to find different molecules with identical energy levels. The idea to connect this problem with spectral graph theory goes back to Herndon [44, 45].

By now, many constructions of isospectral graphs are known. We refer to [27, 90] to give some examples, but there is much more literature on that topic.

Integral graphs

Motivating it as a *natural question*, in 1974 Harary and Schwenk [42] asked: *Which graphs have integral spectra?* A graph is called *integral* if all its eigenvalues are integers. In [42] Harary and Schwenk constructed several families of integral graphs using graph products, but they already remarked that this problem appears intractable. Indeed, so far there is no satisfying answer to that question. It is not even clear

whether in general there is any connection between the structure of a graph and its property of having integral eigenvalues.

Integral circulant graphs. However, the search for such a connection does not seem completely desperate: In 2005, So [92] found a complete characterization of integral circulant graphs. For a proper divisor d of n let

$$G_n(d) := \{x \in \mathbb{Z}_n \mid \gcd(x, n) = d\}.$$

Then, So's characterization is as follows:

THEOREM 3 ([92, Theorem 7.1]). *A circulant graph* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *is integral if and only if* S *is a union of some* $G_n(d)$*-sets.*

One direction of this theorem was independently proven by Klotz and Sander [57] whilst their study of *unitary* Cayley graphs. Those are Cayley graphs of the form $\mathrm{Cay}(\mathbb{Z}_n, \mathbb{Z}_n^*) = \mathrm{Cay}(\mathbb{Z}_n, G_n(1))$.

In fact, the study of integral circulant graphs has a much older origin. In 1979 Bridges and Mena [21] studied the algebra of rational circulant matrices and already found a similar characterization of integral (they called it *rational*) circulant graphs although their motivation was rather different. Later on, they figured out a link to the theory of Schur rings (cf. [22]). It turned out that a circulant graph is rational if and only if it corresponds to a so-called *rational* Schur ring. Rational Schur rings were introduced by Schur himself (as Schur rings *of traces*) but already in 1964 Wielandt [102] denoted them as *rational* Schur rings. In 1993, Muzychuk [72] gave a classification thereof. For recent results and a good overview about rational circulant graphs and Schur rings we refer to [53].

Recently, integral circulant graphs gained new attention since they turned out to model the behavior of *periodic* quantum systems (cf. [89]).

In view of his result and several computer experiments, So [92] conjectured the following:

CONJECTURE 4 (So's conjecture). *Let* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *and* $\mathrm{Cay}(\mathbb{Z}_n, T)$ *be integral circulant graphs. If* $S \neq T$*, then* $\mathrm{spec}(\mathrm{Cay}(\mathbb{Z}_n, S)) \neq \mathrm{spec}(\mathrm{Cay}(\mathbb{Z}_n, T))$*, hence* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *and* $\mathrm{Cay}(\mathbb{Z}_n, T)$ *are non-isomorphic.*

In fact, the second part of this conjecture (the *isomorphism part*) was proven in 2012 with Muzychuk's solution of the isomorphism problem for circulant graphs and the tools he used for this. The proof can be found in [53] and implies that there are exactly $2^{\tau(n)-1}$ integral loop-free circulant graphs on n vertices, where $\tau(n)$ denotes the number of proper divisors of n.

The stronger claim (the *spectral part*) of So's conjecture is still an open problem. So himself verified in his paper [92] the cases where n is

a prime power or a product of two distinct primes. The conjecture has also been confirmed in [47] for n being square-free on condition that the connection sets S and T are of the form $G_n(p) \cup G_n(q)$ for distinct prime divisors p, q of n. In a private conversation So said that his conjecture has been checked for all pairs of integral circulant graphs up to 1000 vertices (with the help of a computer) and no counter example has been found. A few approaches to solve this problem were evolved by Sander and Sander [87, 86].

Integral Cayley graphs. More generally, the task of classifying all integral Cayley graphs seems to be much harder. There is no complete answer yet.

A natural approach is to generalize the $G_n(d)$-sets as they generate a Booelan algebra with respect to intersection, union and complement of sets. Indeed, it turned out that a Cayley graph $\mathrm{Cay}(G, S)$ over an abelian group G is integral if and only if $S \subseteq G$ belongs to the Boolean algebra generated by the subgroups of G (cf. [58, 59, 7]). In particular, in [7] they also studied integral Cayley graphs over some non-abelian groups as well as the respective Boolean algebras.

As introduced by Klotz and Sander [58] in 2010, a finite group G is called *Cayley integral* if every simple Cayley graph over G is integral. Only a few years later, Ahmady et. al. [5] characterized all Cayley integral groups by the following:

THEOREM 5 ([5, Theorem 4.2]). *The only Cayley integral groups are*

$$\mathbb{Z}_2^n \times \mathbb{Z}_3^m,\ \mathbb{Z}_2^n \times \mathbb{Z}_4^m,\ Q_8 \times \mathbb{Z}_2^n,\ S_3 \text{ and } \mathrm{Dic}_{12},$$

where m, n are arbitrary non-negative integers, Q_8 is the quaternion group of order 8, and Dic_{12} is the dicyclic group of order 12.

As a converse concept, a group is called *Cayley integral simple group* (*CIS group* for short) if it admits only trivial (i.e. complete multipartite) simple integral Cayley graphs. This notion was introduced by Abdollahi and Jazaeri [1] in 2013. A classification of all CIS groups is also given in [5]:

THEOREM 6 ([5, Theorem 3.2]). *Let G be a CIS group. Then G is abelian and isomorphic to either a cyclic group of order p or p^2 for some prime p, or is isomorphic to $\mathbb{Z}_2^2$.*

This, in particular, shows that every finite non-abelian group admits a non-trivial Cayley graph whose eigenvalues are all integral.

We also want to mention that So's conjecture is definitely not true for integral Cayley graphs in general. To see that, consider the symmetric group S_3. As proven in [2] and [5], every simple Cayley graph over S_3 is integral. Moreover, in [4] it is shown that for every $n > 2$

the graphs $\mathrm{Cay}(S_n, \{(i\ j)\})$ for $i, j \in \{1, 2, \ldots, n\}$, $i \neq j$ are all isomorphic. Therefore, the graphs $\mathrm{Cay}(S_3, \{(1\ 2)\})$, $\mathrm{Cay}(S_3, \{(1\ 3)\})$ and $\mathrm{Cay}(S_3, \{(2\ 3)\})$ are isomorphic integral Cayley graphs. Hence, in general, integral Cayley graphs are not uniquely determined by their connection sets or spectra. At least it seems promising that (the isomorphism part of) So's conjecture is true for integral Cayley graphs over abelian groups.

The algebraic degree of a graph

Since eigenvalues of graphs are algebraic integers, from a number-theoretical point of view, it seems more natural to ask the more general question (than the one of Harary and Schwenk [42]): *Which graphs have the same algebraic degree?* This question was raised by Steuding, Stumpf and the author [70]. Given a graph $\mathcal{G}$, the *algebraic degree* $\deg(\mathcal{G})$ is defined as the dimension of the splitting field of the characteristic polynomial of the adjacency matrix $A(\mathcal{G})$ over the rationals. By definition, this splitting field is the smallest field which contains all eigenvalues of the spectrum of the graph. It seems to be an interesting question whether there is a connection between the structural properties of a graph and its algebraic degree.

It is well-known that every totally real algebraic integer is an eigenvalue of some simple graph (cf. [30, 15, 85]).

Aim and structure of this thesis

The aim of this thesis is to find new relations between the spectrum of a graph and its structural properties. We mainly focus on algebraic characteristics of the eigenvalues, and, in particular, investigate the question whether the algebraic degree of a graph provides information about the graph structure.

In CHAPTER 2, we start with a short survey on graph products since the spectra of products of graphs often can easily be derived from the eigenvalues of the respective factor graphs. We will use some of those results and ideas in the further course of this thesis.

Moreover, we summarize our results regarding the algebraic degree of arbitrary simple graph. We present a lower bound for the algebraic degree of a graph in terms of its diameter and maximum vertex degree. In particular, we introduce a family of graphs where every member seems to be of maximum algebraic degree. Graphs of maximum algebraic degree are of particular interest since they can be considered a counterpart of integral graphs.

Of course, it is difficult to find such relations which apply to any graph. Therefore, in CHAPTER 3, we restrict our considerations to Cayley and circulant graphs. Our aim is to understand the eigenvalues

of Cayley graphs in terms of the structural properties of their connection sets.

In Section 3.1 of CHAPTER 3 we start with an investigation of connection sets S, T which provide isospectral circulant graphs $\mathrm{Cay}(\mathbb{Z}_n, S)$, $\mathrm{Cay}(\mathbb{Z}_n, T)$. We characterize such pairs by generalizing known counterexamples to Ádám's conjecture. Our constructions yield infinitely many new examples of this kind. Subsequently, we compare all pairs of isospectral circulant graphs up to 21 vertices with the number of pairs which arise from one of our constructions, and conjecture that this construction provides all pairs of isospectral circulant graphs on $n = pq$ vertices, where p and q are distinct primes. Our observations finally lead us to a new approach where we construct pairs of isospectral circulant graphs by considering the difference set

$$\mathrm{D}(S) := \{s_1 - s_2 \mid s_1, s_2 \in S\}$$

of a connection set $S \subseteq \mathbb{Z}_n$.

In Section 3.2 of CHAPTER 3 we give a survey on the most important basic results connecting Cayley graphs and Schur ring theory. We give detailed proofs of those results as well as several examples to make the topic more accessible. Those concepts and results will be of great importance in the remaining sections of this chapter.

In Section 3.3 of CHAPTER 3, we present three proofs of the isomorphism part of So's conjecture. The first two proofs rely on the theory of Schur rings, whereas the third proof uses a much simpler, combinatorial result of Vilfred [98]. However, we are questioning the accuracy of Vilfred's elementary proof. Furthermore, we verify a new case of the spectral part of So's conjecture proving that the conjecture is true for $n = p^2q$ where p and q are distinct odd primes.

We already know from So's [92] characterization that integral circulant graphs are related to connection sets $S \subseteq \mathbb{Z}_n$ with plenty of structure. Moreover, Klotz and Sander [59] gave a complete characterization of (simple) integral Cayley graphs over abelian groups. They proved that a simple Cayley graph $\mathrm{Cay}(G, S)$ (for G being an abelian group) is integral if and only if the set S bears special algebraic structure. Thus, motivated by the question of how deviation from structure of a connection set S is encoded in the algebraic degree of $\mathrm{Cay}(\mathbb{Z}_n, S)$, in the last section of CHAPTER 3, Section 3.4, we determine precisely the algebraic degree of circulant graphs, again using Schur ring theory.

Let H be a subgroup of $\mathrm{Aut}(\mathbb{Z}_n)$. For an element $x \in \mathbb{Z}_n$, let

$$x^H := \{\sigma(x) \mid \sigma \in H\}$$

be the *orbit* of x under H, and for $S \subseteq \mathbb{Z}_n$ let

$$S^H := \bigcup_{s \in S} s^H.$$

Furthermore, for $\zeta_n = \exp(2\pi i/n)$ let $\mathbb{Q}(\zeta_n)^H$ be the fixed field of H, i.e. the unique maximum subfield of $\mathbb{Q}(\zeta_n)$ where each element is fixed by every automorphism in H. Our main result in this section is the following:

THEOREM (Main theorem). *The splitting field of* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *is given by* $\mathbb{Q}(\zeta_n)^H$*, where* H *is the maximum subgroup of* $\mathrm{Aut}(\mathbb{Z}_n)$ *such that* $S^H = S$*.*

In layman's terms, this implies that the less structure a connection set of a circulant graph has, the larger its algebraic degree is.

Moreover, we solve the inverse Galois problem for circulant graphs showing that every finite abelian extension of the rationals is the splitting field of some circulant graph. Since isospectral graphs must have the same splitting field, our results also provide some new necessary criteria for isospectrality of circulant graphs. Finally, we give a graph-theoretical interpretation of the algebraic degree of circulant graphs: we prove that the algebraic degree of a circulant graph is determined by the automorphism group of the graph. This answers the question of Harary and Schwenk [42] and our generalized question (cf. [70]) at least for circulant graphs.

Besides that, we also follow up a combinatorial approach (where no Schur ring theory is needed) to determine the algebraic degree of circulant graphs on a prime number of vertices.

In the last chapter of this thesis, CHAPTER 4, we study the spectra of zero-divisor graphs. Our aim is to find relations between the eigenvalues of $\Gamma(R)$ and the (algebraic) properties of the respective ring R.

We introduce a graph product $\times_\Gamma$ with the property that

$$\Gamma(R) \cong \Gamma(R_1) \times_\Gamma \ldots \times_\Gamma \Gamma(R_r)$$

whenever $R \cong R_1 \times \ldots \times R_r$. With this product, we find relations between the number of vertices of the zero-divisor graph $\Gamma(R)$, the compressed zero-divisor graph, the structure of the ring R and the eigenvalues of $\Gamma(R)$. In particular, we determine the nullity of zero-divisor graphs and present a technique to compute the eigenvalues of zero-divisor graphs of direct products of rings of integers modulo n. From this we derive the spectra of $\Gamma(\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p)$ and $\Gamma(\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p)$ in terms of a prime number p. We also provide the characteristic polynomials of $\Gamma(\mathbb{Z}_{p^2} \times \mathbb{Z}_p)$ and $\Gamma(\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_q)$ for primes $q \neq p$. This generalizes the results of Sharma et. al. [91] and Young [104].

Note that CHAPTER 2 basically provides an overview of interesting results with respect to our research question and introduces some ideas which we will use in the further course of this thesis. Our main results are presented in CHAPTER 3 and CHAPTER 4.

CHAPTER 2

Properties of Graph Spectra

2.1. Graph products

The main idea of introducing graph products is the aim to decompose graphs into smaller graphs in order to make the study of big graphs easier. For example, it was shown by Sabidussi [84] that for every connected graph there is a unique prime factorization with respect to the Cartesian product. Besides that, the spectrum of the product of two graphs is often closely related to the spectra of the respective factor graphs. Therefore, graph products are a helpful tool in spectral graph theory. In this section, we introduce the most common graph products and give a short survey on their spectral properties and applications thereof.

2.1.1. Associative products defined on the Cartesian product of the vertex sets. The most natural way to define a graph product $*$ of two simple graphs $\mathcal{G}$ and $\mathcal{H}$ is to define it on the Cartesian product $\times$ of the sets of vertices $V(\mathcal{G})$, $V(\mathcal{H})$, i.e.

$$V(\mathcal{G} * \mathcal{H}) = V(\mathcal{G}) \times V(\mathcal{H}) = \{(v, w) \mid v \in V(\mathcal{G}), w \in V(\mathcal{H})\}.$$

In order to decide whether two vertices (v_1, w_1) and (v_2, w_2) are adjacent in $\mathcal{G}*\mathcal{H}$ it only matters whether the pairs v_1, v_2 and w_1, w_2 are pairs of adjacent, identical or non-adjacent vertices in the respective factors. In 1975, Imrich and Izbicki [48] showed that there are exactly 20 such products, where only ten of them actually depend on the structure of both factors. For each of those products, there is exactly one product which is the *complementary product* of the respective product. That is, for a graph product $*$, the product $\overline{\mathcal{G}} * \overline{\mathcal{H}}$, where $\overline{\mathcal{G}}$ denotes the complement graph of $\mathcal{G}$, i.e. the graph with adjacency matrix $J - I - A(\mathcal{G})$ for J being the all-1 matrix. Therefore, there are essentially only five associative products of simple graphs to be considered, namely the *direct product*, also known as *categorical product*, *Kronecker product*, *cardinal product* or *conjunction*, the *Cartesian product* (or *sum*), the *strong product*, the *equivalence product* and the *lexicographic product*. The last one, the lexicographic product, is the only self-complementary and non-commutative associative graph product.

In the following let $\mathcal{G}$ and $\mathcal{H}$ be two simple graphs. The respective definitions of the latter listed graph products are given as follows:

DEFINITION 2.1.1 (Direct product). Two vertices (v_1, w_1), $(v_2, w_2) \in V(\mathcal{G}) \times V(\mathcal{H})$ are adjacent in the *direct product* $\mathcal{G} \times \mathcal{H}$ of $\mathcal{G}$ and $\mathcal{H}$ if and only if $(v_1, v_2) \in E(\mathcal{G})$ and $(w_1, w_2) \in E(\mathcal{H})$.

DEFINITION 2.1.2 (Cartesian product). Two vertices (v_1, w_1), $(v_2, w_2) \in V(\mathcal{G}) \times V(\mathcal{H})$ are adjacent in the *Cartesian product* $\mathcal{G} \,\square\, \mathcal{H}$ of $\mathcal{G}$ and $\mathcal{H}$ if and only if either $\big(v_1 = v_2$ and $(w_1, w_2) \in E(\mathcal{H})\big)$ or $\big((v_1, v_2) \in E(\mathcal{G})$ and $w_1 = w_2\big)$.

DEFINITION 2.1.3 (Strong product). Two vertices (v_1, w_1), $(v_2, w_2) \in V(\mathcal{G}) \times V(\mathcal{H})$ are adjacent in the *strong product* $\mathcal{G} \boxtimes \mathcal{H}$ of $\mathcal{G}$ and $\mathcal{H}$ if and only if either $\big((v_1, v_2) \in E(\mathcal{G})$ and $(w_1, w_2) \in E(\mathcal{H})\big)$ or $\big(v_1 = v_2$ and $(w_1, w_2) \in E(\mathcal{H})\big)$ or $\big((v_1, v_2) \in E(\mathcal{G})$ and $w_1 = w_2\big)$.

DEFINITION 2.1.4 (Equivalence product). Two vertices (v_1, w_1), $(v_2, w_2) \in V(\mathcal{G}) \times V(\mathcal{H})$ are adjacent in the *equivalence product* $\mathcal{G} \,\tilde{\boxtimes}\, \mathcal{H}$ of $\mathcal{G}$ and $\mathcal{H}$ if and only if either $\big((v_1, v_2) \in E(\mathcal{G})$ and $(w_1, w_2) \in E(\mathcal{H})\big)$ or $\big((v_1, v_2) \notin E(\mathcal{G})$ and $(w_1, w_2) \notin E(\mathcal{H})\big)$ or $\big(v_1 = v_2$ and $(w_1, w_2) \in E(\mathcal{H})\big)$ or $\big((v_1, v_2) \in E(\mathcal{G})$ and $w_1 = w_2\big)$.

DEFINITION 2.1.5 (Lexicographic product). Two vertices (v_1, w_1), $(v_2, w_2) \in V(\mathcal{G}) \times V(\mathcal{H})$ are adjacent in the *lexicographic product* $\mathcal{G}[\mathcal{H}]$ of $\mathcal{G}$ and $\mathcal{H}$ if and only if either $\big((v_1, v_2) \in E(\mathcal{G})\big)$ or $\big(v_1 = v_2$ and $(w_1, w_2) \in E(\mathcal{H})\big)$.

Later, such products were called B-products (cf. [23]) since the following definition describes all those associative graph products:

DEFINITION 2.1.6 (B-product). For a graph $\mathcal{G}$ let $\mathcal{G}_1, \mathcal{G}_2, \mathcal{G}_3 \subseteq V(\mathcal{G}) \times V(\mathcal{G})$ with $\mathcal{G}_1 = E(\mathcal{G})$, $\mathcal{G}_2 = \{(v, v) \mid v \in V(\mathcal{G})\}$ and $\mathcal{G}_3$ being the set of non-adjacent pairs of vertices. Moreover, let

$$A := \{1, 2, 3\}^2 - \{(2, 2)\}.$$

Now, if $B \subseteq A$, then the B-product of two graphs $\mathcal{G}$ and $\mathcal{H}$, denoted by $\mathcal{G} \oplus_B \mathcal{H}$, is the graph $(V(\mathcal{G}) \times V(\mathcal{H}), T)$, where

$$\begin{aligned} T &:= \bigcup_{(i,j)\in B} \mathcal{G}_i\mathcal{H}_j \\ &:= \bigcup_{(i,j)\in B} \big\{\{(v_1, w_1), (v_2, w_2)\} \mid (v_1, v_2) \in \mathcal{G}_i, (w_1, w_2) \in \mathcal{H}_j\big\}. \end{aligned}$$

In view of this definition, we have that

$$\begin{aligned} \mathcal{G} \times \mathcal{H} &= \mathcal{G} \oplus_{\{(1,1)\}} \mathcal{H}, \\ \mathcal{G} \,\square\, \mathcal{H} &= \mathcal{G} \oplus_{\{(1,2),(2,1)\}} \mathcal{H}, \\ \mathcal{G} \boxtimes \mathcal{H} &= \mathcal{G} \oplus_{\{(1,1),(1,2),(2,1)\}} \mathcal{H}, \\ \mathcal{G} \,\tilde{\boxtimes}\, \mathcal{H} &= \mathcal{G} \oplus_{\{(1,1),(1,2),(2,1),(3,3)\}} \mathcal{H}, \\ \mathcal{G}[\mathcal{H}] &= \mathcal{G} \oplus_{\{(1,1),(1,2),(1,3),(2,1)\}} \mathcal{H}. \end{aligned}$$

Note that the equivalence product is the only one of these products which does not have the property that at least one of the projections of the product onto its factors is a so-called *weak homomorphism* (edges are mapped to edges or to vertices). The other four graph products are known as the *standard graph products* and have been studied by many researchers.

2.1.2. Other graph products. Of course, there is no reason to restrict the investigation of graph products to associative products defined on the Cartesian product of the respective sets of vertices.

The simplest of all graph products is the *union* of graphs. That is, for graphs $\mathcal{G}$ and $\mathcal{H}$ the graph

$$\mathcal{G} \cup \mathcal{H} := (V(\mathcal{G}) \cup V(\mathcal{H}), E(\mathcal{G}) \cup E(\mathcal{H})).$$

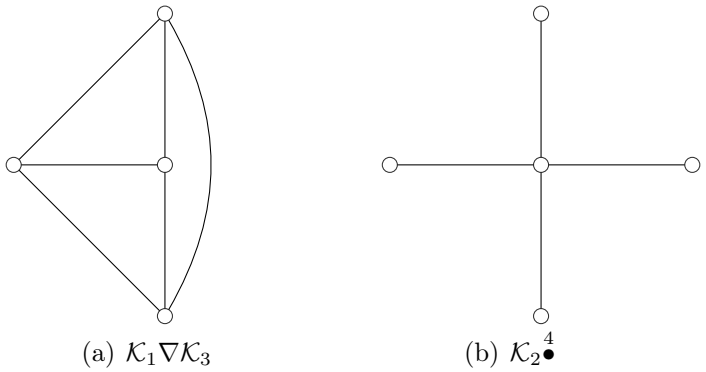
In particular, we write $a\mathcal{G}$ for the disjoint union of a copies of $\mathcal{G}$.

Moreover, we want to introduce the following two graph products:

DEFINITION 2.1.7 (Complete product). The *complete product* $\mathcal{G}\nabla\mathcal{H}$ has vertex set $V(\mathcal{G}) \cup V(\mathcal{H})$, and two vertices v, w are adjacent in $\mathcal{G}\nabla\mathcal{H}$ if and only if either $\big(v \in V(\mathcal{G})$ and $w \in V(\mathcal{H})\big)$ or $\big((v, w) \in E(\mathcal{G})$ or $(v, w) \in E(\mathcal{H})\big)$.

DEFINITION 2.1.8 (Point identification). Let $v \in V(\mathcal{G})$ and $w \in V(\mathcal{H})$. Then, the *point identification* (or *coalescence*) $\mathcal{G} \bullet \mathcal{H}$ is the graph obtained from $\mathcal{G}$ and $\mathcal{H}$ by identifying the vertices v and w.

In particular, the graph arising from applying point identification a times to the same graph $\mathcal{G}$ and the same vertex of $\mathcal{G}$ is denoted by $\mathcal{G}\overset{a}{\bullet}$. The latter products are illustrated in Figure 2.1.



(a) $\mathcal{K}_1\nabla\mathcal{K}_3$ (b) $\mathcal{K}_2\overset{4}{\bullet}$

FIGURE 2.1. Complete product and point identification.

2.1.3. Spectra and characteristic polynomials of graph products. For many graph products $*$, the spectrum of $\mathcal{G}*\mathcal{H}$ can easily be obtained from the spectra of $\mathcal{G}$ and $\mathcal{H}$. Let $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$ and $\mu_1 \geq \mu_2 \geq \ldots \geq \mu_m$ denote the eigenvalues of $\mathcal{G}$ and $\mathcal{H}$, respectively.

Table 2.1 describes the spectrum of $\mathcal{G} * \mathcal{H}$ in terms of the eigenvalues λ_i, μ_j for $*$ running through the previously introduced graph products. All results can be found in [14].

TABLE 2.1. Eigenvalues of graph products.

Graph	Eigenvalues
$\mathcal{G} \times \mathcal{H}$	$\lambda_i \mu_j$
$\mathcal{G} \square \mathcal{H}$	$\lambda_i + \mu_j$
$\mathcal{G} \boxtimes \mathcal{H}$	$\lambda_i \mu_j + \lambda_i + \mu_j$
$\mathcal{G} \cup \mathcal{H}$	λ_i, μ_j

In particular, if $\mathcal{H}$ is k-regular, then the eigenvalues of $\mathcal{G}[\mathcal{H}]$ are given by the values $\lambda_i m + k$ and μ_j.

Moreover, note that if $\mathcal{G}$ is k-regular, then the eigenvalues of $\overline{\mathcal{G}}$ are given by $-\lambda_i - 1$ and $n - k - 1$.

In some cases, we can also derive a formula for the characteristic polynomial. For example, in [27, Theorem 2.6] it is proven that the characteristic polynomial $\chi_{\overline{\mathcal{G}}}$ (for $\mathcal{G}$ being k-regular) is given by

$$\chi_{\overline{\mathcal{G}}}(x) = (-1)^n \frac{x - n + k + 1}{x + k + 1} \chi_{\mathcal{G}}(-x - 1),$$

where $\chi_{\mathcal{G}}$ denotes the characteristic polynomial of $\mathcal{G}$.

In the following let $\mathcal{G}$ and $\mathcal{H}$ be simple graphs on n and m vertices, respectively. If $v \in V(\mathcal{G})$, then $\mathcal{G} - v$ denotes the graph obtained by removing the vertex v as well as all edges connected to v.

LEMMA 2.1.9 ([27, p. 159]). *Let $v \in V(\mathcal{G})$ and $w \in V(\mathcal{H})$. Then the point-identification $v = w$ yields*

$$\chi_{\mathcal{G} \bullet \mathcal{H}}(x) = \chi_{\mathcal{G}}(x) \chi_{\mathcal{H}-w}(x) + \chi_{\mathcal{G}-v}(x) \chi_{\mathcal{H}}(x) - x \chi_{\mathcal{G}-v}(x) \chi_{\mathcal{H}-w}(x).$$

LEMMA 2.1.10 ([27, Theorem 2.7]). *The characteristic polynomial of the complete product of $\mathcal{G}$ and $\mathcal{H}$ equals*

$$\begin{aligned}\chi_{\mathcal{G} \nabla \mathcal{H}}(x) = (-1)^m \chi_{\mathcal{G}}(x) \chi_{\overline{\mathcal{H}}}(-x - 1) + (-1)^n \chi_{\mathcal{H}}(x) \chi_{\overline{\mathcal{G}}}(-x - 1) - \\ - (-1)^{n+m} \chi_{\overline{\mathcal{G}}}(-x - 1) \chi_{\overline{\mathcal{H}}}(-x - 1).\end{aligned}$$

In particular, if $\mathcal{G}$ is k-regular and $\mathcal{H}$ is r-regular, then $\chi_{\mathcal{G} \nabla \mathcal{H}}$ is given by

$$\chi_{\mathcal{G} \nabla \mathcal{H}}(x) = \frac{\chi_{\mathcal{G}}(x) \chi_{\mathcal{H}}(x)}{(x - k)(x - r)} \big((x - k)(x - r) - nm \big).$$

2.1.4. Applications of graph products. We want to mention some examples where graph products are a powerful tool.

2.1.4.1. *Products and factorization of circulant graphs.* Once a graph is identified as a circulant graph, its properties can be derived easily. In 2004 Evdokimov and Ponomarenko [32] proved that circulant graphs can be recognized efficiently, i.e. they found a polynomial time algorithm which decides whether a given graph is circulant or not. However, an older and more constructive approach to identify circulant graphs is to study products and factorization thereof. We summarize some notable results.

Let $\mathcal{G}$ and $\mathcal{H}$ be simple circulant graphs on n and m vertices, respectively. In [23] Broere and Hattingh showed that whenever $\gcd(n, m) = 1$, then every B-product of $\mathcal{G}$ and $\mathcal{H}$ is again a circulant graph.

In 1982, Alspach and Parsons [9] introduced the family of so-called *metacirculant graphs* as a generalization of circulant or rather vertex-transitive graphs. A graph $\mathcal{G}$ is called *vertex-transitive* if for any two vertices v, w there is an automorphism of $\mathcal{G}$ which maps v onto w. Note that every circulant graph is vertex-transitive. The definition of a metacirculant graph is a bit technical: Let m, n be two fixed integers, $\alpha \in \mathbb{Z}_n^*$, and $S_0, S_1, \ldots, S_{\lfloor m/2 \rfloor}$ be subsets of $\mathbb{Z}_n$ with the following four properties:

(1) $S_0 = -S_0$,
(2) $0 \notin S_0$,
(3) $\alpha^m S_k = S_k$ for $0 \leq k \leq \lfloor m/2 \rfloor$,
(4) If m is even, then $\alpha^{m/2} S_{m/2} = -S_{m/2}$.

Then, the *metacirculant graph* $G(m, n, \alpha, S_0, \ldots, S_{\lfloor m/2 \rfloor})$ is the graph with vertex set $\mathbb{Z}_m \times \mathbb{Z}_n$, which can be partitioned into m disjoint sets $V_0, V_1, \ldots, V_{m-1}$ for $V_i := \{(i, j) \mid 0 \leq j \leq n-1\}$, where two vertices (i, j) and $(i + k, h)$ (for $0 \leq k \leq \lfloor m/2 \rfloor$) are adjacent if and only if $h - j \in \alpha^i S_k$.

The sets $V_0, V_1, \ldots, V_{m-1}$ are called the *layers* of the metacirculant graph. Every metacirculant graph with m layers and n vertices per layer is referred to as an (m, n)-*metacirculant graph*.

Besides that, metacirculant graphs can be described in terms of their automorphism group:

THEOREM 2.1.11 ([9, Theorem 1]). *Let $\mathcal{G}$ be a graph with $V(\mathcal{G}) = \mathbb{Z}_m \times \mathbb{Z}_n$. Then, $\mathcal{G}$ is a (m, n)-metacirculant graph if and only if the vertices of $\mathcal{G}$ can be labeled in such a way that $\mathrm{Aut}(\mathcal{G})$ contains two permutations ρ and τ where ρ is a rotation on each V_i given by $(i, j)^\rho = (i, j+1)$, and τ is a twisted rotation that maps V_i onto V_{i+1} and is given by $(i, j)^\tau = (i + 1, \alpha j)$ for a fixed $\alpha \in \mathbb{Z}_n^*$.*

EXAMPLE 2.1.12 (cf. [9, Example 1]). The metacirculant graph $G(2, 5, 2, \{1, 4\}, \{0\})$ is the Petersen graph (cf. Figure 2.2).

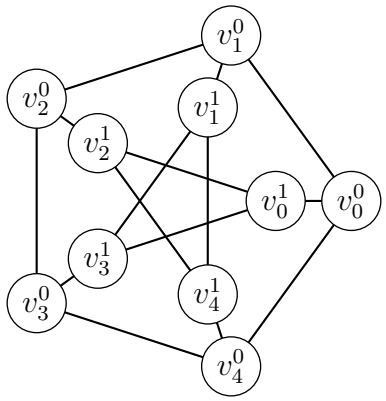


FIGURE 2.2. The Petersen graph $G(2, 5, 2, \{1, 4\}, \{0\})$.

In 2002, Sanders [88] showed that every B-product of two circulant graphs is a metacirculant graph with parameters that can easily be described in terms of the product graphs. In particular, for the standard products, he proved the following:

THEOREM 2.1.13 ([88, Corollary 5.1]). *Let* $\mathcal{G} = \mathrm{Cay}(\mathbb{Z}_m, S)$ *and* $\mathcal{H} = \mathrm{Cay}(\mathbb{Z}_n, T)$ *be simple circulant graphs. Then*

$$\mathcal{G} \times \mathcal{H} = G(m, n, 1, \emptyset, S_1, \ldots, S_{\lfloor m/2 \rfloor}) \quad \textit{for} \quad S_k = \begin{cases} \emptyset & \textit{if } k \notin S \\ T & \textit{if } k \in S, \end{cases}$$

$$\mathcal{G} \,\square\, \mathcal{H} = G(m, n, 1, T, S_1, \ldots, S_{\lfloor m/2 \rfloor}) \quad \textit{for} \quad S_k = \begin{cases} \emptyset & \textit{if } k \notin S \\ \{0\} & \textit{if } k \in S, \end{cases}$$

$$\mathcal{G} \boxtimes \mathcal{H} = G(m, n, 1, T, S_1, \ldots, S_{\lfloor m/2 \rfloor}) \quad \textit{for} \quad S_k = \begin{cases} \emptyset & \textit{if } k \notin S \\ T \cup \{0\} & \textit{if } k \in S, \end{cases}$$

$$\mathcal{G}[\mathcal{H}] = G(m, n, 1, T, S_1, \ldots, S_{\lfloor m/2 \rfloor}) \quad \textit{for} \quad S_k = \begin{cases} \emptyset & \textit{if } k \notin S \\ \mathbb{Z}_n & \textit{if } k \in S. \end{cases}$$

Furthermore, Vilfred [98] developed a theory of factorization of simple connected circulant graphs with respect to the Cartesian product (similar to the theory of product and factorization of natural numbers), following the idea of Sabidussi [84]. Vilfred's main results are

THEOREM 2.1.14 (Factorization theorem for circulant graphs (cf. [98, Theorem 36])). *Let* m *and* n *be relatively prime integers. If* $R \subseteq \mathbb{Z}_m$, $S \subseteq \mathbb{Z}_n$, *and* $T \subseteq \mathbb{Z}_{mn}$ *(such that the respective circulant graphs are simple and connected) with*

$$T = dnR \cup dmS$$

for some d *such that* $\gcd(mn, d) = 1$, *then*

$$\mathrm{Cay}(\mathbb{Z}_{mn}, T) \cong \mathrm{Cay}(\mathbb{Z}_m, R) \,\square\, \mathrm{Cay}(\mathbb{Z}_n, S).$$

THEOREM 2.1.15 (Fundamental theorem for circulant graphs (cf. [98, Theorem 41])). *Every connected (simple) circulant graph is the unique product of prime circulant graphs (up to isomorphism).*

Therein, a *prime circulant graph* is defined as a circulant graph whose only divisors are improper.

2.1.4.2. *Spectra of unitary Cayley graphs.* Unitary Cayley graphs were introduced by Dejter and Giudici [28] in 1995 as the graphs $\mathrm{Cay}(\mathbb{Z}_n, \mathbb{Z}_n^*)$. Since

$$\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n \mid \gcd(x, n) = 1\} = G_n(1),$$

two vertices $x, y \in \mathbb{Z}_n$ are adjacent in the unitary Cayley graph $\mathrm{Cay}(\mathbb{Z}_n, \mathbb{Z}_n^*)$ if and only if $\gcd(x - y, n) = 1$. Since then, unitary Cayley graphs have been studied as objects of independent interest (cf. [18, 35, 57, 6, 52, 51, 62]).

In particular, in 2007 Klotz and Sander [57] studied the eigenvalues of unitary Cayley graphs and (the more general) gcd-graphs (that are graphs of the form $\mathrm{Cay}(\mathbb{Z}_n, G_n(d))$ for d being a proper divisor of n) and it turned out that they are always integral (in fact, this was already proven by So [92], but Klotz and Sander were not familiar with So's result at that time).

Besides that, Fuchs [35] generalized the definition of unitary Cayley graphs as follows: given a finite commutative ring R with unit element $1 \neq 0$, let $\mathrm{Cay}(R, R^*)$ be the graph with vertex set R such that two vertices $x, y \in R$ are adjacent if and only if $x - y \in R^*$, where R^* denotes the set of units in R.

Surprisingly, the spectra of generalized unitary Cayley graphs were determined precisely by Akhtar et. al. [6]. The key observation for this was the following: since R is a finite ring, it can be written as a direct product of finite local rings R_i, i.e.

$$R \cong R_1 \times \ldots \times R_t,$$

where each R_i has maximal ideal $\mathfrak{m}_i$. Since $(u_1, \ldots, u_t)$ is a unit in R if and only if each u_i is a unit in R_i, it follows that $\mathrm{Cay}(R, R^*)$ is the direct product of the graphs $\mathrm{Cay}(R_i, R_i^*)$, i.e.

$$\mathrm{Cay}(R, R^*) \cong \mathrm{Cay}(R_1, R_1^*) \times \ldots \times \mathrm{Cay}(R_t, R_t^*).$$

Hence, by the fact that the eigenvalues of the direct product of graphs are given by the products of eigenvalues of the respective factors, it suffices to study eigenvalues of $\mathrm{Cay}(R, R^*)$ for R being a finite local ring.

THEOREM 2.1.16 ([6, Proposition 10.2 and Corollary 10.3]).

(1) Let F be a field with n elements. Then

$$\mathrm{spec}(\mathrm{Cay}(F, F^*)) = \{n - 1, -1^{[n-1]}\},$$

i.e. $\mathrm{Cay}(F, F^*)) \cong \mathcal{K}_n$.

(2) *Let R be a local ring which is not a field, having (non-zero) maximal ideal $\mathfrak{m}$ of size m. Then*

$$\operatorname{spec}(\operatorname{Cay}(R, R^*)) = \{-m^{[\#S/m]}, 0^{[(\#S/m)(m-1)]}\}.$$

(3) *Let R be a finite ring and suppose R has t local factors, none of which are fields. Then*

$$\operatorname{spec}(\operatorname{Cay}(R, R^*)) = \{(-1)^t \#\mathfrak{R}_R^{[\#(R/\mathfrak{R}_R)]}, 0^{\#R-\#(R/\mathfrak{R}_R)}\},$$

where $\mathfrak{R}_R$ denotes the (unique) maximal ideal of R.

In particular, this shows that generalized unitary Cayley graphs also have integer eigenvalues only.

Further results on the spectra of generalized unitary Cayley graphs are given in [52, 51, 62].

2.1.4.3. *Constructions of integral graphs.* Harary and Schwenk [42] studied families of integral graphs with respect to graph products since all the standard graph products are closed under integrality.

A similar approach was obtained by Hansen et. al. [41] who characterized integral complete products. In particular, they proved the following:

THEOREM 2.1.17 ([41, Corollary 1]). *For $i = 1, 2$ let $\mathcal{G}_i$ be regular graphs of degree r_i with n_i vertices. Then, the complete product $\mathcal{G}_1 \nabla \mathcal{G}_2$ is an integral graph if and only if both, $\mathcal{G}_1$ and $\mathcal{G}_2$, are integral graphs and there exists $k \in \mathbb{N}$ such that*

$$n_1 n_2 = k(k + |r_1 - r_2|).$$

Similarly, Wang et. al. [100] proved the following conditions by investigating the point identification of graphs:

THEOREM 2.1.18 ([100, Theorem 3]).

(1) *If $\mathcal{G}$ and $\mathcal{K}_{1,r} \bullet \mathcal{G}$ are integral graphs, then $r\mathcal{G}$ is integral.*
(2) *If $\mathcal{G}$ and $r\mathcal{G}$ are integral graphs, then $\mathcal{K}_{1,r} \bullet \mathcal{G}$ is integral, too.*

Further constructions of integral graphs using the point identification are stated in [99].

Following the ideas of Hansen et. al. [41] and Wang et. al. [100], in his Master's thesis [36] Gardemann found new families of integral graphs by considering complete products and point identification of complete and complete bipartite graphs. In particular, he proved:

THEOREM 2.1.19 ([36, Korollar 5.1.1 and Theorem 5.3.1]). *If there exists $k \in \mathbb{Z}$ such that*

$$a(n-1) = k(k+n-2),$$

then the graph $\mathcal{K}_n \overset{a}{\bullet}$ is integral.

Moreover, the graph $\mathcal{K}_{n,m} \overset{a}{\bullet}$ is integral if and only if $(n-1)m$ and $m(a+n-1)$ are squares.

Some of the results in [36] are published in [37].

The last aspect we want to mention here is a paper of Klotz and Sander [60] which, in some sense, combines the theory of this section and the previous ones. In fact, Klotz and Sander found a relation between the (algebraically defined) Cayley graphs and the (combinatorially defined) graph products. They considered gcd-graphs over abelian groups (as a generalization of the gcd-graphs $\mathrm{Cay}(\mathbb{Z}_n, G_n(d))$ over $\mathbb{Z}_n$). Their main result is that every gcd-graph is isomorphic to a so-called NEPS (non-complete extended p-sum) of complete graphs, and, conversely, that every NEPS of complete graphs is isomorphic to a gcd-graph over some abelian group. We skip the definition of NEPS here and only remark that it is based on a similar idea as the one of B-products. We refer the interested reader to [26].

2.2. Properties of the algebraic degree of graphs

In this section, we consider simple graphs with respect to algebraic properties of their eigenvalues.

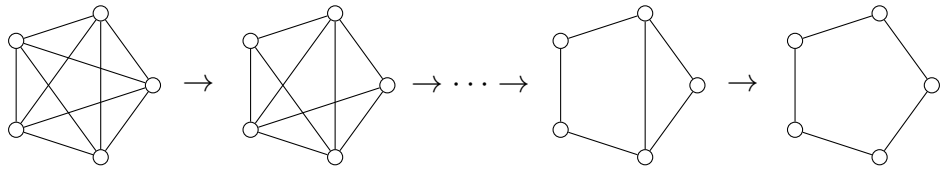


FIGURE 2.3. A descent on simple graphs: $\mathcal{K}_5 \to \mathcal{K}_5$ minus one edge $\to \cdots \to \mathcal{C}_5$ plus one edge $\to \mathcal{C}_5$.

2.2.1. A decent on simple graphs. Starting from a simple graph, we sequentially remove edges (cf. Figure 2.3). It appears that a graph with large diameter has some eigenvalues of large algebraic degree. This is well illustrated in Table 2.2 listing the diameter and the algebraic degree of the complete graph $\mathcal{K}_n$, the complete bipartite graph $\mathcal{K}_{n-m,m}$, the Payley graph $\mathrm{Pal}(n)$ (existent if $n \equiv 1 \bmod 4$ is a prime power), and the cycle graph $\mathcal{C}_n$ on n vertices for sufficiently large n, respectively.

TABLE 2.2. Diameter and algebraic degree of some graphs.

Graph	Diameter	Algebraic degree
$\mathcal{K}_n$	1	1
$\mathcal{K}_{n-m,m}$	$\leqslant 2$	$\leqslant 2$
$\mathrm{Pal}(n)$	2	2
$\mathcal{C}_n$	$\approx n/2$	$\geqslant n/(2\log\log n)$

In fact, we could prove a lower bound for the algebraic degree of a graph in terms of its diameter and maximum vertex degree.

It is well-known that a graph $\mathcal{G}$ has at least $\operatorname{diam}(\mathcal{G}) + 1$ distinct eigenvalues and, if k denotes the maximum vertex degree of $\mathcal{G}$, then all eigenvalues of $\mathcal{G}$ are contained in the interval $[-k, k]$ (note that all eigenvalues are real since $\mathcal{G}$ is assumed to be simple and, therefore, has a symmetric adjacency matrix). Thus, it is an easy consequence that whenever

$$\operatorname{diam}(\mathcal{G}) + 1 > \#([-k, k] \cap \mathbb{Z}) = 2k + 1,$$

then $\mathcal{G}$ must have at least one non-integral eigenvalue (i.e. at least one eigenvalue of degree > 1). Similar bounds can be obtained for graphs which must have an eigenvalue of degree $> n$ by counting the number of algebraic integers of degree $\leq n$ in the interval $[-k, k]$. That is

THEOREM 2.2.1 ([70, Theorem 1]). *Let $\mathcal{G}$ be a simple graph on n vertices and let k denote the maximum vertex degree of $\mathcal{G}$.*

(1) If $\operatorname{diam}(\mathcal{G}) > 2k$, then there exists an eigenvalue of algebraic degree at least two and $\deg(\mathcal{G}) \geq 2$.
(2) If $\operatorname{diam}(\mathcal{G}) > 16k^3+4k^2+8k+1$, then there exists an eigenvalue of algebraic degree at least three and $\deg(\mathcal{G}) \geq 3$.
(3) Let $A(d, k)$ be the number of totally real algebraic integers α of degree $\leq d$ for which α and all conjugates lie inside the interval $[-k, k]$. For all positive integers d and k the quantity $A(d, k)$ is finite. If $\operatorname{diam}(\mathcal{G})+1 > A(d, k)$, then there exists an eigenvalue of algebraic degree at least $d+1$ and $\deg(\mathcal{G}) \geq d+1$.

In particular, if there is one eigenvalue of algebraic degree m, then there are at least m eigenvalues of algebraic degree m.

A proof of this result and further approaches to determine the algebraic degree of simple graphs can be found in our paper [70].

2.2.2. A family of graphs of maximum algebraic degree. For $n \geq 7$, we consider the family of graphs $\mathcal{M}_n$ with adjacency matrix

$$A(\mathcal{M}_n) = C_n + B_n + B_n^{\mathsf{t}},$$

for C_n being the adjacency matrix of $\operatorname{Cay}(\mathbb{Z}_n, \{1, n-1\})$ and B_n being the $(n \times n)$-matrix with zero entries except for the first row $(0 \cdots 0\,1\,1\,0\,1\,0)$. The graphs are illustrated in Figure 2.4.

Computations showed that at least for all $n \leq 100$ the characteristic polynomial of $\mathcal{M}_n$ is irreducible and the Galois group of the splitting field of $\mathcal{M}_n$ equals S_n. Therefore, we conjecture that $\{\mathcal{M}_n \mid n \geq 7\}$ is a family of graphs of maximum algebraic degree $n!$.

Unfortunately, until now, we were not able to prove this. At least we found a recursive formula for the characteristic polynomial of $\mathcal{M}_n$.

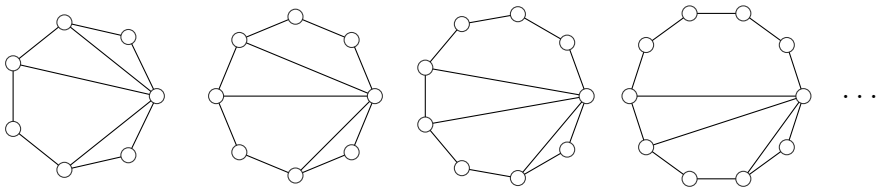


FIGURE 2.4. Family $\mathcal{M}_n$ of graphs of maximum algebraic degree.

THEOREM 2.2.2. *The characteristic polynomial $\chi_{\mathcal{M}_n}$ of $\mathcal{M}_n$ for $n \geq 9$ is given by*

$$\chi_{\mathcal{M}_n}(x) = \chi_{\mathcal{M}_{n-1}}(x)x - \chi_{\mathcal{M}_{n-2}}(x) + 2(x-1)^2(x+1)(x-2)(x+2),$$

for

$$\chi_{\mathcal{M}_7}(x) = x^7 - 10x^5 - 6x^4 + 19x^3 + 12x^2 - 9x - 4$$

and

$$\chi_{\mathcal{M}_8}(x) = x^8 - 11x^6 - 4x^5 + 28x^4 + 8x^3 - 19x^2 - 2x + 1.$$

PROOF. Let

$$\begin{aligned}\chi_{\mathcal{M}_n}(x) &= \det(xI - A(\mathcal{M}_n)) \\ &= \det\begin{pmatrix} x & -1 & 0 & \cdots & \cdots & 0 & -1 & -1 & 0 & -1 & -1 \\ -1 & x & -1 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & -1 & x & -1 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & 0 & -1 & x & -1 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ \vdots & & \ddots & \ddots & \ddots & \ddots & \ddots & & & & \vdots \\ \vdots & & & \ddots & \ddots & \ddots & \ddots & \ddots & & & \vdots \\ 0 & \cdots & \cdots & 0 & -1 & x & -1 & 0 & 0 & 0 & 0 \\ -1 & 0 & \cdots & \cdots & 0 & -1 & x & -1 & 0 & 0 & 0 \\ -1 & 0 & \cdots & \cdots & \cdots & 0 & -1 & x & -1 & 0 & 0 \\ 0 & 0 & \cdots & \cdots & \cdots & \cdots & 0 & -1 & x & -1 & 0 \\ -1 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & -1 & x & -1 \\ -1 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & -1 & x \end{pmatrix} \\ &=: \det(M_n(x)).\end{aligned}$$

The proof is due to Laplace expansion along the first row of the matrix $M_n(x)$. Since the computation is cumbersome, we only give a short sketch of the proof.

Let $M_n(x)_{i,j}$ denote the matrix obtained by deleting the i-th row and the j-th column of $M_n(x)$. Furthermore, let $\chi_{\mathcal{P}_n}$ denote the characteristic polynomial of the path graph on n vertices, that is

$$\chi_{\mathcal{P}_n}(x) = \det(xI - A(\mathcal{P}_n))$$
$$= \det\begin{pmatrix} x & -1 & 0 & \cdots & \cdots & \cdots & 0 \\ -1 & x & -1 & 0 & \cdots & \cdots & 0 \\ 0 & -1 & x & -1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & -1 & x & -1 & 0 \\ 0 & \cdots & \cdots & 0 & -1 & x & -1 \\ 0 & \cdots & \cdots & \cdots & 0 & -1 & x \end{pmatrix}.$$

Laplace expansion along the first row of this matrix directly yields the recursion

$$\chi_{\mathcal{P}_n}(x) = \chi_{\mathcal{P}_{n-1}}(x)x - \chi_{\mathcal{P}_{n-2}}(x). \tag{1}$$

Since $M_n(x)_{1,1} = \chi_{\mathcal{P}_{n-1}}(x)$, we may write

$$\begin{aligned} \det(M_n(x)) = \chi_{\mathcal{P}_{n-1}}(x)x + M_n(x)_{1,2} + \\ + (-1)^{n-1}\big(M_n(x)_{1,n-3} + M_n(x)_{1,n-1}\big) + \\ + (-1)^n\big(M_n(x)_{1,n-4} + M_n(x)_{1,n}\big). \end{aligned} \tag{2}$$

Now, for each of the latter minors $M_n(x)_{i,j}$ we can derive an expression in terms of characteristic polynomials of path graphs (using Laplace expansion again and again). Applying all expressions to (2) and using the recursion (1) finally yields the stated formula. □

Note that for $n = 6$, the graph with adjacency matrix

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

is of maximum algebraic degree, whereas for $n \leq 5$ there is no graph on n vertices and of maximum algebraic degree.

CHAPTER 3

Cayley Graphs and Circulant Graphs

3.1. Isospectral circulant graphs

Our motivation for constructing isospectral circulant graphs is the generalization of counterexamples to Ádám's conjecture [3]. We can easily see that if there is an $m \in \mathbb{Z}_n^*$ such that $S = mT = \{mt \mid t \in T\}$, then $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$ are isomorphic. If such m exists, we say that the connection sets S and T are *proportional*, and write $S \sim T$. As already mentioned in the introduction, Ádám conjectured that the converse is also true, i.e. that for all isomorphic circulant graphs $\mathrm{Cay}(\mathbb{Z}_n, S), \mathrm{Cay}(\mathbb{Z}_n, T)$ it already follows that $S \sim T$. But Elspas and Turner [29] found a quite simple counterexample. Since then, further counterexamples were given, in particular, by Alspach and Parsons [8] or Mans, Pappalardi and Shparlinski [64].

Given connection sets $S, T \subseteq \mathbb{Z}_n$, we introduce some techniques to decide whether the corresponding graphs $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$ are isospectral or not without determining their spectra explicitly. These techniques arise from generalizing known examples of isospectral circulant graphs and provide constructions of new examples as well. All results in this section were published in [68]. Our constructions yield non-isomorphic as well as isomorphic graphs, even though, our aim is to find *non-trivial* examples of isospectral circulant graphs, i.e. circulant graphs with non-proportional connection sets. Thus, every pair of isospectral graphs which arises from one of our constructions is either non-isomorphic or provides a counterexample to Ádám's conjecture. In particular, we show that every such pair relates to vanishing sums of roots of unity.

For a set $S = \{s_1, \ldots, s_m\} \subseteq \mathbb{Z}_n$ we always write $\gcd(S, n)$ instead of $\gcd(s_1, \ldots, s_m, n)$. Note that, as proven by Boesch and Tindell [20], a circulant graph $\mathrm{Cay}(\mathbb{Z}_n, S)$ is connected if and only if $\gcd(S, n) = 1$. Moreover, Vilfred [97] showed that a non-connected circulant graph $\mathrm{Cay}(\mathbb{Z}_n, S)$ consists of $\gcd(S, n)$ copies of the graph

$$\mathrm{Cay}(\mathbb{Z}_{n/\gcd(S,n)}, S/\gcd(S, n)),$$

where $S/\gcd(S, n)$ denotes the set $\{s_1/\gcd(S, n), \ldots, s_m/\gcd(S, n)\}$. However, in this section, we do not want to restrict our considerations to particular connection sets S, thus we do not assume S to be symmetric or $\mathrm{Cay}(\mathbb{Z}_n, S)$ to be connected. Moreover, if $S = T$ for sets

$S, T \subseteq \mathbb{Z}_n$, in the following we write $S \equiv T \bmod n$ instead since our constructions mainly rely on changing the modulus n.

3.1.1. General observations and notations. Let here and in the following $\zeta_n := \exp(2\pi i/n)$ and $\mathrm{e}(x) := \exp(2\pi i x)$. Recall that the spectrum of a circulant graph $\mathrm{Cay}(\mathbb{Z}_n, S)$ is given by

$$\mathrm{spec}(\mathrm{Cay}(\mathbb{Z}_n, S)) = \Big\{ \sum_{s\in S} \zeta_n^{sk} \mid k = 0, \ldots, n-1 \Big\}.$$

Therefore, two circulant graphs $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$ are isospectral if and only if for every $k \in \mathbb{Z}_n$ there is an $l \in \mathbb{Z}_n$ such that

$$\sum_{s\in S} \zeta_n^{sk} = \sum_{t\in T} \zeta_n^{tl}$$

and vice versa, i.e. there exists a bijection (permutation) $\sigma : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ such that

$$\sum_{s\in S} \zeta_n^{sk} = \sum_{t\in T} \zeta_n^{t\sigma(k)}$$

for all $k \in \mathbb{Z}_n$. In the following, we call such bijection a *spectral bijection* of S and T. Note that for $k = 0$ the corresponding eigenvalue of $\mathrm{Cay}(\mathbb{Z}_n, S)$ equals the number of elements in S, and that two circulant graphs have the same number of edges if and only if their connection sets have the same cardinality. This, in combination with the fact that isospectral graphs have the same number of vertices and edges, yields $\sigma(0) = 0$ for every spectral bijection σ. Therefore, we neglect this case here and elsewhere.

Another fundamental observation is stated in the next lemma:

LEMMA 3.1.1. *Let* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *and* $\mathrm{Cay}(\mathbb{Z}_n, T)$ *be isospectral circulant graphs. Then,* $\gcd(S, n) = \gcd(T, n)$.

PROOF. The graph $\mathrm{Cay}(\mathbb{Z}_n, S)$ consists of $\gcd(S, n)$ isomorphic connected components, where each component is a circulant graph and, therefore, regular (cf. Vilfred [97, Proposition 4.5]). According to the Perron-Frobenius theorem (see [39], for example), each component has the eigenvalue $\lambda = \#S = \#T$ and all other eigenvalues are smaller than λ in absolute value. The spectrum of $\mathrm{Cay}(\mathbb{Z}_n, S)$ is the union of the spectra of its connected components. Thus, $\mathrm{Cay}(\mathbb{Z}_n, S)$ contains exactly $\gcd(S, n)$ times the eigenvalue λ. Equivalently, λ is an eigenvalue of $\mathrm{Cay}(\mathbb{Z}_n, T)$ of multiplicity $\gcd(T, n)$. Since $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$ are isospectral, the statement follows. □

Now, we define the polynomial $G_{S,T,k,l}$ by

$$G_{S,T,k,l}(x) = \sum_{s\in S} x^{s\cdot k} - \sum_{t\in T} x^{t\cdot l}$$

(where all exponents are understood to be taken modulo n).

Let $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$ be isospectral circulant graphs with connection sets $S, T \subseteq \mathbb{Z}_n$ and spectral bijection σ. Then, we observe that $G_{S,T,k,\sigma(k)}(\zeta_n) = 0$ for all $k \in \mathbb{Z}_n$, since $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$ are isospectral, whereas $G_{S,T,1,\sigma(1)}$ equals the zero polynomial if and only if $S \equiv \sigma(1)T \bmod n$. The following theorem shows that the latter statement is already equivalent to $S \sim T$:

THEOREM 3.1.2. *Let* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *and* $\mathrm{Cay}(\mathbb{Z}_n, T)$ *be isospectral circulant graphs with* $S \equiv lT \bmod n$ *for any (not necessarily invertible)* $l \in \mathbb{Z}_n$*. Then,* S *and* T *are proportional.*

PROOF. By Lemma 3.1.1, we already know that

$$\gcd(S, n) = \gcd(T, n) =: d.$$

Therefore, $S \equiv lT \bmod n$ is equivalent to

$$S/d \equiv l(T/d) \bmod n/d,$$

where the expression S/d denotes the set $\{s/d \mid s \in S\}$. From this equation we deduce that l is invertible in $\mathbb{Z}_{n/d}$, because otherwise we would have $\gcd(l(T/d), n/d) > 1 = \gcd(S/d, n/d)$. Now, let $k := x(n/d) + l$ for $x \in \mathbb{Z}_n$ with $0 \leq x < d$. Then, it follows that

$$kT = (x(n/d)+l)T = x(n/d)T + lT = xn(T/d) + lT \equiv lT \equiv S \bmod n.$$

Note that $\gcd(n, l)$ is a divisor of d since $l \in \mathbb{Z}_{n/d}^*$. Therefore, we may write $n = p_1 \cdots p_N$ for some $N \in \mathbb{N}$ and not necessarily distinct prime numbers p_i, and, without loss of generality, $d = p_1 \cdots p_m$ for $m \leq N$ and $l = p_1 \cdots p_r q_1 \cdots q_z$ for $r \leq m$, $z \in \mathbb{N}$ and not necessarily distinct prime numbers $q_i \neq p_j$ for all $j = 1, \ldots, N$. Now, let x be the product of all prime numbers in the set $\{p_{r+1}, \ldots, p_m\} \backslash \{p_1, \ldots, p_r\}$, then

$$k = x(n/d) + l = x p_{m+1} \cdots p_N + p_1 \cdots p_r q_1 \cdots q_z.$$

Since l and n/d are relatively prime, we have that

$$\{p_{m+1}, \ldots, p_N\} \cap \{p_1, \ldots, p_r\} = \emptyset.$$

Hence, every prime divisor p_i of n either is a divisor of $x(n/d)$ but not a divisor of l, or vice versa. Thus, it follows that $\gcd(k, n) = 1$ and, therefore, $S \sim T$, since $S \equiv kT \bmod n$. □

Note that a similar approach was already undertaken by Litow and Mans [61] within their proof of their main result and it is also stated in the paper of Mans, Pappalardi and Shparlinski [64, Lemma 3]. Lemma 3.1.1 and Theorem 3.1.2 show that this approach also works for non-connected circulant graphs. Moreover, we observe that if $G_{S,T,k,\sigma(k)}(\zeta_n) = 0$, the minimal polynomial of ζ_n, i.e. the n-th cyclotomic polynomial, is a divisor of $G_{S,T,k,\sigma(k)}$. Thus, in this case, every primitive n-th root of unity is a root of $G_{S,T,k,\sigma(k)}$.

Our constructions of non-trivial examples of isospectral circulant graphs rely on this necessary condition.

Since it seems difficult to gain further necessary conditions for isospectrality of circulant graphs, we now investigate sufficient conditions and present some explicit constructions and examples thereof.

3.1.2. Constructions of isospectral circulant graphs. Our fundamental idea for the construction of non-trivial examples of isospectral circulant graphs is stated in the following theorem. It generalizes an example given by Godsil, Holton and McKay [38] (here presented as Example 3.1.4).

THEOREM 3.1.3. *Assume $n \in \mathbb{N}$ and $S, T \subseteq \mathbb{Z}_n$ such that there exists $l \in \mathbb{Z}_n^*$ with $G_{S,T,1,l}(\zeta_n) = 0$. If there is an $m \in \mathbb{Z}_n^*$ such that $S \equiv mT \bmod \frac{n}{p}$ for every prime divisor p of n, then $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$ are isospectral.*

PROOF. We define

$$\sigma : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n, \quad k \mapsto \begin{cases} lk, & \text{if } \gcd(k,n) = 1, \\ mk, & \text{otherwise.} \end{cases}$$

Since $l, m \in \mathbb{Z}_n^*$, the map σ is bijective. We show that σ is a spectral bijection of S and T. If $\gcd(k,n) = 1$, then ζ_n^k is still a primitive n-th root of unity and, therefore, $G_{S,T,k,\sigma(k)}(\zeta_n) = G_{S,T,1,l}(\zeta_n^k) = 0$. On the other hand, if p is a divisor of k and n, then we may write $k = \kappa p$ and we observe that

$$\sum_{s \in S} \zeta_n^{s \cdot k} = \sum_{s \in S} \mathrm{e}\left(\frac{s\kappa}{\frac{n}{p}}\right) = \sum_{t \in T} \mathrm{e}\left(\frac{mt\kappa}{\frac{n}{p}}\right) = \sum_{t \in T} \zeta_n^{t \cdot \sigma(k)},$$

since $S \equiv mT \bmod \frac{n}{p}$. This implies $G_{S,T,k,\sigma(k)}(\zeta_n) = 0$ for all k with $\gcd(k,n) > 1$. □

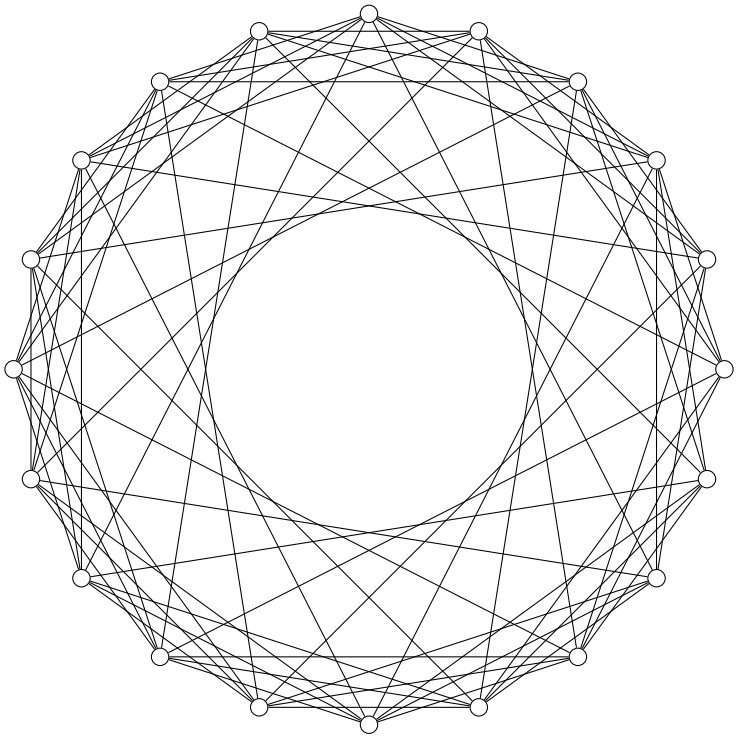
This theorem does not require the existence of an $m \in \mathbb{Z}_n^*$ satisfying $S \equiv mT \bmod n$. Therefore, it provides also non-trivial examples of isospectral circulant graphs:

EXAMPLE 3.1.4. Let $n = 20$, $S = \{2, 3, 4, 7, 13, 16, 17, 18\}$ and $T = \{3, 6, 7, 8, 12, 13, 14, 17\}$. Then, for all $l \in \mathbb{Z}_{20}^*$, we have that $G_{S,T,1,l}(\zeta_n) = 0$ but $S \not\equiv lT \bmod 20$. Since $S \equiv T \bmod 10$ and $S \equiv T \bmod 4$, by Theorem 3.1.3 we get that $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$ are isospectral but non-proportional.

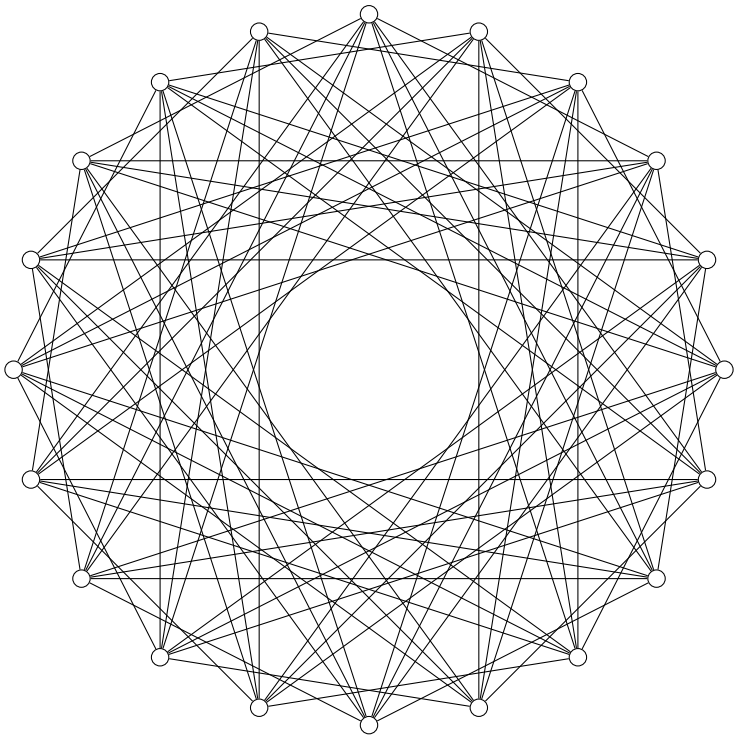
This example was stated by Godsil, Holton and McKay [38] and seems to be the first published example of isospectral non-isomorphic *undirected* circulant graphs. The graphs are shown in Figure 3.1.

In order to find new examples, first of all, we construct sets $S, T \subseteq \mathbb{Z}_n$ such that there exists $l \in \mathbb{Z}_n$ with

$$G_{S,T,1,l}(\zeta_n) = 0 \quad \text{and} \quad G_{S,T,1,l} \neq 0 \text{ (as a polynomial).} \tag{3}$$



(a) $S = \{2, 3, 4, 7, 13, 16, 17, 18\}$



(b) $T = \{3, 6, 7, 8, 12, 13, 14, 17\}$

FIGURE 3.1. Non-isomorphic isospectral circulant graphs.

The main idea for this is to use subsets $\mathrm{Eq} \subseteq \mathbb{Z}_n$ which have the property that

$$\sum_{j \in \mathrm{Eq}} \zeta_n^j = 0. \tag{4}$$

Indeed, we will see that every non-trivial pair of isospectral circulant graphs arises from such sets or rather can be constructed starting from such a set. Motivated by Rédei [83], we call a set Eq satisfying Equation (4) *equilibrium set*. In his paper, Rédei gave a complete characterization of those sets. In the following, we will use his results, but adapt some notations.

It is well-known that for fixed $n \in \mathbb{N}$, the set $\{0, 1, \ldots, n-1\}$ is an equilibrium set, i.e.

$$\sum_{j=0}^{n-1} \zeta_n^j = \sum_{j=0}^{n-1} \mathrm{e}\left(\frac{j}{n}\right) = 0.$$

Therefore, if d is a divisor of n, the set $\{0, \frac{n}{d}, 2\frac{n}{d}, \ldots, (d-1)\frac{n}{d}\}$ is also an equilibrium set, since

$$\sum_{j \in \{0, \frac{n}{d}, 2\frac{n}{d}, \ldots, (d-1)\frac{n}{d}\}} \mathrm{e}\left(\frac{j}{n}\right) = \sum_{j=0}^{d-1} \mathrm{e}\left(\frac{j}{d}\right) = 0.$$

Finally, multiplying both sides by $\mathrm{e}\left(\frac{a}{n}\right)$, for any $a \in \mathbb{Z}_n$, yields the equilibrium set

$$\left\{a, a + \frac{n}{d}, a + 2\frac{n}{d}, \ldots, a + (d-1)\frac{n}{d}\right\} =: [a, n, d].$$

Rédei called such sets *trivial* equilibrium sets. We observe that every trivial equilibrium set is an arithmetic progression in $\mathbb{Z}_n$ of length d with common difference $\frac{n}{d}$ for some divisor d of n. In the following, we denote an arithmetic progression of length d with common difference $\frac{n}{d}$ and initial value a by $[a, n, d] \subseteq \mathbb{Z}_n$. Note that if d is not a prime number, then, for each prime divisor p of d, the arithmetic progression $[a, n, d]$ equals the union

$$\bigcup_{i=1}^{d/p} [a_i, n, p]$$

for suitable values of a_i. Therefore, we call $[a, n, d]$ *indecomposable* if d is a prime number and *decomposable* else. Furthermore, it is clear that for every $k \in \mathbb{Z}_n$ with $\gcd(k, d) = 1$ the set $k \cdot [a, n, d]$ is still an equilibrium set. If $\gcd(k, d) > 1$ but d does not divide k, then we may write

$$k \cdot [a, n, d] = \bigcup_{i=1}^{\gcd(k,d)} [a_i, n, \frac{d}{\gcd(k, d)}]$$

for suitable values of a_i, i.e. $k \cdot [a, n, d]$ remains an equilibrium set as well.

Now, we construct non-trivial examples of isospectral circulant graphs by using such trivial equilibrium sets. We use the idea of Theorem 3.1.3 as a foundation but we can weaken the second condition of this theorem by exploiting the properties of equilibrium sets. The following theorem provides a sufficient criterion for two circulant graphs to be isospectral:

THEOREM 3.1.5. *Let $n \in \mathbb{N}$ and d be a divisor of n. Furthermore, define*

$$\mathrm{Eq}_S := \bigcup_{i=1}^{r} [a_i, n, d] \text{ and } \mathrm{Eq}_T := \bigcup_{i=1}^{r} [b_i, n, d],$$

for some $a_i, b_i \in \mathbb{Z}_n$ and pairwise disjoint sets $[a_i, n, d]$ and $[b_i, n, d]$, respectively. Finally, let $S := S' \cup \mathrm{Eq}_S$ and $T := T' \cup \mathrm{Eq}_T$ for $S', T' \subseteq \mathbb{Z}_n$ with $S' \cap \mathrm{Eq}_S = \emptyset = T' \cap \mathrm{Eq}_T$ such that there exists $l \in \mathbb{Z}_n^*$ with $S' \equiv lT' \bmod n$. If there is some m with $\gcd(m, \frac{n}{d}) = 1$ such that $S \equiv mT \bmod \frac{n}{d}$, then the circulant graphs $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$ are isospectral.

In particular, if $\mathrm{Eq}_S \not\equiv l\,\mathrm{Eq}_T \bmod n$ for every $l \in \mathbb{Z}_n^*$ with $S' \equiv lT' \bmod n$, then S and T are non-proportional.

PROOF. We define

$$\sigma : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n, \quad k \mapsto \begin{cases} lk, & \text{if } d \nmid k, \\ mk, & \text{if } d \mid k. \end{cases}$$

Since $l \in \mathbb{Z}_n^*$ and $m \in \mathbb{Z}_{\frac{n}{d}}^*$, the map σ is bijective. We show that σ is a spectral bijection of S and T. If d is not a divisor of k, then $k \cdot \mathrm{Eq}_S$ and $lk \cdot \mathrm{Eq}_T$ are still equilibrium sets (as mentioned above) and, therefore,

$$G_{S,T,k,\sigma(k)}(\zeta_n) = \sum_{s \in S} \zeta_n^{s \cdot k} - \sum_{t \in T} \zeta_n^{t \cdot \sigma(k)} = \sum_{s \in S'} \zeta_n^{s \cdot k} - \sum_{t \in T'} \zeta_n^{t \cdot lk} = 0.$$

On the other hand, if d is a divisor of k, we may write $k = \kappa d$. Since, by assumption, $S \equiv mT \bmod \frac{n}{d}$, we observe that

$$\sum_{s \in S} \zeta_n^{s \cdot k} = \sum_{s \in S} \mathrm{e}\left(\frac{s\kappa}{\frac{n}{d}}\right) = \sum_{t \in T} \mathrm{e}\left(\frac{mt\kappa}{\frac{n}{d}}\right) = \sum_{t \in T} \zeta_n^{t \cdot \sigma(k)}.$$

Thus, we get $G_{S,T,k,\sigma(k)}(\zeta_n) = 0$ also in this case. □

Note that if $\mathrm{Cay}(\mathbb{Z}_n, S)$ is undirected, then $[a, n, d] \subseteq S$ if and only if $[-a, n, d] \subseteq S$. In the following we write $[\pm a, n, d]$ instead of $[a, n, d] \cup [-a, n, d]$.

Example 3.1.4 arises from both, Theorem 3.1.3 and Theorem 3.1.5. But there are also examples of non-trivial isospectral circulant graphs which satisfy Theorem 3.1.5 only:

EXAMPLE 3.1.6. The first known counterexample to Ádám's conjecture, published by Elspas and Turner [29], suffices Theorem 3.1.5: Let $n = 16$, $S = \{1, 2, 7, 9, 14, 15\}$ and $T = \{2, 3, 5, 11, 13, 14\}$. Then, S and T are non-proportional and we may write $S = \{2, 14\} \cup [\pm 1, 16, 2]$ and $T = \{2, 14\} \cup [\pm 3, 16, 2]$. Since $S \equiv 3 \cdot T \bmod 8$, the graphs $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$ are isospectral by Theorem 3.1.5.

Unfortunately, as Example 3.1.4 and 3.1.6 show, the theorem neither guarantees that the isospectral graphs are non-isomorphic nor that they are isomorphic.

We can easily generalize Theorem 3.1.5 by considering distinct divisors of n. In the following, let $\mathcal{P}(M)$ denote the power set of a set M.

THEOREM 3.1.7. *Let $n \in \mathbb{N}$ and $d_1, \ldots, d_z$ be divisors of n which are pairwise relatively prime. Furthermore, let*

$$\mathrm{Eq}_S := \bigcup_{j=1}^{z} \bigcup_{i=1}^{r_j} [a_{ij}, n, d_j] \text{ and } \mathrm{Eq}_T := \bigcup_{j=1}^{z} \bigcup_{i=1}^{r_j} [b_{ij}, n, d_j],$$

for some $a_{ij}, b_{ij} \in \mathbb{Z}_n$ and pairwise disjoint sets $[a_{ij}, n, d_j]$ and $[b_{ij}, n, d_j]$, respectively. Finally, let $S := S' \cup \mathrm{Eq}_S$ and $T := T' \cup \mathrm{Eq}_T$ for $S', T' \subseteq \mathbb{Z}_n$ with $S' \cap \mathrm{Eq}_S = \emptyset = T' \cap \mathrm{Eq}_T$ such that there exists $l \in \mathbb{Z}_n^*$ with $S' \equiv lT' \bmod n$. If for all $\pi \in \mathcal{P}(\{1, \ldots, z\}) \backslash \{\emptyset\}$ there is some m_π with

$$\gcd(m_\pi, \frac{n}{\prod_{j \in \pi} d_j}) = 1$$

such that

$$S' \equiv m_\pi T' \bmod \frac{n}{\prod_{j \in \pi} d_j}$$

and

$$\bigcup_{j \in \pi} \bigcup_{i=1}^{r_j} [a_{ij}, n, d_j] \equiv m_\pi \bigcup_{j \in \pi} \bigcup_{i=1}^{r_j} [b_{ij}, n, d_j] \bmod \frac{n}{\prod_{j \in \pi} d_j},$$

then the circulant graphs $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$ are isospectral.

In particular, if $\mathrm{Eq}_S \not\equiv l\,\mathrm{Eq}_T \bmod n$ for every $l \in \mathbb{Z}_n^*$ with $S' \equiv lT' \bmod n$, then S and T are non-proportional.

PROOF. We define

$$\sigma : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n, \quad k \mapsto \begin{cases} lk, & \text{if } d_j \nmid k \text{ for all } j = 1, \ldots, z, \\ m_\pi k, & \text{if } \prod_{j \in \pi} d_j \mid k \text{ and } d_j \nmid k \text{ for all } j \notin \pi, \end{cases}$$

for all $\pi \in \mathcal{P}(\{1, \ldots, z\}) \backslash \{\emptyset\}$. By the same argument as in the proof of Theorem 3.1.5, we can see that σ is bijective. We show that σ is

a spectral bijection of S and T. If no d_j divides k, then $k \cdot \mathrm{Eq}_S$ and $lk \cdot \mathrm{Eq}_T$ are still equilibrium sets and, therefore,

$$G_{S,T,k,\sigma(k)}(\zeta_n) = \sum_{s\in S} \zeta_n^{s\cdot k} - \sum_{t\in T} \zeta_n^{t\cdot\sigma(k)} = \sum_{s\in S'} \zeta_n^{s\cdot k} - \sum_{t\in T'} \zeta_n^{t\cdot lk} = 0.$$

Now, let $\pi \in \mathcal{P}(\{1,\dots,z\})\backslash\{\emptyset\}$ and define $\mathrm{Eq}_{S_\pi} := \bigcup_{j\in\pi}\bigcup_{i=1}^{r_j}[a_{ij}, n, d_j]$ and $\mathrm{Eq}_{T_\pi} := \bigcup_{j\in\pi}\bigcup_{i=1}^{r_j}[b_{ij}, n, d_j]$. If $\prod_{j\in\pi} d_j \mid k$ and $d_j \nmid k$ for all $j \notin \pi$, then $k\cdot(\mathrm{Eq}_S \setminus \mathrm{Eq}_{S_\pi})$ and $m_\pi k\cdot(\mathrm{Eq}_T \setminus \mathrm{Eq}_{T_\pi})$ are still equilibrium sets due to the fact that the d_j's are relatively prime. Since, by assumption, we have

$$\mathrm{Eq}_{S_\pi} \equiv m_\pi \,\mathrm{Eq}_{T_\pi} \bmod \frac{n}{\prod_{j\in\pi} d_j} \text{ and } S' \equiv m_\pi T' \bmod \frac{n}{\prod_{j\in\pi} d_j},$$

it follows that

$$\begin{aligned}\sum_{s\in S'\cup \mathrm{Eq}_{S_\pi}} \zeta_n^{s\cdot k} &= \sum_{s\in S'\cup \mathrm{Eq}_{S_\pi}} \mathrm{e}\left(\frac{s\kappa_\pi}{\frac{n}{d_\pi}}\right) = \\ &= \sum_{t\in T'\cup \mathrm{Eq}_{T_\pi}} \mathrm{e}\left(\frac{m_\pi t\kappa_\pi}{\frac{n}{d_\pi}}\right) = \sum_{t\in T'\cup \mathrm{Eq}_{T_\pi}} \zeta_n^{t\cdot\sigma(k)}\end{aligned}$$

for $d_\pi = \prod_{j\in\pi} d_j$ and $\kappa_\pi = k/d_\pi$. Thus, we get $G_{S,T,k,\sigma(k)}(\zeta_n) = 0$. □

Example 3.1.8. Let $n = 120$ and let $\mathrm{Eq}_S := [\pm 5, 120, 5] \cup [\pm 9, 120, 2]$ and $\mathrm{Eq}_T := [\pm 1, 120, 5] \cup [\pm 27, 120, 2]$. Furthermore, let $S := \{34, 86\} \cup \mathrm{Eq}_S$ and $T := \{2, 118\} \cup \mathrm{Eq}_T$. Since

$$\begin{aligned}&[\pm 5, 120, 5] \equiv 5 \cdot [\pm 1, 120, 5] \bmod \tfrac{120}{5} \\ &\qquad\qquad \text{and } \{34, 86\} \equiv 5 \cdot \{2, 118\} \bmod \tfrac{120}{5}, \\ &[\pm 9, 120, 2] \equiv 13 \cdot [\pm 27, 120, 2] \bmod \tfrac{120}{2} \\ &\qquad\qquad \text{and } \{34, 86\} \equiv 13 \cdot \{2, 118\} \bmod \tfrac{120}{2}, \\ &\mathrm{Eq}_S \equiv 5 \cdot \mathrm{Eq}_T \bmod \tfrac{120}{10} \\ &\qquad\qquad \text{and } \{34, 86\} \equiv 5 \cdot \{2, 118\} \bmod \tfrac{120}{10},\end{aligned}$$

the undirected circulant graphs $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$ are isospectral by Theorem 3.1.7. In particular, the graphs are non-isomorphic, thus S and T are non-proportional.

So far, we only used trivial equilibrium sets in order to construct isospectral circulant graphs. Now we also want to consider so-called *non-trivial* equilibrium sets. Rédei [83, Theorem 10] proved that every non-trivial equilibrium set arises from the trivial ones. We reformulate his theorem in the following way:

LEMMA 3.1.9. *Let $p_1, \dots, p_r, \tilde{p}_1, \dots, \tilde{p}_s$ be (not necessarily distinct) prime divisors of n and let*

$$A := \bigcup_{i=1}^{r} [a_i, n, p_i], \qquad B := \bigcup_{j=1}^{s} [b_j, n, \tilde{p}_j]$$

for some values $a_i, b_j \in \mathbb{Z}_n$, $i = 1, \dots, r$, $j = 1, \dots, s$. If $B \subseteq A$, then $A \backslash B$ is an equilibrium set. In particular, all equilibrium sets are of this form.

This lemma not only includes every equilibrium set, but, on top of that, also yields a construction of sets $S, T \subseteq \mathbb{Z}_n$ satisfying (3): we observe that for every prime divisor p of n we have that

$$-\zeta_n^a = \sum_{j \in [a,n,p] \backslash \{a\}} \zeta_n^j. \tag{5}$$

Therefore, every equation of the form $G_{S,T,1,l}(\zeta_n) = 0$ is equivalent to an equation of the form

$$\sum_{j \in \mathrm{Eq}(S,T,l,p)} \zeta_n^j = 0,$$

with an equilibrium set $\mathrm{Eq}(S, T, l, p)$ which depends on S, T, p and l only. Thus, in particular, we can construct every pair of sets $S, T \subseteq \mathbb{Z}_n$ satisfying (3) from an equilibrium set. This yields a new way to construct non-trivial isospectral circulant graphs:

THEOREM 3.1.10. *Let $n \in 4\mathbb{N}$ and $\mathrm{Eq} := \bigcup_{i=1}^{r} [a_i, n, d]$ be an equilibrium set for pairwise disjoint sets $[a_i, n, d]$ and for d being an even divisor of n such that all elements of* Eq *are odd. Let S be a set containing exactly half of the elements of each set $[a_i, n, d]$ for $i = 1, \dots, r$ and let either $T := \mathrm{Eq} \backslash S$ or $T := \mathrm{Eq} \backslash S + \frac{n}{2} = \{t + \frac{n}{2} \mid t \in \mathrm{Eq} \backslash S\}$. Then, for every set $Z \subseteq 2\mathbb{Z}_n$, the circulant graphs $\mathrm{Cay}(\mathbb{Z}_n, S \cup Z)$ and $\mathrm{Cay}(\mathbb{Z}_n, T \cup Z)$ are isospectral.*

PROOF. Let $T = \mathrm{Eq} \backslash S$ and define

$$\sigma_1 : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n, \quad k \mapsto \begin{cases} k + \frac{n}{2}, & \text{if } d \nmid k, \\ k, & \text{if } d \mid k. \end{cases}$$

Obviously, the map σ_1 is bijective. We show that σ_1 is a spectral bijection of $S \cup Z$ and $T \cup Z$.

We observe that for every $k \in \mathbb{Z}_n$ with $d \mid k$ we have

$$0 = \sum_{j \in \mathrm{Eq}} \zeta_n^{jk} = \sum_{s \in S} \zeta_n^{sk} + \sum_{t \in T} \zeta_n^{tk},$$

or, equivalently,

$$\sum_{s \in S} \zeta_n^{sk} = -\sum_{t \in T} \zeta_n^{tk} = \sum_{t \in T} \zeta_n^{t(k + \frac{n}{2})}$$

since every $t \in T$ is odd. Moreover, we get

$$\sum_{z\in Z} \zeta_n^{z(k+\frac{n}{2})} = \sum_{z\in Z} \mathrm{e}\left(\frac{zk}{n} + \frac{z}{2}\right) = \sum_{z\in Z} \zeta_n^{zk}$$

since $2 \mid z$ for every $z \in Z$. Therefore, $G_{S\cup Z,T\cup Z,k,\sigma_1(k)}(\zeta_n) = 0$ follows for all k with $d \nmid k$.

If d divides k, for every $i = 1, \ldots, r$ we observe that $k \cdot [a_i, n, d] \equiv \{ka_i, \ldots, ka_i\} \bmod n$. Since S and T contain the same number of elements of each set $[a_i, n, d]$, it follows that $kS \equiv kT \bmod n$ and, therefore, we get that $G_{S\cup Z,T\cup Z,k,\sigma_1(k)}(\zeta_n) = 0$. Thus, σ_1 is a spectral bijection of $S \cup Z$ and $T \cup Z$.

Now, let $T = \mathrm{Eq} \setminus S + \frac{n}{2}$ and define

$$\sigma_2 : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n, \quad k \mapsto \begin{cases} k + \frac{n}{2}, & \text{if } d \nmid k \text{ and } 2 \mid k, \\ k, & \text{otherwise.} \end{cases}$$

Then, for all $k \in \mathbb{Z}_n$ with $d \nmid k$ we get

$$0 = \sum_{j\in \mathrm{Eq}} \zeta_n^{jk} = \sum_{s\in S} \zeta_n^{sk} + \sum_{t\in T} \zeta_n^{(t-\frac{n}{2})k},$$

and

$$\sum_{s\in S} \zeta_n^{sk} = -\sum_{t\in T} \zeta_n^{(t-\frac{n}{2})k} = \begin{cases} \sum_{t\in T} \zeta_n^{tk}, & \text{if } 2 \nmid k, \\ -\sum_{t\in T} \zeta_n^{tk}, & \text{if } 2 \mid k. \end{cases}$$

If k is odd, then $G_{S\cup Z,T\cup Z,k,\sigma_2(k)}(\zeta_n) = 0$ obviously holds true, and since

$$-\sum_{t\in T} \zeta_n^{tk} = \sum_{t\in T} \zeta_n^{t(k+\frac{n}{2})} \quad \text{and} \quad \sum_{z\in Z} \zeta_n^{zk} = \sum_{z\in Z} \zeta_n^{z(k+\frac{n}{2})},$$

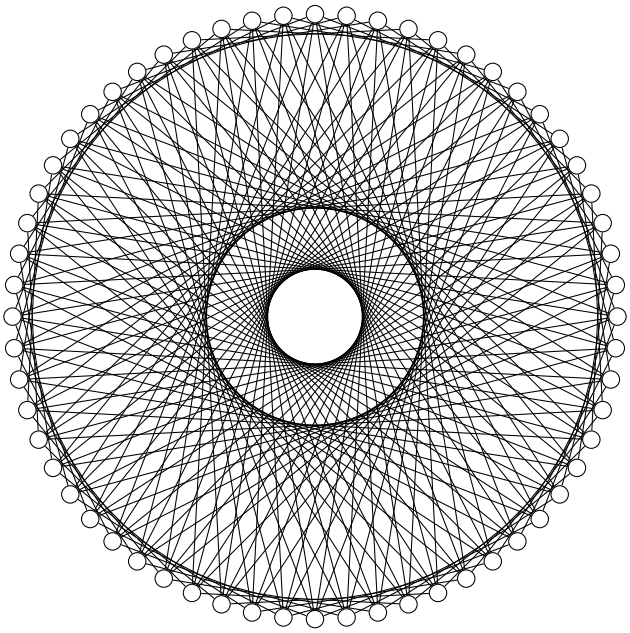
the equation is also true for all even k.

By the same argument as in the first case, again, we have $G_{S\cup Z,T\cup Z,k,\sigma_2(k)}(\zeta_n) = 0$ for all k with $d \mid k$. Therefore, σ_2 is a spectral bijection of $S \cup Z$ and $T \cup Z$. □

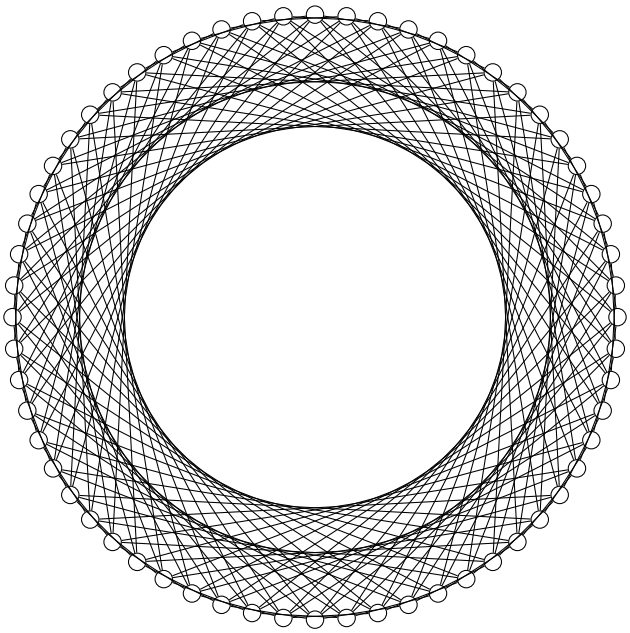
Note that the condition that all elements of Eq are odd is fulfilled if and only if a_i is odd for every $i = 1, \ldots, r$ and $\frac{n}{d}$ is even. Therefore, we assume $n \in 4\mathbb{N}$. We remark that this theorem provides an explicit construction of isospectral circulant graphs. Unfortunately, we cannot generalize this result simply by exploiting Equation (5) with $p > 2$.

Example 3.1.11. Let $n = 60$ and $\mathrm{Eq} := [\pm 3, 60, 6]$. Furthermore, define $S := \{\pm 23, \pm 33, \pm 53\} \subseteq \mathrm{Eq}$, $T_1 := \mathrm{Eq} \setminus S = \{\pm 3, \pm 13, \pm 43\}$ and $T_2 := \mathrm{Eq} \setminus S + 30 = \{\pm 13, \pm 33, \pm 43\}$. By Theorem 3.1.10, we get that for every set $Z \subseteq 2\mathbb{Z}_{60}$ the circulant graphs $\mathrm{Cay}(\mathbb{Z}_n, S \cup Z)$, $\mathrm{Cay}(\mathbb{Z}_n, T_1 \cup Z)$ and $\mathrm{Cay}(\mathbb{Z}_n, T_2 \cup Z)$ are isospectral. In particular, these graphs are undirected if and only if $Z \equiv -Z \bmod n$. If we choose, for example, $Z = \{2, 58\}$, then the circulant graphs $\mathrm{Cay}(\mathbb{Z}_n, S \cup Z)$, $\mathrm{Cay}(\mathbb{Z}_n, T_1 \cup Z)$ and $\mathrm{Cay}(\mathbb{Z}_n, T_2 \cup Z)$ are isospectral

with pairwise non-proportional connection sets. Moreover, we observe that $\mathrm{Cay}(\mathbb{Z}_n, S)$ is neither isomorphic to $\mathrm{Cay}(\mathbb{Z}_n, T_1)$ nor $\mathrm{Cay}(\mathbb{Z}_n, T_2)$, whereas $\mathrm{Cay}(\mathbb{Z}_n, T_1)$ and $\mathrm{Cay}(\mathbb{Z}_n, T_2)$ are isomorphic. Figure 3.2 shows the non-isomorphic isospectral circulant graphs $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T_1)$.



(a) $S = \{\pm 23, \pm 33, \pm 53\}$



(b) $T_1 = \{\pm 3, \pm 13, \pm 43\}$

FIGURE 3.2. Non-isomorphic isospectral circulant graphs.

3.1.3. Further examples of isospectral circulant graphs. Apart from the latter theorems, it seems that there are still several other ways to construct isospectral circulant graphs. For example, we can think of combining some of these results or exploiting the equilibrium sets in more complex ways as it is done in the following example:

EXAMPLE 3.1.12. We consider an example of a pair of cospectral circulant graphs with directed edges stated in the paper of Elspas and Turner [29]. Let $n = 32$ and $S = \{1, 2, 6, 18, 22, 25\}$, $T = \{2, 6, 7, 18, 22, 31\}$. We observe that the subset $\{2, 6, 18, 22\} \subseteq S, T$ is an equilibrium set which may be written as $\{2, 6, 18, 22\} = [2, 32, 2] \cup [6, 32, 2]$, i.e. the union of two arithmetic progression with common difference $\frac{32}{2} = 16$. We have that $\{1, 25\} \equiv 31 \cdot \{7, 31\} \bmod 32$ but there is no m with $\gcd(m, \frac{32}{2}) = 1$ satisfying $\{2, 6, 18, 22\} \equiv m \cdot \{2, 6, 18, 22\} \bmod 16$ and $\{1, 25\} \equiv m \cdot \{7, 31\} \bmod 16$. Therefore, Theorem 3.1.5 does not apply in this example. But the point here is that $2 \cdot \{1, 25\} \equiv \{2, 18\} \bmod 32$ and $2 \cdot \{7, 31\} \equiv \{14, 30\} \bmod 32$ are still equilibrium sets of common difference 16. Thus, it suffices to find m with $\gcd(m, \frac{32}{2^2}) = 1$ such that $\{2, 6, 18, 22\} \equiv m \cdot \{2, 6, 18, 22\} \bmod 8$ and $\{1, 25\} \equiv m \cdot \{7, 31\} \bmod 8$ hold true. Because then, the map

$$\sigma : \mathbb{Z}_{32} \longrightarrow \mathbb{Z}_{32}, \quad k \mapsto \begin{cases} 31k, & \text{if } 4 \nmid k, \\ mk, & \text{if } 4 \mid k \end{cases}$$

provides a spectral bijection of S and T. Indeed, $m = 7$ fulfills these requirements.

Thus, it is natural to ask how many pairs of isospectral or cospectral circulant graphs arise from the latter constructions (i.e. from Theorem 3.1.5, Theorem 3.1.7 and Theorem 3.1.10). This question was investigated by Witschel [103] and the author. As a foundation for our tests we used Muzychuk's algorithm [75] implemented by Berger [16] to generate a list of all non-isomorphic circulant graphs up to 21 vertices. On that basis, we computed the characteristic polynomials of those graphs and found all pairs of cospectral circulant graphs up to 21 vertices.

Within these examples we quickly found several pairs of cospectral circulant graphs which indeed do not arise from one of our above constructions. The smallest example is the following one:

EXAMPLE 3.1.13. Let $n = 12$, $S = \{5, 7, 11\}$ and $T = \{3, 9, 11\}$. Then, the graphs $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$ are isospectral, but it is straightforward to see that they do not arise from Theorem 3.1.5, Theorem 3.1.7 or Theorem 3.1.10.

Besides that, we developed an algorithm testing whether an isospectral pair of circulant graphs arises from the construction of Theorem 3.1.5 (unfortunately, for Theorem 3.1.7 and Theorem 3.1.10 we have not yet succeeded to implement one).

Before we present more details of our test results, we want to reference some theoretical results.

THEOREM 3.1.14 ([29, Corollary 2 and 3]). *Two circulant graphs on a prime number of vertices are isospectral if and only if their connection sets are proportional.*

Therefore, it is not interesting to consider circulant graphs on a prime number of vertices in order to find non-trivial pairs of isospectral circulant graphs. In view of our above observations, this is closely related to the following fact:

THEOREM 3.1.15 ([83, Satz 13]). *For a prime number p there are no equilibrium sets* $\mathrm{Eq} \subseteq \mathbb{Z}_p$ *except* $\{0\}$ *and* $\{0, 1, \ldots, p-1\}$.

For n being a product of two distinct primes, there are also some interesting results:

THEOREM 3.1.16 ([83, Satz 14]). *If n is a product of two distinct primes, then every equilibrium set* $\mathrm{Eq} \subseteq \mathbb{Z}_n$ *is trivial.*

THEOREM 3.1.17 ([8, Theorem 2]). *If n is a product of two distinct primes, then* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *and* $\mathrm{Cay}(\mathbb{Z}_n, T)$ *are isomorphic if and only if S and T are proportional.*

Table 3.1 shows our test results. The variable n therein denotes the number of vertices of the respective circulant graphs. Note that for $n < 10$ there are no pairs of cospectral circulant graphs. In view of Theorem 3.1.14, circulant graphs on a prime number of vertices are neglected.

TABLE 3.1. Cospectral pairs of circulant graphs up to 21 vertices.

n	Cospectral pairs	Arising from Theorem 3.1.5
10	2	2
12	50	8
14	48	48
15	10	10
16	476	276
18	1200	852
20	9922	1320
21	524	524

It is notable that (so far) all cospectral pairs of circulant graphs on n vertices arise from Theorem 3.1.5 if and only if n is a product of two distinct primes. Moreover, it is noticeable that for $n = 12$ only 16% of all examples arise from Theorem 3.1.5, whereas it is $\sim$58% for $n = 16$ and even 71% for $n = 18$. For $n = 20$ it goes back to only $\sim$13%. Hence, it seems that whenever n is of the form $4p$ for some prime number p, then only very few cospectral pairs of circulant graphs on n vertices arise from Theorem 3.1.5.

The first of our observations is certainly related to the above mentioned Theorem 3.1.16. It is clear that if n is a product of two distinct primes, then n is never of the form $4m$ for $m \in \mathbb{N}$ and, therefore, none of these examples arise from Theorem 3.1.10. Moreover, such examples never properly arise from Theorem 3.1.7 meaning that whenever an isospectral pair of circulant graphs on n vertices for n being a product of two distinct primes arises from Theorem 3.1.7, it already arises from Theorem 3.1.5. To show this, we assume that a connection set S contains the equilibrium sets $[a, n, p]$ and $[b, n, q]$ for $n = pq$ and $a, b \in \mathbb{Z}_n$. From Bézout's lemma we deduce that $[a, n, p]$ and $[b, n, q]$ intersect non-trivially which already contradicts the assumptions in Theorem 3.1.7. In view of all those observations, we conjecture that all pairs of isospectral circulant graphs on $n = pq$ vertices arise from Theorem 3.1.5, that is:

CONJECTURE 3.1.18. *Let $n = pq$ be a product of two distinct primes. Then,* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *and* $\mathrm{Cay}(\mathbb{Z}_n, T)$ *are isospectral if and only if S and T can be written as disjoint unions*

$$S = S' \cup \mathrm{Eq}_S \quad \text{and} \quad T = T' \cup \mathrm{Eq}_T,$$

for Eq_S *and* Eq_T *being trivial equilibrium sets of the form*

$$\mathrm{Eq}_S := \bigcup_{i=1}^{r} [a_i, n, d] \text{ and } \mathrm{Eq}_T := \bigcup_{i=1}^{r} [b_i, n, d],$$

for some $a_i, b_i \in \mathbb{Z}_n$, $d \in \{p, q\}$ and pairwise disjoint sets $[a_i, n, d]$ and $[b_i, n, d]$, respectively, such that there exist $l \in \mathbb{Z}_n^*$ and $m \in \mathbb{Z}_{\frac{n}{d}}^*$ with $S' \equiv lT' \bmod n$ and $S \equiv mT \bmod \frac{n}{d}$.

Together with Theorem 3.1.17 this would imply that constructions via Theorem 3.1.5 lead exactly to the cospectral pairs of circulant graphs on $n = pq$ vertices.

3.1.4. A new approach: Constructing isospectral circulant graphs from difference sets. For a set S let

$$\mathrm{D}(S) := \{s_1 - s_2 \mid s_1, s_2 \in S\}$$

denote the *difference set* of S (considered as a multiset).

Having a closer look at Example 3.1.13, it is notable that the respective difference sets

$$\mathrm{D}(S) = \{0^{[3]}, 2, 4, 6^{[2]}, 8, 10\} = \mathrm{D}(T)$$

of the two connection sets are the same. Thus, there might be a relation between isospectral circulant graphs and the associated difference sets. At least for undirected circulant graphs we could prove such connection and, therefore, found a new construction method for isospectral circulant graphs:

THEOREM 3.1.19. *Let $n \in \mathbb{N}$ be even and $S, T \subseteq \mathbb{Z}_n$ with $S \equiv -S \bmod n$ and $T \equiv -T \bmod n$. If $S, T \subseteq \mathbb{Z}_n \backslash 2\mathbb{Z}_n$ such that $\#S = \#T$ and $\mathrm{D}(S) \equiv m\,\mathrm{D}(T) \bmod n$, then the circulant graphs $\mathrm{Cay}(\mathbb{Z}_n, S), \mathrm{Cay}(\mathbb{Z}_n, T)$ are isospectral.*

PROOF. Since $T \sim mT$ (i.e. $\mathrm{Cay}(\mathbb{Z}_n, T)$ and $\mathrm{Cay}(\mathbb{Z}_n, mT)$ are isospectral, in particular) and $D(mT) \equiv mD(T) \bmod n$, we may assume w.l.o.g. that $D(S) \equiv D(T) \bmod n$. Now, let

$$\lambda_k = \sum_{s \in S} \zeta_n^{sk}, \quad \mu_k = \sum_{t \in T} \zeta_n^{tk}$$

denote the eigenvalues of $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$, respectively. Since $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$ are undirected graphs, all eigenvalues are real. Thus, we have that

$$\begin{aligned}\lambda_k^2 = \lambda_k \cdot \overline{\lambda_k} &= \Big(\sum_{s \in S} \zeta_n^{sk}\Big)\Big(\sum_{s \in S} \zeta_n^{-sk}\Big) = \sum_{s_1, s_2 \in S} \zeta_n^{(s_1 - s_2)k} = \sum_{d \in \mathrm{D}(S)} \zeta_n^{dk} = \\ &= \sum_{d \in \mathrm{D}(T)} \zeta_n^{dk} = \sum_{t_1, t_2 \in T} \zeta_n^{(t_1 - t_2)k} = \Big(\sum_{t \in T} \zeta_n^{tk}\Big)\Big(\sum_{t \in T} \zeta_n^{-tk}\Big) = \\ &= \mu_k \cdot \overline{\mu_k} = \mu_k^2,\end{aligned}$$

i.e. $\lambda_k = \pm\mu_k$. Now, let $0 \leq l < n$ with $l \equiv \frac{n}{2} + k \bmod n$. Then, we observe that

$$\lambda_l = \sum_{s \in S} \zeta_n^{s(\frac{n}{2}+k)} = \sum_{s \in S} \exp\Big(\pi i s + \frac{2\pi i s k}{n}\Big) = -\sum_{s \in S} \zeta_n^{sk} = -\lambda_k$$

since every $s \in S$ is odd, and the same holds true for the eigenvalues of $\mathrm{Cay}(\mathbb{Z}_n, T)$. Therefore, for all $0 \leq k < n$, we have that $\{\lambda_k, \lambda_l\} = \{\mu_k, \mu_l\}$ and, hence, $\mathrm{spec}(\mathrm{Cay}(\mathbb{Z}_n, S)) = \mathrm{spec}(\mathrm{Cay}(\mathbb{Z}_n, T))$. □

EXAMPLE 3.1.20. Let $n = 24$, $S = \{5, 7, 11, 13, 17, 19\}$ and $T = \{3, 9, 11, 13, 15, 21\}$. Then, we have that

$$\begin{aligned}\mathrm{D}(S) &= \{0^{[6]}, 2^{[3]}, 4^{[2]}, 6^{[4]}, 8^{[2]}, 10^{[2]}, 12^{[4]}, 14^{[2]}, 16^{[2]}, 18^{[4]}, 20^{[2]}, 22^{[3]}\} \\ &= D(T).\end{aligned}$$

Thus, by Theorem 3.1.19, the graphs $\mathrm{Cay}(\mathbb{Z}_{24}, S)$ and $\mathrm{Cay}(\mathbb{Z}_{24}, T)$ are isospectral. In particular, the graphs are neither isomorphic, nor the connection sets S and T are proportional.

3.2. The isomorphism problem for Cayley graphs

As already mentioned in the introduction, the isomorphism problem for circulant graphs was (in particular) solved by Muzychuk [75]. In fact, he solved an even more general problem, namley the isomorphism problem for so-called *colored* circulant graphs. He made his breakthrough by using the connection between (colored) Cayley graphs and Schur rings, and by studying Schur rings intensively.

We now give a survey on the most important basic results connecting Cayley graphs and Schur ring theory. Note that we rather focus on usual Cayley graphs than colored Cayley graphs, but we will use colored Cayley graphs in order to illustrate all graphical interpretations of the subsequent results. Unless indicated otherwise, all results are (implicitly) stated in [77, 76, 75].

In the following, we always consider the sets $\mathbb{Z}_n$ and C_n as the additive group of integers modulo n and the multiplicative cyclic group of order n, respectively.

3.2.1. Colored Cayley graphs. Let $\Pi = (P_1, \dots, P_r)$ be an ordered partition of a group G, i.e. $P_i \cap P_j = \emptyset$ for all $i, j = 1, \dots, r$ and $\bigcup_i P_i = G$. Then, the *colored Cayley graph* $\mathrm{Cay}(G, \Pi)$ is defined as the ordered tuple $(\mathrm{Cay}(G, P_1), \dots, \mathrm{Cay}(G, P_r))$ of Cayley graphs. Thus, every colored Cayley graph $\mathrm{Cay}(G, \Pi)$ can be considered as the complete graph $K_{\#G}$ with colored edges having the property that whenever $x - y \in P_i$ and $u - v \in P_i$ for some $i \in \{1, \dots, r\}$, the edges (x, y) and (u, v) are of the same color. An illustrating example is given in Figure 3.3. In particular, every Cayley graph $\mathrm{Cay}(G, S)$ can be considered as the colored Cayley graph $\mathrm{Cay}(G, (S, G \backslash S))$ (and here we can imagine the set $G \backslash S$ as the 'color' transparent).

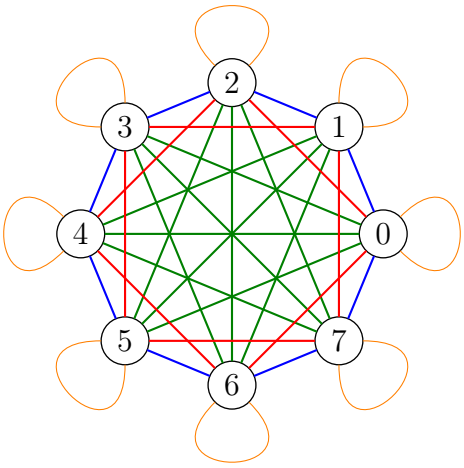


FIGURE 3.3. The (undirected) colored Cayley graph $\mathrm{Cay}(\mathbb{Z}_8, (\{0\}, \{1, 7\}, \{2, 6\}, \{3, 4, 5\}))$.

Two colored Cayley graphs $\mathrm{Cay}(G, (P_1, \ldots, P_r))$ and $\mathrm{Cay}(H, (S_1, \ldots, S_r))$ are called *isomorphic* if there exists a bijection $f : G \longrightarrow H$ such that $\mathrm{Cay}(G, P_i)^f = \mathrm{Cay}(H, S_i)$ for all $i = 1, \ldots, r$. Note that, in this case, if $0 \in P_i$, then $0 \in S_i$. The isomorphism problem for colored Cayley graphs is formulated in the same way as the one for usual Cayley graphs.

3.2.2. Schur ring theory. Schur rings over a group G are defined as algebraic objects, namely as special subalgebras of a group algebra $\mathbb{Q}G$. On the other hand, every Schur ring over a group G can be identified with a partition of G. Therefore, talking about Schur rings, we can also think about combinatorial objects (the partitions) equipped with some structure.

3.2.2.1. *Group algebras.* Let $(G, \bullet)$ be a finite group with group operation $\bullet$ and $(R, +, \cdot)$ be a ring. The *group algebra* RG of G over R is the set of all formal sums

$$\sum_{g \in G} \alpha_g g \quad \text{for } \alpha_g \in R,$$

equipped with two operations, addition

$$\sum_{g \in G} \alpha_g g + \sum_{g \in G} \beta_g g := \sum_{g \in G} (\alpha_g + \beta_g) g$$

and multiplication

$$\Big(\sum_{g \in G} \alpha_g g\Big)\Big(\sum_{h \in G} \beta_h h\Big) := \sum_{g,h \in G} (\alpha_g \cdot \beta_h)(g \bullet h).$$

In particular, RG is an R-module with scalar multiplication

$$\alpha\Big(\sum_{g \in G} \alpha_g g\Big) := \sum_{g \in G} (\alpha \cdot \alpha_g) g \quad \text{for } \alpha \in R.$$

Furthermore, for $k \in \mathbb{Z}$ and $x = \sum_{g \in G} \alpha_g g \in RG$, we define

$$x^{(k)} := \sum_{g \in G} \alpha_g (\underbrace{g \bullet g \bullet \ldots \bullet g}_{k \text{ times}}).$$

Note that if, for example, $x \in \mathbb{Q}C_n$, then $x^{(k)} = \sum_{g \in C_n} \alpha_g g^k$. In contrast, if $x \in \mathbb{Q}\mathbb{Z}_n$, then $x^{(k)} = \sum_{g \in \mathbb{Z}_n} \alpha_g (kg)$.

3.2.2.2. *Schur rings.* For a finite group $(G, \bullet)$ and a subset $S \subseteq G$ let

$$\underline{S} := \sum_{g \in S} g \in \mathbb{Q}G.$$

Elements of this form are called *simple quantities*. In the following, let e denote the identity element of G, and for $g \in G$ let g^{-1} denote the inverse element of g with respect to $\bullet$. A subalgebra $\mathcal{A}$ of the group

algebra $\mathbb{Q}G$ is called *Schur ring* (or *S-ring*) over G, if it satisfies the following properties:

(R1) $\mathcal{A}$ has a basis of simple quantities $\underline{S_0}, \dots, \underline{S_r}$, where $S_0 = \{e\}$,
(R2) $\{S_0, \dots, S_r\}$ is a partition of G (i.e. $S_i \cap S_j = \emptyset$ for all $i \neq j$ and $\bigcup_{i=0}^{r} S_i = G$),
(R3) $S_i^{-1} := \{s^{-1} \mid s \in S_i\} \in \{S_0, \dots, S_r\}$ for each $i \in \{0, \dots, r\}$.

Note that $\mathcal{A}$ being a subalgebra of $\mathbb{Q}G$ implies that $\mathcal{A}$ is closed under the group algebra multiplication (and, of course, also the group algebra addition, but this is fulfilled trivially), i.e. for every $i, j \in \{0, \dots, r\}$ there exist $p_{i,j}^k \in \mathbb{Q}$ such that

$$\underline{S_i}\underline{S_j} = \sum_{k=0}^{r} p_{i,j}^k \underline{S_k}.$$

Since for a given S-ring $\mathcal{A}$ the basis $\underline{S_0}, \dots, \underline{S_r}$ is uniquely determined, we may write $\mathcal{A} = \langle \underline{S_0}, \dots, \underline{S_r} \rangle$. The sets S_i are called the *basic sets* of $\mathcal{A}$ and we write $\mathrm{Basic}(\mathcal{A})$ for the set $\{S_0, \dots, S_r\}$.

3.2.2.3. *Schur partitions.* A partition $\{S_0, \dots, S_r\}$ of a group G is called *Schur partition* (or *S-partition*) if the subalgebra $\langle \underline{S_0}, \dots, \underline{S_r} \rangle$ of $\mathbb{Q}G$ generated by $\underline{S_0}, \dots, \underline{S_r}$ is an S-ring. Therefore, we may identify each S-rings over G with an S-partition of G.

In particular, if $(G, +)$ is an additive group, we can easily see that a partition $\{S_0, \dots, S_r\}$ is an S-partition if and only if it satisfies the following three conditions:

(P1) $S_0 = \{0\}$,
(P2) $-S_i \in \{S_0, \dots, S_r\}$,
(P3) Each multiset $S_i + S_j := \{s_i + s_j \mid s_i \in S_i, s_j \in S_j\}$ can be written as

$$S_i + S_j = \bigcup_{k=0}^{r} S_k^{[p_{i,j}^k]} \quad \text{for } p_{i,j}^k \in \mathbb{N}_0,$$

where $S_k^{[p_{i,j}^k]}$ denotes the multiset $\underbrace{S_k \cup \ldots \cup S_k}_{p_{i,j}^k \text{ times}}$.

In contrast to the (algebraic) definition of S-rings and S-partitions, the latter notation is more from a combinatorial perspective.

Example 3.2.1. We consider the partition

$$\mathbb{Z}_8 = \{\{0\}, \{1, 3, 5, 7\}, \{2, 6\}, \{4\}\}$$

of $\mathbb{Z}_8$ with $S_0 = \{0\}, S_1 = \{1, 3, 5, 7\}, S_2 = \{2, 6\}$ and $S_3 = \{4\}$. We can easily see that the condition (P1) is fulfilled trivially and (P2) is fulfilled since each set S_i is symmetric, i.e. $-S_i = S_i$ for $i = 0, 1, 2, 3$. Furthermore, the (i, j)-th entry of Table 3.2 equals the sum $S_i + S_j$ and, therefore, shows that (P3) also holds true. Thus, the partition

$\{S_0, S_1, S_2, S_3\}$ is an S-partition and the subalgebra $\langle \underline{S_0}, \ldots, \underline{S_r} \rangle$ of $\mathbb{Q}\mathbb{Z}_8$ is an S-ring.

TABLE 3.2. Addition table for $S_0 = \{0\}, S_1 = \{1,3,5,7\}, S_2 = \{2,6\}$ and $S_3 = \{4\}$ over $\mathbb{Z}_8$

	S_0	S_1	S_2	S_3
S_0	S_0	S_1	S_2	S_3
S_1	S_1	$S_0^{[4]} \cup S_2^{[4]} \cup S_3^{[4]}$	$S_1^{[2]}$	S_1
S_2	S_2	$S_1^{[2]}$	$S_0^{[2]} \cup S_3^{[2]}$	S_2
S_3	S_3	S_1	S_2	S_0

EXAMPLE 3.2.2. Now, we consider the same example but from a more algebraic point of view. In order not to confuse the elements of $\mathbb{Q}$ with the elements of a group G, it is common to write the respective group G multiplicatively. In the following, we denote the multiplicative cyclic group of order n by

$$C_n = \{e, g^1, \ldots, g^{n-1}\},$$

where g is a generator. Obviously, the partition in Example 3.2.1 is equivalent to the partition

$$C_8 = \{\{e\}, \{g^1, g^3, g^5, g^7\}, \{g^2, g^6\}, \{g^4\}\}.$$

In order to show that $\mathcal{A} := \langle e, g^1+g^3+g^5+g^7, g^2+g^6, g^4 \rangle$ is a subalgebra of $\mathbb{Q}C_8$, we have to verify that $\mathcal{A}$ is closed under the group algebra multiplication. This can be retraced in Table 3.3, where $\underline{S_0} := e$, $\underline{S_1} := g^1 + g^3 + g^5 + g^7$, $\underline{S_2} := g^2 + g^6$ and $\underline{S_3} := g^4$. It is no coincidence, of course, that the numbers $p_{i,j}^k$ from this example coincide with the ones from Example 3.2.1.

TABLE 3.3. Multiplication table for $\underline{S_0} = e$, $\underline{S_1} = g^1 + g^3 + g^5 + g^7$, $\underline{S_2} = g^2 + g^6$ and $\underline{S_3} = g^4$ over C_8

	$\underline{S_0}$	$\underline{S_1}$	$\underline{S_2}$	$\underline{S_3}$
$\underline{S_0}$	$\underline{S_0}$	$\underline{S_1}$	$\underline{S_2}$	$\underline{S_3}$
$\underline{S_1}$	$\underline{S_1}$	$4\underline{S_0} + 4\underline{S_2} + 4\underline{S_3}$	$2\underline{S_1}$	$\underline{S_1}$
$\underline{S_2}$	$\underline{S_2}$	$2\underline{S_1}$	$2\underline{S_0} + 2\underline{S_3}$	$\underline{S_2}$
$\underline{S_3}$	$\underline{S_3}$	$\underline{S_1}$	$\underline{S_2}$	$\underline{S_0}$

EXAMPLE 3.2.3. We now want to give some less specific examples of S-rings over a finite group G. Let e_G denote the identity element of G. It immediately follows from the definition of S-rings that $\mathbb{Q}G$ and $\langle \underline{\{e_G\}}, \underline{G \backslash \{e_G\}} \rangle$ are S-rings. Moreover, for a subgroup H of $\mathrm{Aut}(G)$, let

$$\mathbb{Q}G^H := \{\alpha \in \mathbb{Q}G \mid \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}.$$

Then, $\mathbb{Q}G^H$ is the largest subring of $\mathbb{Q}G$ which is fixed by the automorphism group H. It is shown in [65, Example 2.20, Theorem B.3] that $\mathbb{Q}G^H$ is always an S-ring, a so-called *orbit Schur ring*.

It is easy to see that the S-partition of $\mathbb{Q}G^H$ is the set of *orbits* $g^H := \{\sigma(g) \mid \sigma \in H\}$ of the group elements with respect to H.

3.2.2.4. *Schur rings and colored Cayley graphs.* There is a notable relation between Schur rings (or Schur partitions) and colored Cayley graphs. Let $\mathcal{A} = \langle \underline{S_0}, \ldots, \underline{S_r} \rangle$ be a Schur ring over a group G. Then, a basic set $S_i \in \mathrm{Basic}(\mathcal{A})$ corresponds to the (in general directed) Cayley graph $\mathrm{Cay}(G, S_i)$. Moreover, every colored Cayley graph $\mathrm{Cay}(G, \Pi)$ for any ordered partition Π of G into the basic sets S_i corresponds to the Schur ring $\mathcal{A}$. In particular, the union of the graphs $\mathrm{Cay}(G, S_i)$ yields any of those colored Cayley graphs $\mathrm{Cay}(G, \Pi)$.

EXAMPLE 3.2.4. Consider the Schur ring with Schur partition $\{\{0\}, \{1,3,5,7\}, \{2,6\}, \{4\}\}$ from Example 3.2.1. The graphs in Figure 3.4 illustrate the connection between (colored) Cayley graphs and this Schur ring.

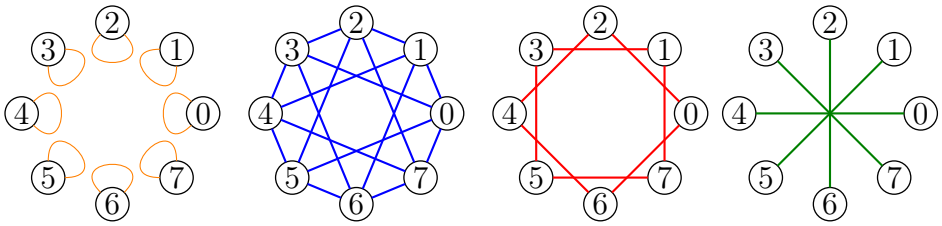
3.2.2.5. *The Schur-Hadamard product.* Let G be a group. The *Schur-Hadamard product* $\circ$ in the group algebra $\mathbb{Q}G$ is defined as

$$\Big(\sum_{g \in G} \alpha_g g\Big) \circ \Big(\sum_{g \in G} \beta_g g\Big) := \sum_{g \in G} (\alpha_g \cdot \beta_g) g.$$

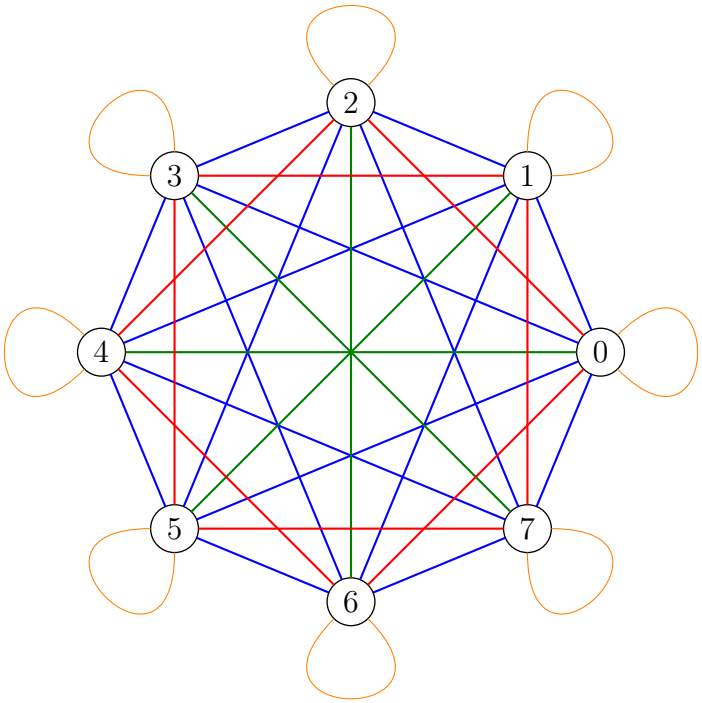
It is well-known that S-rings can be characterized in the following way (where e_G denotes the identity element of G):

THEOREM 3.2.5 ([73, Lemma 1.3]). *Let $\mathcal{A} \subseteq \mathbb{Q}G$ be a subalgebra of the group algebra $\mathbb{Q}G$. Then, $\mathcal{A}$ is an S-ring over G if and only if $\underline{e_G} \in \mathcal{A}$, $\underline{G} \in \mathcal{A}$ and $\mathcal{A}$ is closed with respect to $\circ$ and $^{(-1)}$.*

REMARK 3.2.6. It immediately follows from Theorem 3.2.5 that the intersection of S-rings over a group G is also an S-ring over the same group G.



$\mathrm{Cay}(\mathbb{Z}_8, \{0\})$ $\mathrm{Cay}(\mathbb{Z}_8, \{1,3,5,7\})$ $\mathrm{Cay}(\mathbb{Z}_8, \{2,6\})$ $\mathrm{Cay}(\mathbb{Z}_8, \{4\})$



Colored Cayley graph $\mathrm{Cay}(\mathbb{Z}_8, \Pi)$ for Π being any ordered partition of $\mathbb{Z}_8$ into the sets $\{0\}, \{1,3,5,7\}, \{2,6\}$ and $\{4\}$.

FIGURE 3.4. Schur rings and (colored) Cayley graphs.

3.2.2.6. *Schur ring isomorphisms.* Two S-rings $\mathcal{A}$ and $\mathcal{B}$ are called *isomorphic*, notation $\mathcal{A} \cong \mathcal{B}$, if there exists a bijection $g : \mathrm{Basic}(\mathcal{A}) \longrightarrow \mathrm{Basic}(\mathcal{B})$ such that the map

$$f_g : \mathcal{A} \longrightarrow \mathcal{B}, \quad \sum \alpha_i \underline{S_i} \mapsto \sum \alpha_i \underline{g(S_i)}$$

is an isomorphism between the algebras $\mathcal{A}$ and $\mathcal{B}$. In this case, we call f_g an *S-ring isomorphism*. Note that the map f_g is an S-ring isomorphism if and only if it respects group algebra addition (this is trivial by definition of f_g) and multiplication (this is not trivial in general).

EXAMPLE 3.2.7. The following list is a list of all non-isomorphic S-partitions over $\mathbb{Z}_8$:

$$\{\{0\}, \{1,2,3,4,5,6,7\}\}$$
$$\{\{0\}, \{1,3,5,7\}, \{2,6,4\}\}$$
$$\{\{0\}, \{1,3,5,7,2,6\}, \{4\}\}$$
$$\{\{0\}, \{1,3,5,7\}, \{2,6\}, \{4\}\}$$
$$\{\{0\}, \{1,3,5,7\}, \{2\}, \{6\}, \{4\}\}$$
$$\{\{0\}, \{1,5\}, \{3,7\}, \{2\}, \{6\}, \{4\}\}$$
$$\{\{0\}, \{1,5\}, \{3,7\}, \{2,6\}, \{4\}\}$$
$$\{\{0\}, \{1,3\}, \{5,7\}, \{2,6\}, \{4\}\}$$
$$\{\{0\}, \{1,7\}, \{3,5\}, \{2,6\}, \{4\}\}$$
$$\{\{0\}, \{1\}, \{7\}, \{3\}, \{5\}, \{2\}, \{6\}, \{4\}\}$$

The subsequent theorem is a consequence of Theorem 3.2.5 and gives a better idea of how S-ring isomorphisms look like:

THEOREM 3.2.8 ([73, Proposition 1.4]). *Let f be an S-ring isomorphism between two S-rings $\mathcal{A} = \langle \underline{S_0}, \ldots, \underline{S_r} \rangle$ and $\mathcal{B} = \langle \underline{T_0}, \ldots, \underline{T_r} \rangle$. Then there exists a permutation $\sigma : \mathbb{Z}_r \longrightarrow \mathbb{Z}_r$ such that*

$$f(\underline{S_i}) = \underline{T_{\sigma(i)}} \quad \text{for } i = 0, \ldots, r.$$

3.2.2.7. *Generated Schur rings.*

THEOREM 3.2.9. *Let G be a group and $S \subseteq G$. Then there is a unique least S-ring which contains the element $\underline{S}$.*

PROOF. Assume that there are two non-isomorphic least S-rings $\mathcal{A}$ and $\mathcal{B}$ which contain $\underline{S}$. By Remark 3.2.6, the intersection $\mathcal{C} := \mathcal{A} \cap \mathcal{B}$ is also an S-ring over G which contains $\underline{S}$. Since $\mathcal{A}$ and $\mathcal{B}$ are non-isomorphic, $\mathcal{C}$ is a smaller S-ring than $\mathcal{A}$ and $\mathcal{B}$ that contains $\underline{S}$, a contradiction. □

Thus, in the following, let $\langle\langle S \rangle\rangle$ denote the least S-ring over G which contains $\underline{S}$ (for $S \subseteq G$).

Let $\langle\langle S \rangle\rangle = \langle \underline{S_0}, \ldots, \underline{S_r} \rangle$. Since $\underline{S} \in \langle\langle S \rangle\rangle$, we may write

$$\underline{S} = \sum_{i=1}^{r} p_i \underline{S_i},$$

and since $\underline{S}$ is a simple quantity, it follows that $p_i \in \{0, 1\}$ for $i = 1, \ldots, r$. Hence, S is a union of basic sets S_i. Therefore, we may also say that the respective S-partition of $\langle\langle S \rangle\rangle$ is the coarsest S-partition of G which refines $\{S, G \backslash S\}$.

3.2.2.8. *Cayley graph isomorphisms and Schur rings.* This section presents the main relation between Cayley graph isomorphisms and Schur rings.

THEOREM 3.2.10. *Let $f : G \longrightarrow H$ be a normalized isomorphism between the Cayley graphs* $\mathrm{Cay}(G, S)$ *and* $\mathrm{Cay}(H, T)$*, and let $\mathcal{A} = \langle \underline{S_0}, \ldots, \underline{S_r} \rangle$ be an S-ring over G which contains the element $\underline{S}$. Then there exists an S-ring $\mathcal{B} = \langle \underline{T_0}, \ldots, \underline{T_r} \rangle$ over H which contains $\underline{T}$ such that f is a bijection between* $\mathrm{Basic}(\mathcal{A})$ *and* $\mathrm{Basic}(\mathcal{B})$ *which induces an isomorphism between $\mathcal{A}$ and $\mathcal{B}$.*

In particular,

$$\{\mathrm{Cay}(G, S_i)^f \mid i = 0, \ldots, r\} = \{\mathrm{Cay}(G, T_i) \mid i = 0, \ldots, r\}.$$

PROOF. Since $\mathcal{A}$ is an S-ring which contains $\underline{S}$, the set S can be written in the form

$$S = \dot{\bigcup_{i \in I}} S_i \quad \text{for } I \subseteq \{0, \ldots, r\}.$$

Moreover, since f is normalized (and a bijection), we have that

$$T = f(S) = f\Big(\dot{\bigcup_{i \in I}} S_i\Big) = \dot{\bigcup_{i \in I}} f(S_i) = \dot{\bigcup_{i \in I}} T_i \quad \text{for } T_i := f(S_i)$$

and, in addition, $f(S_0) = f(\{e_G\}) = \{f(e_G)\} = \{e_H\} =: T_0$. The same is true for the set $G \backslash (S \cup \{0\})$ and, therefore, we may define $T_i := f(S_i)$ for all $i = 0, \ldots, r$. Thus, f is a bijection between $\{S_0, \ldots, S_r\}$ and $\{T_0, \ldots, T_r\}$. It remains to show that the set $\langle \underline{T_0}, \ldots, \underline{T_r} \rangle$ is an S-ring, which is equivalent to $f^* : \sum \alpha_i \underline{S_i} \mapsto \sum \alpha_i \underline{f(S_i)}$ being an S-ring isomorphism. It is clear by definition that $\underline{f^*(S_i)} = \underline{f(S_i)} = \underline{T_i}$. The only thing left to verify is that f^* preserves group algebra multiplication, because then we also have that

$$\underline{T_i}\,\underline{T_j} = f^*(\underline{S_i}) f^*(\underline{S_j}) = f^*(\underline{S_i}\,\underline{S_j}) = f^*\Big(\sum_{k=0}^{r} p_{i,j}^k \underline{S_k}\Big) = \\ = \sum_{k=0}^{r} p_{i,j}^k f^*(\underline{S_k}) = \sum_{k=0}^{r} p_{i,j}^k \underline{T_k}.$$

Now, we show that the equation $f^*(\underline{S_i}) f^*(\underline{S_j}) = f^*(\underline{S_i}\,\underline{S_j})$ indeed holds true: For a subset B of G, let $A(B)$ denote the adjacency matrix of $\mathrm{Cay}(G, B)$. Then, the map

$$\gamma : \sum_{i=0}^{r} \alpha_i \underline{S_i} \mapsto \sum_{i=0}^{r} \alpha_i A(S_i)$$

is an isomorphism between $\mathcal{A}$ and the vector space $\mathrm{Span}\{A(S_i) \mid i = 0, \ldots, r\}$, since it preserves addition due the fact that

$$\gamma(\underline{S_i} + \underline{S_j}) = A(S_i \cup S_j) = A(S_i) + A(S_j) = \gamma(\underline{S_i}) + \gamma(\underline{S_j}),$$

and multiplication since

$$\gamma(\underline{S_i}\underline{S_j}) = A(S_i + S_j) = A(S_i)A(S_j) = \gamma(\underline{S_i})\gamma(\underline{S_j}).$$

Now, since f is an isomorphism between $\mathrm{Cay}(G,S)$ and $\mathrm{Cay}(H,T)$ which maps S_i onto T_i, we particularly have that

$$\mathrm{Cay}(G,S_i)^f = \mathrm{Cay}(G,T_i) \quad \text{for } i = 0,\dots,r.$$

Thus, there exists a permutation matrix P such that

$$A(f(S_i)) = P^{-1}A(T_i)P,$$

for $i = 0,\dots,r$. Let γ^{-1} denote the inverse mapping of γ, then we finally derive with

$$\begin{aligned} f^*(\underline{S_i})f^*(\underline{S_j}) &= \gamma^{-1}\big(A(f(S_i))\big)\gamma^{-1}\big(A(f(S_j))\big) \\ &= \gamma^{-1}\big(A(f(S_i))A(f(S_j))\big) \\ &= \gamma^{-1}\big(P^{-1}A(T_i)PP^{-1}A(T_j)P\big) \\ &= \gamma^{-1}\big(P^{-1}A(T_i)A(T_j)P\big) \\ &= \gamma^{-1}\big(P^{-1}A(T_i+T_j)P\big) \\ &= \gamma^{-1}\big(A\big(f(S_i+S_j)\big)\big) = f^*(\underline{S_i}\underline{S_j}). \end{aligned}$$

□

Remark 3.2.11. Theorem 3.2.10 can be illustrated in the following way: Let $f : G \longrightarrow H$ be a normalized isomorphism between the Cayley graphs $\mathrm{Cay}(G,S)$ and $\mathrm{Cay}(H,T)$, and let $\mathcal{A} = \langle \underline{S_0},\dots,\underline{S_r}\rangle$ be an S-ring over G which contains the element $\underline{S}$. Then, we may write

$$S = \dot{\bigcup_{i\in I}} S_i \quad \text{for } I \subseteq \{0,\dots,r\}.$$

Let $C = \{0,\dots,r\}$ be a set of colors. We color all edges (x,y) of $\mathrm{Cay}(G,S)$ satisfying $x - y \in S_i$ with the color $i \in C$. Analogously, we color all edges (x,y) of $\mathrm{Cay}(H,T)$ satisfying $f(x) - f(y) \in f(S_i)$ with the color $i \in C$. Then, Theorem 3.2.10 says that the isomorphism f maps all edges from $\mathrm{Cay}(G,S)$ of color i to all edges of $\mathrm{Cay}(H,T)$ of the same color. If $x - y \notin S$, we may think of edges having the color 'transparent'.

Corollary 3.2.12. *Let $f : G \longrightarrow H$ be a normalized isomorphism between the Cayley graphs $\mathrm{Cay}(G,S)$ and $\mathrm{Cay}(H,T)$. Then f is also an S-ring isomorphism between $\langle\langle S\rangle\rangle$ and $\langle\langle T\rangle\rangle$. In particular,*

$$\#\mathrm{Basic}(\langle\langle S\rangle\rangle) = \#\mathrm{Basic}(\langle\langle T\rangle\rangle).$$

Consequently, if $\langle\langle S\rangle\rangle$ and $\langle\langle T\rangle\rangle$ are non-isomorphic, then $\mathrm{Cay}(G,S)$ and $\mathrm{Cay}(H,T)$ are non-isomorphic.

PROOF. Let $\langle\langle S\rangle\rangle = \langle \underline{S_0}, \dots, \underline{S_r}\rangle$ and $\langle\langle T\rangle\rangle = \langle \underline{T_0}, \dots, \underline{T_{r'}}\rangle$. Without loss of generality, let $r \geq r'$ (otherwise, consider f^{-1}). We assume that $r > r'$. Then, by Theorem 3.2.10, there is an S-ring over H containing T which is isomorphic to $\langle\langle S\rangle\rangle$, a contradiction to the definition of $\langle\langle T\rangle\rangle$. Thus, we have that $r = r'$. Furthermore, since by Theorem 3.2.9 there are no other S-rings over G or H with $r+1$ basic sets which contain $\underline{S}$ or $\underline{T}$, respectively, the statement follows from Theorem 3.2.10. □

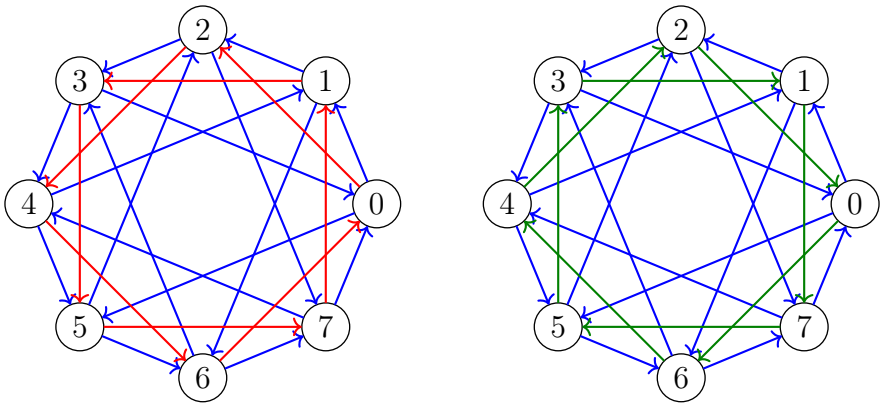
From the latter results we deduce the following main observations:

(1) If $\langle\langle S\rangle\rangle$ and $\langle\langle T\rangle\rangle$ are non-isomorphic, then $\mathrm{Cay}(G, S)$ and $\mathrm{Cay}(H, T)$ are non-isomorphic.
(2) Two Cayley graphs $\mathrm{Cay}(G, S)$ and $\mathrm{Cay}(H, T)$ are isomorphic only if for each S-ring $\mathcal{A}$ with $\underline{S} \in \mathcal{A}$, there is an S-ring $\mathcal{B}$ (of the same size as $\mathcal{A}$) with $\underline{T} \in \mathcal{B}$ such that there is an S-ring isomorphism between $\mathcal{A}$ and $\mathcal{B}$ which maps $\underline{S}$ onto $\underline{T}$.
(3) In particular, two Cayley graphs $\mathrm{Cay}(G, S)$ and $\mathrm{Cay}(H, T)$ are isomorphic only if there is an S-ring isomorphism between $\langle\langle S\rangle\rangle$ and $\langle\langle T\rangle\rangle$ which maps $\underline{S}$ onto $\underline{T}$.

Note that the other direction of statement (2) is not true in general, i.e. not every Schur ring isomorphism induces a Cayley graph isomorphism.

EXAMPLE 3.2.13. We consider the circulant graph $\mathrm{Cay}(\mathbb{Z}_8, S)$ for $S = \{1, 2, 5\}$. In the list of Example 3.2.7 we can see that the partition $\{\{0\}, \{1, 5\}, \{3, 7\}, \{2\}, \{6\}, \{4\}\}$ is the coarsest partition which refines $\{\{1, 2, 5\}, \{0, 3, 4, 6, 7\}\}$. Thus, $\langle\langle S\rangle\rangle = \langle \underline{\{0\}}, \underline{\{1, 5\}}, \underline{\{3, 7\}}, \underline{\{2\}}, \underline{\{6\}}, \underline{\{4\}}\rangle$ is the least S-ring which contains $\underline{S}$. Moreover, the permutation $(2\ 6)(3\ 7)$ is a normalized isomorphism between $\mathrm{Cay}(\mathbb{Z}_8, S)$ and the graph $\mathrm{Cay}(\mathbb{Z}_8, T)$ for $T = \{1, 5, 6\}$. By coloring $\mathrm{Basic}(\langle\langle S\rangle\rangle) = \mathrm{Basic}(\langle\langle T\rangle\rangle)$ like $\{\{0\}, \{1, 5\}, \{3, 7\}, \{2\}, \{6\}, \{4\}\}$, we observe that f maps red edges to green edges (and the other way round) and edges of any other color c to edges of the same color c. Figure 3.5 illustrates the isomorphic circulant graphs $\mathrm{Cay}(\mathbb{Z}_8, \{1, 2, 5\})$ and $\mathrm{Cay}(\mathbb{Z}_8, \{1, 5, 6\})$. Note that this was one of the first stated counterexamples to Ádám's conjecture (cf. [29]).

3.2.2.9. *Schur rings over cyclic groups.* Section 3.2.2.8 shows that there is a deep connection between isomorphisms of Cayley graphs and the structure of S-rings. Thus, given a group G, it is helpful to study S-ring isomorphisms in order to solve the isomorphism problem for Cayley graphs over G. An important step for Muzychuk's [75] solution to the isomorphism problem for circulant graphs was to gain insight into the structure of S-rings over cyclic groups and their isomorphisms. In [73], he obtained the following fundamental result:



$\mathrm{Cay}(\mathbb{Z}_8, \{1, 2, 5\})$ $\mathrm{Cay}(\mathbb{Z}_8, \{1, 5, 6\})$

FIGURE 3.5. Two isomorphic Cayley graphs.

THEOREM 3.2.14 ([73, Theorem 1.1]). *Two S-rings over the same cyclic group are isomorphic if and only if they coincide.*

To prove this theorem, Muzychuk showed the following statement:

THEOREM 3.2.15 ([73, Theorem 1.1']). *Let $f : \mathcal{A} \longrightarrow \mathcal{B}$ be an S-ring isomorphism between two S-rings over the same cyclic group, and let S be a basic set of $\mathcal{A}$. Then*

$$f(\underline{S}) = \underline{S}^{(m)} \quad \text{for } m \in \mathbb{Z}_n^*.$$

Note that, by definition, if $S \subseteq \mathbb{Z}_n$, then $\underline{S}^{(m)} = \underline{mS}$ for $mS = \{ms \mid s \in S\}$.

REMARK 3.2.16. Theorem 3.2.14 (together with Theorem 3.2.10) implies that every Cayley graph isomorphism between Cayley graphs over cyclic groups induces an S-ring *automorphism*.

Recall from the introduction that for a divisor $d \neq n$ of n the set $G_n(d)$ is defined as

$$G_n(d) := \{x \in \mathbb{Z}_n \mid \gcd(x, n) = d\}.$$

Now, for a set $S \subseteq \mathbb{Z}_n$ let

$$(S)_d := S \cap G_n(d).$$

The subset $(S)_d$ is called the *d-th layer* of S. With the latter results it is indeed not much left to prove the following theorem which was published in [76] called 'Zibin's conjecture' (and already proven in [77, Theorem 2.10]):

THEOREM 3.2.17 (Zibin's conjecture). *Let $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$ be two isomorphic circulant graphs. Then, for each divisor d of n there exists $m_d \in \mathbb{Z}_n^*$ such that $m_d(S)_d = (T)_d$.*

In other words, the theorem states that if $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$ are isomorphic, then the respective d-th layers of S and T are proportional. This indicates that Ádám's conjecture [3] was indeed not that wrong, but a bit too naive.

In the following, let $S, T \subseteq \mathbb{Z}_n$. We summarize some basic observations in Figure 3.6.

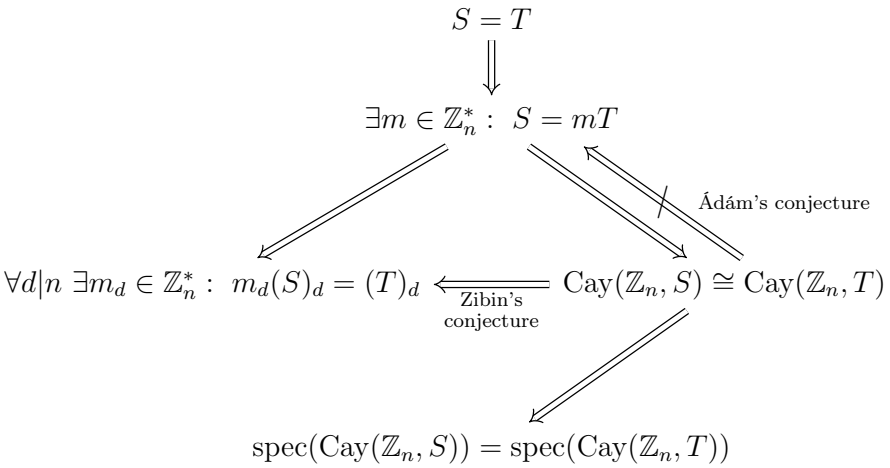


FIGURE 3.6. Overview: Circulant graph isomorphisms.

3.3. Integral circulant graphs

Recall So's characterization of integral circulant graphs:

THEOREM 3.3.1 ([92, Theorem 7.1]). *A circulant graph* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *is integral if and only if* S *is a union of* $G_n(d)$*-sets for proper divisors* d *of* n*.*

In his paper, So [92] restricted his considerations to simple circulant graphs. But his proof actually works for directed circulant graphs as well. Since, therefore, the connection set of *every* integral circulant graph is a union of $G_n(d)$-sets, and since every $G_n(d)$-set is symmetric, we immediately get the following:

THEOREM 3.3.2. *Every integral circulant graph is an undirected graph.*

Moreover, only with a tiny adaption of his proof, it is easy to see that Theorem 3.3.1 also remains true for $d = n$ with $G_n(n) := \{0\}$. Note that if $G_n(n) \in S$, then the respective graph $\mathrm{Cay}(\mathbb{Z}_n, S)$ has loops.

We briefly want to sketch So's proof of Theorem 3.3.1: By considering Ramanujan sums it is easy to see that $\mathrm{Cay}(\mathbb{Z}_n, S)$ is integral if S is a union of $G_n(d)$-sets. For the other direction let $\mathbf{v}_d \in \mathbb{R}^n$ be the vector with 1 at the j-th entry for all $j \in G_n(d)$, and 0 elsewhere.

Furthermore, let F be the $(n \times n)$-matrix with the (i,j)-th entry ζ_n^{ij} and $i,j = 0,\dots,n-1$. Note that F is invertible and, if $\mathbf{v}$ denotes the vector with 1 at the j-th entry for all $j \in S$ and 0 otherwise, then

$$F\mathbf{v} = (\lambda_0(S), \lambda_1(S), \dots, \lambda_{n-1}(S)), \tag{6}$$

where $\lambda_k(S) = \sum_{s\in S} \zeta_n^{sk}$ denotes the k-th eigenvalue of $\mathrm{Cay}(\mathbb{Z}_n, S)$. Sander and Sander [87] called this vector the *spectral vector* of $\mathrm{Cay}(\mathbb{Z}_n, S)$. Now, it can be shown that the vectors $\mathbf{v}_d$ provide a basis of the vector space $\mathcal{A} := \{\mathbf{v} \in \mathbb{Q}^n \mid F\mathbf{v} \in \mathbb{Q}^n\}$ (cf. [92, Corollary 6.3]). Therefore, if the spectral vector

$$F\mathbf{v} = (\lambda_0(S), \lambda_1(S), \dots, \lambda_{n-1}(S))$$

of $\mathrm{Cay}(\mathbb{Z}_n, S)$ has rational entries only, then $\mathbf{v} \in \mathcal{A}$ and, therefore, $\mathbf{v}$ can be written as

$$\mathbf{v} = \sum_{d|n} c_d \mathbf{v}_d.$$

Since $\mathbf{v}$ and the $\mathbf{v}_d$'s are $(0,1)$-vectors, the coefficients c_d are either 0 or 1 and, consequently, S is a union of $G_n(d)$-sets (for those d where $c_d = 1$).

Now, recall So's conjecture:

Conjecture 3.3.3 (So's conjecture). *Let* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *and* $\mathrm{Cay}(\mathbb{Z}_n, T)$ *be integral circulant graphs. If* $S \neq T$ *then* $\mathrm{spec}(\mathrm{Cay}(\mathbb{Z}_n, S)) \neq \mathrm{spec}(\mathrm{Cay}(\mathbb{Z}_n, T))$*, hence* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *and* $\mathrm{Cay}(\mathbb{Z}_n, T)$ *are non-isomorphic.*

In 2015, Sander and Sander [87] proved an allegedly weaker version of So's conjecture, namely (implicitly) that two integral circulant graphs are isomorphic if and only if their spectral vectors are the same. But in view of (6) it immediately follows that circulant graphs with different connection sets never have the same spectral vector (not even if they are isomorphic). Thus, the theorem of Sander and Sander is trivial and should not be considered a weaker version of So's conjecture.

3.3.1. So's conjecture and Schur rings. Unfortunately, by now there seem to be no promising approach for solving So's conjecture completely. At least we could solve the isomorphism part of So's conjecture with the Schur ring theory of Section 3.2.2. In fact, the statement follows directly from Zibin's conjecture 3.2.17:

Theorem 3.3.4. *Let* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *and* $\mathrm{Cay}(\mathbb{Z}_n, T)$ *be integral circulant graphs. If* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *and* $\mathrm{Cay}(\mathbb{Z}_n, T)$ *are isomorphic, then* $S = T$.

Proof. Let $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$ be integral circulant graphs and let d be a divisor of n. By Theorem 3.2.17 there exists $m_d \in \mathbb{Z}_n^*$ with

$$m_d(S)_d = (T)_d. \tag{7}$$

Since $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$ are integral, by So's characterization we observe that $(S)_d = S \cap G_n(d) \in \{\emptyset, G_n(d)\}$ and also $(T)_d = T \cap G_n(d) \in \{\emptyset, G_n(d)\}$. Thus, from (7) we deduce $(S)_d = (T)_d$. Moreover, since the $G_n(d)$-sets form a partition of $\mathbb{Z}_n$, we have that

$$S = \bigcup_{d|n} (S)_d \quad \text{and} \quad T = \bigcup_{d|n} (T)_d.$$

Therefore, we finally conclude $S = T$. □

In particular, this shows that Ádám's conjecture is true for integral circulant graphs. Moreover, as an easy consequence we may deduce

COROLLARY 3.3.5. *Let $\tau(n)$ be the number of divisors of n. Then there are exactly $2^{\tau(n)}$ (or $2^{\tau(n)-1}$ loop-free) non-isomorphic integral circulant graphs on n vertices.*

Note that the latter results were already published in [53].

We also want to mention that it is not even necessary to use Zibin's conjecture for the proof. It actually appears more natural within the theory of Schur rings in the following way:

PROPOSITION 3.3.6. *Let $\{d_1, \ldots, d_s\}$ denote the set of divisors of n. Then, the partition $\{G_n(d_1), \ldots, G_n(d_s)\}$ of $\mathbb{Z}_n$ is always an S-partition.*

PROOF. Recall the definition of orbit Schur rings from Example 3.2.3. Now, the $G_n(d)$-sets are exactly the orbits of the elements of $\mathbb{Z}_n$ with respect to the group $\mathrm{Aut}(\mathbb{Z}_n) = \mathbb{Z}_n^*$. Thus, $\{G_n(d_1), \ldots, G_n(d_s)\}$ is the S-partition of the orbit Schur ring for $H = \mathrm{Aut}(\mathbb{Z}_n)$. □

In the following, we call the S-ring $\langle \underline{G_n(d_1)}, \ldots, \underline{G_n(d_s)} \rangle$ the $G_n(d)$-*ring*. In fact, in the literature, every subring of the $G_n(d)$-ring which is a Schur ring is called *rational Schur ring* ([21, 22, 72, 53]).

ALTERNATIVE PROOF OF THEOREM 3.3.4. Since $\mathrm{Cay}(\mathbb{Z}_n, S)$ is integral, we my write

$$S = \bigcup_{d \in D} G_n(d) \quad \text{for } D \subseteq \{d \in \mathbb{Z}_n \mid d|n\}.$$

Thus, the $G_n(d)$-ring is an S-ring which contains $\underline{S}$. Since $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$ are isomorphic, there exists a normalized isomorphism f between them which maps S onto T. By Theorem 3.2.10, the map f induces an isomorphism f^* between the $G_n(d)$-ring and an S-ring $\mathcal{B}$ which contains $\underline{T}$. From Theorem 3.2.14 we deduce that, therefore, $\mathcal{B}$ is also the $G_n(d)$-ring. Moreover, by Theorem 3.2.15, we have that $\underline{T} = f^*(\underline{S}) = \underline{S}^{(m)} = \underline{mS} = \underline{S}$ for $m \in \mathbb{Z}_n^*$. The last equation holds true since $mG_n(d) = G_n(d)$ for all divisors d of n. Therefore, $S = T$. □

Note that, conversely, if the circulant graph $\mathrm{Cay}(\mathbb{Z}_n, S)$ is non-integral, then the S-ring $\langle\langle S\rangle\rangle$ is not contained in the $G_n(d)$-ring. Hence, it is easy to prove that there always exists a non-trivial automorphism of $\langle\langle S\rangle\rangle$ which induces an isomorphism between $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$ for $S \neq T$. This leads us to the following theorem:

THEOREM 3.3.7. *Integral circulant graphs are the only circulant graphs which are uniquely determined by their connection set, i.e. if* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *is not integral, then there is* $T \neq S$ *with* $\mathrm{Cay}(\mathbb{Z}_n, S) \cong \mathrm{Cay}(\mathbb{Z}_n, T)$.

PROOF. Let $\mathrm{Cay}(\mathbb{Z}_n, S)$ be a circulant graph. We already know that the map $f : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n, x \mapsto mx$ for $m \in \mathbb{Z}_n^*$ is an isomorphism between the graphs $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, mS)$. Now, if $\mathrm{Cay}(\mathbb{Z}_n, S)$ is non-integral, then there exist a divisor d of n and $s_1, s_2 \in G_n(d)$ with $s_1 \in S$ and $s_2 \notin S$. Moreover, since $\gcd(s_1, n) = \gcd(s_2, n)$, there is $m \in \mathbb{Z}_n^*$ with $s_2 = ms_1$. Thus, $\mathrm{Cay}(\mathbb{Z}_n, S) \cong \mathrm{Cay}(\mathbb{Z}_n, mS)$ and $S \neq mS$. □

To sum up, the overview in Figure 3.6 changes for integral circulant graphs to the following one in Figure 3.7.

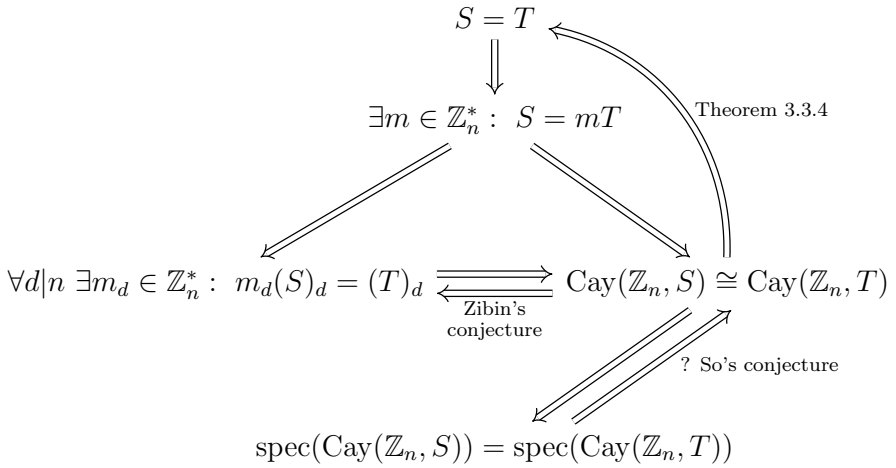


FIGURE 3.7. Overview: Integral circulant graph isomorphisms.

3.3.2. So's conjecture and a result of Vilfred. In [98] Vilfred stated the following theorem:

THEOREM 3.3.8 ([98, Theorem 3]). *If* $\mathrm{Cay}(\mathbb{Z}_n, S) \cong \mathrm{Cay}(\mathbb{Z}_n, T)$, *then there is a bijection* f *from* S *to* T *such that for all* $s \in S$,

$$\gcd(n, s) = \gcd(n, f(s)).$$

He remarked that the proof would be by induction on the order of S and that details could be found in his Ph.D. thesis [97]. But in the section where he proved this theorem in his thesis, he restricted himself to circulant graphs with proportional connection sets. Of course, the statement is true since it is an easy consequence of Zibin's conjecture, but we are questioning the accuracy of Vilfred's elementary proof.

In fact, the isomorphism part of So's conjecture already follows from Vilfred's theorem:

Second alternative proof of Theorem 3.3.4. Let $s \in S$ and $d = \gcd(s, n)$. Since $\mathrm{Cay}(\mathbb{Z}_n, S)$ is integral, by Theorem 3.3.1 $G_n(d) \subseteq S$. Moreover, by Theorem 3.3.8 there is an element $t \in T$ with $\gcd(t, n) = d$. Again, since $\mathrm{Cay}(\mathbb{Z}_n, T)$ is integral, $G_n(d) \subseteq T$ follows. Therefore, we may conclude that S and T are unions of $G_n(d)$-sets for the same divisors d of n and, hence, $S = T$. □

Thus, assuming Vilfred's proof of Theorem 3.3.8 to be correct implies that there is a simple combinatorial proof of the isomorphism part of So's conjecture where no Schur ring theory is needed.

3.3.3. On the spectral part of So's conjecture. As already mentioned, the spectral part of So's conjecture is still an open problem. However, So [92] verified his conjecture at least for n being a prime power or n being a product of two distinct primes. We now prove that it is also true for $n = p^2q$ where p and q are distinct odd primes.

We use a combinatorial approach exploiting the fact that isospectral undirected graphs $\mathcal{G}, \mathcal{H}$ have the same number of closed walks of length k for all $k \in \mathbb{N}$. This can easily be seen as follows: The (i, j)-th entry of the matrix $A(\mathcal{G})^k$ equals the number of walks from vertex i to vertex j in $\mathcal{G}$ of length k (see, for example, [24, Proposition 1.3.1]). Thus, $\mathrm{tr}(A(\mathcal{G})^k)$ is the total number of closed walks of length k in $\mathcal{G}$. Since $A(\mathcal{G})$ is symmetric, it is similar to the diagonal matrix $D(\mathcal{G})$ with diagonal entries λ_i, where $\lambda_0, \ldots, \lambda_{n-1}$ denote the eigenvalues of $\mathcal{G}$. Since $\mathrm{tr}(A(\mathcal{G})^k) = \mathrm{tr}(D(\mathcal{G})^k)$ and $\mathrm{tr}(D(\mathcal{G})^k) = \mathrm{tr}(D(\mathcal{H})^k)$ whenever $\mathcal{G}$ and $\mathcal{H}$ are isospectral, the statement follows. In particular, for $k = 1$ this shows that $\mathcal{G}$ and $\mathcal{H}$ are isospectral only if they have the same number of loops. Thus, in the following, we may restrict our considerations to simple graphs.

Now, let $\mathrm{Cay}(\mathbb{Z}_n, S)$ be a simple circulant graph and let $(v_0, v_1, \ldots, v_{k-1}, v_k = v_0)$ be a closed walk of length k. Since v_i and v_{i+1} are adjacent, we may write $v_{i+1} - v_i \in S$, i.e. there is $s_i \in S$ such that $v_{i+1} - v_i = s_i$, i.e. $v_{i+1} = s_i + v_i$. Since $v_k = v_0$, we get that

$$0 = v_k - v_0 = s_{k-1} + v_{k-1} - v_0 = \ldots =$$

$$= s_{k-1} + s_{k-2} + \ldots + s_1 + s_k + v_0 - v_0 = \sum_{i=1}^{k} s_k.$$

Hence, there is a one-to-one correspondence between the number of closed walks of length k based at a fixed vertex v_0 in $\mathrm{Cay}(\mathbb{Z}_n, S)$ and the number of ways of expressing 0 as a sum of k (not necessarily distinct) elements of S. Since circulant graphs are vertex-transitive, the choice of the fixed vertex is immaterial.

This approach was undertaken in [34] and they proved the following:

THEOREM 3.3.9 ([34, Proposition 1]). *Let* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *be a simple circulant graph and let* p *be an odd prime. Let* $t_p(S)$ *be the total number of closed walks of length* p *based at a fixed vertex of* $\mathrm{Cay}(\mathbb{Z}_n, S)$*, and let* $r_p(S)$ *be the number of elements of (additive) order* p *in* S*. Then* $t_p(S) \equiv r_p(S) \bmod p$.

Note that with this notation the number of closed walks of length k in $\mathrm{Cay}(\mathbb{Z}_n, S)$ is given by $n \cdot t_k(S)$.

THEOREM 3.3.10. *Let* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *and* $\mathrm{Cay}(\mathbb{Z}_n, T)$ *be isospectral integral circulant graphs and let* p *be an odd prime divisor of* n*. Then* $G_n\left(\frac{n}{p}\right) \subseteq S$ *if and only if* $G_n\left(\frac{n}{p}\right) \subseteq T$.

PROOF. Since $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$ are integral, they are undirected graphs and S and T are unions of $G_n(d)$-sets (cf. Theorem 3.3.1 and 3.3.2). Moreover, as mentioned above, we may assume that $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$ are loop-free. By definition, all elements in $G_n\left(\frac{n}{p}\right)$ are of (additive) order p (which also implies that there are no other elements of order p in $\mathbb{Z}_n$ since the $G_n(d)$-sets form a partition of $\mathbb{Z}_n$). Thus, if $G_n\left(\frac{n}{p}\right) \subseteq S$, by Theorem 3.3.9 we have that

$$t_p(S) \equiv r_p(S) = \#G_n\left(\frac{n}{p}\right) = \varphi(p) = p - 1 \equiv -1 \bmod p,$$

where φ denotes Euler's totient function. Otherwise, if $G_n\left(\frac{n}{p}\right) \not\subseteq S$, then S contains no element of order p, i.e. $r_p(S) = 0$ and, hence, $t_p(S) \equiv 0 \bmod p$ by Theorem 3.3.9. Since $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$ are isospectral, we get that $n \cdot t_p(S) = n \cdot t_p(T)$ or, equivalently, $t_p(S) \equiv t_p(T) \bmod p$ and, therefore, the statement follows. □

THEOREM 3.3.11. *So's conjecture is true for* $n = p^2q$ *where* p *and* q *are distinct odd primes.*

PROOF. Let $n = p^2q$ for p, q being distinct odd primes. Moreover, let $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$ be two isospectral integral circulant graphs. Since isospectral graphs have the same number of edges, we have that $\#S = \#T$. We show that $\#S = \#T$ already implies $S = T$. Therefore, we may assume that S and T intersect trivially and, in view of Theorem 3.3.10, we may assume that $G_n(p^2), G_n(pq)$ are not contained in S nor T. Thus, S and T are unions of the sets $G_n(1), G_n(p)$ and $G_n(q)$. Note that $\#G_n(1) = \varphi(n) = p(p-1)(q-1)$, $\#G_n(p) = \varphi\left(\frac{n}{p}\right) = \varphi(pq) = (p-1)(q-1)$ and $\#G_n(q) = \varphi(p^2) = p(p-1)$. Since p

and q are odd, we have that $p \neq q-1$ and, therefore, $\#G_n(p) \neq \#G_n(q)$. Moreover, $\#G_n(1) > \#G_n(p), \#G_n(q)$. Thus, the only possibility left is (w.l.o.g.) the case $S = G_n(1)$ and $T = G_n(p) \cup G_n(q)$ which implies that $\#G_n(1) = \#G_n(p)+\#G_n(q)$, i.e. $p(p-1)(q-1) = (p-1)(q-1+p)$ or, equivalently, $p(q-1) = p+q-1$. Rearranging yields $q = \frac{2p-1}{p-1}$. Since q is an integer, it follows that $2p-1 \equiv 0 \bmod p-1$, i.e. $2p \equiv 1 \bmod p-1$. Moreover, since $p-1 \geq 2$ and $p \equiv 1 \bmod p-1$, this implies $2 \equiv 1 \bmod p-1$, a contradiction. Hence, $S = T$. □

REMARK 3.3.12. Note that this result is part of current research. We hope that in future work we can exploit Theorem 3.3.10 to verify other cases of So's conjecture. Another idea is to generalize Theorem 3.3.9 in order to extend Theorem 3.3.10.

3.4. The algebraic degree of circulant graphs

We now do not restrict our considerations to integral circulant graphs anymore but rather study the interplay between the algebraic degree of a circulant graph and its respective graph properties. In particular, we investigate the question of how deviation from structure of a connection set S is encoded in the algebraic degree of $\mathrm{Cay}(\mathbb{Z}_n, S)$. We first start with a more combinatorial approach and restrict ourselves to circulant graphs on a prime number of vertices. Subsequently, we determine precisely the splitting fields and algebraic degrees of arbitrary circulant graphs using Schur ring theory.

All results of Section 3.4.1 and 3.4.2 are published in [69], the results of Section 3.4.3 are presented in [67].

3.4.1. Some general observations. Let $\mathrm{Cay}(\mathbb{Z}_n, S)$ be a circulant graph on $n \in \mathbb{N}$ vertices. We observe that every eigenvalue λ of $\mathrm{Cay}(\mathbb{Z}_n, S)$ is contained in the field $\mathbb{Q}(\zeta_n)$ since λ is a linear combination of powers of ζ_n. Thus, the algebraic degree of $\mathrm{Cay}(\mathbb{Z}_n, S)$ is smaller or equal to $\varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$. In fact, if $\mathrm{Cay}(\mathbb{Z}_n, S)$ is undirected, i.e. the adjacency matrix of $\mathrm{Cay}(\mathbb{Z}_n, S)$ is symmetric, and $n > 2$, all eigenvalues of $\mathrm{Cay}(\mathbb{Z}_n, S)$ are real and, therefore, λ is contained in the maximal real subfield F of $\mathbb{Q}(\zeta_n)$. It is well-known that F is given by $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ and that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] = 2$. Hence, it follows that

$$\deg(\mathrm{Cay}(\mathbb{Z}_n, S)) \leq [\mathbb{Q}(\zeta_n + \zeta_n^{-1}) : \mathbb{Q}] = \varphi(n)/2.$$

Furthermore, the following proposition gives a more precise upper bound for the algebraic degree of undirected circulant graphs:

PROPOSITION 3.4.1. *Let $n \in \mathbb{N}$, $n > 2$ and let $S \subseteq \mathbb{Z}_n$ be a connection set with $S = -S$ and $d := \gcd(S, n)$. Then,*

$$\deg(\mathrm{Cay}(\mathbb{Z}_n, S)) \leq \frac{\varphi(n/d)}{2}.$$

PROOF. Since $\gcd(S, n) = d$, every eigenvalue of $\mathrm{Cay}(\mathbb{Z}_n, S)$ can be rewritten as

$$\sum_{s\in S} \mathrm{e}\Big(\frac{s}{n}\Big)^k = \sum_{s\in S} \mathrm{e}\left(\frac{s/d}{n/d}\right)^k.$$

Thus, every eigenvalue of $\mathrm{Cay}(\mathbb{Z}_n, S)$ appears as a linear combination of powers of $\zeta_{n/d}$, and, since all eigenvalues are real, it follows that every element in $\mathrm{spec}(\mathrm{Cay}(\mathbb{Z}_n, S))$ is contained in $\mathbb{Q}(\zeta_{n/d}+\zeta_{n/d}^{-1})$. Thus, $\deg(\mathrm{Cay}(\mathbb{Z}_n, S)) \leq [\mathbb{Q}(\zeta_{n/d} + \zeta_{n/d}^{-1}) : \mathbb{Q}] = \varphi(n/d)/2$. □

Recall that $\mathrm{Cay}(\mathbb{Z}_n, S)$ is connected if and only if $d = 1$. The theorem below shows that, indeed, the upper bound in Proposition 3.4.1 is sharp.

THEOREM 3.4.2. *The family of undirected cycle graphs $\{\mathcal{C}_n \mid 2 < n \in \mathbb{N}\}$ provides a family of circulant graphs of maximum algebraic degree within the family of all undirected circulant graphs.*

PROOF. We show that if $\{\pm s\}$ is a connection set and $d := \gcd(s, n)$, we have that $\deg(\mathrm{Cay}(\mathbb{Z}_n, \{\pm s\})) = \varphi(n/d)/2$. From Proposition 3.4.1 we deduce that $\deg(\mathrm{Cay}(\mathbb{Z}_n, \{\pm s\})) \leq \varphi(n/d)/2$. The eigenvalues of $\mathrm{Cay}(\mathbb{Z}_n, \{\pm s\})$ are given by

$$\lambda_k := \zeta_n^{sk} + \zeta_n^{-sk}, \quad \text{for } k = 0, \ldots, n-1.$$

We may write $\lambda_1 = \omega + \omega^{-1}$ for $\omega := \mathrm{e}\big(\frac{s}{n}\big)$. Since

$$\mathrm{e}\Big(\frac{s}{n}\Big) = \mathrm{e}\left(\frac{s/d}{n/d}\right),$$

we observe that ω is a primitive (n/d)-th root of unity, and $\mathbb{Q}(\omega + \omega^{-1}) = \mathbb{Q}(\lambda_1)$. Hence, it follows that $\deg(\mathrm{Cay}(\mathbb{Z}_n, \{\pm s\})) \geq [\mathbb{Q}(\omega + \omega^{-1}) : \mathbb{Q}] = \varphi(n/d)/2$.

Since, for example, $\mathcal{C}_n \cong \mathrm{Cay}(\mathbb{Z}_n, \{1, n-1\})$ for all $n > 2$, the statement follows. □

Having the question of Harary and Schwenk [42] in mind, graphs of maximum algebraic degree seem to be interesting for future studies, as they can be considered a counterpart of integral graphs.

For the sake of determining the algebraic degree of circulant graphs other than cycle graphs or unions thereof, the next lemma provides some information about the minimal polynomial of the eigenvalues of a circulant graph.

LEMMA 3.4.3. *Let $n \in \mathbb{N}$, $S \subseteq \mathbb{Z}_n$ and $k \in \mathbb{Z}_n$. Then, all elements in the multiset*

$$\mathfrak{C}_n(k) = \Big\{ \sum_{s\in S} \zeta_n^{sk'} \mid k' \in \mathbb{Z}_n,\ \gcd(k', n) = \gcd(k, n) \Big\}$$

are conjugates of $\sum_{s\in S} \zeta_n^{sk}$ and all conjugates of $\sum_{s\in S} \zeta_n^{sk}$ are contained in $\mathfrak{C}_n(k)$.

PROOF. Let Ψ_k denote the minimal polynomial of $\sum_{s\in S}\zeta_n^{sk}$ and let $d := \gcd(k,n)$. Furthermore, let σ_y be the $\mathbb{Q}$-automorphism of $\mathbb{Q}(\zeta_{n/d})$ given by $\sigma_y(\zeta_{n/d}) = \zeta_{n/d}^y$ for some $y \in \mathbb{Z}_n$ with $\gcd(y, n/d) = 1$. Then,

$$\sigma_y\Big(\sum_{s\in S}\zeta_n^{sk}\Big) = \sum_{s\in S}\Big(\sigma_y\big(\zeta_n^{sk}\big)\Big) = \sum_{s\in S}\zeta_n^{sky}.$$

Thus,

$$\begin{aligned} 0 = \sigma_y(0) = \sigma_y\big(\Psi_k\Big(\sum_{s\in S}\zeta_n^{sk}\Big)\big) = \\ = \Psi_k\big(\sigma_y\Big(\sum_{s\in S}\zeta_n^{sk}\Big)\big) = \Psi_k\Big(\sum_{s\in S}\zeta_n^{sky}\Big) \end{aligned}$$

and, therefore, $\sum_{s\in S}\zeta_n^{sky}$ is also a root of Ψ_k, where $\gcd(k,n) = \gcd(k',n)$ for $k' := ky$.

Since all $\mathbb{Q}$-automorphisms on $\mathbb{Q}(\zeta_{n/d})$ are of this form, Ψ_k does not have any other roots. □

In order to determine the algebraic degree of $\mathrm{Cay}(\mathbb{Z}_n, S)$, we first have to identify the degrees of the irreducible factors of the characteristic polynomial of the adjacency matrix of $\mathrm{Cay}(\mathbb{Z}_n, S)$. These factors correspond to the minimal polynomials of the eigenvalues of $\mathrm{Cay}(\mathbb{Z}_n, S)$. From Lemma 3.4.3 we deduce that the number of conjugates, i.e. the degree of the minimal polynomial, of $\sum_{s\in S}\zeta_n^{sk}$ equals the number of distinct elements in $\mathfrak{C}_n(k)$. In order to get this number, we have to determine all solutions to the equation

$$\sum_{s\in S}\zeta_n^{sk_1} = \sum_{s\in S}\zeta_n^{sk_2} \tag{8}$$

for $k_1, k_2 \in \mathbb{Z}_n$ with $\gcd(k_1,n) = \gcd(k_2,n) = \gcd(k,n)$. Since, in general, this problem is hard, in the following, we restrict us to the case where $n = p$ is a prime number.

3.4.2. The algebraic degree of circulant graphs on a prime number of vertices. If $n = p$ is a prime number, Equation (8) holds true if and only if the summands on the left-hand side are equal to the summands on the right-hand side. This follows easily from Theorem 3.1.15: Assume that

$$\sum_{s\in S}\zeta_p^s = \sum_{t\in T}\zeta_p^t \tag{9}$$

for $S, T \subseteq \mathbb{Z}_p$. Then,

$$0 = \sum_{s\in S}\zeta_p^s - \sum_{t\in T}\zeta_p^t = \sum_{s\in S}\zeta_p^s + \sum_{t\in\mathbb{Z}_p\setminus T}\zeta_p^t = \sum_{s\in S\cup(\mathbb{Z}_p\setminus T)}\zeta_p^t,$$

since $\sum_{k\in\mathbb{Z}_p}\zeta_p^k = 0$. By Theorem 3.1.15 there are no equilibrium sets $\mathrm{Eq} \subseteq \mathbb{Z}_p$ except $\{0\}$ and $\mathbb{Z}_p$. Hence, we either have $S = \{0\}$ and $T = \mathbb{Z}_p$ (or the other way round) or $\mathbb{Z}_p = S\cup(\mathbb{Z}_p\setminus T)$ and, thus, $S \equiv T \mod p$.

Since Equation (8) is a special case of Equation (9), it follows that $k_1 S \equiv k_2 S \bmod p$, which is equivalent to $S \equiv k_2 k_1^{-1} S \bmod p$. The following lemma provides a characterization of such equivalences:

LEMMA 3.4.4. *Let p be a prime, $S \subseteq \mathbb{Z}_p^*$ with $M := \#S$ and $k \in \mathbb{Z}_p$. Then, $S \equiv kS \bmod p$ if and only if there exists a common divisor m of M and $p-1$ such that $k^m \equiv 1 \bmod p$ and S may be written as*

$$S = \bigcup_{i=1}^{M/m} S_i$$

with $\#S_i = m$ and $s_{i,1}^m \equiv \cdots \equiv s_{i,m}^m \bmod p$ for $s_{i,j} \in S_i$ and $i = 1, \ldots, M/m$.

PROOF. Let $S \equiv kS \bmod p$. Then,

$$\prod_{s \in S} s \equiv k^M \prod_{s \in S} s \bmod p$$

and, therefore, $k^M \equiv 1 \bmod p$. Thus, $\mathrm{ord}_p(k)$ divides M and $k^m \equiv 1 \bmod p$ for $m := \mathrm{ord}_p(k)$. By Fermat's little theorem, m is a divisor of $p-1$. Now, let $s_1 \in S$. Since $S \equiv kS \bmod p$, we observe that $k^j s_1 \bmod p \in S$ for $j = 0, \ldots, m-1$ and that these elements are pairwise distinct, since S is a set, $s_1 \neq 0$, $\gcd(k, p) = 1$ and $k^j \not\equiv 1 \bmod p$ for $j = 1, \ldots, m-1$. Thus, by defining

$$S_1 := \{s_1, k s_1, k^2 s_1, \ldots, k^{m-1} s_1\} \bmod p$$

and

$$S_i := \{s_i, k s_i, k^2 s_i, \ldots, k^{m-1} s_i\} \bmod p \quad \text{with} \quad s_i \in S \setminus \bigcup_{j=1}^{i-1} S_j$$

for $i = 2, \ldots, M/m$, it follows that

$$S = \bigcup_{i=1}^{M/m} S_i$$

with $\#S_i = m$ and

$$s_i^m \equiv (k s_i)^m \equiv (k^2 s_i)^m \equiv \ldots \equiv (k^{m-1} s_i)^m \bmod p$$

or, equivalently,

$$s_i^m \equiv k^m s_i^m \equiv (k^m)^2 s_i^m \equiv \ldots \equiv (k^m)^{m-1} s_i^m \bmod p$$

for $i = 1, \ldots, M/m$, since $k^m \equiv 1 \bmod p$.

For the other direction, since S is a set, we observe that for $i = 1, \ldots, M/m$ the elements of S_i are the m distinct solutions to the equation $x^m \equiv c_i \bmod p$ for a constant $c_i \in \mathbb{Z}_p$. On the other hand, the elements $k s_{i,1}, k s_{i,2}, \ldots, k s_{i,m}$ are all incongruent modulo p and are also solutions to $x^m \equiv c_i \bmod p$, since $k^m \equiv 1 \bmod p$. Thus, $S_i \equiv kS_i \bmod p$ for $i = 1, \ldots, M/m$ and, therefore, $S \equiv kS \bmod p$. □

The lemma shows that Equation (8) holds true only if the connection set S bears special structure. In the following, for a common divisor m of M and $p-1$, we say that a set $S \subseteq \mathbb{Z}_p$ with $M := \#S$ is *m-decomposable* if S can be written as

$$S = \bigcup_{i=1}^{M/m} S_i$$

with $\#S_i = m$ such that $s_{i,1}^m \equiv \cdots \equiv s_{i,m}^m \bmod p$ for $s_{i,j} \in S_i$ and $i = 1, \ldots, M/m$.

In order to find all solutions $k \in \mathbb{Z}_p$ to the equation $S \equiv kS \bmod p$, it actually suffices to consider the maximum number $m \in \mathbb{Z}_p$ such that S is m-decomposable: Assume that S is m_1-decomposable and m_2-decomposable for $m_1 \neq m_2$. Then, by Lemma 3.4.4, it follows that $S \equiv k_l S \bmod p$ for all k_l satisfying $k_l^{m_l} \equiv 1 \bmod p$ for $l = 1, 2$. In particular, this holds true for elements k_l of order m_l. Thus, we have that $S \equiv k_1^i k_2^j S \bmod p$ for all $i, j \in \mathbb{Z}_p$, and there exists an element $k_1^i k_2^j$ of order $\operatorname{lcm}(m_1, m_2)$ in $\mathbb{Z}_p$, since k_1, k_2 generate a cyclic group of order $\operatorname{lcm}(m_1, m_2)$. Hence, again by Lemma 3.4.4, it follows that S is m-decomposable for $m := \operatorname{lcm}(m_1, m_2) \geq m_1, m_2$.

Now, we are able to determine the algebraic degree of circulant graphs on a prime number of vertices:

THEOREM 3.4.5. *Let p be a prime number and $S \subseteq \mathbb{Z}_p$ be a connection set with $M := \#S$. Furthermore, let m be the maximum common divisor of M and $p-1$ such that S is m-decomposable. Then,*

$$\deg(\operatorname{Cay}(\mathbb{Z}_p, S)) = \frac{p-1}{m}.$$

In particular, if $\deg(\operatorname{Cay}(\mathbb{Z}_p, S)) = \frac{p-1}{m}$, then S is m-decomposable.

PROOF. The p eigenvalues of $\operatorname{Cay}(\mathbb{Z}_p, S)$ are given by $\lambda_k = \sum_{s \in S} \zeta_n^{sk}$ for $k = 0, \ldots, p-1$. We have that $\lambda_0 = M \in \mathbb{Z}$. Furthermore, by Lemma 3.4.3, we observe that every two eigenvalues of the remaining eigenvalues are conjugated or equal. Let $k \in \{1, \ldots, p-1\}$, then

$$p - 1 = [\mathbb{Q}(\zeta_p) : \mathbb{Q}(\lambda_k)][\mathbb{Q}(\lambda_k) : \mathbb{Q}].$$

The $\mathbb{Q}$-automorphisms on $\mathbb{Q}(\zeta_p)$ are induced by $\sigma_y : \zeta_p \mapsto \zeta_p^y$ for $y = 1, \ldots, p-1$. By the fundamental theorem of Galois theory, the number of elements in the subgroup $\{\sigma \in \operatorname{Aut}\big(\mathbb{Q}(\zeta_p)|\mathbb{Q}\big) \mid \sigma(\lambda_k) = \lambda_k\}$ equals $[\mathbb{Q}(\zeta_p) : \mathbb{Q}(\lambda_k)]$. As shown in the beginning of this section, $\sigma_y(\lambda_k) = \lambda_k$ holds true only if $S \equiv yS \bmod p$. In view of our assumptions, from Lemma 3.4.4 we deduce that $S \equiv yS \bmod p$ for all $y \in \mathbb{Z}_p$ satisfying $y^m \equiv 1 \bmod p$. On the other hand, these are all $y \in \mathbb{Z}_p$ satisfying $S \equiv yS \bmod p$ since m was chosen maximally. Since m divides $p-1$, there exist exactly m solutions to $y^m \equiv 1 \bmod p$, i.e. $\#\operatorname{Aut}\big(\mathbb{Q}(\zeta_p)|\mathbb{Q}(\lambda_k)\big) = [\mathbb{Q}(\zeta_p) : \mathbb{Q}(\lambda_k)] = m$. The Galois group of $\mathbb{Q}(\zeta_p)|\mathbb{Q}$ is given by the

group of units in $\mathbb{Z}_p$ which we denote by $\mathbb{Z}_p^*$. Since $\mathbb{Z}_p^*$ is cyclic, for every divisor d of $\#\mathbb{Z}_p^*$, there exists exactly one subgroup of $\mathbb{Z}_p^*$ of order d. Hence, by the fundamental theorem of Galois theory, there exists only one intermediate field of $\mathbb{Q}(\zeta_p)|\mathbb{Q}$ of degree d over $\mathbb{Q}$. Since $[\mathbb{Q}(\zeta_p) : \mathbb{Q}(\lambda_k)] = m$ holds true for every $k \in \{1, \ldots, p-1\}$, we therefore observe that $\mathbb{Q}(\lambda_1) = \ldots = \mathbb{Q}(\lambda_{p-1})$, i.e. $\lambda_1, \ldots, \lambda_{p-1} \in \mathbb{Q}(\lambda_k)$. Thus, $\deg(\mathrm{Cay}(\mathbb{Z}_p, S)) = [\mathbb{Q}(\lambda_k) : \mathbb{Q}] = \frac{p-1}{m}$. □

COROLLARY 3.4.6. *Let p be a prime number and $S \subseteq \mathbb{Z}_p$ be a connection set with $M := \#S$. Then,*

$$\frac{p-1}{M} \leq \deg(\mathrm{Cay}(\mathbb{Z}_p, S)) \leq p-1.$$

In particular, $\mathrm{Cay}(\mathbb{Z}_p, S)$ is integral if and only if $M = p-1$, i.e. $\mathrm{Cay}(\mathbb{Z}_p, S) \cong \mathcal{K}_p$.

Note that $(p-1)/M$ is not necessarily an integer. More precisely, we have that $\lceil (p-1)/M \rceil \leq \deg(\mathrm{Cay}(\mathbb{Z}_p, S))$, where $\lceil x \rceil$ denotes the least integer greater or equal to x.

In some special cases, we can already deduce that $\mathrm{Cay}(\mathbb{Z}_p, S)$ is of maximum algebraic degree from considering the numbers M and $p-1$ only:

COROLLARY 3.4.7. *Let p be a prime number and $S \subseteq \mathbb{Z}_p$ be a connection set with $M := \#S$. If $\gcd(M, p-1) = 1$, then $\deg(\mathrm{Cay}(\mathbb{Z}_p, S)) = p-1$.*

In particular, if $p > 2$ and $\mathrm{Cay}(\mathbb{Z}_n, S)$ is undirected, i.e. $S = -S$, then, if $\gcd(M, p-1) = 2$, it follows that $\deg(\mathrm{Cay}(\mathbb{Z}_p, S)) = \frac{p-1}{2}$.

This corollary also yields a lower bound for the number of non-isomorphic circulant graphs on a prime number of vertices and of maximum algebraic degree:

COROLLARY 3.4.8. *Let p be a prime number. Then there exist at least $\varphi(p-1)$ non-isomorphic circulant graphs on p vertices and of maximum algebraic degree within the family of all circulant graphs.*

PROOF. By Corollary 3.4.7, a circulant graph $\mathrm{Cay}(\mathbb{Z}_p, S)$ is of maximum algebraic degree whenever $\gcd(M, p-1) = 1$ for $M = \#S$. Since

$$\#\{M \mid M \in \mathbb{N},\ 0 \leq M \leq p-1,\ \gcd(M, p-1) = 1\} = \varphi(p-1)$$

and isomorphic graphs have the same number of edges, the statement follows. □

EXAMPLE 3.4.9. Let $p = 31$ and $S = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 7\}$. Since $\gcd(M, p-1) = \gcd(14, 30) = 2$, we deduce from Corollary 3.4.7 that $\deg(\mathrm{Cay}(\mathbb{Z}_{31}, S)) = 30/2 = 15$, i.e. $\mathrm{Cay}(\mathbb{Z}_{31}, S)$ is of maximum algebraic degree within the family of all undirected circulant graphs (and is not isomorphic to a cycle graph, in particular).

EXAMPLE 3.4.10. Let $p = 31$ and $S = \{\pm 2, \pm 3, \pm 10, \pm 12, \pm 13, \pm 15\}$. Since $\gcd(M, p-1) = \gcd(12, 30) = 6$, we first check whether S is 6-decomposable. We observe that $(\pm 2)^6 \equiv (\pm 10)^6 \equiv (\pm 12)^6 \equiv 2 \bmod 31$ and $(\pm 3)^6 \equiv (\pm 13)^6 \equiv (\pm 15)^6 \equiv 16 \bmod 31$. Thus, by Theorem 3.4.5, the algebraic degree of $\langle S \rangle_{31}$ equals $30/6 = 5$. Indeed, the factorized characteristic polynomial of the adjacency matrix of $\mathrm{Cay}(\mathbb{Z}_n, S)$ is given by

$$\chi = -(-12 + x)(67 + 16x - 44x^2 - 17x^3 + 2x^4 + x^5)^6$$

with Galois group $\mathrm{Gal}(\chi|\mathbb{Q}) \cong \mathbb{Z}_5$.

EXAMPLE 3.4.11. Corollary 3.4.6 shows that the number of edges in a circulant graph on a prime number of vertices gives a lower bound for its algebraic degree. However, there also exist graphs with the same number of vertices and edges but different algebraic degree: Let $p = 13$ and $S_1 = \{\pm 1, \pm 5\}$. Since $\gcd(M, p-1) = \gcd(4, 12) = 4$, we first check whether S_1 is 4-decomposable. Indeed, we observe that $(\pm 1)^4 \equiv (\pm 5)^4 \equiv 1 \bmod 13$. Thus, by Theorem 3.4.5, the algebraic degree of $\mathrm{Cay}(\mathbb{Z}_{13}, S_1)$ equals $12/4 = 3$.

Now, let $S_2 = \{\pm 1, \pm 6\}$. Again, we first try whether S_2 is 4-decomposable, but $1 \equiv 1^4 \not\equiv 6^4 \equiv 9 \bmod 13$. Thus, S_2 is only 2-decomposable and, therefore, by Theorem 3.4.5, the algebraic degree of $\mathrm{Cay}(\mathbb{Z}_{13}, S_2)$ equals $12/2 = 6$.

Hence, $\mathrm{Cay}(\mathbb{Z}_{13}, S_1)$ and $\mathrm{Cay}(\mathbb{Z}_{13}, S_2)$ have the same number of vertices and edges, but different algebraic degree. The graphs are shown in Figure 3.8. Note that this is a minimal example with respect to the number p of vertices.

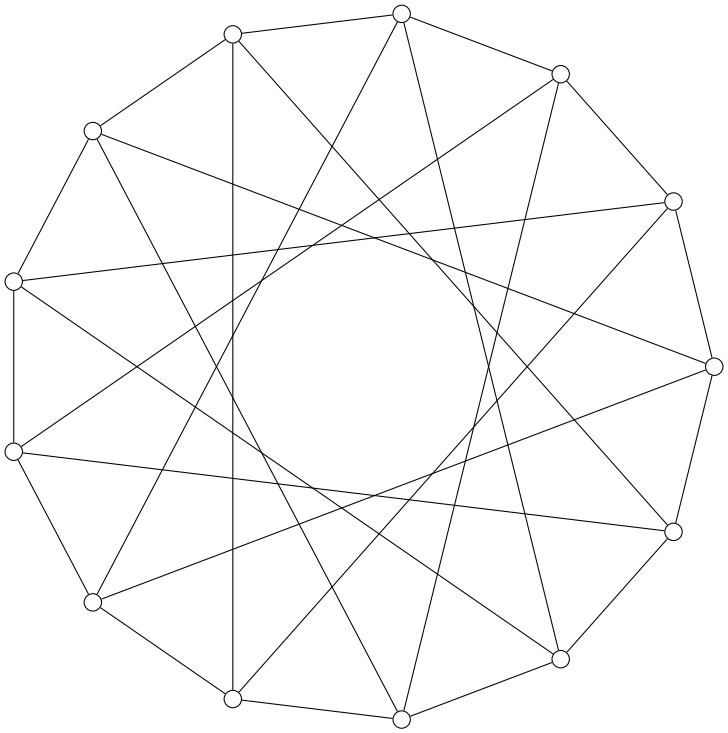
EXAMPLE 3.4.12 (Paley graphs). Recall that the spectrum of the Paley graph $\mathrm{Pal}(q)$ for a prime power $q \equiv 1 \bmod 4$ and vertex set $V = \mathbb{F}_q$ is given by

$$\mathrm{spec}(\mathrm{Pal}(q)) = \left\{(q-1)/2, (\sqrt{q}-1)/2^{[(q-1)/2]}, (-\sqrt{q}-1)/2^{[(q-1)/2]}\right\}.$$

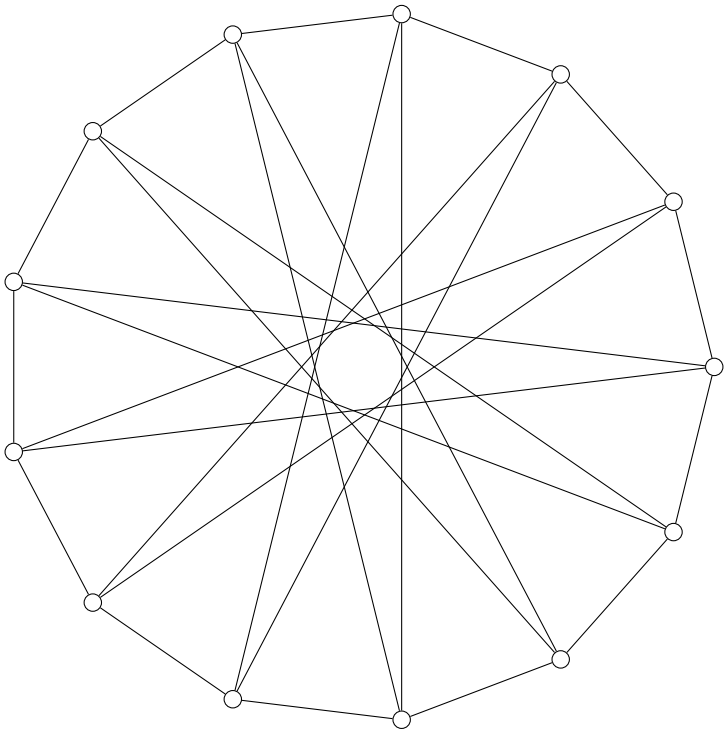
Thus, the eigenvalues of $\mathrm{Pal}(q)$ are of degree at most 2. If q is a prime number, $\mathrm{Pal}(q)$ is a circulant graph, i.e. $\mathrm{Pal}(q) \cong \mathrm{Cay}(\mathbb{Z}_q, S)$ for some $S \subseteq \mathbb{Z}_q$, and $\mathrm{Pal}(q)$ is of algebraic degree 2. We now want to verify this using Theorem 3.4.5. Since $\mathrm{Pal}(q)$ is $(q-1)/2$-regular, $\#S = (q-1)/2$. By definition, there exists an edge between two vertices i, j in $\mathrm{Pal}(q)$ if and only if $i - j$ is a quadratic residue modulo q. Moreover, since $\mathrm{Pal}(q)$ is circulant, we also have $i - j \in S$ in this case. In particular, since $s - 0 \in S$ for all $s \in S$, every element in S is a quadratic residue modulo q. Thus, for every $s \in S$ there exists $a_s \in \{1, \ldots, q-1\}$ such that $s \equiv a_s^2 \bmod q$. Hence, from Euler's Theorem it follows that

$$s^{(q-1)/2} \equiv (a_s^2)^{(q-1)/2} = a_s^{q-1} \equiv 1 \bmod q, \quad \text{for all } s \in S.$$

Therefore, by Theorem 3.4.5, the algebraic degree of $\mathrm{Pal}(q)$ equals $\frac{q-1}{(q-1)/2} = 2$.



(a) $S_1 = \{\pm 1, \pm 5\}$



(b) $S_2 = \{\pm 1, \pm 6\}$

FIGURE 3.8. Circulant graphs with same number of vertices and edges but different algebraic degree.

3.4.3. Splitting fields of circulant graphs and Schur rings. In view of Equation (8), it is hard to generalize our latter approach in order to determine the algebraic degree of circulant graphs on an arbitrary number of vertices. Thus, we now approach the problem more algebraically, in particular by using Schur ring theory. From the previous sections, we already know that structural properties of a Cayley graph $\mathrm{Cay}(G, S)$ are connected to algebraic properties of the Schur ring $\langle\langle S\rangle\rangle$. We now show that there is also a relation between Schur rings and the eigenvalues of Cayley graphs. More precisely, the algebraic degree of $\mathrm{Cay}(G, S)$ is in fact related to the least orbit Schur ring which contains the connection set S. To prove this, we use a result of Misseldine [65] connecting orbit Schur rings and cyclotomic fields.

3.4.3.1. *Orbit Schur rings and cyclotomic fields.* Recall that for a subgroup H of $\mathrm{Aut}(G)$, the respective orbit Schur ring $\mathbb{Q}G^H$ is defined by

$$\mathbb{Q}G^H := \{\alpha \in \mathbb{Q}G \mid \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\},$$

and is the largest subring of $\mathbb{Q}G$ which is fixed by the automorphism group H (cf. Example 3.2.3).

Example 3.4.13. The subgroups of $\mathrm{Aut}(\mathbb{Z}_{12}) \cong \mathbb{Z}_{12}^*$ are the multiplicative groups $\{1\}$, $\{1,5\}$, $\{1,7\}$, $\{1,11\}$ and $\{1,5,7,11\} = \mathbb{Z}_{12}^*$. The respective orbit S-rings are

$$\begin{aligned}
\mathbb{Q}\mathbb{Z}_{12}^{\{1\}} &= \langle \underline{\{0\}}, \underline{\{1\}}, \underline{\{2\}}, \underline{\{3\}}, \underline{\{4\}}, \ldots, \underline{\{10\}}, \underline{\{11\}} \rangle \\
\mathbb{Q}\mathbb{Z}_{12}^{\{1,5\}} &= \langle \underline{\{0\}}, \underline{\{3\}}, \underline{\{6\}}, \underline{\{9\}}, \underline{\{1,5\}}, \underline{\{2,10\}}, \underline{\{4,8\}}, \underline{\{7,11\}} \rangle \\
\mathbb{Q}\mathbb{Z}_{12}^{\{1,7\}} &= \langle \underline{\{0\}}, \underline{\{2\}}, \underline{\{4\}}, \underline{\{6\}}, \underline{\{8\}}, \underline{\{10\}}, \underline{\{1,7\}}, \underline{\{3,9\}}, \underline{\{5,11\}} \rangle \\
\mathbb{Q}\mathbb{Z}_{12}^{\{1,11\}} &= \langle \underline{\{0\}}, \underline{\{6\}}, \underline{\{1,11\}}, \underline{\{2,10\}}, \underline{\{3,9\}}, \underline{\{4,8\}}, \underline{\{5,7\}} \rangle \\
\mathbb{Q}\mathbb{Z}_{12}^{\{1,5,7,11\}} &= \langle \underline{\{0\}}, \underline{\{6\}}, \underline{\{2,10\}}, \underline{\{3,9\}}, \underline{\{4,8\}}, \underline{\{1,5,7,11\}} \rangle.
\end{aligned}$$

In the following, let $\hat{\omega}_n$ be the well-known group isomorphism between the (additive) group $\mathbb{Z}_n$ and the (multiplicative) group of all n-th roots of unity defined by $\hat{\omega}_n(k) = \zeta_n^k$. It is clear that $\hat{\omega}_n$ induces a $\mathbb{Q}$-algebra homomorphism ω_n between the group algebra $\mathbb{Q}\mathbb{Z}_n$ and the cyclotomic field $\mathbb{Q}(\zeta_n)$ via

$$\omega_n\Big(\sum_{k\in\mathbb{Z}_n} \alpha_k k\Big) = \sum_{k\in\mathbb{Z}_n} \alpha_k \hat{\omega}_n(k).$$

Theorem 3.4.14 ([65, Theorem 4.8 and Corollary 4.4]). *The lattice of orbit Schur rings over $\mathbb{Z}_n$ is isomorphic via ω_n to the lattice of subfields of the cyclotomic field $\mathbb{Q}(\zeta_n)$.*

In particular, $\omega_n(\mathbb{Q}\mathbb{Z}_n^H)$ is the unique maximum subfield of $\mathbb{Q}(\zeta_n)$ where each element is fixed by every automorphism in H.

The latter theorem says that there is a one-to-one correspondence between orbit Schur rings over $\mathbb{Z}_n$ and subfields of the cyclotomic field $\mathbb{Q}(\zeta_n)$. Moreover, by the fundamental theorem of Galois theory, there is

a one-to-one correspondence between these subfields and the subgroups of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q})$, the group of $\mathbb{Q}$-automorphisms of $\mathbb{Q}(\zeta_n)$. Finally, those subgroups are isomorphic to the subgroups of $\mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^*$, which generate the orbit Schur rings over $\mathbb{Z}_n$.

In the following, we denote by $\mathbb{Q}(\zeta_n)^H$ the fixed field of H, i.e. the unique maximum subfield of $\mathbb{Q}(\zeta_n)$ where each element is fixed by every automorphism in H. By Theorem 3.4.14, we have that

$$\mathbb{Q}(\zeta_n)^H = \omega_n(\mathbb{Q}\mathbb{Z}_n^H).$$

EXAMPLE 3.4.15. Figure 3.9 shows the one-to-one correspondence between the lattice of orbit Schur rings over $\mathbb{Z}_{12}$ (see Example 3.4.13) and the lattice of subfields of $\mathbb{Q}(\zeta_{12})$.

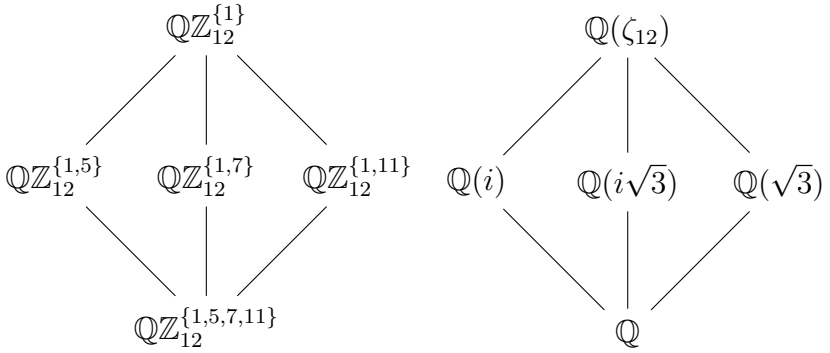


FIGURE 3.9. Lattice of orbit Schur rings over $\mathbb{Z}_{12}$ (left) and lattice of subfields of $\mathbb{Q}(\zeta_{12})$ (right).

3.4.3.2. *The least orbit Schur ring of a set.* From Theorem 3.4.14 and the fundamental theorem of Galois theory it follows that for subgroups $H, F \leq \mathrm{Aut}(\mathbb{Z}_n) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q})$ we have that

$$\mathbb{Q}\mathbb{Z}_n^H \subseteq \mathbb{Q}\mathbb{Z}_n^F \iff \omega_n(\mathbb{Q}\mathbb{Z}_n^H) \subseteq \omega_n(\mathbb{Q}\mathbb{Z}_n^F) \iff F \subseteq H.$$

Thus, if S is a subset of $\mathbb{Z}_n$ such that $\underline{S} \in \mathbb{Q}\mathbb{Z}_n^H$ and $\underline{S} \in \mathbb{Q}\mathbb{Z}_n^F$, it easily follows that

$$\underline{S} \in \mathbb{Q}\mathbb{Z}_n^H \cap \mathbb{Q}\mathbb{Z}_n^F = \mathbb{Q}\mathbb{Z}_n^{\langle H \cup F \rangle},$$

where $\mathbb{Q}\mathbb{Z}_n^{\langle H \cup F \rangle}$ is a smaller orbit S-ring which contains $\underline{S}$. Therefore, we may write $\langle\langle S \rangle\rangle_{\mathcal{O}}$ for the unique least orbit S-ring which contains $\underline{S}$.

3.4.3.3. *Orbit Schur rings and circulant graph spectra.* In the following, let $\lambda_k(S)$ denote the eigenvalue $\sum_{s \in S} \zeta_n^{sk}$ of $\mathrm{Cay}(\mathbb{Z}_n, S)$. By definition, we immediately get that

$$\omega_n(\underline{S}^{(k)}) = \lambda_k(S), \quad \text{for } k = 0, \ldots, n-1.$$

The following lemma shows that all eigenvalues of $\mathrm{Cay}(\mathbb{Z}_n, S)$ arise from elements of the same orbit Schur ring.

LEMMA 3.4.16. *Let $H \leq \mathrm{Aut}(\mathbb{Z}_n)$ and $S \subseteq \mathbb{Z}_n$. If $\underline{S} \in \mathbb{QZ}_n^H$, then $\underline{S}^{(k)} \in \mathbb{QZ}_n^H$ for all $k \in \mathbb{Z}$.*

PROOF. Since $\underline{S} \in \mathbb{QZ}_n^H$, we may write

$$\underline{S} = \sum_{T \in \mathrm{Basic}(\mathbb{QZ}_n^H)} \underline{T}.$$

Moreover, since

$$\Big(\sum_{T \in \mathrm{Basic}(\mathbb{QZ}_n^H)} \underline{T} \Big)^{(k)} = \sum_{T \in \mathrm{Basic}(\mathbb{QZ}_n^H)} \underline{T}^{(k)},$$

we may restrict us to the case where S is a basic set of $\mathbb{QZ}_n^H$.

In the following, for $x \in \mathbb{Z}_n$, let $H_x := \{\sigma \in H \mid \sigma(x) = x\}$ denote the stabilizer of x in H. It is well-known that

$$\sum_{h \in H} hx = \#H_x \Big(\sum_{y \in x^H} y \Big).$$

By definition, S is of the form $x^H = \{\sigma(x) \mid \sigma \in H\}$ for some $x \in \mathbb{Z}_n$, and since H can be identified with a multiplicative subgroup of $\mathbb{Z}_n$, we may write $x^H = \{xh \mid h \in H\} = \{hx \mid h \in H\}$. Thus,

$$\underline{S} = \sum_{y \in x^H} y = \frac{1}{\#H_x} \sum_{h \in H} xh.$$

Moreover, we have that

$$\underline{S}^{(k)} = \frac{1}{\#H_x} \sum_{h \in H} kxh = \frac{1}{\#H_x} \#H_{kx} \Big(\sum_{y \in (kx)^H} y \Big) \in \mathbb{QZ}_n^H.$$

□

THEOREM 3.4.17. *Let $\mathrm{Cay}(\mathbb{Z}_n, S)$ be a circulant graph. Then all eigenvalues of $\mathrm{Cay}(\mathbb{Z}_n, S)$ are contained in the subfield $\omega_n(\langle\langle S \rangle\rangle_{\mathcal{O}})$ of $\mathbb{Q}(\zeta_n)$.*

In particular, if H denotes the subgroup of $\mathrm{Aut}(\mathbb{Z}_n)$ such that $\langle\langle S \rangle\rangle_{\mathcal{O}} = \mathbb{QZ}_n^H$, then $\lambda_k(S) \in \mathbb{Q}(\zeta_n)^H$ for $k = 0, \ldots, n-1$.

PROOF. By Lemma 3.4.16, $\underline{S}^{(k)} \in \langle\langle S \rangle\rangle_{\mathcal{O}}$ for all $k \in \mathbb{Z}$. Thus, by Theorem 3.4.14, we get that $\omega_n(\underline{S}^{(k)}) = \lambda_k(S) \in \omega_n(\langle\langle S \rangle\rangle_{\mathcal{O}})$ for $k = 0, \ldots, n-1$. □

3.4.3.4. *Splitting fields and least orbit Schur rings.* By Theorem 3.4.17, every eigenvalue of a circulant graph $\mathrm{Cay}(\mathbb{Z}_n, S)$ is contained in the subfield $\mathbb{Q}(\zeta_n)^H$ of $\mathbb{Q}(\zeta_n)$, where H is defined via $\langle\langle S \rangle\rangle_{\mathcal{O}} = \mathbb{QZ}_n^H$. The aim of this section is to show that $\mathbb{Q}(\zeta_n)^H$ is indeed the smallest subfield of $\mathbb{Q}(\zeta_n)$ which contains all eigenvalues of $\mathrm{Cay}(\mathbb{Z}_n, S)$. Our proof for this is based on So's proof [92, Section 6] (cf. Section 3.3) for integral circulant graphs and provides a generalization thereof.

For a subgroup H of $\mathrm{Aut}(\mathbb{Z}_n)$ let $\{S_0, S_1, \ldots, S_r\}$ be the basic set of $\mathbb{Q}\mathbb{Z}_n^H$ and let $K_{\scriptscriptstyle H} := \mathbb{Q}(\zeta_n)^H$. Moreover, let $\mathbf{v}_i(H) \in K_{\scriptscriptstyle H}^n$ be the vector with 1 at the j-th entry for all $j \in S_i$ and 0 elsewhere, and let F be the invertible $(n \times n)$-matrix defined by $F_{st} = \zeta_n^{st}$, for $s, t = 0, \ldots, n-1$. Finally, let $\mathcal{A}_H$ be the $K_{\scriptscriptstyle H}$-vector space

$$\mathcal{A}_H := \{\mathbf{v} \in K_{\scriptscriptstyle H}^n \mid F\mathbf{v} \in K_{\scriptscriptstyle H}^n\}.$$

From Theorem 3.4.17 we deduce that $\mathbf{v}_i(H) \in \mathcal{A}_H$ for $i = 0, \ldots, n-1$. Furthermore, we have the following:

LEMMA 3.4.18. $\mathcal{A}_H = \mathrm{span}\{\mathbf{v}_i(H) \mid i = 0, \ldots, r\}$.

PROOF. Since $\{S_0, S_1, \ldots, S_r\}$ is a partition of $\mathbb{Z}_n$, the $\mathbf{v}_i(H)$'s are linearly independent. Let $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})^{\mathsf{t}} \in \mathcal{A}_H$ and $F\mathbf{v} = \mathbf{u} = (u_0, u_1, \ldots, u_{n-1})^{\mathsf{t}}$. To prove that $\mathbf{u} \in \mathrm{span}\{\mathbf{v}_i(H) \mid i = 0, \ldots, r\}$, it suffices to show that $u_s = u_t$ whenever $s, t \in S_i$ for some $i \in \{0, \ldots, n-1\}$. By definition, we may write $S_i = s^H$. Thus, there is $h \in H$ such that $hs = t$. Moreover, since $\mathbf{u} \in K_{\scriptscriptstyle H}^n$, we have that $\sigma(u_s) = u_s$ for all $\sigma \in H$, so in particular $\sigma_h(u_s) = u_s$, where σ_h denotes the automorphism uniquely determined by $\sigma_h(s) = hs$. Hence,

$$u_s = \sigma_h(u_s) = \sigma_h\Big(\sum_{j=0}^{n-1} v_j \zeta_n^{sj}\Big) = \sum_{j=0}^{n-1} v_j \zeta_n^{\sigma_h(sj)} = \\ = \sum_{j=0}^{n-1} v_j \zeta_n^{\sigma_h(s)j} = \sum_{j=0}^{n-1} v_j \zeta_n^{tj} = u_t.$$

Therefore, $F(\mathcal{A}_H) \subseteq \mathrm{span}\{\mathbf{v}_i(H) \mid i = 0, \ldots, r\} \subseteq \mathcal{A}_H$. Moreover, since F is invertible, $\dim \mathcal{A}_H = \dim F(\mathcal{A}_H)$, i.e. $F(\mathcal{A}_H) = \mathrm{span}\{\mathbf{v}_i(H) \mid i = 0, \ldots, r\} = \mathcal{A}_H$. □

THEOREM 3.4.19. *If all eigenvalues of* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *are contained in* $\mathbb{Q}(\zeta_n)^H$ *for* $H \leq \mathrm{Aut}(\mathbb{Z}_n)$*, then* $\underline{S} \in \mathbb{Q}\mathbb{Z}_n^H$.

PROOF. Let $\mathbf{v}^{\mathsf{t}}$ denote the first row of the adjacency matrix of $\mathrm{Cay}(\mathbb{Z}_n, S)$, i.e. the j-th entry of $\mathbf{v}$ equals 1 whenever $j \in S$ and 0 elsewhere. Since all eigenvalues of $\mathrm{Cay}(\mathbb{Z}_n, S)$ are contained in $\mathbb{Q}(\zeta_n)^H$, we have that $F\mathbf{v} = (\lambda_0(S), \ldots, \lambda_{n-1}(S))^{\mathsf{t}} \in K_{\scriptscriptstyle H}^n$ and hence $\mathbf{v} \in \mathcal{A}_H$. Thus, by Lemma 3.4.18, we may write

$$\mathbf{v} = \sum_{i=0}^{n-1} a_i \mathbf{v}_i(H).$$

Since all entries of $\mathbf{v}$ and the $\mathbf{v}_i(H)$'s are 0 or 1, we conclude that $a_i \in \{0, 1\}$. Therefore, S is a union of the basic sets $\{S_0, S_1, \ldots, S_r\}$ of $\mathbb{Q}\mathbb{Z}_n^H$ for those i where $a_i = 1$, i.e. $\underline{S} \in \mathbb{Q}\mathbb{Z}_n^H$. □

THEOREM 3.4.20. *The splitting field of* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *is given by* $\mathbb{Q}(\zeta_n)^H$*, where* $H \leq \mathrm{Aut}(\mathbb{Z}_n)$ *is defined by* $\langle\langle S \rangle\rangle_{\mathcal{O}} = \mathbb{Q}\mathbb{Z}_n^H$.

PROOF. By Theorem 3.4.17, all eigenvalues of $\mathrm{Cay}(\mathbb{Z}_n, S)$ are contained in $\omega_n(\langle\langle S\rangle\rangle_{\mathcal{O}})$. Let H be the subgroup of $\mathrm{Aut}(\mathbb{Z}_n)$ such that $\langle\langle S\rangle\rangle_{\mathcal{O}} = \mathbb{Q}\mathbb{Z}_n^H$. Assume that the splitting field of $\mathrm{Cay}(\mathbb{Z}_n, S)$ is smaller than $\mathbb{Q}(\zeta_n)^H$, i.e. there exists a group F with $F \not\leq H$ such that $\lambda_k(S) \in \mathbb{Q}(\zeta_n)^F$ for $k = 0, \ldots, n-1$. Then, by Theorem 3.4.19, we have that $\underline{S} \in \mathbb{Q}\mathbb{Z}_n^F$. Hence, $\underline{S} \in \mathbb{Q}\mathbb{Z}_n^H \cap \mathbb{Q}\mathbb{Z}_n^F = \mathbb{Q}\mathbb{Z}_n^{\langle H\cup F\rangle}$ where $\mathbb{Q}\mathbb{Z}_n^{\langle H\cup F\rangle}$ is a smaller S-ring than $\langle\langle S\rangle\rangle_{\mathcal{O}}$ which contains $\underline{S}$, a contradiction to the definition of $\langle\langle S\rangle\rangle_{\mathcal{O}}$. □

EXAMPLE 3.4.21. We consider the graph $\mathrm{Cay}(\mathbb{Z}_{12}, \{3, 7, 11\})$. In view of Example 3.4.13, we have that $\langle\langle\{3, 7, 11\}\rangle\rangle_{\mathcal{O}} = \mathbb{Q}\mathbb{Z}_{12}^{\{1,5\}}$. Therefore, the splitting field of $\mathrm{Cay}(\mathbb{Z}_{12}, \{3, 7, 11\})$ is given by $\mathbb{Q}(\zeta_{12})^{\{1,5\}} = \mathbb{Q}(i)$. Indeed,

$$\mathrm{spec}(\mathrm{Cay}(\mathbb{Z}_{12}, \{3, 7, 11\})) = \{3, 0, 0, -3i, 0, 0, -3, 0, 0, 3i, 0, 0\}.$$

3.4.3.5. *Proof of the main theorem.* Recall that $S^H := \bigcup_{s\in S} s^H$.

LEMMA 3.4.22. *Let $S \subseteq \mathbb{Z}_n$ and $H \leq \mathrm{Aut}(\mathbb{Z}_n)$. Then, $S^H = S$ if and only if $\underline{S} \in \mathbb{Q}\mathbb{Z}_n^H$.*

PROOF. If $S^H = S$, then $s^H \subseteq S$ for all $s \in S$. Therefore, S is a union of orbits s^H, i.e. $\underline{S} \in \mathbb{Q}\mathbb{Z}_n^H$. Conversely, if $\underline{S} \in \mathbb{Q}\mathbb{Z}_n^H$, then S is a union of orbits x^H for some $x \in \mathbb{Z}_n$. Since each orbit is fixed under H, this is also true for S, i.e. $S^H = S$. □

LEMMA 3.4.23. *Let $\underline{S} \in \mathbb{Q}\mathbb{Z}_n^H$. Then, $\mathbb{Q}\mathbb{Z}_n^H = \langle\langle S\rangle\rangle_{\mathcal{O}}$ if and only if H is the maximum subgroup of $\mathrm{Aut}(\mathbb{Z}_n)$ such that $S^H = S$.*

PROOF. Let $\mathbb{Q}\mathbb{Z}_n^H = \langle\langle S\rangle\rangle_{\mathcal{O}}$. Due to the minimality of $\langle\langle S\rangle\rangle_{\mathcal{O}}$, the group H must be the maxmimum subgroup of $\mathrm{Aut}(\mathbb{Z}_n)$ such that $\underline{S} \in \mathbb{Q}\mathbb{Z}_n^H$. By Lemma 3.4.22, $S^H = S$ follows.

Now, let H be the maximum subgroup of $\mathrm{Aut}(\mathbb{Z}_n)$ such that $S^H = S$. Furthermore, let $\langle\langle S\rangle\rangle_{\mathcal{O}} = \mathbb{Q}\mathbb{Z}_n^F$ for $F \leq \mathrm{Aut}(\mathbb{Z}_n)$. Then by Lemma 3.4.22 we have that $S^F = S$. Hence, due to the maximality of H, either $F = H$ follows or F contains less elements than H. But in the latter case, we observe that F is a proper subgroup of $\langle F \cup H\rangle$ and therefore, $\mathbb{Q}\mathbb{Z}_n^{\langle F\cup H\rangle}$ is a smaller S-ring than $\mathbb{Q}\mathbb{Z}_n^F$ which contains $\underline{S}$, a contradiction. Thus, $F = H$. □

THEOREM 3.4.24 (Main theorem). *The splitting field of $\mathrm{Cay}(\mathbb{Z}_n, S)$ is given by $\mathbb{Q}(\zeta_n)^H$, where H is the maximum subgroup of $\mathrm{Aut}(\mathbb{Z}_n)$ such that $S^H = S$.*

PROOF. By Theorem 3.4.20, the subgroup H is given by the equality $\langle\langle S\rangle\rangle_{\mathcal{O}} = \mathbb{Q}\mathbb{Z}_n^H$. By Lemma 3.4.23, this is equivalent to H being the maximum subgroup of $\mathrm{Aut}(\mathbb{Z}_n)$ such that $S^H = S$. □

3.4.3.6. *The algebraic degree of circulant graphs.*

THEOREM 3.4.25. *Let* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *be a circulant graph and* H *be the unique subgroup of* $\mathrm{Aut}(\mathbb{Z}_n)$ *such that* $\langle\langle S\rangle\rangle_{\mathcal{O}} = \mathbb{Q}\mathbb{Z}_n^H$. *Then,*

$$\deg(\mathrm{Cay}(\mathbb{Z}_n, S)) = \frac{\varphi(n)}{\#H}.$$

PROOF. By Theorem 3.4.20, the splitting field of the eigenvalues of $\mathrm{Cay}(\mathbb{Z}_n, S)$ is given by $\mathbb{Q}(\zeta_n)^H$. Moreover, we have that

$$\varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n)^H][\mathbb{Q}(\zeta_n)^H : \mathbb{Q}] = \#H[\mathbb{Q}(\zeta_n)^H : \mathbb{Q}].$$

Since $\deg(\mathrm{Cay}(\mathbb{Z}_n, S)) = [\mathbb{Q}(\zeta_n)^H : \mathbb{Q}]$, the statement follows. □

3.4.3.7. *Circulant graphs of maximum algebraic degree.* It is easy to see that our results imply So's [92] characterization of integral circulant graphs. On the other hand, by Theorem 3.4.25 every circulant graph over $\mathbb{Z}_n$ is of algebraic degree at most $\varphi(n)$. Therefore, the circulant graphs of maximum algebraic degree (within the family of all circulant graphs) can be classified as follows:

COROLLARY 3.4.26. *A circulant graph* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *is of maximum algebraic degree if and only if* $\langle\langle S\rangle\rangle_{\mathcal{O}} = \mathbb{Q}\mathbb{Z}_n$.

COROLLARY 3.4.27. *A circulant graph* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *is of maximum algebraic degree if and only if* $S^H \neq S$ *for all* $H \leq \mathrm{Aut}(\mathbb{Z}_n)$ *with* $H \neq \{1\}$.

EXAMPLE 3.4.28. Every circulant graph of the form $\mathrm{Cay}(\mathbb{Z}_n, \{1, 2, 3\})$ for $n \geq 5$ (cf. Figure 3.10) is of maximum algebraic degree: Let $H \leq \mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^*$ and $1 \neq h \in H$. If $h \in \{4, \ldots, n-1\}$, then $h \cdot 1 \notin \{1, 2, 3\}$. If $h \in \{2, 3\}$ and $n > 5$, then $h \cdot 2 \in \{4, 6\}$. If $n = 5$ and $h = 3$, then $h \cdot 3 = 4 \notin \{1, 2, 3\}$. Thus, in all cases $\{1, 2, 3\}^H \neq \{1, 2, 3\}$.

Similarly, it can be shown that every circulant graph of the form $\mathrm{Cay}(\mathbb{Z}_n, \{1, 2, \ldots, r\})$ for $r < n - 1$ is of maximum algebraic degree.

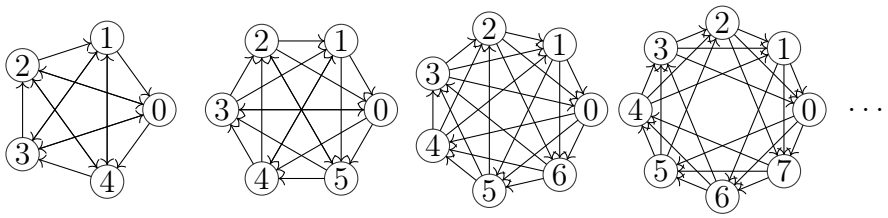


FIGURE 3.10. Family of circulant graphs $\mathrm{Cay}(\mathbb{Z}_n, \{1, 2, 3\})$ of maximum algebraic degree $\varphi(n)$.

3.4.3.8. *The inverse Galois problem for circulant graphs.* Since every splitting field of a circulant graph is a subfield of some cyclotomic field, it is natural to ask whether *every* subfield of a cyclotomic field is the splitting field of some circulant graph. In view of our results, we can give a positive answer to that question: Let $\mathbb{Q}(\zeta_n)^H$ be a subfield of the cyclotomic field $\mathbb{Q}(\zeta_n)$. Then, by Theorem 3.4.24 the field $\mathbb{Q}(\zeta_n)^H$ is the splitting field of the circulant graph $\mathrm{Cay}(\mathbb{Z}_n, H)$ since, obviously, $F = H$ is the maximum subgroup of $\mathrm{Aut}(\mathbb{Z}_n)$ such that $H^F = H$. Together with the well-known Kronecker-Weber theorem (see, for example, [78]), we deduce the following:

COROLLARY 3.4.29 (Inverse Galois problem for circulant graphs). *Every finite abelian extension of the rationals is the splitting field of some circulant graph.*

3.4.3.9. *New necessary criteria for isospectrality of circulant graphs.* It is clear that if two circulant graphs $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$ are isospectral, then their respective splitting fields must be the same. Therefore, as immediate consequences of Theorem 3.4.20 and Theorem 3.4.24, respectively, we get the following:

COROLLARY 3.4.30. *Let* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *and* $\mathrm{Cay}(\mathbb{Z}_n, T)$ *be two isospectral circulant graphs. Then,* $\langle\langle S\rangle\rangle_{\mathcal{O}} = \langle\langle T\rangle\rangle_{\mathcal{O}}$.

COROLLARY 3.4.31. *Let* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *and* $\mathrm{Cay}(\mathbb{Z}_n, T)$ *be two isospectral circulant graphs and let* $H \leq \mathrm{Aut}(\mathbb{Z}_n)$. *Then,* $S^H = S$ *if and only if* $T^H = T$.

3.4.3.10. *Automorphism groups of circulant graphs.* Recall that for a circulant graph $\mathrm{Cay}(\mathbb{Z}_n, S)$, a bijection $\sigma : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ is an automorphism of $\mathrm{Cay}(\mathbb{Z}_n, S)$ if $i - j \in S$ if and only if $\sigma(i) - \sigma(j) \in S$ for all $i, j \in \mathbb{Z}_n$.

THEOREM 3.4.32. *The field* $\mathbb{Q}(\zeta_n)^H$ *is the splitting field of* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *if and only if* H *is the maximum subgroup of* $\mathrm{Aut}(\mathbb{Z}_n)$ *such that* $H \leq \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_n, S))$.

PROOF. Let $\mathbb{Q}(\zeta_n)^H$ be the splitting field of $\mathrm{Cay}(\mathbb{Z}_n, S)$. Then $S^H = S$ by Theorem 3.4.24. In particular, $\sigma(S) = \{\sigma(s) \mid s \in S\} = S$ for all $\sigma \in H$. Now, let $i, j \in \mathbb{Z}_n$ with $i - j \in S$ and $\sigma \in H$. Since σ is an automorphism of $\mathbb{Z}_n$, it follows that

$$\sigma(i) - \sigma(j) = \sigma(i - j) \in \sigma(S) = S,$$

i.e. $\sigma \in \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_n, S))$. Conversely, if $i - j \notin S$, then $\sigma(i) - \sigma(j) \notin S$. This shows $H \leq \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_n, S))$. Assume that there is a bigger subgroup $F \leq \mathrm{Aut}(\mathbb{Z}_n)$ than H such that $F \leq \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_n, S))$. We may assume that $H \leq F$ (otherwise consider $\langle H \cup F\rangle$ instead of F). Let $\delta \in F$ with $\delta \notin H$. Since δ is an automorphism of $\mathrm{Cay}(\mathbb{Z}_n, S)$,

we have that $i - j \in S$ whenever $\delta(i) - \delta(j) = \delta(i - j) \in S$. Thus, $\delta(s) \in S$ for all $s \in S$, i.e. $\delta(S) \subseteq S$. Since δ is bijective, $\#\delta(S) = \#S$ and, therefore, $\delta(S) = S$. Moreover, since δ was chosen arbitrarily, we conclude that $S^F = S$. By Theorem 3.4.24 it follows that the splitting field of $\mathrm{Cay}(\mathbb{Z}_n, S)$ is given by $\mathbb{Q}(\zeta_n)^F$. But this is a subfield of $\mathbb{Q}(\zeta_n)^H$, a contradiction. This proves the first direction of the theorem. The proof for the other direction works analogously. □

Therefore, we may interpret the algebraic degree of circulant graphs as follows:

The smaller the algebraic degree of a circulant graph, the more automorphisms of $\mathbb{Z}_n$ are also automorphisms of the respective circulant graphs.

This shows that circulant graphs with lots of structure have a small algebraic degree. In particular, we may deduce the following:

COROLLARY 3.4.33. *The graph* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *is integral if and only if* $\mathrm{Aut}(\mathbb{Z}_n) \leq \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_n, S))$.

3.4.3.11. *Again: Circulant graphs on a prime number of vertices.* For a prime p, the structure of Schur rings over $\mathbb{Z}_p$ is simple:

THEOREM 3.4.34 ([65, Theorem 4.21]). *Every Schur ring over* $\mathbb{Z}_p$ *is an orbit S-ring for some subgroup of* $\mathrm{Aut}(\mathbb{Z}_p)$.

We may identify the automorphism group of $\mathbb{Z}_p$ with the multiplicative group $\mathbb{Z}_p^*$. Its proper subgroups are generated by the elements of $\mathbb{Z}_p^*$ which are not primitive roots modulo p. For each divisor d of $p - 1$ there is a unique subgroup of $\mathbb{Z}_p^*$ of order d. Let H_d denote this subgroup. Then, for every $k \in \mathbb{Z}_p$ with $k \neq 0$, the orbit k^{H_d} contains exactly d elements. Therefore, every Schur partition over $\mathbb{Z}_p$ is a union of $\{\{0\}\}$ and $(p-1)/d$ sets of size d for some divisor d of $p - 1$.

EXAMPLE 3.4.35. We consider the group $\mathbb{Z}_{13}$. Its automorphism group has the six subgroups $\{1\}, \{1, 3, 9\}, \{1, 3, 4, 9, 10, 12\}, \{1, 5, 8, 12\}$, $\{1, 12\}$ and $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$. Computing the respective orbits leads to the following six Schur partitions:

$\{\{0\}, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{6\}, \{7\}, \{8\}, \{9\}, \{10\}, \{11\}, \{12\}\}$

$\{\{0\}, \{1, 3, 9\}, \{2, 5, 6\}, \{4, 10, 12\}, \{7, 8, 11\}\}$

$\{\{0\}, \{1, 3, 4, 9, 10, 12\}, \{2, 5, 6, 7, 8, 11\}\}$

$\{\{0\}, \{1, 5, 8, 12\}, \{2, 3, 10, 11\}, \{4, 6, 7, 9\}\}$

$\{\{0\}, \{1, 12\}, \{2, 11\}, \{3, 10\}, \{4, 9\}, \{5, 8\}, \{6, 7\}\}$

$\{\{0\}, \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}\}$.

As a final remark, we want to sketch the connection between Theorem 3.4.5 and Theorem 3.4.25 (for the case where n is a prime number). As mentioned earlier, every Schur partition over $\mathbb{Z}_p$ is a union of $\{\{0\}\}$ and $(p-1)/d$ sets of size d for some divisor d of $p-1$. Therefore, if $0 \notin S$, we may always write S as a union of sets S_i of the same size m (say). Moreover, by the structure of $\langle\langle S\rangle\rangle_{\mathcal{O}}$, every set S_i is of the form $kH_m = \{kh \mid h \in H_m\}$ where $H_m \leq \mathbb{Z}_p^*$ denotes the unique subgroup of $\mathbb{Z}_p^*$ of order m. Hence, every element in H_m has order m and, therefore, $s_{i,1}^m = \ldots = s_{i,m}^m$ with $s_{i,j} \in S_i$ holds true for all $i = 1, \ldots, \#S/m$. This shows that $\langle\langle S\rangle\rangle_{\mathcal{O}} = \mathbb{Q}{\mathbb{Z}_p}^{H_m}$ if and only if m is the maximum common divisor of $\#S$ and $p-1$ such that S is m-decomposable.

3.4.4. Further questions. In view of the inverse Galois problem for circulant graphs, we wonder whether our results can be extended to Cayley graphs over non-cyclic groups.

Recall from the introduction that if G is abelian, every eigenvalue λ of a Cayley graph $\mathrm{Cay}(G, S)$ can be written in the form

$$\lambda = \chi(S) = \sum_{s \in S} \chi(S)$$

for some character χ of G. Let $\#G = n$ and $g \in G$. Since χ is a homomorphism, it follows that

$$(\chi(g))^n = \chi(ng) = \chi(0) = 1.$$

Thus, the minimal polynomial of $\chi(g)$ is a divisor of the polynomial

$$x^n - 1 = \prod_{i=0}^{n-1} (x - \zeta_n^i).$$

Hence, $\chi(g)$ and, therefore, every eigenvalue of $\mathrm{Cay}(G, S)$ is a linear combination of n-th roots of unity which implies that the splitting field of $\mathrm{Cay}(G, S)$ is a subfield of the cyclotomic field $\mathbb{Q}(\zeta_n)$. We wonder whether this is also true for Cayley graphs over non-abelian groups. In particular, we ask which number fields appear as splitting fields of Cayley graphs.

CHAPTER 4

Zero-divisor Graphs

4.1. Concept and intention

In this chapter, we study the interplay between graph-theoretic properties of the zero-divisor graph $\Gamma(R)$, the spectrum of $\Gamma(R)$ and the ring properties of R. As already mentioned, by now, surprisingly little is known about the eigenvalues and adjacency matrices of zero-divisor graphs.

We first clarify our definitions:

DEFINITION 4.1.1 (Zero-divisor graph). Let R be a finite commutative ring with $1 \neq 0$ and let $Z(R)$ denote its set of zero-divisors. Then, the *zero-divisor graph* $\Gamma(R)$ is defined as the graph with vertex set $Z^*(R) = Z(R)\backslash\{0\}$ where two (not necessarily distinct) vertices x, y are adjacent if and only if $xy = 0$.

DEFINITION 4.1.2 (Compressed zero-divisor graph). For an element $r \in R$ let $[r]_R = \{s \in R \mid \operatorname{ann}_R(r) = \operatorname{ann}_R(s)\}$ and $R_E = \{[r]_R \mid r \in R\}$. Then, the *compressed zero-divisor graph* $\Gamma_E(R)$ is defined as the graph with vertex set R_E where two (not necessarily distinct) vertices $[x]_R, [y]_R$ are adjacent if and only if $[x]_R[y]_R = [xy]_R = [0]_R$, i.e. $xy = 0$.

Note that by definition $\Gamma(R)$ has no multiple edges, and we can easily see that $\Gamma(R)$ is undirected if and only if R is commutative. Moreover, as already proven by Anderson and Livingston [11, Theorem 2.2], the graph $\Gamma(R)$ is finite if and only if R is finite or an integral domain. In the latter case, though, R has no zero-divisors at all and is just the empty graph. Hence, all our rings are assumed to be finite and commutative. However, in contrast to the original definition of Anderson and Livingston [11], we do not want to eliminate potential loops of our zero-divisor graphs since these loops provide important information of the structure of the ring R.

Motivated by the study of spectra of unitary Cayley graphs (cf. Section 2.1.4.2 of Chapter 2), our main approach is the following: since R is a finite ring, it can be written as $R \cong R_1 \times \ldots \times R_r$, where each R_i is a finite local ring. A proof for this and further results within the theory of finite commutative rings can be found in [19]. In Section 4.2 we introduce a graph product x_Γ with the property that

$$\Gamma(R) \cong \Gamma(R_1) \times_\Gamma \ldots \times_\Gamma \Gamma(R_r)$$

whenever $R \cong R_1 \times \ldots \times R_r$. With this graph product, in Section 4.3 we find a relation between the number of vertices of $\Gamma_E(R)$ and the property of R being a local ring. Moreover, we derive formulas for the number of vertices of the zero-divisor graph $\Gamma(R)$ and the compressed zero-divisor graph $\Gamma_E(R)$ in terms of the local rings R_i. From these formulas we can deduce a lower bound for the nullity of $\Gamma(R)$. In Section 4.4 we restrict our considerations to rings which are isomorphic to direct products of rings of integers modulo n, i.e. $R \cong \mathbb{Z}_{{p_1}^{t_1}} \times \ldots \times \mathbb{Z}_{{p_r}^{t_r}}$ for (not necessarily distinct) prime numbers p_i and positive integers r, t_i. For these rings, we find a criterion which may detect a local ring by considering its zero-divisor graph and the respective nullity. Moreover, we find the exact nullity of $\Gamma(R)$ and present an easy approach to determine also the non-zero eigenvalues of $\Gamma(R)$.

All results in this chapter are published in [66].

4.2. Products of zero-divisor graphs

Let $R \cong R_1 \times \ldots \times R_r$ be a ring, where each R_i is a finite local ring. Note that in this case $\#R_i = p_i^{t_i}$ for some prime numbers p_i and $t_i \in \mathbb{N}$. Our aim is to define a graph product $\times_\Gamma$ such that

$$\Gamma(R) \cong \Gamma(R_1) \times_\Gamma \ldots \times_\Gamma \Gamma(R_r)$$

whenever

$$R \cong R_1 \times \ldots \times R_r.$$

Since two vertices $(v_1, \ldots, v_r), (v_1', \ldots, v_r') \in R_1 \times \ldots \times R_r$ are adjacent in $\Gamma(R_1 \times \ldots \times R_r)$ if and only if $v_i, v_i' \in Z^*(R_i)$ or either $v_i = 0$ or $v_i' = 0$, our idea is the following: we first add the vertex $0 \in R_i$ and the units of R_i to the vertices of each zero-divisor graph $\Gamma(R_i)$, as well as edges from 0 to every other vertex. Then, we take the direct product of these somehow *extended zero-divisor graphs*, each of which we will denote by $\mathrm{E}\Gamma(R_i)$, which yields the extended zero-divisor graph $\mathrm{E}\Gamma(R)$. Finally, by removing the vertex $0 \in R$ with all its edges, as well as all units of R, we end up with the zero-divisor graph $\Gamma(R)$.

To formalize this, we define the *unit graph* $\mathrm{U}(R_i)$ of R_i as the graph with vertex set R_i^* and empty edge set. Moreover, let $\mathrm{Z}(R_i)$ and $\mathrm{Z}_\mathrm{L}(R_i)$ be the *zero graphs* with vertex set $\{0\}$ (where $0 \in R_i$) and empty edge set or edge set $\{\{0,0\}\}$, respectively (i.e. both graphs consist of one vertex only, and, in contrast to $\mathrm{Z}(R)$, the graph $\mathrm{Z}_\mathrm{L}(R)$ also has a loop at that vertex; we need this distinction for our result in Section 4.5).

Definition 4.2.1 (Extended zero-divisor graph). Let R be a finite commutative ring with $1 \neq 0$. Then, the *extended zero-divisor graph* $\mathrm{E}\Gamma(R)$ is defined as the graph with vertex set R where two (not necessarily distinct) vertices $x, y \in R$ are adjacent if and only if $xy = 0$.

In view of those definitions, the extended zero-divisor graph $\mathrm{E}\Gamma(R_i)$ is given by

$$\mathrm{E}\Gamma(R_i) = \big(\Gamma(R_i) \nabla \mathrm{Z}(R_i)\big) \overset{\{0\}}{\bullet} \big(\mathrm{U}(R_i) \nabla \mathrm{Z}_{\mathrm{L}}(R_i)\big),$$

and we have that

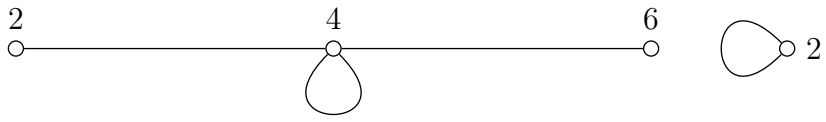
$$\Big(\Gamma(R) \cup \big(\mathrm{U}(R_1) \times \ldots \times \mathrm{U}(R_r)\big)\Big) \nabla \mathrm{Z}(R) \cong \mathrm{E}\Gamma(R_1) \times \ldots \times \mathrm{E}\Gamma(R_r).$$

Hence, we define the associative product $\times_\Gamma$ by

$$\Gamma(R_1) \times_\Gamma \Gamma(R_2) := \Big(\mathrm{E}\Gamma(R_1) \times \mathrm{E}\Gamma(R_2)\Big) \backslash \Big(V\big(\mathrm{Z}(R_1 \times R_2)\big) \cup V\big(\mathrm{U}(R_1 \times R_2)\big)\Big),$$

where $G\backslash\{v\}$ denotes the graph G without the vertex $v \in V(G)$ and all its adjacent edges. Note that $\mathrm{Z}(R_1 \times R_2) \cong \mathrm{Z}(R_1) \times \mathrm{Z}(R_2)$ and $\mathrm{U}(R_1 \times R_2) \cong \mathrm{U}(R_1) \times \mathrm{U}(R_2)$. The product $\times_\Gamma$ is illustrated in the following example:

Example 4.2.2. Let $R = \mathbb{Z}_8 \times \mathbb{Z}_4$. Figure 4.1 shows the zero-divisor graphs $\Gamma(\mathbb{Z}_8)$ and $\Gamma(\mathbb{Z}_4)$ and Figure 4.2 the extended zero-divisor graphs $\mathrm{E}\Gamma(\mathbb{Z}_8)$ and $\mathrm{E}\Gamma(\mathbb{Z}_4)$. In Figure 4.3 we see the direct product $\mathrm{E}\Gamma(\mathbb{Z}_8) \times \mathrm{E}\Gamma(\mathbb{Z}_4) \cong \mathrm{E}\Gamma(\mathbb{Z}_8 \times \mathbb{Z}_4)$ and Figure 4.4 finally illustrates the graph product $\Gamma(\mathbb{Z}_8) \times_\Gamma \Gamma(\mathbb{Z}_4) \cong \Gamma(\mathbb{Z}_8 \times \mathbb{Z}_4)$ arising from removing the vertices $(0,0)$ and $V(\mathrm{U}(\mathbb{Z}_8 \times \mathbb{Z}_4))$ from the graph $\mathrm{E}\Gamma(\mathbb{Z}_8) \times \mathrm{E}\Gamma(\mathbb{Z}_4)$.



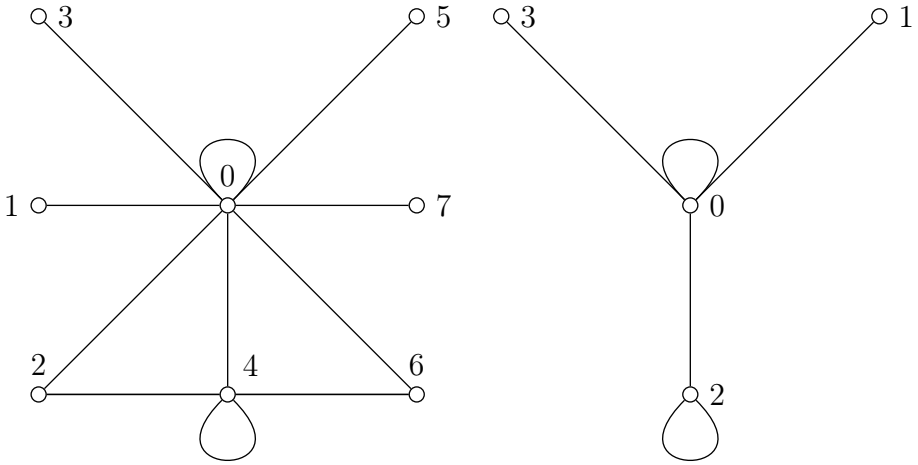
(a) $\Gamma(\mathbb{Z}_8)$ (b) $\Gamma(\mathbb{Z}_4)$

Figure 4.1. Zero-divisor graphs $\Gamma(\mathbb{Z}_8)$ and $\Gamma(\mathbb{Z}_4)$.

The same also holds true for the compressed zero-divisor graph, i.e. we have that $\Gamma_E(R) \cong \Gamma_E(R_1) \times_\Gamma \ldots \times_\Gamma \Gamma_E(R_r)$ whenever $R_E \cong R_{1E} \times \ldots \times R_{rE}$. In Section 4.5 we deduce a relation between the characteristic polynomial of $\Gamma(R)$ and the one of the extended zero-divisor graph $\mathrm{E}\Gamma(R)$.

4.3. Nullity of zero-divisor graphs of finite commutative rings

The following lemma follows directly from the construction of the product $\times_\Gamma$:



(a) $E\Gamma(\mathbb{Z}_8)$ (b) $E\Gamma(\mathbb{Z}_4)$

FIGURE 4.2. Extended zero-divisor graphs $E\Gamma(\mathbb{Z}_8)$ and $E\Gamma(\mathbb{Z}_4)$.

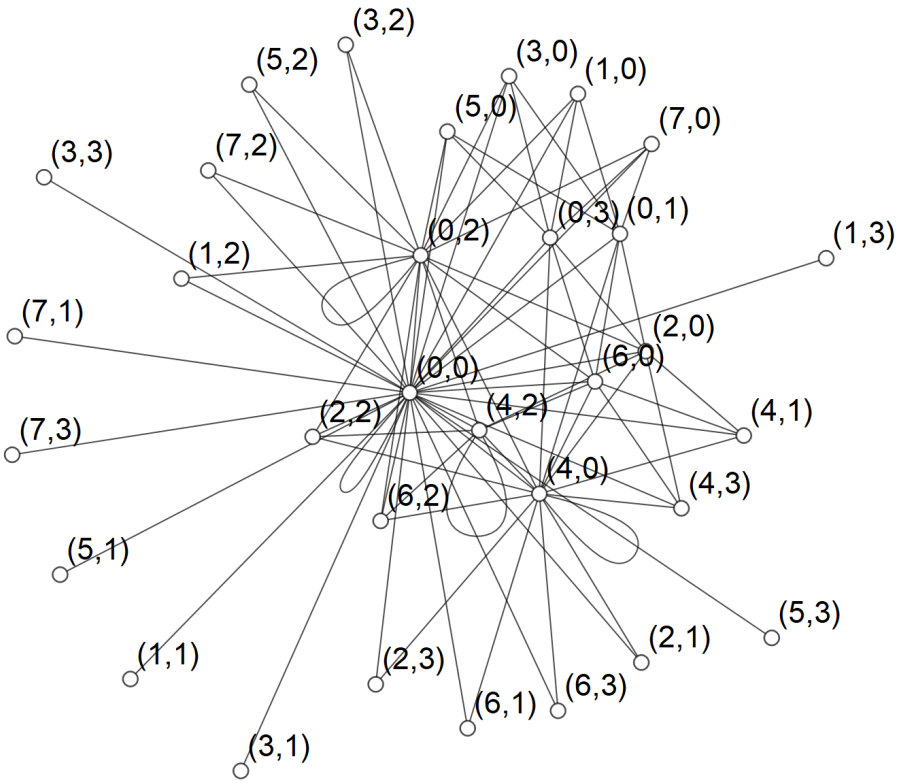


FIGURE 4.3. Direct product $E\Gamma(\mathbb{Z}_8) \times E\Gamma(\mathbb{Z}_4) \cong E\Gamma(\mathbb{Z}_8 \times \mathbb{Z}_4)$.

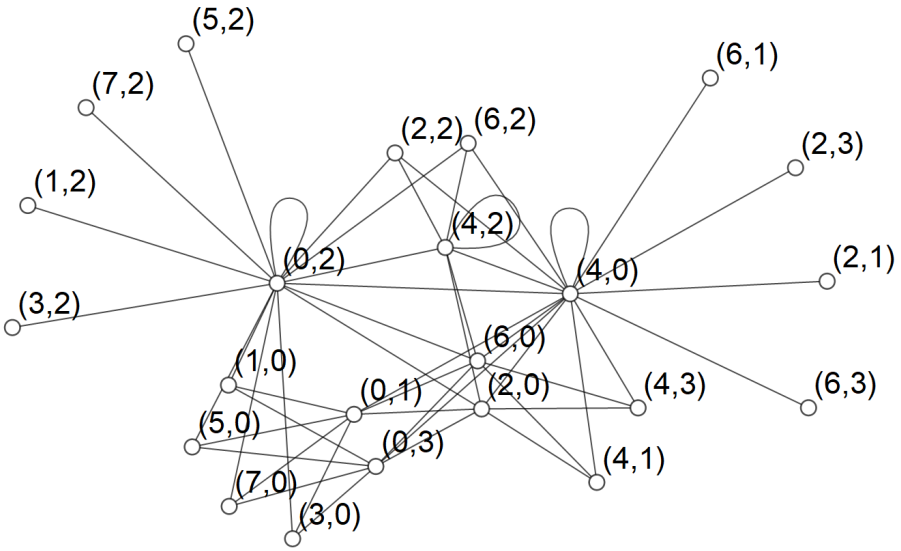


FIGURE 4.4. Zero-divisor graph $\Gamma(\mathbb{Z}_8 \times \mathbb{Z}_4) \cong \Gamma(\mathbb{Z}_8) \times_\Gamma \Gamma(\mathbb{Z}_4)$.

LEMMA 4.3.1. *Let $R \cong R_1 \times \ldots \times R_r$ with local rings R_i. Then the number of non-zero zero-divisors of R, i.e. the number of vertices of the zero-divisor graph $\Gamma(R)$ equals*

$$\begin{aligned}\#V(\Gamma(R)) &= \prod_{i=1}^{r} \#R_i - \prod_{i=1}^{r} \#V(\mathrm{U}(R_i)) - 1 \\ &= \prod_{i=1}^{r} \#R_i - \prod_{i=1}^{r} \#R_i^* - 1.\end{aligned}$$

PROOF. We have that $\#V(\mathrm{E}\Gamma(R_i)) = \#Z^*(R_i) + \#R_i^* + 1 = \#R_i$ since $R_i = Z^*(R_i) \cup R_i^* \cup \{0\}$. Taking into account that $\mathrm{E}\Gamma(R) \cong \mathrm{E}\Gamma(R_1) \times \ldots \times \mathrm{E}\Gamma(R_r)$, we therefore get that $\#V(\mathrm{E}\Gamma(R)) = \prod_{i=1}^{r} \#R_i$. Finally, since $\Gamma(R)$ arises from $\mathrm{E}\Gamma(R)$ by removing the vertex $0 \in R$ and all units of R (where each unit of R is a direct product of units of the R_i's), the statement follows. □

Moreover, we get a similar result for the number of vertices of the compressed zero-divisor graph:

LEMMA 4.3.2. *Let $R \cong R_1 \times \ldots \times R_r$ with local rings R_i. Then the number of vertices of the compressed zero-divisor graph $\Gamma_E(R)$ equals*

$$\begin{aligned}\#V(\Gamma_E(R)) &= \prod_{i=1}^{r} \big(\#V(\Gamma_E(R_i)) + 2\big) - 2 \\ &= \prod_{i=1}^{r} \#R_{iE} - 2.\end{aligned}$$

PROOF. Since the R_i's are finite rings, each element of R_i is either a zero-divisor or a unit. Thus, the elements of R_{iE} are exactly the vertices of $\Gamma_E(R_i)$ together with $[0]_{R_i}$ and $[1]_{R_i}$ (since the elements of $[1]_{R_i}$ are exactly the units of R_i). The statement follows from the construction of $\times_\Gamma$. □

Of course, those results are not very surprising since every non-zero-divisor of a finite commutative ring is a unit, i.e. $\#Z^*(R) = \#R - \#U(R) - 1$. However, from the latter lemma we observe that if $\#V(\Gamma_E(R)) + 2$ is a prime number, then R must be a local ring. This provides a notable relation between combinatorial objects (the zero-divisor graphs) and algebraic structures (the respective rings).

EXAMPLE 4.3.3. Let $R = \mathbb{Z}_3[[X,Y]]/(XY, X^3, Y^3, X^2 - Y^2)$. The respective compressed zero-divisor graph $\Gamma_E(R)$ has 5 vertices, see Figure 4.5. Since $5 + 2 = 7$ is a prime number, R has to be a local ring.

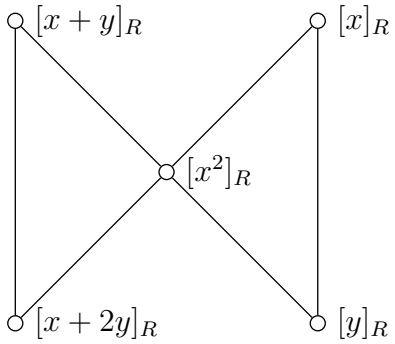


FIGURE 4.5. Compressed Zero-divisor graph $\Gamma_E(R)$ for $R = \mathbb{Z}_3[[X,Y]]/(XY, X^3, Y^3, X^2 - Y^2)$.

Moreover, we can derive a lower bound for the nullity of zero-divisor graphs:

THEOREM 4.3.4. *Let $R \cong R_1 \times \ldots \times R_r$ with local rings R_i. Then the nullity of the zero-divisor graph $\Gamma(R)$ is at least*

$$\eta(\Gamma(R)) \geq \prod_{i=1}^{r} \#R_i - \prod_{i=1}^{r} \#R_i^* - \prod_{i=1}^{r} \big(\#V(\Gamma_E(R_i)) + 2\big) + 1.$$

PROOF. Each element of $[r]_R \in V(\Gamma_E(R))$ contributes exactly the same row to the adjacency matrix $A(\Gamma(R))$. Thus, $\operatorname{rank} A(\Gamma(R)) \leq \#Z^*(R_E) = \#V(\Gamma_E(R))$. Since $\eta(\Gamma(R)) = \dim A(\Gamma(R)) - \operatorname{rank}(A(\Gamma(R)))$ and $\dim A(\Gamma(R)) = \#Z^*(R) = \#V(\Gamma(R))$, we have that $\eta(\Gamma(R)) \geq \#V(\Gamma(R)) - \#V(\Gamma_E(R))$. The statement follows with Theorems 4.3.1 and 4.3.2. □

4.4. Spectra of zero-divisor graphs of direct products of rings of integers modulo n

As already observed by Young [104], the adjacency matrix of the compressed zero-divisor graph is a so-called *equitable partition* of the adjacency matrix of $\Gamma(R)$. A formal definition for this is given in [24]. We define the *weighted adjacency matrix* $\mathcal{A}(\Gamma_E(R))$ of the compressed zero-divisor graph as the matrix with (i,j)-th entry

$$\mathcal{A}(\Gamma_E(R))_{i,j} = \begin{cases} 0, & \text{if } A(\Gamma_E(R))_{i,j} = 0, \\ \#[j]_R, & \text{else.} \end{cases}$$

From [24, Lemma 2.3.1] it follows that every eigenvalue of $\mathcal{A}(\Gamma_E(R))$ is also an eigenvalue of $A(\Gamma(R))$. In general, it is not clear whether these eigenvalues are exactly the non-zero eigenvalues of $\Gamma(R)$, i.e. whether $\mathcal{A}(\Gamma_E(R))$ always has full rank. But assuming that R is a product of rings of integers modulo n, we can prove the following:

THEOREM 4.4.1. *Let $R \cong \mathbb{Z}_{{p_1}^{t_1}} \times \ldots \times \mathbb{Z}_{{p_r}^{t_r}}$ for prime numbers p_j and $r, t_j \in \mathbb{N}$. Then,*

$$\operatorname{rank} A(\Gamma(R)) = \operatorname{rank} \mathcal{A}(\Gamma_E(R)) = \#V(\Gamma_E(R)).$$

PROOF. We can easily see that $\operatorname{rank} A(\Gamma(R)) = \operatorname{rank} \mathcal{A}(\Gamma_E(R))$ since for every $r \in R$, each element of $[r]_R$ contributes exactly the same row to the adjacency matrix $A(\Gamma(R))$. Thus, it suffices to show that $\operatorname{rank} \mathcal{A}(\Gamma_E(R)) = \#V(\Gamma_E(R))$. The matrix $\mathcal{A}(\Gamma_E(R_i))$ for $R_i = \mathbb{Z}_{{p_i}^{t_i}}$ is of the form

$$\begin{pmatrix} 0 & 0 \cdots\cdots\cdots\cdots 0 & p_i - 1 \\ 0 & 0 \cdots\cdots\cdots\cdots p_i(p_i-1) & p_i - 1 \\ \vdots & \vdots \qquad\qquad \iddots \qquad \vdots & \vdots \\ 0 & p_i^{t_i-3}(p_i-1) \cdots\cdots p_i(p_i-1) & p_i - 1 \\ p_i^{t_i-2}(p_i-1) & p_i^{t_i-3}(p_i-1) \cdots\cdots p_i(p_i-1) & p_i - 1 \end{pmatrix}$$

since $V(\Gamma_E(R_i)) = \{[p_i]_{R_i}, [p_i^2]_{R_i}, \ldots, [p_i^{t_i-1}]_{R_i}\}$ and

$$\#[p_i^k]_{R_i} = \#\{x \mid \gcd(x, {p_i}^{t_i}) = p_i^k\} = \varphi({p_i}^{t_i}/p_i^k) = {p_i}^{t_i-k-1}(p_i - 1).$$

Obviously, this matrix has full rank $\#V(\Gamma_E(R_i))$. Now, the graph $\mathrm{E}\Gamma_E(R_i)$ arises from $\Gamma_E(R_i)$ by adding the vertices $[1]_{R_i}$ and $[0]_{R_i}$ and the edges $\{[1]_{R_i}, [0]_{R_i}\}$,$\{[0]_{R_i}, [r]_{R_i}\}$ for all $[r]_{R_i} \in V(\Gamma_E(R_i))$. With an appropriate enumeration of the vertices of $\mathrm{E}\Gamma_E(R_i)$, it follows that the matrix $\mathcal{A}(\mathrm{E}\Gamma_E(R_i))$ equals

$$\begin{pmatrix} 0 & 0 \cdots\cdots\cdots\cdots 0 & 1 \\ 0 & & 1 \\ \vdots & \mathcal{A}\big(\Gamma_E(R_i)\big) & \vdots \\ 0 & & 1 \\ p_i^{t_i-1}(p-1) & p_i^{t_i-2}(p-1) \cdots\cdots p_i - 1 & 1 \end{pmatrix}.$$

This matrix has full rank, too. Since $\mathrm{E}\Gamma_E(R) \cong \mathrm{E}\Gamma_E(R_1) \times \ldots \times \mathrm{E}\Gamma_E(R_r)$, the matrix $\mathcal{A}(\mathrm{E}\Gamma_E(R))$ equals the Kronecker product $\mathcal{A}(\mathrm{E}\Gamma_E(R_1)) \otimes \ldots \otimes \mathcal{A}(\mathrm{E}\Gamma_E(R_r))$ which has the form

$$\begin{pmatrix} 0 & 0 \cdots\cdots\cdots\cdots 0 & 1 \\ 0 & & 1 \\ \vdots & \mathcal{A}\big(\Gamma_E(R)\big) & \vdots \\ 0 & & 1 \\ x_1 & x_2 \cdots\cdots x_{\#V(\Gamma_E(R))+1} & 1 \end{pmatrix}$$

for non-zero entries x_j. By the fact that the rank of the Kronecker product of two matrices equals the product of the ranks of these two matrices, we finally conclude that $\mathcal{A}(\mathrm{E}\Gamma_E(R))$, and therefore also $\mathcal{A}(\Gamma_E(R))$ has full rank, i.e. $\operatorname{rank}\mathcal{A}(\Gamma_E(R)) = \#V(\Gamma_E(R))$. □

With this result, we can easily prove the following corollary, which illustrates the interplay between rings of integers modulo n, zero-divisor graphs and their eigenvalues:

COROLLARY 4.4.2. *Let $R \cong \mathbb{Z}_{{p_1}^{t_1}} \times \ldots \times \mathbb{Z}_{{p_r}^{t_r}}$ for prime numbers p_j and $r, t_j \in \mathbb{N}$ and let $\Gamma(R)$ be its zero-divisor graph. If*

$$\#V(\Gamma(R)) - \eta(\Gamma(R)) + 2$$

is a prime number, then R is a local ring (i.e. $r = 1$).

PROOF. Since $\eta(\Gamma(R)) = \dim A(\Gamma(R)) - \operatorname{rank}(A(\Gamma(R))) = \#V(\Gamma(R)) - \operatorname{rank}(A(\Gamma(R)))$ and $\operatorname{rank}(A(\Gamma(R))) = \#V(\Gamma_E(R))$ by Theorem 4.4.1, we get that $\#V(\Gamma_E(R)) = \#V(\Gamma(R)) - \eta(\Gamma(R))$. As already mentioned above, if $\#V(\Gamma_E(R)) + 2$ is a prime number, then R must be a local ring. Thus, the statement follows. □

Moreover, we are able to improve Theorem 4.3.4:

THEOREM 4.4.3. *Let $R \cong \mathbb{Z}_{{p_1}^{t_1}} \times \ldots \times \mathbb{Z}_{{p_r}^{t_r}}$ for prime numbers p_j and $r, t_j \in \mathbb{N}$. Then the zero-divisor graph $\Gamma(R)$ has*

$$\prod_{i=1}^{r}(t_i + 1) - 2$$

non-zero eigenvalues, and the nullity of $\Gamma(R)$ equals

$$\eta(\Gamma(R)) = \prod_{i=1}^{r} p_i^{t_i - 1}\Big(\prod_{i=1}^{r} p_i - \prod_{i=1}^{r}(p_i - 1)\Big) - \prod_{i=1}^{r}(t_i + 1) + 1.$$

PROOF. By Theorem 4.4.1, the number of non-zero eigenvalues of $\Gamma(R)$ equals the number of vertices of the compressed zero-divisor graph $\Gamma_E(R)$. Since $V(\Gamma_E(R_i)) = \{[p_i]_{R_i}, [p_i^2]_{R_i}, \ldots, [p_i^{t_i - 1}]_{R_i}\}$, we deduce form Theorem 4.3.2 that

$$\#V(\Gamma_E(R)) = \prod_{i=1}^{r}(t_i + 1) - 2.$$

Moreover, the number of units in R_i is given by $\varphi(p_i^{t_i}) = p_i^{t_i-1}(p_i-1)$. Thus, by Theorem 4.3.1, we get that

$$\begin{aligned}\#V(\Gamma(R)) &= \prod_{i=1}^{r} p_i^{t_i} - \prod_{i=1}^{r} p_i^{t_i-1}(p_i-1) - 1 \\ &= \prod_{i=1}^{r} p_i^{t_i-1}\Big(\prod_{i=1}^{r} p_i - \prod_{i=1}^{r}(p_i-1)\Big) - 1.\end{aligned}$$

Since $\eta(\Gamma(R)) = \#V(\Gamma(R)) - \#V(\Gamma_E(R))$, the statement follows. □

Note that the number of non-zero eigenvalues of $\Gamma(\mathbb{Z}_{p_1{}^{t_1}} \times \ldots \times \mathbb{Z}_{p_r{}^{t_r}})$ does not depend on the prime numbers p_i but on the powers t_i only.

Now, we can easily determine the eigenvalues of $\Gamma(R)$ for $R \cong \mathbb{Z}_{p_1{}^{t_1}} \times \ldots \times \mathbb{Z}_{p_r{}^{t_r}}$. Theorem 4.4.3 gives us the number of eigenvalues equal to zero. The non-zero eigenvalues can be computed as in the proof of Theorem 4.4.1. We illustrate this in the following examples. Note that the eigenvalues of the graphs $\Gamma(\mathbb{Z}_{p^2}), \Gamma(\mathbb{Z}_{p^3}), \Gamma(\mathbb{Z}_p \times \mathbb{Z}_q)$ and $\Gamma(\mathbb{Z}_{p^2} \times \mathbb{Z}_q)$ for prime numbers $p \neq q$ were already determined by Young [104], and the ones of $\Gamma(\mathbb{Z}_p \times \mathbb{Z}_p)$ by Sharma et. al. [91].

Example 4.4.4. Let p be a prime number and $R \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$. By Theorem 4.4.3 the multiplicity of the eigenvalue 0 of $\Gamma(R)$ equals

$$\eta(\Gamma(R)) = (p^3 - (p-1)^3) - 2^3 + 1 = 3(p+1)(p-2).$$

The ring $\mathbb{Z}_p$ has no zero-divisors and, therefore, $\Gamma(\mathbb{Z}_p)$ is the empty graph. Thus, the matrix $\mathcal{A}(\mathrm{E}\Gamma_E(\mathbb{Z}_p))$ is given by

$$\mathcal{A}(\mathrm{E}\Gamma_E(\mathbb{Z}_p)) = \begin{pmatrix} 0 & 1 \\ p-1 & 1 \end{pmatrix}.$$

Now, we compute the Kronecker product

$$\mathcal{A}(\mathrm{E}\Gamma_E(\mathbb{Z}_p)) \otimes \mathcal{A}(\mathrm{E}\Gamma_E(\mathbb{Z}_p)) \otimes \mathcal{A}(\mathrm{E}\Gamma_E(\mathbb{Z}_p))$$

which yields the matrix

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & p-1 & 1 \\ 0 & 0 & 0 & 0 & 0 & p-1 & 0 & 1 \\ 0 & 0 & 0 & 0 & (p-1)^2 & p-1 & p-1 & 1 \\ 0 & 0 & 0 & p-1 & 0 & 0 & 0 & 1 \\ 0 & 0 & (p-1)^2 & p-1 & 0 & 0 & p-1 & 1 \\ 0 & (p-1)^2 & 0 & p-1 & 0 & p-1 & 0 & 1 \\ (p-1)^3 & (p-1)^2 & (p-1)^2 & (p-1) & (p-1)^2 & p-1 & p-1 & 1 \end{pmatrix}.$$

Hence, $\mathcal{A}(\Gamma_E(R))$ equals the submatrix

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & p-1 \\ 0 & 0 & 0 & 0 & p-1 & 0 \\ 0 & 0 & 0 & (p-1)^2 & p-1 & p-1 \\ 0 & 0 & p-1 & 0 & 0 & 0 \\ 0 & (p-1)^2 & p-1 & 0 & 0 & p-1 \\ (p-1)^2 & 0 & p-1 & 0 & p-1 & 0 \end{pmatrix},$$

which has characteristic polynomial

$$\begin{aligned}\chi_{\Gamma(R)}(x) = &-(-1+3p-3p^2+p^3+(1-p)x-x^2)^2\times \\ &\times(-1+3p-3p^2+p^3+2(p-1)x-x^2).\end{aligned}$$

The roots of this polynomial, i.e. the non-zero eigenvalues of $\Gamma(R)$, are

$$\lambda_{1,2} = \frac{1}{2}\big(1-p\pm(p-1)\sqrt{4p-3}\big), \quad \lambda_{3,4} = p-1\pm\sqrt{p-2p^2+p^3},$$

and, therefore, the spectrum of $\Gamma(R)$ equals

$$\operatorname{spec}(\Gamma(R)) = \big\{\lambda_1^{[2]}, \lambda_2^{[2]}, \lambda_3^{[1]}, \lambda_4^{[1]}, 0^{[3(p+1)(p-2)]}\big\} \quad \text{for } p>2,$$

and

$$\operatorname{spec}(\Gamma(\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2)) = \big\{\lambda_1^{[2]}, \lambda_2^{[2]}, \lambda_3^{[1]}, \lambda_4^{[1]}\big\}.$$

EXAMPLE 4.4.5. Let p be a prime number and $R\cong\mathbb{Z}_p\times\mathbb{Z}_p\times\mathbb{Z}_p\times\mathbb{Z}_p$. By Theorem 4.4.3 the multiplicity of the eigenvalue 0 of $\Gamma(R)$ equals

$$\eta(\Gamma(R)) = p^4-(p-1)^4-2^4+1.$$

Analogously as in Example 4.4.4, we find the matrix $\mathcal{A}(\Gamma_E(R))$ as a submatrix of the Kronecker product

$$\mathcal{A}(\mathrm{E}\Gamma_E(\mathbb{Z}_p))\otimes\mathcal{A}(\mathrm{E}\Gamma_E(\mathbb{Z}_p))\otimes\mathcal{A}(\mathrm{E}\Gamma_E(\mathbb{Z}_p))\otimes\mathcal{A}(\mathrm{E}\Gamma_E(\mathbb{Z}_p)).$$

The characteristic polynomial of this matrix is

$$\begin{aligned}\chi_{\Gamma(R)}(x) = &-(1-2p+p^2-x)^5(1-2p+p^2+x)\times \\ &\times\big(1-4p+6p^2-4p^3+p^4+(1+p-2p^2)x+x^2\big)\times \\ &\times\big(1-4p+6p^2-4p^3+p^4+(1-3p+2p^2)x+x^2\big)^3\end{aligned}$$

and has roots

$$\begin{aligned}\lambda_1 = (p-1)^2, \quad \lambda_2 = -p^2+p-1,\\ \lambda_{3,4} = \frac{1}{2}\big(-2p^2+3p-1\pm(p-1)\sqrt{4p-3}\big),\\ \lambda_{5,6} = \frac{1}{2}\big(2p^2-p-1\pm\sqrt{3}\sqrt{4p^3-9p^2+6p-1}\big).\end{aligned}$$

Hence, the spectrum of $\Gamma(R)$ is given by

$$\operatorname{spec}(\Gamma(R)) = \big\{\lambda_1^{[5]}, \lambda_2^{[1]}, \lambda_3^{[3]}, \lambda_4^{[3]}, \lambda_5^{[1]}, \lambda_6^{[1]}, 0^{[p^4-(p-1)^4-2^4+1]}\big\} \quad \text{for } p>2,$$

and

$$\operatorname{spec}(\Gamma(\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2)) = \big\{\lambda_1^{[5]}, \lambda_2^{[1]}, \lambda_3^{[3]}, \lambda_4^{[3]}, \lambda_5^{[1]}, \lambda_6^{[1]}\big\}.$$

EXAMPLE 4.4.6. Unfortunately, if we consider not only products of the ring $\mathbb{Z}_p$ but also of rings of the form $\mathbb{Z}_{p^t}$ for $t > 1$ or of the form $\mathbb{Z}_q$ for a prime $q \neq p$, the eigenvalues of $\Gamma(R)$ get very cumbersome. However, at least we want to include the characteristic polynomials of the graphs $\Gamma(\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_q)$ and $\Gamma(\mathbb{Z}_{p^2} \times \mathbb{Z}_p)$. Note that

$$\mathcal{A}(\mathrm{E}\Gamma_E(\mathbb{Z}_p)) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & p-1 & 1 \\ p(p-1) & p-1 & 1 \end{pmatrix}.$$

With the same method as in the latter examples, we find the polynomials

$$\begin{aligned}\chi_{\mathbb{Z}_p\times\mathbb{Z}_p\times\mathbb{Z}_q}(x) = &-(p-1)^6(q-1)^3 + (p-1)^3(q-1)\big(p(3q-2)-q\big)x^2 - \\ &- 2(p-1)^2(q-1)x^3 - (p-1)\big(p(3q-2)-q\big)x^4 + x^6,\end{aligned}$$

$$\chi_{\mathbb{Z}_{p^2}\times\mathbb{Z}_p}(x) = (p-1)^5 p + (p-1)^3 px - 2(p-1)^2 px^2 - (p-1)x^3 + x^4.$$

REMARK 4.4.7. It is clear that two rings are isomorphic only if their respective zero-divisor graphs are isomorphic. Moreover, two graphs are isomorphic only if they have the same characteristic polynomial. Thus, in order to see that two rings are non-isomorphic, it might help to compare the characteristic polynomials of their corresponding zero-divisor graphs.

4.5. The characteristic polynomial of zero-divisor graphs

In this section, we deduce a relation between $\chi_{\Gamma(R)}$ and $\chi_{\mathrm{E}\Gamma(R)}$.

Recall Lemma 2.1.9 and 2.1.10 from Chapter 2. We can easily see that the formula in Lemma 2.1.9 still holds true for graphs with loops if the graphs do not have loops on both vertices, v and w. Moreover, Hwang and Park [46] generalized the result of Lemma 2.1.10:

LEMMA 4.5.1 ([46, Theorem 2.5]). *Let $A \in \mathbb{R}^{m\times m}, B \in \mathbb{R}^{n\times n}, a, c \in \mathbb{R}^m, b, d \in \mathbb{R}^n$,*

$$M = \begin{pmatrix} A & ad^{\mathsf{t}} \\ bc^{\mathsf{t}} & B \end{pmatrix}$$

and $\tilde{A} = ac^{\mathsf{t}} - A, \tilde{B} = bd^{\mathsf{t}} - B$. Then

$$\begin{aligned}\chi_M(x) = (-1)^m\chi_{\tilde{A}}(-x)\chi_B(x) + (-1)^n\chi_A(x)\chi_{\tilde{B}}(-x) \\ - (-1)^{m+n}\chi_{\tilde{A}}(-x)\chi_{\tilde{B}}(-x).\end{aligned}$$

Therefore, in the following let $\overline{\mathcal{G}}$ denote the *generalized complement* of $\mathcal{G}$, i.e. the graph with same vertex set as $\mathcal{G}$, where two not necessarily distinct vertices are adjacent in $\overline{\mathcal{G}}$ whenever they are non-adjacent in $\mathcal{G}$. That is, the graph with adjacency matrix $A(\overline{\mathcal{G}}) = J - A(\mathcal{G})$, where J denotes the all-1 matrix. Now, we are able to prove the following:

THEOREM 4.5.2. *Let R be a finite commutative ring and $n = \#R^*$, i.e. the number of units in R. Then we have that*

$$\chi_{\mathrm{E}\Gamma(R)}(x) = x^{n-1}\big((-1)^{n+1}\chi_{\overline{\Gamma(R)}}(-x)x + \chi_{\Gamma(R)}(x)(x^2-n)\big).$$

PROOF. We recall that

$$\mathrm{E}\Gamma(R) = \big(\Gamma(R)\nabla\,\mathrm{Z}(R)\big) \overset{\{0\}}{\bullet} \big(\,\mathrm{U}(R)\nabla\,\mathrm{Z_L}(R)\big).$$

We first determine the characteristic polynomial of $\mathrm{U}(R)\nabla\,\mathrm{Z_L}(R)$ by applying Lemma 4.5.1 for $A = \big(1\big)$ and B being the zero-matrix of dimension $n \times n$. We can easily see that $\chi_A(x) = x - 1$, $\chi_{\tilde{A}}(x) = x$, $\chi_B(x) = x^n$ and $\chi_{\tilde{B}}(x) = x^{n-1}(x-n)$. Thus, we get

$$\begin{aligned}
\chi_{\mathrm{U}(R)\nabla\,\mathrm{Z_L}(R)}(x) &= \chi_M(x) \\
&= (-1)(-x)x^n + (-1)^n(x-1)(-x)^{n-1}(-x-n) - \\
&\quad - (-1)^{n+1}(-x)(-x)^{n-1}(-x-n) \\
&= x^{n-1}(x^2 - x - n).
\end{aligned}$$

Analogously, we find the characteristic polynomial of $\Gamma(R)\nabla\,\mathrm{Z}(R)$ for $A = \big(0\big)$ and $B = A(\Gamma(R))$ to be

$$\chi_{\Gamma(R)\nabla\,\mathrm{Z}(R)}(x) = (-1)^{n+1}\chi_{\overline{\Gamma(R)}}(-x) + \chi_{\Gamma(R)}(x)(x+1).$$

Finally, with Lemma 2.1.9 we get

$$\begin{aligned}
\chi_{\mathrm{E}\Gamma(R)}(x) &= \chi_{\mathrm{U}(R)\nabla\,\mathrm{Z_L}(R)}(x)\chi_{\Gamma(R)} + x^n\chi_{\Gamma(R)\nabla\,\mathrm{Z}(R)}(x) - x\cdot x^n\chi_{\Gamma(R)} \\
&= x^{n-1}(x^2-x-n)\chi_{\Gamma(R)}(x) + \\
&\quad + x^n\big((-1)^{n+1}\chi_{\overline{\Gamma(R)}}(-x) + \chi_{\Gamma(R)}(x)(x+1)\big) - \\
&\quad - x^{n+1}\chi_{\Gamma(R)}(x) \\
&= x^{n-1}\big((-1)^{n+1}\chi_{\overline{\Gamma(R)}}(-x)x + \chi_{\Gamma(R)}(x)(x^2-n)\big).
\end{aligned}$$

□

REMARK 4.5.3. If $R \cong R_1 \times \ldots \times R_r$, we can apply Theorem 4.5.2 to each of the rings R_i, which gives us the characteristic polynomials $\chi_{\mathrm{E}\Gamma(R_i)}$. By computing the roots of $\chi_{\mathrm{E}\Gamma(R_i)}$, we find the eigenvalues of $\mathrm{E}\Gamma(R)$ to be all possible products of these roots, since $\mathrm{E}\Gamma(R) \cong \mathrm{E}\Gamma(R_1) \times \ldots \times \mathrm{E}\Gamma(R_r)$. Unfortunately, it is difficult to extrapolate the eigenvalues of $\Gamma(R)$ from the ones of $\mathrm{E}\Gamma(R)$, since the characteristic polynomial $\chi_{\Gamma(R)}$ not only depends on $\chi_{\mathrm{E}\Gamma(R)}$, but also on the characteristic polynomial of the generalized complement of $\Gamma(R)$.

Bibliography

[1] A. Abdollahi and M. Jazaeri. On groups admitting no integral Cayley graphs besides complete multipartite graphs. *Applicable Analysis and Discrete Mathematics*, 7:119–128, 2013.

[2] A. Abdollahi and M. Jazaeri. Groups all of whose undirected Cayley graphs are integral. *European Journal of Combinatorics*, 38:102–109, 2014.

[3] A. Ádám. Research problem 2-10. *Journal of Combinatorial Theory*, 2:393, 1967.

[4] C. Adiga and H. Ariamanesh. Some Properties of Cayley Graphs on Symmetric Groups S_n. *International Journal of Algebra*, 6(17):807–813, 2012.

[5] A. Ahmady, J.P. Bell, and B. Mohar. Integral Cayley graphs and groups. *SIAM Journal on Discrete Mathematics*, 28(2):685–701, 2014.

[6] R. Akhtar, M. Boggess, T. Jackson-Henderson, I. Jiménez, R. Karpman, A. Kinzel, and D. Pritikin. On the unitary Cayley graph of a finite ring. *The Electronic Journal of Combinatorics*, 16(1), 2009, #R117.

[7] R.C. Alperin and B.L. Peterson. Integral sets and cayley graphs of finite groups. *The Electronic Journal of Combinatorics*, 19, 2012, #P44.

[8] B. Alspach and T.D. Parsons. Isomorphism of circulant graphs and digraphs. *Discrete Mathematics*, 25:97–108, 1979.

[9] B. Alspach and T.D. Parsons. A construction for vertex-transitive graphs. *Canadian Journal of Mathematics*, XXXIV(2):307–318, 1982.

[10] D.F. Anderson and J.D. LaGrange. Some remarks on the compressed zero-divisor graph. *Journal of Algebra*, 447:297–321, 2016.

[11] D.F. Anderson and P.S. Livingston. The Zero-Divisor Graph of a Commutative Ring. *Journal of Algebra*, 217:434–447, 1999.

[12] L. Babai. Spectra of cayley graphs. *Journal of Combinatorial Theory, Series B*, 27:180–189, 1979.

[13] L. Babai. Graph Isomorphism in Quasipolynomial Time [Extended Abstract]. In *Proceedings of the Forty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '16, page

684–697, New York, NY, USA, 2016. Association for Computing Machinery.

[14] S. Barik, D.Kalita, S.Pati, and G.Sahoo. Spectra of graphs resulting from various graph operations and products: a survey. *Special Matrices*, 6:323–342, 2018.

[15] H. Bass, D.R. Estes, and R.M. Guralnick. Eigenvalues of Symmetric Matrices and Graphs. *Journal of Algebra*, 168:536–567, 1994.

[16] D. Berger. Das Isomorphieproblem für zirkuläre Graphen. Bachelor's thesis, Universität Würzburg, 2020.

[17] J.C. Bermond, F. Comellas, and D.F. Hsu. Distributed Loop Computer-Networks: A Survey. *Journal of Parallel and Distributed Computing*, 24(1):2–10, 1995.

[18] P. Berrizbeitia and R.E. Giudici. On cycles in the sequence of unitary Cayley graphs. *Discrete Mathematics*, 282(1–3):239–243, 2004.

[19] G. Bini and F. Flamini. *Finite Commutative Rings and Their Applications*. Kluwer Academic Publisher, 2002.

[20] A. Boesch and R. Tindell. Circulants and Their Connectivities. *Journal of Graph Theory*, 8:487–499, 1984.

[21] W.G. Bridges and R.A. Mena. Rational Circulants with rational Spectra and Cyclic Strongly Regular Graphs. *Ars Combinatoria*, 8:143–161, 1979.

[22] W.G. Bridges and R.A. Mena. Rational g-matrices with rational eigenvalues. *Journal of Combinatorial Theory, Series A*, 32:264–280, 1982.

[23] I. Broere and J.H. Hattingh. Products of circulant graphs. *Quaestiones Mathematicae*, 13(2):192–216, 1990.

[24] A.E. Brouwer and W.H. Haemers. *Spectra of Graphs*. Springer-Verlag New York, 1st edition, 2012.

[25] L. Collatz and U. Sinogowitz. Spektren endlicher Grafen. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 21:63–77, 1957.

[26] D. M. Cvetković and S. Simić. Non-complete extended p-sum of graphs, graph angles and star partitions. *Publications de l'institut Mathématique*, 53(67):4–16, 1993.

[27] D.M. Cvetković, M. Doob, and H. Sachs. *Spectra of Graphs: Theory and Applications*. Academic Press, 1st edition, 1980.

[28] I.J. Dejter and R.E. Giudici. On Unitary Cayley Graphs. *Journal of Combinatorial Mathematics and Combinatorial Computing*, 18:121–124, 1995.

[29] B. Elspas and J. Turner. Graphs with Circulant Adjacency Matrices. *Journal of Combinatorial Theory*, 9:297–307, 1970.

[30] D.R. Estes. Eigenvalues of Symmetric Integer Matrices. *Journal of Number Theory*, 42:292–296, 1992.

[31] L. Euler. Solutio problematis ad geometriam situs pertinentis. *Euler Archive - All Works*, 53, 1741.

[32] S.A. Evdokimov and I.N. Ponomarenko. Circulant graphs: Recognizing and isomorphism testing in polynomial time. *St. Petersburg Mathematical Journal*, 15(6):813–835, 2004.

[33] M.E. Fisher. On Hearing the Shape of a Drum. *Journal of Combinatorial Theory*, 1:105–125, 1966.

[34] D. Fronček, A. Rosa, and J. Širáň. The Existence of Selfcomplementary Circulant Graphs. *European Journal of Combinatorics*, 17:625–628, 1996.

[35] E. Fuchs. Longest Induced Cycles in Circulant Graphs. *The Electronic Journal of Combinatorics*, 12, 2005, #R52.

[36] T. Gardemann. Konstruktionen integraler graphen. Master's thesis, Universität Würzburg, 2019.

[37] T. Gardemann and K. Mönius. Constructions of new integral graph families. *Electronic Journal of Graph Theory and Applications*, 9(1):207–213, 2021.

[38] C. Godsil, D.A. Holton, and B. McKay. The Spectrum of a Graph. In A. Dold, B. Eckmann, and C.H.C. Little, editors, *Lecture Notes in Mathematics*, pages 91–117. Springer, 1976.

[39] C. Godsil and G. Royle. *Algebraic Graph Theory*. Springer-Verlag New York, 2001.

[40] I. Gutman and B. Borovicanin. Nullity of graphs: an updated survey. *Zbornik Radova*, 14(22):137–154, 2011.

[41] P. Hansen, H. Mélot, and D. Stevanović. Integral complete split graphs. *Univerzitet u Beogradu. Publikacije Elektrotehničkog Fakulteta. Serija Matematika*, 13:89–95, 2002.

[42] F. Harary and A.J. Schwenk. *Which graphs have integral spectra?*, pages 45–51. Springer Berlin Heidelberg, Berlin, Heidelberg, 1974.

[43] E. Hückel. Quantentheoretische Beiträge zum Benzolproblem. *Zeitschrift für Physikalische Chemie*, 70:204–286, 1931.

[44] W.C. Herndon. Isospectral molecules. *Tetrahedron Letters*, 15(8):671–674, 1974.

[45] W.C. Herndon and M.L. Ellzey. Isospectral graphs and molecules. *Tetrahedron*, 31(2):99–107, 1975.

[46] S. Hwang and J. Park. Characteristic polynomial of a generalized complete product of matrices. *Linear Algebra and its Applications*, 434:1362–1369, 2011.

[47] A. Ilić and M. Bašić. New results on the energy of integral circulant graphs. *Applied Mathematics and Computation*, 218(7):3470–3482, 2011.

[48] W. Imrich and H. Izbicki. Associative Products of Graphs. *Monatshefte für Mathematik*, 80:277–281, 1975.

[49] G.A. Jones. Paley and the paley graphs. In Gareth A. Jones, Ilia Ponomarenko, and Jozef Širáň, editors, *Isomorphisms, Symmetry and Computations in Algebraic Graph Theory*, pages 155–183, Cham, 2020. Springer International Publishing.

[50] M. Kac. Can One Hear the Shape of a Drum? *The American Mathematical Monthly*, 73(4, Part 2: Papers in Analysis):1–23, 1966.

[51] D. Kiani and M.M.H. Aghaei. On the Unitary Cayley Graph of a Ring. *The Electronic Journal of Combinatorics*, 19(2), 2012, #P10.

[52] D. Kiani, M.M.H. Aghaei, Y. Meemark, and B. Suntornpoch. Energy of unitary Cayley graphs and gcd-graphs. *Linear Algebra and its Applications*, 435:1336–1343, 2011.

[53] M. Klin and I. Kovács. Automorphism groups of rational circulant graphs. *The Electronic Journal of Combinatorics*, 2012, #P35.

[54] M.C. Klin, N.L. Najmark, and R. Pöschel. Schur-rings over $\mathbb{Z}_{2^m}$. *Akademie der Wissenschaften der DDR, Berlin*, P-MATH-14/81, 1981.

[55] M.C. Klin and R. Pöschel. The isomorphism problern for circulant digraphs with p^n vertices. *Akademie der Wissenschaften der DDR, Berlin*, P-34/80, 1980.

[56] M.H. Klin and R. Pöschel. The König problem, the isomorphism problem for cyclic graphs and the characterization of Schur rings. *Colloquia Mathematica Societatis János Bolyai, 25. Algebraic Methods in Graph Theory, Szeged (Hungary)*, 1978.

[57] W. Klotz and T. Sander. Some properties of unitary Cayley graphs. *The Electronic Journal of Combinatorics*, 14(1), 2007, #R45.

[58] W. Klotz and T. Sander. Integral Cayley graphs over abelian groups. *The Electronic Journal of Combinatorics*, 17, 2010, #R81.

[59] W. Klotz and T. Sander. Integral Cayley graphs defined by greatest common divisors. *The Electronic Journal of Combinatorics*, 18(1), 2011, #P94.

[60] W. Klotz and T. Sander. GCD-Graphs and NEPS of Complete Graphs. *ARS Mathematica Contemporanea*, 6:289–299, 2013.

[61] B. Litow and B. Mans. A note on the Ádám conjecture for double loops. *Information Processing Letters*, 66(3):149–153, 1998.

[62] X. Liu and S. Zhou. Spectral properties of unitary Cayley graphs of finite commutative rings. *The Electronic Journal of Combinatorics*, 19(4), 2012, #P13.

[63] L. Lovász. Spectra of Graphs with transitive Groups. *Periodica Mathematica Hungarica*, 6(2):191–195, 1975.

[64] B. Mans, F. Pappalardi, and I.E. Shparlinski. On the spectral Ádám property for circulant graphs. *Discrete Mathematics*,

254:309–329, 2002.

[65] A.F. Misseldine. *Algebraic and Combinatorial Properties of Schur Rings over Cyclic Groups*. PhD thesis, Brigham Young University, https://scholarsarchive.byu.edu/etd/5259, 2014.

[66] K. Mönius. Eigenvalues of zero-divisor graphs of finite commutative rings. *Journal of Algebraic Combinatorics*, 2020, https://doi.org/10.1007/s10801-020-00989-6.

[67] K. Mönius. Splitting fields of spectra of circulant graphs. 2020, submitted.

[68] K. Mönius. Constructions of isospectral circulant graphs. *Elemente der Mathematik*, 75(2):45–57, 2020.

[69] K. Mönius. The algebraic degree of spectra of circulant graphs. *Journal of Number Theory*, 208:295–304, 2020.

[70] K. Mönius, J. Steuding, and P. Stumpf. Which Graphs have Non-integral Spectra? *Graphs and Combinatorics*, 34(6):1507–1518, 2018.

[71] S.B. Mulay. Cycles and symmetries of zero-divisors. *Communications in Algebra*, 30(7):3533–3558, 2007.

[72] M. Muzychuk. The Structure of Rational Schur Rings over Cyclic Groups. *European Journal of Combinatorics*, 14:479–490, 1993.

[73] M. Muzychuk. On the structure of basic sets of schur rings over cyclic groups. *Journal of Algebra*, 169:655–678, 1994.

[74] M. Muzychuk. On Ádám's conjecture for circulant graphs. *Discrete Mathematics*, 167/168:497–510, 1997.

[75] M. Muzychuk. A solution of the isomorphism problem for circulant graphs. *Proceedings of the London Mathematical Society*, 88(3):1–41, 2004.

[76] M. Muzychuk, M. Klin, and R. Pöschel. The isomorphism problem for circulant graphs via Schur ring theory. *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, 56:241–264, 2001.

[77] M. Muzychuk and R. Pöschel. Isomorphism criteria for circulant graphs, 1999. Preprint Math-AL-91999, Technische Universität Dresden.

[78] J. Neukirch. *Algebraische Zahlentheorie*. Springer, 1992.

[79] N.F. Omondi, O.M. Onyango, and O.M. Oduor. On the Adjacency and Incidence matrices of the Zero divisor graphs of A class of the Square Radical Zero finite commutative Rings. *International Journal of Pure and Applied Mathematics*, 118(3):773–789, 2018.

[80] R.E.A.C. Paley. On orthogonal matrices. *Journal of Mathematics and Physics*, 14(1–4):311–320, 1933.

[81] T.D. Parsons. Circulant graphs imbeddings. *Journal of Combinatorial Theory, Series B*, 29:310–320, 1980.

[82] S. Pirzada and M. Imran Bhat. Computing metric dimension of compressed zero divisor graphs associated to rings. *Acta Universitatis Sapientiae, Mathematica*, 10(2):298–318, 2018.

[83] L. Rédei. Natürliche Basen des Kreisteilungskörpers, Teil I. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 23:180–200, 1959.

[84] G. Sabidussi. Graph multiplication. *Mathematische Zeitschrift*, 72(1):446–457, 1959.

[85] J. Salez. Every totally real algebraic integer is a tree eigenvalue. *Journal of Combinatorial Theory, Series B*, 111:249–256, 2015.

[86] J.W. Sander. Structural properties and formulae of the spectra of integral circulant graphs. *Acta Arithmetica*, 184:297–315, 2018.

[87] J.W. Sander and T. Sander. On So's conjecture for integral circulant graphs. *Applicable Analysis and Discrete Mathematics*, 9(1):59–72, 2015.

[88] R.S. Sanders. Products of circulant graphs are metacirculant. *Journal of Combinatorial Theory, Series B*, 85:197–206, 2002.

[89] N. Saxena, S. Severini, and I.E. Shparlinski. Parameters of integral circulant graphs and periodic quantum dynamics. *International Journal of Quantum Information*, 5(3), 2007.

[90] Á. Seress. Large Families of Cospectral Graphs. *Designs, Codes and Cryptography*, 21:205–208, 2000.

[91] P. Sharma, A. Sharma, and R.K. Vats. Analysis of Adjacency Matrix and Neighborhood Associated with Zero Divisor Graph of Finite Commutative Rings. *International Journal of Computer Applications*, 14(3):38–42, 2011.

[92] W. So. Integral circulant graphs. *Discrete Mathematics*, 306:153–158, 2005.

[93] S. Spiroff and C. Wickham. A zero divisor graph determined by equivalence classes of zero divisors. *Communications in Algebra*, 39:2338–2348, 2011.

[94] D. Stevanović. Applications of graph spectra in quantum physics. In *Selected Topics on Applications of Graph Spectra*, pages 85–111. Beograd: Matematički Institut SANU, 2011.

[95] R.G. Tirop, O.M. Oduor, and O.L. Olwamba. On the Adjacency Matrices of the Anderson-Livingston Zero Divisor Graphs of Galois Rings. *International Journal of Algebra*, 13(4):153–160, 2019.

[96] S. Toida. A Note on Ádám's conjecture. *Journal of Combinatorial Theory*, 23:239–246, 1977.

[97] V. Vilfred. *Σ-labelled graphs and circulant graphs*. PhD thesis, University of Kerala, Thiruvananthapuram, India, 1994.

[98] V. Vilfred. A Theory of Cartesian Product and Factorization of Circulant Graphs. *Journal of Discrete Mathematics*, 2013, Article ID 163740, 2013.

[99] L. Wang, H. Broersma, C. Hoede, X. Li, and G. Still. Some families of integral graphs. *Discrete Mathematics*, 308:6383–6391, 2008.

[100] L. Wang, X. Li, and S. Zhang. Construction of integral graphs. *Applied Mathematics-A Journal of Chinese Universities Series B*, 15:239–246, 2000.

[101] D. Weber. Zero-Divisor Graphs and Lattices of Finite Commutative Rings. *Rose-Hulman Undergraduate Mathematics Journal*, 12(1):57–70, 2011.

[102] H. Wielandt. *Finite permutation groups*. Academic Press, New York, 1964.

[103] J. Witschel. Eine Analyse isospektraler, zirkulärer Graphen mithilfe von computerberechneten Beispielen. Bachelor's thesis, Universität Würzburg, 2019.

[104] M. Young. Adjacency matrices of zero-divisor graphs of integers modulo n. *Involve*, 8(5):753–762, 2015.

[105] F. Zhang. *Matrix Theory*. Springer-Verlag New York, 2nd edition, 2011.