Diplomarbeit

Theory of m-Schemes and Applications to Polynomial Factoring

(m-Schemes und ihre Anwendungen in der Polynomfaktorisierung)

Angefertigt am
Mathematischen Institut

Vorgelegt der
Mathematisch-Naturwissenschaftlichen Fakultät der
Rheinischen Friedrich-Wilhelms-Universität Bonn

06/2010

Von

Manuel Arora

Kurzfassung

Im Folgenden fasse ich in verkürzter Form die wichtigsten Ideen und Resultate meiner Diplomarbeit mit dem Titel "Theory of m-Schemes and Applications to Polynomial Factoring" (zu Deutsch: "m-Schemes und ihre Anwendungen in der Polynomfaktorisierung") in deutscher Sprache zusammen. Das Thema dieser Arbeit ist ein neuer Ansatz für die Polynomfaktorisierung über endlichen Körpern, kürzlich vorgeschlagen von Ivanyos, Karpinski und Saxena (siehe [16]). Die Polynomfaktorisierung über endlichen Körpern ist ein Problem mit wesentlichen Anwendungen in der Kodierungstheorie und in der Faktorisierung natürlicher Zahlen, allerdings konnte für dieses Problem bisher kein deterministischer Polynomialzeitalgorithmus gefunden werden.

Die Diplomarbeit ist unterteilt in insgesamt fünf Kapitel. In den ersten zwei Kapiteln dieser Diplomarbeit beschäftigen wir uns mit "association schemes", kombinatorische Objekte für welche im deutschen Sprachraum noch kein einheitlicher Terminus gefunden wurde. Eine exakte Definition von "association schemes" ist wie folgt:

Definition 0.1 (Association Scheme)**.** *Sei X eine endliche Menge und G eine Menge bestehend aus Teilmengen von $X \times X$. Wir nennen (X, G) ein association scheme, wenn*

(i) $X \times X$ *eine disjunkte Vereinigung der* $g \in G$ *ist*

(ii) G *die triviale Relation* $1 := \{(x, x) \mid x \in X\}$ *enthält*

(iii) Für alle $g \in G$ *gilt:* $g^* := \{(y, x) \mid (x, y) \in g\} \in G$

(iv) Für alle $f, g, h \in G$ *existiert eine natürliche Zahl* a_{fgh} *sodass für alle* $(\alpha, \beta) \in h$ *gilt:*

$$a_{fgh} = |\{\gamma \in X \mid (\alpha, \gamma) \in f \text{ and } (\gamma, \beta) \in g\}| \ .$$

Ein Element $g \in G$ wird als Relation (oder Farbe) von (X, G) bezeichnet. Wir nennen $|X|$ die Ordnung von (X, G) und $n_g = a_{gg^*1}$ die Valenz von $g \in G$. Wenn $a_{fgh} = a_{gfh}$ für alle $f, g, h \in G$, dann nennen wir (X, G) ein kommutatives association scheme.

Das Hauptergebnis aus den ersten zwei Kapiteln lautet wie folgt: Ist die Ordnung eines association scheme (X, G) eine Primzahl, d.h. $|X| = p$, dann haben alle

$1 \neq g \in G$ die selbe Valenz (siehe [13]). Dieses relativ einfach anmutende Resultat basiert auf schwerwiegenden Theoremen aus Algebra und Darstellungstheorie - wir werden diese in aller Ausführlichkeit in den ersten beiden Kapiteln erklären.

In Kapitel 3 verallgemeinern wir den Begriff des association scheme, und führen das m-scheme ein (siehe [16]). Leider lässt sich die Definition eines m-scheme nicht in der selben Kürze angeben wie die des association scheme, daher verweisen wir an dieser Stelle auf Sektion 3.1 der Diplomarbeit. Es macht dennoch Sinn, in dieser Kurzfassung einige der Eigenheiten von m-schemes zu besprechen; hier geht es uns vor allem um die sog. "Matchings", kombinatorische Substrukturen innerhalb des m-scheme. Wir zeigen in der Diplomarbeit, unter welchen Umständen ein m-scheme ein Matching enthalten muss, und besprechen in diesem Zusammenhang auch die bisher unbewiesene Schemes Conjecture, welche die Existenz von Matchings in einen sehr generellen Zusammenhang setzt. Als Beispiel für unsere Überlegungen über m-schemes dienen uns die sog. orbit m-schemes, welche in einer speziellen, einfachen Weise entstehen (durch Gruppenaktion), und für welche die Schemes Conjecture sogar schon bewiesen ist.

Wir erweitern unsere Kenntnis über m-schemes in Kapitel 4, wenn wir mit Hilfe der algebraischen Topologie versuchen, zu einem geometrisches Verständnis von m-schemes zu gelangen. Unser Ansatz basiert auf der Feststellung, dass m-schemes als Δ-Mengen (auch simpliziale Mengen genannt) klassifiziert werden können, welche sehr häufig in der algebraischen Topologie auftauchen (siehe [27]). Damit lassen sie sich auf die übliche Weise geometrisch realisieren und mit Mitteln der Homologie untersuchen. Wir glauben, dass die geometrische Anschauung den kombinatorischen Definitionen noch mehr Deutlichkeit verleiht, und dass der vorgestellte Ansatz in der kommenden Zeit interessante Möglichkeiten für weitere Forschung bietet.

Im finalen Kapitel 5 wenden wir uns dann der Anwendung der Theorie der m-schemes in der Polynomfaktorisierung über endlichen Körpern zu. Wir stellen einen neuen Ansatz für dieses Problem vor, welcher von Ivanyos, Karpinski und Saxena entdeckt wurde (siehe [16]). Die o.g. Forscher haben einen Algorithmus entwickelt (im folgenden IKS-Algorithmus genannt), welcher auf Eingabe eines Polynomes entweder einen nichttrivialen Faktor desselben ausgibt oder ein Matching-freies m-scheme konstruiert und ausgibt. Nun kommt der Clue: Da der IKS-Algorithmus nur m-schemes von sehr spezieller Beschaffenheit ausgeben kann, können wir in einigen Fällen mit Sicherheit davon ausgeben, dass diese ein Matching enthalten müssen. Der entstehende Widerspruch sorgt dafür, dass in einigen wichtigen Fällen der Algorithmus

einen nichttrivialen Faktor ausgeben muss! Genau dieser Sachverhalt wird uns in Kapitel 5 zugute kommen, und sorgt dafür, dass sich die Laufzeitabschätzungen des IKS-Algorithmus bisweilen auf komplett kombinatorische Probleme reduzieren.

Bevor wir diese Kurzfassung abschließen, möchte ich noch kurz auf die benötigten Vorkenntnisse für das Studium dieser Diplomarbeit eingehen. Mit Hilfe des ersten Kapitels, "Algebraic Prerequisites", hoffen wir, die Zeit des Einlesens auf ein Minimum reduzieren zu können. Für eine Vertiefung der relevanten Gebiete Algebra und Darstellungstheorie empfehlen wir überdeß das Buch von Nagao und Tsushima (siehe [23]), welches fast alle relevanten Definitionen und Sätze enthält, die wir in dieser Arbeit brauchen. Eine zusätzliche wichtige Vorraussetzung für das Lesen dieses Textes ist ein solides Verständnis von linearer Algebra.

Introduction

The present text, titled "Theory of m-Schemes and Applications to Polynomial Factoring", constitutes my Diplom thesis, written under the supervision of Prof. Dr. Nitin Saxena at the Hausdorff Center for Mathematics in Bonn. It describes a new approach to the computational problem of polynomial factoring over finite fields, suggested recently by Ivanyos, Karpinski and Saxena (see [16]). Polynomial factoring over finite fields is a problem with major applications to coding theory and integer factoring, but no determinstic polynomial-time algorithm has been found for it so far.

The emphasis of this work is on the explanation of the combinatorial results leading to Ivanyos, Karpinski and Saxena's discovery of a new GRH-based deterministic algorithm for the factoring problem (called *IKS-algorithm* in the following). The core idea of the IKS-algorithm is the use of combinatorial schemes (association schemes, m-schemes) in the manipulation of algebraic data generated by the input polynomial. While the reader may have come across association schemes before - there are plenty of introductory texts on this subject, for example [4] or [31] - it is unlikely that he or she had much exposure to the more general m-schemes, since they have sprung in direct conjunction with the IKS-algorithm and only been studied in [16] so far. In this work, I explain all the necessary definitions and results for the use of association schemes and m-schemes in the context of the IKS-algorithm in a concise and self-contained manner. Furthermore, I suggest a new way to study m-schemes and their structure using methods from algebraic topology.

The material is organized in five chapters. In Chapter 1, a thorough overview of the algebraic prerequisites for the study of this work is given. It is entirely possible to use Chapter 1 for referencial purposes only, since much of the material is common knowledge at graduate level. A lot of these prerequisites are needed in Chapter 2, when we introduce the theory of association schemes.

In Chapter 2, we give a detailed and self-contained introduction to the theory of association schemes. Our goal is to understand Hanaki and Uno's classification results for association schemes of prime order, which span several journal papers (see [10], [13]). These classification results will be very important to us in later chapters, as they have great implications for the running time of certain special instances of the IKS-algorithm.

In Chapter 3, we discuss m-schemes, and we learn about an important, purely combinatorial conjecture whose correctness would imply that the IKS-algorithm runs in deterministic polynomial time on all instances under GRH (the *Schemes Conjecture* - see Section 3.5). Also, we will show that m-schemes provide a natural generalization of the notion of association schemes.

In Chapter 4, we introduce some new ideas for studying m-schemes, which are based on methods from combinatorial algebraic topology. These ideas are intended to enhance our understanding of m-schemes on a geometric level. The emphasis in this chapter is on the explanation of algebraic-topological methods; we believe that they could help us gain new insights into m-scheme properties that interest us in the context of polynomial factoring.

In Chapter 5, we discuss the application of m-schemes in polynomial factoring over finite fields; this includes a detailed description of the IKS-algorithm. Based on Hanaki and Uno's classification results, we show that the IKS-algorithm has determinstic polynomial running time in the factorization of certain prime-degree polynomials. Moreover, we discuss how the deterministic running time of the IKS-algorithm is connected to the previously-mentioned Schemes Conjecture.

Acknowledgements

I would like to thank Prof. Dr. Nitin Saxena for his advice and mentoring in the past months, and for suggesting the topic of polynomial factoring for my Diplom thesis. He has taken a lot of time for the discussion and correction of this work, and I look forward with great excitement to be his PhD student.

I would like to thank Prof. Dr. Marek Karpinski for agreeing to be the second corrector of my Diplom thesis, which (given his expertise on the subject) has saved me the time and trouble of explaining my entire Diplom thesis to someone not acquainted with the subject.

I would like to thank Prof. Dr. Aikihide Hanaki from Shinshu University Japan for illuminating me with explanations concerning his remarkable results for association schemes. He has been very kind and enduring in explaining all the key points.

I would like to thank the University of Bonn and the Hausdorff-Center for Mathematics for providing such great opportunities for mathematical education. I am very happy to have chosen the University of Bonn for my studies of mathematics.

I would like to thank my friends and family, without whom this work would not have been possible. Especially, I want to thank my friend Andreas Renghart, who has helped me out tremendously during the time of writing.

Contents

1 Algebraic Prerequisites

The purpose of this chapter is to provide the background in algebra which is needed to understand the rest of this text. I kept the sections short so as to make it possible to quickly reference them. Note that most of the results below (alongside a proof) can be found in [23] and [32]. Instead of reproving them, I will give citations whenever needed.

Also note that the term algebra will be used as a synonym for finitely generated algebra throughout this chapter.

1.1 Completely Reducible Modules

In the following, let K be a field and $\mathcal{A}$ an algebra over K such that $dim_K(\mathcal{A}) \in \mathbb{N}$. Let V be a right $\mathcal{A}$-module. If there is ambiguity about the ring V belongs to, we write V_A (resp. ${}_AV$) for a right (resp. left) $\mathcal{A}$-module. We say that V is *irreducible* (or *simple*) if it contains no proper submodule. If V is a direct sum of irreducible submodules of V, we say V is *completely reducible* (or *semisimple*).

The next Lemma characterizes this property (taken from [32], Prop. 3.3.2).

Lemma 1.1. *The following statements are equivalent:*

(i) V *is the sum of irreducible submodules*

(ii) For each submodule $U \leq V$ *there exists a submodule* $T \leq V$ *such that*

$$U \oplus T = V$$

(iii) 0 *is the intersection of the maximal submodules of* V

(iv) V *is completely reducible*

For completely reducible modules, we have the following important result about their irreducible decompositions (taken from [23], Th. I.7.3).

Theorem 1.2 (Homogenous Decomposition)**.** *Let* V *be a completely reducible* $\mathcal{A}$*-module and let*

$$V = \bigoplus_{i \in I} \bigoplus_{\lambda \in \Lambda_i} V_{i\lambda}$$

be an irreducible decomposition of V such that $V_{i\lambda}$ and $V_{k\mu}$ are isomorphic if and only if $i = k$. Put $U_i = \bigoplus_{\lambda\in\Lambda_i} V_{i\lambda}$ and chose a representative V_i of $\{V_{i\lambda} \mid \lambda \in \Lambda_i\}$ for each $i \in I$. Then

(i) Any irreducible submodule W of V is isomorphic to some $V_{i\lambda}$, in which case $W \subset U_i$.

(ii) $End_{\mathcal{A}}(V)U_i = U_i$.

(iii) If $I = \{1, 2, ..., m\}$ is a finite set and $|\Lambda_i| < \infty$ for all i, then

$$End_{\mathcal{A}}(V) \cong End_{\mathcal{A}}(U_1) \oplus \cdots \oplus End_{\mathcal{A}}(U_m) \quad (ring\ isomorphism)$$

and each $End_{\mathcal{A}}(U_i)$ is isomorphic to the full matrix ring of degree $|\Lambda_i|$ over the division ring $End_{\mathcal{A}}(V_i)$.

In the above situation, $V = \bigoplus_{i\in I} U_i$ is called *homogenous decomposition* of V. The direct summands $\{U_i \mid i \in I\}$ are called *homogenous modules* of V.

1.2 Semisimple Algebras

Throughout this Section, let $\mathcal{A}$ be a finitely generated algebra over some field K. As usually, we write $\mathcal{A}_{\mathcal{A}}$ for $\mathcal{A}$ as a right module over itself. Further, put $J(\mathcal{A})$ the intersection of the maximal submodules of $\mathcal{A}_{\mathcal{A}}$; $J(\mathcal{A})$ is the *Jacobson Radical* of $\mathcal{A}$.

We can characterize $J(\mathcal{A})$ as follows (taken from [23], Th. I.3.3 and Th. I.3.5).

Lemma 1.3. *Let $\mathcal{A}$ be finitely generated K-algebra. Then $J(\mathcal{A})$ is a nilpotent ideal of $\mathcal{A}$. Moreover,*

(i) $J(\mathcal{A})$ is the intersection of all maximal right ideals of $\mathcal{A}$.

(ii) $J(\mathcal{A})$ is the intersection of all maximal left ideals of $\mathcal{A}$.

(iii) $J(\mathcal{A})$ consists exactly of those elements of $\mathcal{A}$ which annihilate all irreducible right $\mathcal{A}$-modules.

By Lemma 1.1, we have:

Theorem 1.4. *$\mathcal{A}_{\mathcal{A}}$ is completely reducible if and only if $J(\mathcal{A}) = 0$.*

In the following, if $\mathcal{A}$ is an algebra and $\mathcal{A}_\mathcal{A}$ is completely reducible (or equivalently: $J(\mathcal{A}) = 0$), we call $\mathcal{A}$ a *semisimple algebra*.

There are many useful structural results for semisimple algebras. The next Theorem is one example (taken from [32], Th. 3.4.2).

Theorem 1.5. *Let $\mathcal{A}$ be finitely generated and semisimple. Then*

(i) Each irreducible $\mathcal{A}$-module is isomorphic to a submodule of $\mathcal{A}_\mathcal{A}$.

(ii) Let V be an $\mathcal{A}$-module such that $dim_K(V) \in \mathbb{N}$. Then V is completely reducible.

As a consequence: If V is some $\mathcal{A}$-module such that $dim_K(V) \in \mathbb{N}$, then there exist irreducible submodules $S_1, ..., S_k$ of $\mathcal{A}_\mathcal{A}$ such that

$$V \cong \lambda_1 S_1 \oplus \cdots \oplus \lambda_k S_k \ ,$$

where $\lambda_1, ..., \lambda_k$ are some multiplicities. Moreover, $S_1, ..., S_k$ can be chosen independently from V; this follows from the next Lemma (taken from [23], Th. I.8.10).

Lemma 1.6. *Let $\mathcal{A}$ be finitely generated and semisimple. Then the number of isomorphism classes of irreducible $\mathcal{A}$-modules is finite.*

We will come back to semisimple algebras in Section (1.4)

1.3 Idempotents

In the following, let $\mathcal{A}$ be a finitely generated algebra over some ring R. An *idempotent* of $\mathcal{A}$ is an element $e \in \mathcal{A}$ such that $e^2 = e$. As usual, two idempotents $e_1, e_2 \in \mathcal{A}$ are called *orthogonal* if $e_1 e_2 = 0$.

If $e \in \mathcal{A}$ is an idempotent and $e_1, e_2, ..., e_n \in \mathcal{A}$ are pairwise orthogonal idempotents such that

$$e = e_1 + e_2 + ... + e_n \ ,$$

we call $e_1 + e_2 + ... + e_n$ an *idempotent decomposition* of e. If there exists no non-trivial idempotent decomposition of e, we call e a *primitive idempotent*. Furthermore, an idempotent decomposition $e = \sum_{i=1}^{n} e_i$ is called *primitive* if each summand e_i is primitive.

The following lemma is of fundamental importance (taken from [23], Th. I.4.1).

Lemma 1.7. *Let e be an idempotent of $\mathcal{A}$. If $e = e_1 + e_2 + ... + e_n$ is an idempotent decomposition, then*

$$e\mathcal{A} = e_1\mathcal{A} \oplus e_2\mathcal{A} \oplus ... \oplus e_n\mathcal{A} \ .$$

Conversely, if $e\mathcal{A}$ is a direct sum of right ideals

$$e\mathcal{A} = I_1 \oplus I_2 \oplus ... \oplus I_n \ ,$$

then there exists an idempotent decomposition $e = e_1 + e_2 + ... + e_n$ such that

$$I_i = e_i\mathcal{A} \ , \quad 1 \leq i \leq n \ .$$

Corollary 1.8. *Let e be an idempotent of $\mathcal{A}$. Then e is primitive if and only if $(e\mathcal{A})_{\mathcal{A}}$ is indecomposable.*

An idempotent e in the center $Z(\mathcal{A})$ of $\mathcal{A}$ is called a *central idempotent*. An idempotent decomposition in $Z(\mathcal{A})$ is called a *central idempotent decomposition*. If e is primitive in $Z(\mathcal{A})$, we call it a *central primitive idempotent*. Similar to Lemma 1.7, we have:

Lemma 1.9. *Let e be a central idempotent of $\mathcal{A}$. If $e = e_1 + e_2 + ... + e_n$ is a central idempotent decomposition, then*

$$e\mathcal{A} = e_1\mathcal{A} \oplus e_2\mathcal{A} \oplus ... \oplus e_n\mathcal{A}$$

holds, as $(\mathcal{A}, \mathcal{A})$-bimodules. Conversely, if $e\mathcal{A}$ is a direct sum of two-sided ideals

$$e\mathcal{A} = I_1 \oplus I_2 \oplus ... \oplus I_n \ ,$$

then there exists a central idempotent decomposition $e = e_1 + e_2 + ... + e_n$ such that

$$I_i = e_i\mathcal{A} \ , \quad 1 \leq i \leq n \ .$$

A proof can be found in [23] (Th. I.4.7). As a Corollary, we have:

Corollary 1.10. *An idempotent e of $\mathcal{A}$ is central primitive if and only if $(e\mathcal{A})_{\mathcal{A}}$ is indecomposable as a two-sided module.*

1.4 Wedderburn's Theorem

I will now outline the consequences of Section (1.3) for semisimple algebras. This will ultimately culminate in Wedderburn's Theorem (see Theorem 1.12).

Let $\mathcal{A}$ be a finitely generated semisimple algebra over some field K and let

$$\mathcal{A}_{\mathcal{A}} = \bigoplus_{i=1}^{k} \bigoplus_{\lambda=1}^{n_i} e_{i\lambda}\mathcal{A}$$

be an irreducible decomposition, where $1 = \sum_{i,\lambda} e_{i\lambda}$ is a primitive idempotent decomposition of the identity, and we assume that $e_{i\lambda}\mathcal{A} \cong e_{j\mu}\mathcal{A}$ if and only if $i = j$ (see Lemma 1.7 and Corollary 1.8). By putting $\mathcal{A}_i = \bigoplus_{\lambda} e_{i\lambda}\mathcal{A}$, we obtain a homogenous decomposition of $\mathcal{A}_{\mathcal{A}}$:

$$\mathcal{A}_{\mathcal{A}} = \mathcal{A}_1 \oplus \mathcal{A}_2 \oplus ... \oplus \mathcal{A}_k \ .$$

Since every element of $End_{\mathcal{A}}(\mathcal{A}_{\mathcal{A}})$ may be interpreted as the left multiplication by some element of $\mathcal{A}$, we have $\mathcal{A}\mathcal{A}_i = \mathcal{A}_i$ by Theorem 1.2 (ii). Thus, each $\mathcal{A}_i$ is actually a two-sided ideal in $\mathcal{A}$, yielding

$$\mathcal{A} \cong \mathcal{A}_1 \oplus \mathcal{A}_2 \oplus ... \oplus \mathcal{A}_k \quad (\textit{ring isomorphism}) \ .$$

Now $D_i = End_{\mathcal{A}}(e_{i1}\mathcal{A})$ is a division algebra over K and $\mathcal{A}_i \cong End_{\mathcal{A}}(\mathcal{A}_i) \cong M_{n_i}(D_i)$ (see Theorem 1.2 (iii)). Moreover, one can show that each $M_{n_i}(D_i)$ is a simple algebra (see [23] Ch. 1.8)). Hence,

$$\mathcal{A} \cong \bigoplus_{i=1}^{k} \mathcal{A}_i \cong \bigoplus_{i=1}^{k} M_{n_i}(D_i)$$

is a decomposition of $\mathcal{A}$ into simple algebras. We call $\{\mathcal{A}_i \,|\, 1 \leq i \leq k\}$ the *simple components* of $\mathcal{A}$.

By Theorem 1.2 the following holds:

Lemma 1.11. *We use the above notation.*

(i) Each irreducible submodule W of $\mathcal{A}_{\mathcal{A}}$ is isomorphic to some $e_{i\lambda}\mathcal{A}$, in which case $W \subset \mathcal{A}_i$.

(ii) There are exactly n_i modules in the irreducible decomposition of $\mathcal{A}_{\mathcal{A}}$ that are isomorphic with $e_{i\lambda}\mathcal{A}$. Moreover, $dim_K(e_{i\lambda}\mathcal{A}) = n_i dim_K(D_i)$.

This leads us to the main result of this Section (taken from [23], Th. I.8.5).

Theorem 1.12 (Wedderburn)**.** *Let $\mathcal{A}$ be a finitely generated K-Algebra. Then the following conditions are equivalent:*

(i) $\mathcal{A}$ is semisimple.

(ii) $\mathcal{A} \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k)$, where each D_i is a division algebra over K.

Proof. $(i) \Rightarrow (ii)$. This has already been shown. $(ii) \Rightarrow (i)$. I will just outline the proof. As already mentioned above, each $M_{n_k}(D_k)$ is a simple algebra. Since simple algebras are also semisimple, we have $J\left(M_{n_i}(D_i)\right) = 0$ for each i. Therefore, $J(\mathcal{A}) = \bigoplus_{i=1}^{k} J\left(M_{n_i}(D_i)\right) = 0$, which means that $\mathcal{A}$ is semisimple. Working out the details will be left to the reader. □

Let us consider the case where $K = \overline{K}$ is algebraically closed. In [23] (Lemma II.3.2), the following fact is shown:

Lemma 1.13. *Let D be a division algebra over some algebraically closed field $\overline{K}$. Then $D = \overline{K}$.*

Hence, if $\mathcal{A}$ is a semisimple algebra over some algebraically closed field $\overline{K}$, then the division algebras in (ii) of Theorem 1.12 are all equal to $\overline{K}$, i.e. $D_1, D_2, ..., D_k = \overline{K}$. This gives us the following Corollary:

Corollary 1.14 (Addendum to Wedderburn's Theorem)**.** *If $\mathcal{A}$ is a finitely generated semisimple algebra over some algebraically closed field $\overline{K}$, then $\mathcal{A}$ splits into a direct sum of full matrix algebras over $\overline{K}$:*

$$\mathcal{A} \cong M_{n_1}(\overline{K}) \oplus \cdots \oplus M_{n_k}(\overline{K}) \ .$$

The following result should now be easy to verify.

Corollary 1.15. *Let $\mathcal{A}$ be a finitely generated semisimple algebra over some algebraically closed field $\overline{K}$. Then $\mathcal{A}$ is commutative if and only if $dim_{\overline{K}}(V) = 1$ for all irreducible $\mathcal{A}$-modules V.*

1.5 Idempotent Equivalence

We will now further our study of idempotents and involve the results of the previous sections in our discussion.

In the following, let $\mathcal{A}$ be a finitely generated semisimple algebra over some field K. Let e and f be idempotents of $\mathcal{A}$. As it is shown in [23] (Th. I.4.4), the following statements are equivalent:

(i) $e\mathcal{A} \cong f\mathcal{A}$ ($\mathcal{A}$-isomorphic),

(ii) $\mathcal{A}e \cong \mathcal{A}f$ ($\mathcal{A}$-isomorphic),

(iii) There exists $a \in f\mathcal{A}e$, $b \in e\mathcal{A}f$ such that $ab = f$, $ba = e$.

If e and f satisfy (i)-(iii), we call them *equivalent*; we denote this by $e \simeq f$. In this Section, we try to characterize all idempotents e of $\mathcal{A}$ that are equivalent with $1_{\mathcal{A}}$.

We start with a special case.

Lemma 1.16. *Let $\mathcal{A} = M_n(K)$ be a full matrix algebra over K. Let e be an idempotent of $\mathcal{A}$. Then*

$$e \simeq 1_{\mathcal{A}} \iff e = 1_{\mathcal{A}} .$$

Proof. This follows immediately from statement (iii) above. □

We will now consider the general case. For an algebra $\mathcal{A}$ over K, let

$$\mathcal{A}_{\mathcal{A}} = \bigoplus_{i=1}^{k} \bigoplus_{\lambda=1}^{n_i} \mathcal{A}_{i\lambda}$$

be an irreducible decomposition of $\mathcal{A}_{\mathcal{A}}$, where we assume that $\mathcal{A}_{i\lambda} \cong \mathcal{A}_{j\mu}$ if and only if $i = j$. Let e be an idempotent of $\mathcal{A}$. Multipliying the above equation with e gives us an irreducible decomposition of $(e\mathcal{A})_{\mathcal{A}}$:

$$(e\mathcal{A})_{\mathcal{A}} = \bigoplus_{i=1}^{k} \bigoplus_{\lambda=1}^{n_i} e\mathcal{A}_{i\lambda} .$$

For each summand $e\mathcal{A}_{i\lambda}$ in the above decomposition, observe that either $e\mathcal{A}_{i\lambda} = 0$ or $e\mathcal{A}_{i\lambda} = \mathcal{A}_{i\lambda}$ by irreducibility. As a consequence:

Lemma 1.17. *In the above situation, $e\mathcal{A}_{i\lambda} \cong \mathcal{A}_{i\lambda}$ for all (i, λ) if and only if $e \simeq 1_{\mathcal{A}}$.*

1.6 Splitting Fields

Throughout this section, let K be a field and $K \subset L$ a field extension. For an algebra $\mathcal{A}$ over K, we define

$$\mathcal{A}^L := L \otimes_K \mathcal{A} \ .$$

Note that $\mathcal{A}^L$ can be regarded as an L-algebra in a natural way. Moreover, note that $\mathcal{A}^L/J\left(\mathcal{A}^L\right)$ is semisimple as an L-algebra; this follows from $J\left(\mathcal{A}^L/J\left(\mathcal{A}^L\right)\right) = 0$. We settle for the following convention: If $\mathcal{A}^L/J\left(\mathcal{A}^L\right)$ splits into a direct sum of full matrix algebras over L,

$$\mathcal{A}^L/J\left(\mathcal{A}^L\right) \cong M_{n_1}(L) \oplus \cdots \oplus M_{n_k}(L) \ ,$$

then L is called a *splitting field* for $\mathcal{A}$. If K is itself a splitting field for $\mathcal{A}$, we call $\mathcal{A}$ a *split K-algebra*.

Note that split K-algebras are always semisimple, but the converse does not hold (see Theorem 1.12). Also note that the algebraic closure $\bar{K}$ of K is a splitting field for every finitely generated K-algebra (see Corollary 1.14)

The following theorem will be of fundamental importance to us:

Theorem 1.18. *Let $\mathcal{A}$ be a finitely generated K-algebra. Then there exists a finite extension field L of K that is a splitting field for $\mathcal{A}$.*

For a complete discussion and proof of this result, see [23] (Th. II.3).

1.7 Matrix Representations

We will now look at some basic concepts of Representation Theory. Note that most of the material we present here was taken from [23] (in particular: Ch. II.1). Readers familiar with Representation Theory may skip through the following section.

Let A be an algebra over some commutative ring R. By a *matrix representation* of A, we mean an R-algebra homomorphism from A into a full matrix ring over R:

$$\mathbf{X} : A \longrightarrow M_n(R) \ , \quad a \longrightarrow X(a) \ .$$

The integer n is called the *degree* of $\mathbf{X}$.

Two matrix representations $\mathbf{X}$ and $\mathbf{Y}$ of A are called *equivalent* if there exists $T \in GL_n(R)$ such that for all $a \in A$,

$$Y(a) = T^{-1}X(a)T \ .$$

If $S \supset R$ are rings having the identity in common and $\mathbf{X}$ is matrix representation of $A^S := S \otimes_R A$, then $\mathbf{X}$ is called *realizable over* R if there exists an $\mathbf{X}$-equivalent matrix representation $\mathbf{Y}$ of A^S such that

$$Y(1_S \otimes a) \in M_n(R) \ , \quad \forall \ a \in A \ .$$

In the following, let V be an A-module with R-basis $(v_1, v_2, ..., v_n)$. For $a \in A$, write

$$v_i a = \sum_{j=1}^{n} \alpha_{ij}(a) v_j \ , \quad i = 1, ..., n \ .$$

Put $X(a) = (\alpha_{ij}(a))_{i,j} \in M_n(R)$. Then the map

$$\mathbf{X} : A \longrightarrow M_n(R) \ , \quad a \longrightarrow X(a)$$

is a matrix representation of A. We call $\mathbf{X}$ the *matrix representation of A afforded by V relative to the basis* $(v_1, v_2, ..., v_n)$. In the above situation, V is called a *representation module* for $\mathbf{X}$.

As the following Lemma shows, every matrix representation of A has a representation module (taken from [23], Ch. II.1).

Lemma 1.19. *Let A be an algebra over some commutative ring R. Let $\boldsymbol{X} : A \longrightarrow M_n(R)$, $a \longrightarrow X(a)$ be a matrix representation of A. Then there exists an R-module V such that V is a representation module for $\boldsymbol{X}$.*

Proof. Assume $X(a) = (\alpha_{ij}(a))_{i,j} \in M_n(R)$. Consider the free R-module

$$V = Rv_1 \oplus \cdots \oplus Rv_n \ .$$

We define the action of each a on v_i by

$$v_i a = \sum_{j=1}^{n} \alpha_{ij}(a) v_j$$

and extend it to all of V linearly. Then V is a right A-module, and the matrix representation of A afforded by V relative to the basis $(v_1, v_2, ..., v_n)$ coincides with $\mathbf{X}$. □

As the next Lemma shows, representation modules can also be used to describe the equivalency of matrix representations. For a proof, see [6] (Ch. II.8).

Lemma 1.20. *Two matrix representations $\boldsymbol{X}$ and $\boldsymbol{Y}$ of A are equivalent if and only if they have isomorphic representation modules.*

1.8 Characters

We will now look at some basic concepts of Character Theory. Note that most of the material we present here was taken from [32] (in particular: Ch. 3.5). Readers familiar with Character Theory may skip through the following section.

Definition 1.21 (Character)**.** *Let $\mathcal{A}$ be an algebra over some field K. Let V be an $\mathcal{A}$-module such that $dim_K(V) \in \mathbb{N}$. For each $a \in \mathcal{A}$, we have a linear map*

$$\varphi_a : V \longrightarrow V \ , \quad v \longrightarrow va \ .$$

The map defined by

$$\chi_V : \mathcal{A} \longrightarrow K \ , \quad a \longrightarrow tr(\varphi_a) \ .$$

is also linear; we call χ_V the character of $\mathcal{A}$ afforded by V. If V is an irreducible module, we call χ_V an irreducible character.

The set of all irreducible characters of $\mathcal{A}$ will be denoted by $Irr(\mathcal{A})$. We will show that the irreducible characters of $\mathcal{A}$ are the building blocks of a much larger class of characters. For this purpose, we need the following Lemma:

Lemma 1.22. *Let V, W be $\mathcal{A}$-modules such that $V \neq 0 \neq W$. Then we have:*

(i) If $V \cong W$, then (using the above notation) $\chi_V = \chi_W$.

(ii) If $U = V \bigoplus W$, then $\chi_U = \chi_V + \chi_W$.

Proof. To certify the above statements, just spell them out in "basis language". The results follow immediately; we leave the details to the reader. □

Now the results from Section (1.2) (esp. Theorem 1.5), give us the following:

Theorem 1.23. *Let $\mathcal{A}$ be a finitely generated semisimple K-algebra and let V be an $\mathcal{A}$-module such that $dim_K(V) \in \mathbb{N}$. Then the character χ_V of $\mathcal{A}$ afforded by V can be written as a linear combination of irreducible characters of $\mathcal{A}$:*

$$\chi_V = \sum_{\chi \in Irr(\mathcal{A})} \lambda_\chi \, \chi \ ,$$

where λ_χ denotes the multiplicity of χ in χ_V.

Note that $Irr(\mathcal{A})$ is finite; this follows from Lemma 1.6.

1.9 Complete Discrete Valuation Rings

In the following, we assume that the reader is familiar with discrete valuation rings and that she understands the notion of completeness in this context. The present discussion only includes some specific results for DVRs which we need in Chapter 2.

The following theorem on idempotent lifting will be very important to us (taken from [23], Th. I.14.1 and I.14.2).

Theorem 1.24. *Let A be a finitely generated algebra over some complete discrete valuation ring R of characteristic 0. Let π be the maximal ideal of R and put $\bar{A} = A/\pi A$. Then the following holds:*

(i) Let $\bar{e}$ be an idempotent of $\bar{A}$ and let

$$\bar{e} = \bar{e_1} + \bar{e_2} + ... + \bar{e_n}$$

be an idempotent decomposition of $\bar{e}$ in $\bar{A}$. Then $\bar{e}$ lifts to an idempotent e of A, meaning there exists an idempotent $e \in A$ such that $e \longrightarrow \bar{e}$ under the canonical epimorphism $A \longrightarrow \bar{A}$. Moreover, there exist orthogonal idempotents $e_1, e_2, ..., e_n \in A$ such that each e_i is a lift of $\bar{e_i}$ and

$$e = e_1 + e_2 + ... + e_n \ .$$

(ii) An idempotent e of A is primitive if and only if its image under the canonical epimorphism $A \longrightarrow \bar{A}$ is a primitive idempotent of $\bar{A}$.

For the next result, remember that a module M over some ring R is called *free* if it has a basis over R. M is called *torsion-free* if there exists no element $0 \neq m \in M$ such that $mr = 0$ for some scalar $0 \neq r \in R$.

Also note that the following lemma holds for arbitrary valuation rings (which have to be neither complete nor discrete). A proof can be found in [8] (Th. 5.2).

Lemma 1.25. *Let R be a valuation ring. Then every finitely generated torsion-free R-module is free.*

We will come back to discrete valuation rings in the next Section.

1.10 p-modular Systems

We will now consider *p-modular systems*. A p-modular system is a triple (K, R, F) of rings such that

(i) R is a complete discrete valuation ring with unique maximal ideal (π)

(ii) K is the field of fractions of R with $char\ K = 0$

(iii) F is the residue field $R/(\pi)$ and $char\ F = p$

Let us first discuss the existence of such a system. For this purpose, we need to be familiar with the notion of *Witt vectors*: Given a field F of characteristic p, the ring $W(F)$ of Witt vectors of F consists of all infinite sequences $(f_0, f_1, f_2, ...)$ of elements of F, and the sum and product of two elements $x, y \in W(F)$ are defined by

$$x + y = (S_n(x, y))_{n \in \mathbb{N}} \ , \qquad x \cdot y = (P_n(x, y))_{n \in \mathbb{N}} \ ,$$

where S_n and P_n for each $n \in \mathbb{N}$ are certain polynomials in $x_0, x_1, ..., x_n$ and $y_0, y_1, ..., y_n$. For the exact definition of S_n and P_n, see [3] (Ch. 4.10).

The classical example for Witt vectors: If $F = \mathbb{F}_p$ is the Galois field of size p, then $W(F) = \mathbb{Z}_p$ is the ring of p-adic integers (see [22]). It is common knowledge that $\mathbb{Z}_p$ is a complete discrete valuation ring of characteristic 0, and that

$$\mathbb{Z}_p/(\pi) \cong F \ ,$$

where (π) denotes the maximal ideal of $\mathbb{Z}_p$. Hence, if $\mathbb{Q}_p$ denotes the ring of p-adic numbers (the quotient field of $\mathbb{Z}_p$), then $(\mathbb{Q}_p, \mathbb{Z}_p, \mathbb{F}_p)$ is a p-modular system.

This example can be generalized as follows (see [22], Th. 3.1.14):

Lemma 1.26 (Witt)**.** *Let F be an algebraically closed field of characteristic p. Then the ring $W(F)$ of Witt vectors of F is a complete discrete valuation ring of characteristic 0. Moreover, if (π) is the maximal ideal of $W(F)$, then*

$$W(F)/(\pi) \cong F \ .$$

As a consequence: If F is an algebraically closed field of characteristic p and $Q_{W(F)}$ denotes the field of fractions of the ring $W(F)$, then $(Q_{W(F)}, W(F), F)$ is a p-modular system.

By the same argument as in [22] (Th. 3.1.22), this generalizes as follows:

Lemma 1.27. *Let F be an algebraically closed field of characteristic p and let $(Q_{W(F)}, W(F), F)$ be the above p-modular system. Assume K is a finite extension field of $Q_{W(F)}$. Then there exists a complete discrete valuation ring R such that (K, R, F) is also a p-modular system.*

This completes our discussion. For more on p-modular systems, see [23] (Ch. III.6).

2 Association Schemes

Association Schemes are standard combinatorial objects that arise in various guises in many areas of mathematics. The present chapter provides an algebraic approach to this subject, utilizing ring theory, representation theory and linear algebra.

Note that the material has been organized in such a way that it requires no previous knowledge of association schemes. All the necessary definitions and elementary theory are discussed in Sections (2.1)-(2.3). In Sections (2.4)-(2.6), we explain some of the more recent results; this includes a systematic treatise of [13].

2.1 Basic Notions

In this section, we discuss the basic definition of an association scheme and look at some notable examples.

Definition 2.1 (Association Scheme)**.** *Let X be a finite set and G a collection of nonempty subsets of $X \times X$. An element $g \in G$ is called a relation (or color) of (X, G). We say that (X, G) is an association scheme if*

(i) $X \times X$ *is a disjoint union of* $g \in G$

(ii) G *contains the trivial relation* $1 := \{(x, x) \mid x \in X\}$

(iii) If $g \in G$*, then* $g^* := \{(y, x) \mid (x, y) \in g\} \in G$

(iv) For all $f, g, h \in G$*, there exists an integer* a_{fgh} *such that for all* $(\alpha, \beta) \in h$*,*

$$a_{fgh} = |\{\gamma \in X \mid (\alpha, \gamma) \in f \text{ and } (\gamma, \beta) \in g\}| \ .$$

We call $|X|$ *the order of* (X, G) *and* $n_g = a_{gg^{*1}}$ *the valency of* $g \in G$*. If* $a_{fgh} = a_{gfh}$ *for all* $f, g, h \in G$*, then we say that* (X, G) *is commutative.*

Let us look at some examples.

Example 2.2 (Cyclotomic Scheme)**.** *Let p be prime power and let $d \mid p - 1$. Fix a generator α of the multiplicative group $\mathbb{F}_p^*$ of $\mathbb{F}_p$ and consider the subgroup $\langle \alpha^d \rangle$ generated by α^d. $\langle \alpha^d \rangle$ is a subgroup of index d in $\mathbb{F}_p^*$, and its cosets are*

$$\alpha^i \langle \alpha^d \rangle \ , \quad i = 0, ..., d - 1 \ .$$

Let $\mathcal{P} := \{P_i \,|\, 0 \leq i \leq d\}$ *be the partition of* $\mathbb{F}_p \times \mathbb{F}_p$ *defined by*

$$P_0 := \{(x, x) \,|\, x \in \mathbb{F}_p\} \ ,$$

$$P_i := \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p \,|\, x - y \in \alpha^i \left\langle \alpha^d \right\rangle\} \ , \quad i = 1, ..., d \ .$$

It is easy to see that $(\mathbb{F}_p, \mathcal{P})$ *is an association scheme. Also, observe that all relations are equal in size:*

$$|P_i| := \frac{p \cdot (p-1)}{d} \ , \quad i = 1, ..., d-1 \ .$$

More interestingly, the definition of this scheme does not depend on the choice of the generator α*: If* β *is another generator of* $\mathbb{F}_p^*$ *, say* $\beta = \alpha^s$ *for some* $s \in \mathbb{N}$*, then*

$$\beta^j \left\langle \beta^d \right\rangle \subset \alpha^{js} \left\langle \alpha^d \right\rangle \ , \quad j = 1, ..., d-1 \ ,$$

and since $\beta^j \left\langle \beta^d \right\rangle$ *and* $\alpha^{js} \left\langle \alpha^d \right\rangle$ *are equal in size,*

$$\beta^j \left\langle \beta^d \right\rangle = \alpha^{js} \left\langle \alpha^d \right\rangle \ , \quad j = 1, ..., d-1 \ .$$

This means that the substitution of β *in place of* α *in the definition of* $(\mathbb{F}_p, \mathcal{P})$ *merely permutes the numbering of the relations; it does not alter the scheme. Hence, the construction of* $(\mathbb{F}_p, \mathcal{P})$ *depends only on the choice of* p *and* d*. We call* $(\mathbb{F}_p, \mathcal{P})$ *the cyclotomic scheme in* (p, d) *and denote it by* $Cyc(p, d)$*.* □

As a special class of the cyclotomic scheme, we consider Paley graphs (see below). Paley graphs are strongly regular hamiltonian graphs which appear in the number theory of quadratic residues. From a graph-theoretic perspective, Paley graphs are often recognized for being self-complementary (see [9], [25]).

Example 2.3 (Paley Graph)**.** *Let* p *be a prime power such that* $p \equiv 1 \ (mod\ 4)$*. By the law of quadratic reciprocity,* -1 *is a quadratic residue in* $\mathbb{F}_p$*. Given* $x, y \in \mathbb{F}_p$*, it follows that* $x - y$ *is a quadratic residue if and only if* $y - x$ *is a quadratic residue. We define the Paley graph of order* p *by*

$$V = \mathbb{F}_p \ , \quad E = \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p \,|\, x - y \textit{ is a quadratic residue}\} \ ,$$

and this is indeed a graph because of the above.

We obtain an association scheme (X, G) by putting

$$X = \mathbb{F}_p \ , \quad G = \{1, E, \bar{E}\} \ ,$$

where 1 denotes the trivial relation and $\bar{E}$ denotes the complement of E as a graph. One can easily see that (X, G) is isomorphic to the cyclotomic scheme $Cyc(p, 2)$. □

We will now consider Schurian association schemes. These schemes arise from the diagonal orbits of transitive permutation groups (see below). In Chapter 3, when we look at m-schemes, the Schurian scheme will appear as a special case of the more general "orbit scheme".

Example 2.4 (Schurian Scheme)**.** *Let $(\mathcal{G}, X)$ be a transitive permutation group, i.e. X is a finite set and for any $x, y \in X$ there exists a permutation $\sigma \in \mathcal{G}$ such that $x^\sigma = y$. Consider the induced action of $\mathcal{G}$ on $X \times X$: Let $G = \{\Lambda_0, \Lambda_1, ..., \Lambda_d\}$ denote the set of orbits by this action, where $\Lambda_0 = \{(x, x) \,|\, x \in X\}$ is the trivial orbit. Then (X, G) is an association scheme; this can be verified easily. We call schemes that arises in the above-described manner Schurian schemes.* □

For more examples of association schemes, see [1] or [4].

2.2 The Adjacency Algebra

In this Section, (X, G) is an association scheme and $n = |X|$ is the order of (X, G). For a relation $g \in G$, we denote its *adjacency matrix* by σ_g. Namely, σ_g is a matrix whose rows and columns are indexed by X and its (x, y)-entry is 1 if $(x, y) \in g$ and 0 otherwise.

Let $\Gamma := \{\sigma_g \,|\, g \in G\}$ be the set of all adjacency matrices of G. It follows from Definition 2.1 that

(i) $\sum_{g \in G} \sigma_g$ is the $n \times n$ matrix with entries all 1.

(ii) $\sigma_1 \in \Gamma$ is the $n \times n$ identity matrix.

(iii) If $\sigma_g \in \Gamma$, then $\sigma_{g^*} = \sigma_g^T \in \Gamma$.

(iv) For all $f, g, h \in G$, there exists an integer a_{fgh} such that

$$\sigma_f \sigma_g = \sum_{h \in G} a_{fgh} \sigma_h \ .$$

To obtain (iv), note that for $(\alpha, \beta) \in h$, the equation

$$a_{fgh} = |\{\gamma \in X \,|\, (\alpha, \gamma) \in f \text{ and } (\gamma, \beta) \in g\}|$$

can also be written as

$$a_{fgh} = \sum_{\gamma \in X} (\sigma_f)_{\alpha\gamma} (\sigma_g)_{\gamma\beta} \ ,$$

and the right hand side is $(\sigma_f \sigma_g)_{\alpha\beta}$ by the definition of matrix multiplication.

It should be clear that we can completely describe an association scheme by its adjacency matrices. Moreover, a system of matrices with the above properties and an association scheme are the same thing. As a result of this duality, we have a new characterization for the commutativity of association schemes:

Lemma 2.5. *An association scheme (X, G) is commutative if and only if its adjacency matrices commute, i.e. if $\sigma_f \sigma_g = \sigma_g \sigma_f$ for all $f, g \in G$.*

For the following discussion, note that the above statements (i)-(iv) still hold if we consider the adjacency matrices $\{\sigma_g \,|\, g \in G\}$ as matrices over some commutive ring R with 1. This gives rise to the following definition:

Definition 2.6 (Adjacency algebra)**.** *Let $\mathfrak{X} = (X, G)$ be an association scheme. Let R be some commutative ring with 1. In accordance with statements (i)-(iv), we can define an R-algebra*

$$R\mathfrak{X} = \bigoplus_{g \in G} R \ \sigma_g \ ,$$

where σ_g is considered as a matrix over the coefficient ring R. We call $R\mathfrak{X}$ the adjacency algebra of $\mathfrak{X}$ over R.

Let us first consider the case that $R = K$ is a field and *char* $K = 0$.

Theorem 2.7. *Let $\mathfrak{X} = (X, G)$ be an association scheme. Let K be some field of characteristic 0. Then the adjacency algebra $K\mathfrak{X}$ is semisimple.*

Proof. It suffices to show $J(K\mathfrak{X}) = 0$. For the sake of contradiction, assume there exists $0 \neq \sigma \in J(K\mathfrak{X})$. Choose $\{r_g \in K \,|\, g \in G\}$ such that

$$\sigma = \sum_{g \in G} r_g \sigma_g \ .$$

Since σ is nontrivial, we can choose $f \in G$ such that $r_{f^*} \neq 0$. We have

$$tr(\sigma_f \sigma) = \sum_{g \in G} r_g \; tr(\sigma_f \sigma_g) = r_{f^*} \, |f| \;\; ,$$

where tr denotes the trace function. Note that the second equality follows from

$$\begin{aligned} tr(\sigma_f \sigma_g) &= \sum_{h \in G} a_{fgh} \; tr(\sigma_h) = \sum_{h \in G} a_{fgh} \; \delta_{1h} \, |X| \\ &= a_{fg1} \, |X| = \delta_{f^* g} \; n_f \, |X| = \delta_{f^* g} \, |f| \;\; . \end{aligned}$$

Now observe that $\sigma_f \sigma$ lies in $J(K\mathfrak{X})$, so it is nilpotent by Lemma 1.3. Hence,

$$tr(\sigma_f \sigma) = 0 \; .$$

Altogether, we have $r_{f^*} \, |f| = 0$. But this contradicts $r_{f^*} \neq 0$. □

We keep the above notation. The following corollaries will be of much importance:

Corollary 2.8. *Let K be a field of characteristic 0. Then there exists a finite extension field L of K such that the adjacency algebra $L\mathfrak{X}$ is a split L-algebra.*

Proof. By Lemma 1.18, there exists a finite extension field L of K such that L is a splitting field for $K\mathfrak{X}$. This means that the semisimple L-algebra $K\mathfrak{X}^L / J(K\mathfrak{X}^L)$ splits into the direct sum of full matrix rings over L. But $K\mathfrak{X}^L \cong L\mathfrak{X}$ (L-isomorphic) and $J(L\mathfrak{X}) = 0$ by Theorem 2.7 ; therefore, $L\mathfrak{X}$ is a split L-algebra. □

Corollary 2.9. *Let $\mathfrak{X} = (X, G)$ be an association scheme and let $\mathbb{C}\mathfrak{X}$ be the complex adjacency algebra. Let 1 be the unity in $\mathbb{C}\mathfrak{X}$. Then*

$$\sum_{\chi \in Irr(\mathbb{C}\mathfrak{X})} \chi(1) \;\; \leq \sum_{\chi \in Irr(\mathbb{C}\mathfrak{X})} \chi(1)^2 \;\; = \;\; |G| \;\; ,$$

and equality holds if and only if (X, G) is commutative.

Proof. Note that

$$\chi_V(1) = tr(id_V) = dim_{\mathbb{C}}(V)$$

for any character χ_V afforded by a module V over $\mathbb{C}\mathfrak{X}$. The assertion then follows from the results of Section (1.4) (see Corollaries 1.14 and 1.15). □

2.3 Characters of Association Schemes

Character Theory is one of the most useful tools when it comes to studying association schemes. In the following, let $\mathfrak{X} = (X, G)$ be an association scheme and let K be a field of characteristic 0. We will study the characters of the adjacency algebra $K\mathfrak{X}$.

Let us fix some terminology. If $\mathbf{X}$ be a matrix representation of $K\mathfrak{X}$,

$$\mathbf{X} : K\mathfrak{X} \longrightarrow M_n(K) \ , \quad \sigma \longrightarrow X(\sigma) \ ,$$

then we define the *character afforded by* $\boldsymbol{X}$ as

$$\chi : K\mathfrak{X} \longrightarrow K \ , \quad \sigma \longrightarrow tr(X(\sigma)) \ .$$

It follows from this definition that χ is afforded by any representation module V of $\mathbf{X}$.

Let us look at some examples.

Example 2.10 (Trivial Character)**.** *Consider the $K\mathfrak{X}$-representation*

$$\boldsymbol{X} : K\mathfrak{X} \longrightarrow K \ , \quad \sigma_g \longrightarrow n_g \ ,$$

where we identify $n_g = n_g \cdot 1_K$. This is indeed a representation, because

$$X(\sigma_e\sigma_f) = \sum_{g\in G} a_{efg} X(\sigma_g) = \sum_{g\in G} a_{efg} n_g = n_e n_f = X(\sigma_e)X(\sigma_f) \ ,$$

where $e, f \in G$ (see [32], Lemma 1.1.4). Let 1_G denote the character afforded by $\boldsymbol{X}$. We call 1_G the trivial character of $K\mathfrak{X}$. Explicitly, we have

$$1_G(\sigma_g) = n_g \ , \quad g \in G \ .$$

Moreover, since $dim_K(T) = 1$ for any representation module T of $\boldsymbol{X}$, the trivial character 1_G is irreducible. □

Example 2.11 (Standard Representation, Standard Character)**.** *Put $n = |X|$ the order of (X, G). We define the standard representation $\boldsymbol{Y}$ of $K\mathfrak{X}$ by*

$$\boldsymbol{Y} : K\mathfrak{X} \longrightarrow M_n(K) \ , \quad \sigma_g \longrightarrow \sigma_g \ .$$

Let γ denote the character afforded by $\boldsymbol{Y}$. We call γ the standard character of $K\mathfrak{X}$. Explicitly, we have

$$\gamma(\sigma_1) = n \ ,$$

$$\gamma(\sigma_g) = 0 \ , \quad 1 \neq g \in G \ .$$

□

Remember that by Theorem 1.23, any character χ_V of $K\mathfrak{X}$ afforded by a $K\mathfrak{X}$-module V such that $dim_K(V) \in \mathbb{N}$ can be written as a linear combination of irreducible characters of G:

$$\chi_V = \sum_{\chi \in Irr(K\mathfrak{X})} \lambda_\chi \ \chi \ ,$$

where λ_χ denotes the multiplicity of χ in χ_V. As a trivial consequence, the standard character γ can also be written as a linear combination of irreducible characters. Because this is such an important special case, we settle for the following convention:

Definition 2.12 (Multiplicity in γ)**.** *The multiplicity of an irreducible character $\chi \in Irr(K\mathfrak{X})$ in the standard character γ is denoted by m_χ and is simply called the multiplicity of χ.*

It is possible to calculate the multiplicities m_χ explicitly; the next theorem provides formulas that accomplish this. We will often refer to these formulas as "orthogonality relations":

Theorem 2.13 (Orthogonality relations)**.** *Let $\phi, \psi \in Irr(G)$ be given and let δ denote the Kronecker symbol. Then we have the following:*

(i) For each $g \in G$,

$$\sum_{e \in G} \sum_{f \in G} \frac{a_{g^* e f}}{|e^*|} \phi(\sigma_{e^*}) \psi(\sigma_f) = \delta_{\phi\psi} \frac{\phi(\sigma_{g^*})}{m_\phi} \ .$$

(ii) We have

$$\sum_{g \in G} \frac{1}{|g^*|} \phi(\sigma_{g^*}) \psi(\sigma_g) = \delta_{\phi\psi} \frac{\phi(\sigma_1)}{m_\phi} \ .$$

Above version of the orthogonality relations, alongside a proof, can be found in [32] (Th. 4.1.5). Baily's book (see [1], Th. 2.12 and Cor. 2.14, 2.15) gives a similar

treatment of the subject, while Bannai and Ito (see [4], Th. II.3.5) only consider the relations in the case of commutative association schemes.

As a consequence of Theorem 2.13, we have the following Corollary:

Corollary 2.14. *The multiplicity m_{1_G} of the trivial character 1_G in the standard character γ is 1.*

Proof. Using the second orthogonality relation, we infer

$$\sum_{g\in G} \frac{1}{|g^*|} 1_G(\sigma_{g^*}) 1_G(\sigma_g) = \frac{1_G(\sigma_1)}{m_{1_G}} \ .$$

By definition of the trivial character (see Example 2.10), this yields

$$\sum_{g\in G} \frac{1}{|g|} n_g^2 = \frac{1}{m_{1_G}} \ ,$$

and the left side is 1 by the identity $n_g \, |X| = |g|$. □

2.4 The Frame number

The Frame number $\mathcal{F}(\mathfrak{X})$ of an association scheme $\mathfrak{X} = (X, G)$ is defined as

$$\mathcal{F}(\mathfrak{X}) := |X|^{|G|} \frac{\prod_{g\in G} n_g}{\prod_{\chi\in Irr(\mathbb{C}\mathfrak{X})} m_\chi{}^{\chi(1)^2}} \ .$$

This number first appeared in a paper by J.S. Frame (see [7], Th. B). In the present section, we show that $\mathcal{F}(\mathfrak{X})$ is a rational integer; this cements the link between the multiplicities and the valencies of $\mathfrak{X}$. Our proof will follow [28] (Th. L 9) and the modified version in [17] (Lemma 3.1.2).

We need the following preliminary lemma (taken from [21], Th. 10.4).

Lemma 2.15. *Let R be a valuation ring, let K be the field of fractions of R. Then every matrix representation of $K\mathfrak{X}$ is realizable over R.*

Proof. Let $\mathbf{Y}$ be a matrix representation of $K\mathfrak{X}$ with representation module U. By [23] (Ch. II.1.2), there exists a finitely generated torsion-free $R\mathfrak{X}$-module V such that

$$V^K := K \otimes_R V \cong U \ .$$

By Lemma 1.25, V is R-free, so we can choose an R-basis $(v_1, v_2, ..., v_n)$ for V. Then $(1 \otimes v_1, 1 \otimes v_2, ..., 1 \otimes v_n)$ is a K-basis of V^K, and the matrix representation $\mathbf{X}$ of $K\mathfrak{X}$ afforded by V^K relative to the basis $(1 \otimes v_1, 1 \otimes v_2, ..., 1 \otimes v_n)$ satisfies

$$\mathbf{X}(\sigma_g) \in M_n(R) \ , \quad \forall \ g \in G \ .$$

Since $\mathbf{X}$ and $\mathbf{Y}$ have isomorphic representation modules, the assertion follows by Lemma 1.20. □

We can now prove the main result of this section.

Lemma 2.16. *The Frame number $\mathcal{F}(\mathfrak{X})$ of an association scheme $\mathfrak{X} = (X, G)$ is a rational integer.*

Proof. We put $K = \bar{\mathbb{Q}}$ (the algebraic closure of $\mathbb{Q}$) and prove that every valuation ring $R \supset \mathbb{Z}$ with field of fractions K contains $\mathcal{F}(\mathfrak{X})$. It then follows from [21] (Th. 10.4) that $\mathcal{F}(\mathfrak{X}) \in \mathbb{Z}$.

Let R be a valuation ring of the above type. Let $S_1, ..., S_k$ be a complete set of representatives of isomorphism classes of irreducible $K\mathfrak{X}$-modules. Put $f_i := dim\ S_i$ $(1 \leq i \leq k)$. For each $i = 1, ..., k$, let $\mathbf{X}_i$ be a matrix representation of $K\mathfrak{X}$ afforded by S_i. By Lemma 2.15, we may assume $\mathbf{X}_i(\sigma_g) \in M_{f_i}(R)$ for all $i = 1, ..., k$ and $g \in G$. In the following, we consider the matrix representation

$$\mathbf{Y} = \begin{pmatrix} diag(\underbrace{(\mathbf{X}_1, ..., \mathbf{X}_1)}_{m_{\chi_1}\ times}) & & 0 \\ & \ddots & \\ 0 & & diag(\underbrace{(\mathbf{X}_k, ..., \mathbf{X}_k)}_{m_{\chi_k}\ times}) \end{pmatrix} .$$

Evidently, $\mathbf{Y}$ has representation module $S = \bigoplus_{i=1}^{k} m_{\chi_i} S_i$. Accordingly, $\mathbf{Y}$ is equivalent to the standard representation (see Lemma 1.20).

Put $|G| = d+1$. Let N be the $(d+1) \times (d+1)$ matrix whose rows and columns are indexed by G and whose entries are $(N)_{gh} = tr\,(\mathbf{Y}(\sigma_{g^*})\mathbf{Y}(\sigma_h))$. Then

$$(N)_{gh} = tr\,(\sigma_{g^*}\sigma_h) = \delta_{gh} n_g\,|X| \ , \tag{1}$$

where the first equality follows from the equivalence of $\mathbf{Y}$ to standard representation.

On the other hand,

$$(N)_{gh} = tr\left(\mathbf{Y}(\sigma_{g^*})\mathbf{Y}(\sigma_h)\right) = \sum_{i=1}^{k} m_{\chi_i} tr\left(\mathbf{X}_i(\sigma_{g^*})\mathbf{X}_i(\sigma_h)\right) \ . \tag{2}$$

For $1 \leq \epsilon, \xi \leq f_i$, let $e^{i,g}_{\epsilon,\xi}$ denote the (ϵ,ξ)-component of $\mathbf{X}_i(\sigma_g)$. Then (2) yields

$$(N)_{gh} = \sum_{i=1}^{k} m_{\chi_i} \sum_{\epsilon=1}^{f_i} \sum_{\xi=1}^{f_i} e^{i,g^*}_{\epsilon,\xi}\, e^{i,h}_{\xi,\epsilon} \ . \tag{3}$$

According to Lemma 2.9, we choose a bijection

$$G \overset{\varphi}{\longleftrightarrow} \{(i,\epsilon,\xi) \,|\, 0 \leq i \leq k,\ 1 \leq \epsilon, \xi \leq f_i\} \ .$$

Let Z', L, Z denote $(d+1) \times (d+1)$ matrices whose rows and columns are indexed by G and whose entries are

$$\begin{aligned}
(Z')_{gh} &= e^{i,g^*}_{\epsilon,\xi} \qquad if\ \varphi(h) = (i,\epsilon,\xi) \\
(L)_{gh} &= \delta_{gh} m_{\chi_i} \quad if\ \varphi(h) = (i,\epsilon,\xi) \\
(Z)_{gh} &= e^{i,g}_{\xi,\epsilon} \qquad if\ \varphi(h) = (i,\epsilon,\xi)
\end{aligned}$$

Then the above equation (3) reduces to

$$N = Z'LZ \ . \tag{4}$$

Combining (1) and (4), if we abbreviate $z = det\ Z$ and $z' = det\ Z'$, we have

$$|X|^{d+1} \prod_{g\in G} n_g = det\ N = zz' det\ L = zz' \prod_{i=1}^{k} m_{\chi_i}^{f_i^2} = zz' \prod_{i=1}^{k} m_{\chi_i}^{\chi_i(1)^2} \ .$$

Hence,

$$|X|^{d+1} \frac{\prod_{g\in G} n_g}{\prod_{i=1}^{k} m_{\chi_i}^{\chi_i(1)^2}} = \mathcal{F}(\mathfrak{X}) = zz' \ .$$

Since $z, z' \in R$, it follows that $\mathcal{F}(\mathfrak{X}) \in R$. This completes the proof. □

2.5 Locality in Characteristic p

In this section, we show that if F is a field of characteristic p, and $\mathfrak{X} = (X, G)$ is a scheme of p-power order, then the adjacency algebra $F\mathfrak{X}$ is local. The proof of this result, alongside the proofs of the introductory lemmas, come from the paper [10].

In the following, K is a field of characteristic 0 and $\mathfrak{X} = (X, G)$ is an association scheme of order $n = |X|$. Also, we assume $\chi_1, \chi_2, ..., \chi_r$ is a complete set of irreducible characters of $K\mathfrak{X}$.

We need the following preliminary lemma (see [10], Lemma 3.2):

Lemma 2.17. *Let* $K\mathfrak{X} \ni u = \sum_{g\in G} \alpha_g \sigma_g,\ \alpha_g \in K$. *Then*

$$\alpha_f = \frac{1}{n_f n} \sum_{i=1}^{r} m_i \chi_i \left(u\sigma_{f^*}\right) \ , \quad f \in G \ .$$

Proof. We have $u\sigma_{f^*} = \sum_{g\in G} \alpha_g \sigma_g \sigma_{f^*}$. Using the explicit formulas for the standard character γ (see Section (2.3)), we get

$$\gamma\left(u\sigma_{f^*}\right) = \alpha_f n_f n \ .$$

Hence,

$$\alpha_f = \frac{\gamma\left(u\sigma_{f^*}\right)}{n_f n} = \frac{1}{n_f n} \sum_{i=1}^{r} m_i \chi_i \left(u\sigma_{f^*}\right) \ .$$

□

In the following, let us assume that the adjacency algebra $K\mathfrak{X}$ is a split K-algebra. This means

$$K\mathfrak{X} \cong M_{n_1}(K) \oplus \cdots \oplus M_{n_r}(K) \ ,$$

where each matrix algebra $M_{n_i}(K)$ corresponds to an irreducible character χ_i. Put

$$e_i := 0 \oplus \cdots \oplus I_{n_i} \oplus \cdots \oplus 0 \ , \quad 1 \le i \le r \ ,$$

where I_{n_i} is the $n_i \times n_i$ identity matrix. Evidently, each e_i is a central idempotent of $K\mathfrak{X}$. This gives us a central idempotent decomposition of the identity $1_{K\mathfrak{X}}$:

$$1_{K\mathfrak{X}} = e_1 + e_2 + ... + e_r \ .$$

We use the above notation in the following Lemma (see [10], Lemma 3.2).

Lemma 2.18. *Let f be a primitive idempotent of $K\mathfrak{X}$. Then:*

(i) There is exactly one e_i such that $e_i f = f$. Moreover, $e_j f = 0$ for all $j \neq i$.

(ii) If $e_i f = f$, then $\chi_i(f) = 1$. Moreover, $\chi_j(f) = 0$ for all $j \neq i$. Especially,

$$f = \frac{m_i}{n}\sigma_1 + \sum_{g \neq 1} \alpha_g \sigma_g \ , \quad \alpha_g \in K \ .$$

Proof. (i) Since $1 = e_1 + e_2 + ... + e_r$, it follows that $f = e_1 f + e_2 f + ... + e_r f$. Evidently, this would be an idempotent decomposition of f if $e_j f \neq 0$ for more than one $j = 1, 2, ..., r$. Hence, there is exactly one e_i such that $e_i f = f$.

(ii) We consider f as an element of $M_{n_1}(K) \oplus \cdots \oplus M_{n_r}(K)$. Because of (i), the only nontrivial entries of f lie in the $M_{n_i}(K)$-component of $M_{n_1}(K) \oplus \cdots \oplus M_{n_r}(K)$. This means that multiplication by f is trivial in any other component than $M_{n_i}(K)$; therefore, $\chi_j(f) = 0$ for $j \neq i$.

We will now show $\chi_i(f) = 1$. For this purpose, consider f as a primitive idempotent matrix in $M_{n_i}(K)$. Idempotent matrices in $M_{n_i}(K)$ have eigenvalues 1 and 0 exclusively, and they are primitive if and only if their rank is 1 (see [29], Ch. 3.5). Hence,

$$\chi_i(f) = tr(f) = 1 \ .$$

The formula for f now follows easily by Lemma 2.17. □

We keep the above notation for $K\mathfrak{X}$ in the following proof (taken from [10], Th. 3.4).

Theorem 2.19. *Let F be a field of characteristic p and let $\mathfrak{X} = (X, G)$ be an association scheme of p-power order. Then the adjacency algebra $F\mathfrak{X}$ is local.*

Proof. It suffices to show that $F\mathfrak{X}$ has a unique idempotent (see [23], Lemma 14.4). For this purpose, we may assume that F is algebraically closed. Then there exists a p-modular system (K, R, F) such that $K\mathfrak{X}$ is a split K-algebra (see Section 1.10).

Let $\bar{e}$ be a primitive idempotent of $F\mathfrak{X}$. Let (π) denote the maximal ideal of R. By Theorem 1.24, $\bar{e}$ is liftable to a primitive idempotent e of $R\mathfrak{X}$; this follows from

$$R\mathfrak{X}/(\pi)R\mathfrak{X} \cong (R/\pi R)\,\mathfrak{X} = F\mathfrak{X} \ .$$

We will custom-build a primitive idempotent decomposition of e in $K\mathfrak{X}$. Let

$$K\mathfrak{X}_{K\mathfrak{X}} = \bigoplus_{i=1}^{r} \bigoplus_{\lambda=1}^{n_i} V_{i\lambda}$$

be an irreducible decomposition of $K\mathfrak{X}_{K\mathfrak{X}}$, where $\bigoplus_{\lambda=1}^{n_i} V_{i\lambda}$ is an irreducible decomposition of the simple component $M_{n_i}(K)$. Multipliying the above equation with e gives us

$$(eK\mathfrak{X})_{K\mathfrak{X}} = \bigoplus_{i=1}^{r} \bigoplus_{\lambda=1}^{n_i} eV_{i\lambda} \ .$$

For each $eV_{i\lambda}$ in the above decomposition, observe that either $eV_{i\lambda} = 0$ or $eV_{i\lambda} = V_{i\lambda}$ by irreducibility. Thus, we have a corresponding primitive idempotent decomposition

$$e = \sum_{i=1}^{r} \sum_{j=1}^{s_i} f_j^{(i)} \ ,$$

where $e_i f_j^{(i)} = f_j^{(i)}$ and $s_i \leq n_i$. Moreover, $s_i = n_i$ if and only if $\sum_{j=1}^{s_i} f_j^{(i)} = e_i$ (see Section 1.5).

Applying Lemma 2.18 (ii) to each $f_j^{(i)}$, we obtain

$$e = \sum_{i=1}^{r} \frac{m_i s_i}{n} \sigma_1 + \sum_{g \neq 1} \alpha_g \sigma_g \ , \quad \alpha_g \in K \ .$$

But $n = \gamma(1_{K\mathfrak{X}}) = \sum_{i=1}^{r} m_i n_i$ and n is a p-power, so the coefficient of σ_1 is in R if and only if $s_i = n_i$ for all i. Hence,

$$e = \sum_{i=1}^{r} \sum_{j=1}^{n_i} f_j^{(i)} = \sum_{i=1}^{r} e_i = 1_{K\mathfrak{X}} \ ,$$

and this implies $\bar{e} = 1_{F\mathfrak{X}}$. Since $\bar{e}$ was arbitrary, the proof is complete. □

Corollary 2.20. *Let F be a field of characteristic p and let $\mathfrak{X} = (X, G)$ be an association scheme of p-power order. Assume that $F\mathfrak{X}/J(F\mathfrak{X})$ is an F-split algebra. Then we have:*

(i) The trivial character $1_G : \sigma_g \longrightarrow n_g$ is the unique irreducible character of $F\mathfrak{X}$,

(ii) $J(F\mathfrak{X}) = \bigoplus_{g \in G} (\sigma_g - n_g \sigma_1)$,

(iii) σ_g has the unique eigenvalue n_g in F.

Proof. (i) It suffices to show that $F\mathfrak{X}$ has a unique irreducible module. This is certainly the case if the split F-algebra $F\mathfrak{X}/J(F\mathfrak{X})$ has a unique irreducible module (see [23], Th. I.8.10). We prove the latter statement.

Assume

$$F\mathfrak{X}/J(F\mathfrak{X}) \cong \bigoplus_{i=1}^{k} M_{n_i}(F) \ .$$

Since $F\mathfrak{X}$ is local, $F\mathfrak{X}/J(F\mathfrak{X})$ is a division ring (see [23], Th. 5.7). It follows that $F\mathfrak{X}/J(F\mathfrak{X})$ has a unique idempotent. But then $F\mathfrak{X}$ can have only one simple component (see Section (1.4)), so we may assume $k = 1$ in the above sum:

$$F\mathfrak{X}/J(F\mathfrak{X}) \cong M_{n_1}(F) \ .$$

Since $F\mathfrak{X}/J(F\mathfrak{X})$ is a division ring, it must be $n_1 = 1$. It follows that

$$F\mathfrak{X}/J(F\mathfrak{X}) \cong F \ ,$$

and the unique irreducible module of this algebra is F itself.

(ii) By Theorem 1.3, $J(F\mathfrak{X})$ consists exactly of those elements of $F\mathfrak{X}$ which annihilate all irreducible right $F\mathfrak{X}$-modules. Evidently, these are exactly the elements which lie in the kernel of 1_G (see statement (i)). Therefore,

$$J(F\mathfrak{X}) = ker\ 1_G = \bigoplus_{g \in G} (\sigma_g - n_g \sigma_1) \ .$$

(iii) This is proven easily. Since $\sigma_g - n_g\sigma_1$ is in the Jacobson Radical of $F\mathfrak{X}$, it is nilpotent (see [23], Th. I.3.5). It follows that all eigenvalues of $\sigma_g - n_g\sigma_1$ are equal to 0. Therefore, all eigenvalues of σ_g must equal n_g. □

2.6 Schemes of Prime Order

In this section, $\mathfrak{X} = (X, G)$ is an association scheme and $\mathbb{C}\mathfrak{X}$ is the complex adjacency algebra with element of unity 1. We will show that if $|X|$ is a prime number, then (X, G) is a commutative association scheme and all valencies of (X, G) coincide (see Theorem 2.28). This result was first proven in [13], and the discussion below closely follows after this reference.

We need the following preliminary result:

Lemma 2.21. *Let* $\boldsymbol{Y}$ *be matrix representation of* $\mathbb{C}\mathfrak{X}$*,*

$$\boldsymbol{Y} : \mathbb{C}\mathfrak{X} \longrightarrow M_k(\mathbb{C}) \ , \quad \sigma \longrightarrow Y(\sigma) \ .$$

Then, for all $\sigma \in \mathbb{C}\mathfrak{X}$*, every eigenvalue of* $Y(\sigma)$ *is also an eigenvalue of* σ*.*

Proof. Put $n := |X|$. Let $f(x)$ be the characteristic polynomial of σ,

$$f(x) = det\,(\sigma - x \cdot I_n) = \sum_{i=1}^{n} a_i x^i \ .$$

Let λ be some eigenvalue of $Y(\sigma)$. Then it suffices to show $f(\lambda) = 0$. For this purpose, note that

$$\sum_{i=1}^{n} a_i \sigma^i = 0$$

by Cayley-Hamilton's Theorem. Applying $\mathbf{Y}$ to both sides of this equation yields

$$\sum_{i=1}^{n} a_i Y(\sigma)^i = 0 \ .$$

Thus, if $0 \neq v \in \mathbb{C}^k$ is some eigenvector of $Y(\sigma)$ associated with λ, we have

$$\sum_{i=1}^{n} a_i Y(\sigma)^i v = 0 \implies \sum_{i=1}^{n} a_i \lambda^i v = 0 \implies f(\lambda)v = 0 \implies f(\lambda) = 0 \ ,$$

from which the assertion follows. □

We can now prove the following important result:

Lemma 2.22. *For any character* χ *of* $\mathbb{C}\mathfrak{X}$*, the character values* $\{\chi(\sigma_g) \,|\, g \in G\}$ *are algebraic integers.*

Proof. Let $\mathbf{Y}$ be a matrix representation of $\mathbb{C}\mathfrak{X}$ that affords χ. For $g \in G$, every eigenvalue of $Y(\sigma_g)$ is also an eigenvalue of σ_g (see Lemma 2.21). But σ_g is an integral matrix; therefore, its eigenvalues are algebraic integers. Hence, $\chi(\sigma_g) = tr(Y(\sigma_g))$ is a sum of algebraic integers and therefore an algebraic integer itself. □

For the next result, let χ be a non-trivial irreducible character of $\mathbb{C}\mathfrak{X}$. Let K be a finite normal extension of the rational number field $\mathbb{Q}$ such that the character values $\{\chi(\sigma_g) \,|\, g \in G\}$ are contained in K and $K\mathfrak{X}$ is a split K-algebra (for the existence of K, see [3] (Ch. 3.5) and [23] (Ch. II.3)). We denote by $Gal(K/\mathbb{Q})$ the Galois group of this extension. The following holds:

Lemma 2.23. *In the above situation, for each $\tau \in Gal(K/\mathbb{Q})$, there exists a character χ^τ of $\mathbb{C}\mathfrak{X}$ such that*

$$\chi^\tau(\sigma_g) = \chi(\sigma_g)^\tau$$

for all $g \in G$. Moreover, χ^τ is also irreducible.

Proof. Let U be an irreducible $\mathbb{C}\mathfrak{X}$-module that affords χ. By [6] (Th. 29.21), there exists an irreducible $K\mathfrak{X}$-module V such that

$$\mathbb{C} \otimes_K V \cong U \ .$$

For $\tau \in Gal(K/\mathbb{Q})$, let σ^τ denote the (entrywise) image of $\sigma \in K\mathfrak{X}$ under τ. We exchange the original scalar product on V with the slightly modified

$$V \times K\mathfrak{X} \longrightarrow V \ , \quad (v, \sigma) \longrightarrow v\sigma^\tau \ ;$$

the resulting $K\mathfrak{X}$-module we denote by V^τ. Clearly, V^τ is an irreducible $K\mathfrak{X}$-module; this follows from the irreducibility of V. Consequently,

$$\mathbb{C} \otimes_K V^\tau =: U^\tau$$

is an irreducible $\mathbb{C}\mathfrak{X}$-module (see [6], Th. 29.21). Moreover, it is evident from the above construction that the character χ^τ of $\mathbb{C}\mathfrak{X}$ afforded by U^τ satisfies

$$\chi^\tau(\sigma_g) = \chi(\sigma_g)^\tau \ , \quad \forall \ g \in G$$

This completes the proof. □

Using the notation of Lemma 2.23, we can define a group action of $Gal(K/\mathbb{Q})$ on the set $Irr(\mathbb{C}\mathfrak{X})$ of irreducible characters of $\mathbb{C}\mathfrak{X}$:

$$Gal(K/\mathbb{Q}) \times Irr(\mathbb{C}\mathfrak{X}) \longrightarrow Irr(\mathbb{C}\mathfrak{X}) \ , \quad (\tau, \chi) \longrightarrow \chi^\tau \ .$$

In the following, we call two characters $\chi, \varphi \in Irr(\mathbb{C}\mathfrak{X})$ *algebraically conjugate* if they lie in the same orbit by this action. Interestingly, this definition does not depend on the choice of K, which the reader may prove himself by using the fact that the restriction homomorphism

$$Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow Gal(K/\mathbb{Q}) \ , \quad \tau \longrightarrow \tau|_K$$

is surjective (see [3], Ch. 4.1).

We can now prove the following important lemma:

Lemma 2.24. *Let χ be an irreducible character of $\mathbb{C}\mathfrak{X}$. Let Φ be the sum of all algebraic conjugates of χ. Then the Φ-values $\{\Phi(\sigma_g) \,|\, g \in G\}$ are rational integers.*

Proof. We use the same notation as in Lemma 2.23. We define by

$$I := \{\tau \in Gal(K/\mathbb{Q}) \,|\, \chi^\tau = \chi\}$$

the stabilizer group of χ in $Gal(K/\mathbb{Q})$. Clearly, $|Gal(K/\mathbb{Q}) : I| < \infty$. Put

$$Gal(K/\mathbb{Q}) = I\tau_1 \cup I\tau_2 \cup \cdots \cup I\tau_r$$

a coset decomposition of $Gal(K/\mathbb{Q})$. Then

$$\{\chi^\tau \,|\, \tau \in Gal(K/\mathbb{Q})\} = \{\chi^{\tau_1}, \chi^{\tau_2}, ..., \chi^{\tau_r}\} \ .$$

Consequently,

$$\Phi = \sum_{i=1}^{r} \chi^{\tau_i} \ .$$

For $g \in G$, it follows that $\Phi(\sigma_g)^\tau = \Phi(\sigma_g)$ for all $\tau \in Gal(K/\mathbb{Q})$. Hence, $\Phi(\sigma_g) \in \mathbb{Q}$. But $\Phi(\sigma_g)$ is an algebraic integer (see Lemma 2.22), so we even have $\Phi(\sigma_g) \in \mathbb{Z}$. This completes the proof. □

I want to mention that proof of the above lemma, as well as the proof of the following corollary, have been pointed out to me by A. Hanaki during our E-mail correspondence (see [12]).

Corollary 2.25. *Let $\mathfrak{X} = (X, G)$ be an association scheme of prime order $p = |X|$. Let χ be an irreducible character of $\mathbb{C}\mathfrak{X}$, and Φ the sum of all algebraic conjugates of χ. Then there exist rational integers $\{u_g \mid g \in G\}$ such that*

$$\Phi(\sigma_g) = n_g\Phi(1) - u_g p \ .$$

Proof. Let K be a finite extension of the rational number field $\mathbb{Q}$ such that for each $g \in G$, the eigenvalues of σ_g are contained in K. Then, by [23] (Ch. I.13.2), there exists a valuation ring R of K with maximal ideal π such that $F := R/\pi$ is a field of characteristic p and

$$\pi \cap \mathbb{Z} = (p) \ .$$

As a valuation ring, R is integrally closed (see [21], Th. 10.3). Especially, for each $g \in G$, the eigenvalues of σ_g are contained in R. Moreover, we know that

(i) $\Phi(\sigma_g)$ is a sum of $\Phi(1)$ eigenvalues of σ_g (see Lemma 2.21)

(ii) All eigenvalues of σ_g are congruent to n_g modulo π (see Corollary 2.20 (iii))

Together, this yields

$$\Phi(\sigma_g) \equiv n_g\Phi(1) \pmod{\pi} \ .$$

Since $\Phi(\sigma_g) - n_g\Phi(1) \in \mathbb{Z}$ by Lemma 2.24, we conclude

$$\Phi(\sigma_g) - n_g\Phi(1) \in \pi \cap \mathbb{Z} = (p) \ .$$

The assertion follows instantly. □

We will now take the first step in the proof of the main result of this section. The following theorem was first shown in [13] (see Lemma 3.1).

Theorem 2.26. *Let $\mathfrak{X} = (X, G)$ be an association scheme. If $|X|$ is a prime number, then all nontrivial irreducible characters of $\mathbb{C}\mathfrak{X}$ are algebraically conjugate. Especially, their multiplicities are constant.*

Proof. Put $p := |X|$. Let 1_G be the trivial character of $\mathbb{C}\mathfrak{X}$ and χ a nontrivial irreducible character of $\mathbb{C}\mathfrak{X}$. Put Φ the sum of all algebraic conjugates of χ, and Ψ the sum of all nontrivial irreducible characters which are not algebraically conjugate to χ. If Ψ is zero, then the assertion holds, so we assume that $\Psi \neq 0$.

By Corollary 2.25, there exist rational integers $\{u_g \mid g \in G\}$ such that

$$\Phi(\sigma_g) = n_g\Phi(1) - u_g p \ .$$

Similarly, there exist rational integers $\{v_g \mid g \in G\}$ such that

$$\Psi(\sigma_g) = n_g\Psi(1) - v_g p \ .$$

By the orthogonality relation (Theorem 2.13 (ii)),

$$\begin{aligned} 0 &= \sum_{g\in G} \frac{1}{n_g} 1_G(\sigma_{g^*})\Phi(\sigma_g) = \sum_{g\in G} \Phi(\sigma_g) \\ &= \sum_{g\in G} (n_g\Phi(1) - u_g p) = p\left(\Phi(1) - \sum_{g\in G} u_g\right) \ . \end{aligned}$$

Hence, $\sum_{g\in G} u_g = \Phi(1)$. Similarly, one can show $\sum_{g\in G} v_g = \Psi(1)$.

Again by the orthogonality relation,

$$\begin{aligned} 0 &= \sum_{g\in G} \frac{1}{n_g}\Phi(\sigma_{g^*})\Psi(\sigma_g) = \sum_{g\in G} \frac{1}{n_g}\left(\Phi(1)n_{g^*} - u_{g^*}p\right)\left(\Psi(1)n_g - v_g p\right) \\ &= \sum_{g\in G} \Phi(1)\Psi(1)n_g - \sum_{g\in G} \Phi(1)v_g p - \sum_{g\in G} \Psi(1)u_{g^*}p + \sum_{g\in G} \frac{1}{n_g} u_{g^*}v_g p^2 \\ &= p\Phi(1)\Psi(1) - p\Phi(1)\Psi(1) - p\Phi(1)\Psi(1) + \sum_{g\in G} \frac{1}{n_g} u_{g^*}v_g p^2 \\ &= -p\Phi(1)\Psi(1) + \sum_{g\in G} \frac{1}{n_g} u_{g^*}v_g p^2 \ . \end{aligned}$$

We conclude

$$\Phi(1)\Psi(1) = \sum_{g\in G} \frac{1}{n_g} u_{g^*}v_g p \ .$$

But $\Phi(1)\Psi(1)$ is relatively prime to p (because $\Phi(1), \Psi(1) < p$), whereas the right hand side is divisible by p (because n_g and p are relatively prime for all $g \in G$). This is a contradiction. □

We will now prove the remaining part of the main result of this section. The following theorem was shown in [13] (see Lemma 3.2).

Theorem 2.27. *If all nontrivial irreducible characters of G have the same multiplicities, then (X, G) is commutative and all nontrivial relations have the same valencies.*

Proof. Suppose $m_\chi = m$ for every nontrivial irreducible character χ of G. By Corollary 2.14, we have

$$|X| = \gamma(1) = \sum_{\chi \in Irr(G)} m_\chi \chi(1) = 1 + m \sum_{\chi \neq 1_G} \chi(1) \ .$$

Hence, m is relatively prime to $|X|$.

Consider the Frame number

$$\mathcal{F}(\mathfrak{X}) = |X|^{|G|} \frac{\prod_{g \in G} n_g}{\prod_{\chi \in Irr(G)} {m_\chi}^{\chi(1)^2}} = |X|^{|G|} \frac{\prod_{g \neq 1} n_g}{m^{|G|-1}} \in \mathbb{Z} \ .$$

Since m is relatively prime to $|X|$, we have

$$\frac{\prod_{g \neq 1} n_g}{m^{|G|-1}} \in \mathbb{Z} \ ,$$

and especially $\prod_{g \neq 1} n_g \geq m^{|G|-1}$.

Note that $\sum_{\chi \neq 1_G} \chi(1) \leq |G| - 1$, and equality holds if and only if (X, G) is commutative (see Corollary 2.9). By the inequality of arithmetic and geometric means, we have

$$\left(\prod_{g \neq 1} n_g \right)^{\frac{1}{|G|-1}} \leq \frac{\sum_{g \neq 1} n_g}{|G| - 1} \leq \frac{\sum_{g \neq 1} n_g}{\sum_{\chi \neq 1} \chi(1)} = \frac{|X| - 1}{\sum_{\chi \neq 1} \chi(1)} = m \ .$$

Since $\prod_{g \neq 1} n_g \geq m^{|G|-1}$, equality must hold in the above inequality. Especially,

$$|G| - 1 = \sum_{\chi \neq 1_G} \chi(1) \ ,$$

so (X, G) is commutative.

Moreover,

$$\left(\prod_{g\neq 1} n_g\right)^{\frac{1}{|G|-1}} = \frac{\sum_{g\neq 1} n_g}{|G|-1} \ ,$$

and this implies that all valencies of nontrivial relations must coincide, yielding $n_g = m$ for all $1 \neq g \in G$. □

Altogether, we have proven the following (see [13], Th. 3.3).

Main Result 2.28. *Let $\mathfrak{X} = (X, G)$ be an association scheme. If $|X|$ is a prime number, then (X, G) is commutative. Moreover, all nontrivial irreducible characters of $\mathbb{C}\mathfrak{X}$ are algebraically conjugate, and all valencies of nontrivial relations and multiplicities of nontrivial irreducible characters coincide.*

This completes our discussion. For more on association schemes of prime order, see [13].

3 m-Schemes

In this chapter, we introduce m-schemes, combinatorial objects that were first defined in [16]. m-Schemes are closely related to association schemes, and as we will see in Chapter 5, they occur naturally as part of a factoring algorithm for polynomials over finite fields. In the following, we give an overview of the basic theory of m-schemes and look at notable examples.

Note that the material has been organized in such a way that it requires no previous knowledge of m-schemes. Also note that in Chapter 4, we will extend the present discussion by a new topological interpretation of m-schemes.

3.1 Basic Notions

In this section, we introduce the necessary vocabulary for our study of m-schemes. For reference purposes, the terminology used here is the same as in the paper [16]. Examples of m-schemes will follow separately in Sections (3.2) and (3.3).

s-tuples: Throughout this section, $V = \{v_1, v_2, ..., v_n\}$ is an arbitrary set of n distinct elements. For $1 \leq s \leq n$, we define the set of s-tuples by

$$V^{(s)} := \{(v_{i_1}, v_{i_2}, ..., v_{i_s}) \mid \ v_{i_1}, v_{i_2}, ..., v_{i_s} \text{ are } s \text{ distinct elements of } V\} \ .$$

Projections: For $s > 1$, we define s projections $\pi_1^s, \pi_2^s ..., \pi_s^s : V^{(s)} \longrightarrow V^{(s-1)}$ by

$$\pi_i^s : (v_1, ..., v_{i-1}, v_i, v_{i+1}, ..., v_s) \longrightarrow (v_1, ..., v_{i-1}, v_{i+1}, ..., v_s) \ .$$

Permutations: The symmetric group on s elements $Symm_s$ acts on $V^{(s)}$ in a natural way by permuting the coordinates of the s-tuples. More accurately, the action of $\tau \in Symm_s$ on $(v_1, ..., v_i, ..., v_s) \in V^{(s)}$ is defined as

$$(v_1, ..., v_i, ..., v_s)^\tau := (v_{1^\tau}, ..., v_{i^\tau}, ..., v_{s^\tau}) \ .$$

m-Collection: For $1 \leq m \leq n$, an *m-collection* on V is a set Π of partitions $\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m$ of $V^{(1)}, V^{(2)}, ..., V^{(m)}$ respectively.

Colors: For $1 \leq s \leq m$, the equivalence relation on $V^{(s)}$ corresponding to the partition $\mathcal{P}_s$ will be denoted by $\equiv_{\mathcal{P}_s}$.

Below, we discuss some natural properties of m-collections that will be relevant to us in the future. In the following, let $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m\}$ be an m-collection on V.

P1 (Compatibility): We say that Π is *compatible* at level $1 < s \leq m$, if $\bar{u} \equiv_{\mathcal{P}_s} \bar{v}$ implies $\pi_i^s(\bar{u}) \equiv_{\mathcal{P}_{s-1}} \pi_i^s(\bar{v})$ for all $1 \leq i \leq s$ and $\bar{u}, \bar{v} \in V^{(s)}$. In other words: If $\bar{u}, \bar{v} \in P \in \mathcal{P}_s$, then compatibility means that for all $1 \leq i \leq s$, there exists $Q \in \mathcal{P}_{s-1}$ such that $\pi_i^s(\bar{u}), \pi_i^s(\bar{v}) \in Q$.

P2 (Regularity): We say that Π is *regular* at level $1 < s \leq m$, if $\bar{u}, \bar{v} \in Q \in \mathcal{P}_{s-1}$ implies

$$|\{\bar{u}' \in P \,|\, \pi_i^s(\bar{u}') = \bar{u}\}| = |\{\bar{v}' \in P \,|\, \pi_i^s(\bar{v}') = \bar{v}\}|$$

for all $1 \leq i \leq s$ and $P \in \mathcal{P}_s$. In other words: If $\bar{u}, \bar{v} \in Q \in \mathcal{P}_{s-1}$, then regularity means that $P \cap (\pi_i^s)^{-1}(\bar{u})$ and $P \cap (\pi_i^s)^{-1}(\bar{v})$ have the same cardinality for all $1 \leq i \leq s$ and $P \in \mathcal{P}_s$.

Fibers: We call the tuples in $P \cap (\pi_i^s)^{-1}(\bar{u})$ the *π_i^s-fibers of $\bar{u}$ in P*.

Subdegree: The above two properties motivate the definition of the *subdegree of a color P over a color Q* as $\frac{|P|}{|Q|}$, assuming that $\pi_i^s(P) = Q$ for some i and that Π is regular at level s.

P3 (Invariance): We say that Π is *invariant* at level $1 < s \leq m$, if for every $P \in \mathcal{P}_s$ and $\tau \in Symm_s$, we have

$$P^\tau := \{\bar{v}^\tau \,|\, \bar{v} \in P\} \in \mathcal{P}_s \ .$$

In other words: If $P \in \mathcal{P}_s$, then invariance means that $\{P^\tau \,|\, \tau \in Symm_s\}$ are also colors in $\mathcal{P}_s$.

P4 (Antisymmetry): We say that Π is *antisymmetric* at level $1 < s \leq m$, if for every $P \in \mathcal{P}_s$ and $id \neq \tau \in Symm_s$, we have $P^\tau \neq P$.

P5 (Symmetry): We say that Π is *symmetric* at level $1 < s \leq m$, if for every $P \in \mathcal{P}_s$ and $\tau \in Symm_s$, we have $P^\tau = P$.

P6 (Homogeneity): We say that Π is *homogeneous* if $|\mathcal{P}_1| = 1$.

Note that an m-collection is called homogeneous, compatible, regular, invariant, symmetric, or antisymmetric if it is at every level $1 < s \leq m$, homogeneous, compatible, regular, invariant, symmetric, or antisymmetric. Moreover, we settle for the following definition:

m-Scheme: We call Π an *m-scheme* if it is compatible, regular and invariant.

In the following Sections, we discuss the basic theory of m-schemes and look at notable examples. In Chapter 5, we utilize this theory to show how m-schemes can be used in polynomial factoring over finite fields.

3.2 Association Schemes at Level 3

In this section, we explain how our current study of m-schemes relates to the preceding study of association schemes. Through our results, we will gain useful insights into the structure of an m-scheme up to level 3.

The following lemma is of much importance (taken from [16], Ex. 2.2).

Lemma 3.1. *Let $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3\}$ be a homogeneous 3-scheme on $V = \{v_1, v_2, ..., v_n\}$. Then $(\mathcal{P}_1, \mathcal{P}_2 \cup \{1\})$ is an association scheme, where $1 := \{(v, v) \,|\, v \in V\}$ denotes the trivial relation.*

Proof. We will show that $(\mathcal{P}_1, \mathcal{P}_2 \cup \{1\})$ satisfies condition (iv) of Definition 2.1. We need to prove: For all $P_i, P_j, P_k \in \mathcal{P}_2 \cup \{1\}$, there exists an integer a_{ijk} such that for all $(\alpha, \beta) \in P_k$,

$$a_{ijk} = |\{\gamma \in V \,|\, (\alpha, \gamma) \in P_i \ , \ (\gamma, \beta) \in P_j\}| \ .$$

We only consider the case $P_i, P_j, P_k \neq 1$ and leave the rest to the reader. By the compatibility and regularity of Π at level 3, there exists a subset $\mathcal{S} \subseteq \mathcal{P}_3$ such that for all $(\alpha, \beta) \in P_k$, the set $\{\gamma \in V \,|\, (\alpha, \gamma) \in P_i \ , \ (\gamma, \beta) \in P_j\}$ can be partitioned as

$$\dot{\cup}_{P \in \mathcal{S}} \{\gamma \in V \,|\, (\alpha, \gamma) \in P_i \ , \ (\gamma, \beta) \in P_j \ , (\alpha, \gamma, \beta) \in P\} \ .$$

By the compatibility of Π at level 3, this partition can simply be written as

$$\dot{\cup}_{P\in\mathcal{S}}\{\gamma \in V \mid (\alpha,\gamma,\beta) \in P\} \ .$$

By the regularity of Π at level 3, the size of each set in the above partition is $\frac{|P|}{|P_k|}$, which means that

$$|\{\gamma \in V \mid (\alpha,\gamma) \in P_i \ , \ (\gamma,\beta) \in P_j\}| = \sum_{P\in\mathcal{S}} \frac{|P|}{|P_k|} \ .$$

Since this equation holds for all $(\alpha,\beta) \in P_k$, condition (iv) of Definition 2.1 is satisfied by $(\mathcal{P}_1, \mathcal{P}_2 \cup \{1\})$. It follows that $(\mathcal{P}_1, \mathcal{P}_2 \cup \{1\})$ is an association scheme. □

We will now consider the converse of the preceding result: The next lemma asserts that, in turn, every association scheme also affords a 3-scheme (see [16], Ex. 2.2).

Lemma 3.2. *Let $(\mathcal{P}_1, \mathcal{P}_2)$ be an association scheme on $V = \{v_1, v_2, ..., v_n\}$. We denote by $\equiv_{\mathcal{P}_2}$ the equivalence relation on $V \times V$ corresponding to the partition $\mathcal{P}_2$. Let $\mathcal{P}_3$ be the partition of $V^{(3)}$ such that for two triples (u_1, u_2, u_3) and (v_1, v_2, v_3), we have $(u_1, u_2, u_3) \equiv_{\mathcal{P}_3} (v_1, v_2, v_3)$ if and only if*

$$(u_1, u_2) \equiv_{\mathcal{P}_2} (v_1, v_2), \quad (u_1, u_3) \equiv_{\mathcal{P}_2} (v_1, v_3), \quad (u_2, u_3) \equiv_{\mathcal{P}_2} (v_2, v_3) \ .$$

Then $\{\mathcal{P}_1, \mathcal{P}_2 - \{1\}, \mathcal{P}_3\}$ is a 3-scheme.

Proof. It is quickly shown that $\{\mathcal{P}_1, \mathcal{P}_2 - \{1\}, \mathcal{P}_3\}$ satisfies compatibility, regularity and invariance. The proof is left as an exercise to the reader. □

3.3 Orbit m-Schemes

In this section, we discuss m-schemes that arise from permutation groups, so called *orbit m-schemes*. Orbit m-schemes can be regarded as a higher-level analog of the Schurian association schemes introduced in Section (2.1) (see Ex. 2.4). We use the term orbit m-scheme to amplify that the colors of these schemes are orbits of a group action. Throughout this section, let $V = \{v_1, v_2, ..., v_n\}$ be a set of n distinct elements and $G \leq Symm_V$ a permutation group.

The following lemma is of fundamental importance (see [16], Ex. 2.3).

Lemma 3.3. *Fix some integer $1 \leq m \leq n$. For $1 \leq s \leq m$, let $\mathcal{P}_s$ be the partition on $V^{(s)}$ such that for any two s-tuples $(u_1, u_2, ..., u_s)$ and $(v_1, v_2, ..., v_s)$, we have $(u_1, u_2, ..., u_s) \equiv_{\mathcal{P}_s} (v_1, v_2, ..., v_s)$ if and only if*

$$\exists\ \sigma \in G: \quad (\sigma(u_1), \sigma(u_2), ..., \sigma(u_s)) = (v_1, v_2, ..., v_s)\ .$$

Then $\{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m\}$ is an m-scheme on V. Moreover:

(i) $\{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m\}$ is homogeneous if and only if G is transitive,

(ii) $\{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m\}$ is antisymmetric if and only if $gcd(m!, |G|) = 1$.

Proof. We will only show statement (ii) and leave the rest as an exercise to the reader. We prove "$\Leftarrow$" by contraposition: Suppose $\{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m\}$ is not antisymmetric at some level $1 < s \leq m$. Then there exists $(u_1, u_2, ..., u_s) \in V^{(s)}$ such that

$$(u_1, u_2, ..., u_s) \equiv_{\mathcal{P}_s} (u_{1^\tau}, u_{2^\tau}, ..., u_{s^\tau})$$

for some $id \neq \tau \in Symm_s$. By the definition of $\{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m\}$, this means there exists $\sigma \in G$ such that

$$(\sigma(u_1), \sigma(u_2), ..., \sigma(u_s)) = (u_{1^\tau}, u_{2^\tau}, ..., u_{s^\tau})\ .$$

Choose an index $j \in \{1, ..., s\}$ such that $\sigma(u_j) \neq u_j$. Then there exists an integer k such that $2 \leq k \leq s$ and

$$\sigma^k(u_j) = u_j\ .$$

Clearly, k divides the order of σ, which in turn divides the order of G. Hence, $gcd(m!, |G|) > 1$. This completes the proof of "$\Leftarrow$". For the converse statement, note that $gcd(m!, |G|) > 1$ implies that there exists $\sigma \in G$ such that $\sigma^k = id$ for some $k \leq m$ (by Sylow's Theorem). The assertion now follows by reversing the proof of "$\Leftarrow$". We leave the details as an exercise to the reader. □

We call m-schemes that arise in the above-described manner *orbit m-schemes*. At the moment, orbit m-schemes are the only examples of homogeneous and antisymmetric m-schemes (where $m \geq 4$) that we know of. Also, they are the only examples of m-schemes for which the important Schemes Conjecture (see Section 3.5) has already been proven. We will study these issues in more detail at a later point.

The following theorem is a variation of a result from the paper [26], which was originally proven for *superschemes*, combinatorial objects that one might describe as "m-schemes satisfying some additional conditions". We just cite it here for completeness, it does not bear any relevance to our future study.

Theorem 3.4. *Every $(n-1)$-scheme on n points is an orbit scheme.*

Proof. By a simple comparison of definitions, we show that every $(n-1)$-scheme on n points can be regarded as a superscheme (in the sense of [26], Def. 2.2). The assertion then follows from [26], Th. 4.4. □

3.4 Matchings

We will now discuss *matchings*, certain special colors of m-schemes that play an important role in the polynomial factoring algorithm of Chapter 5. In the following, let $V = \{v_1, v_2, ..., v_n\}$ be a set of n distinct elements and $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m\}$ be an m-scheme on V.

Matching: A color $P \in \mathcal{P}_s$ at any level $1 < s \leq m$ is called a *matching* if there exists $1 \leq i < j \leq s$ such that $\pi_i^s(P) = \pi_j^s(P)$ and $|\pi_i^s(P)| = |P|$.

As the next lemma shows, an antisymmetric m-scheme on n points always has a matching if $m \geq \log_2 n$ (taken from [16], Lemma 8).

Lemma 3.5. *Let $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m\}$ be an m-scheme on $V = \{v_1, v_2, ..., v_n\}$. Assume that Π is antisymmetric at level 2. Moreover, assume that $|\mathcal{P}_1| < n$ and $m \geq \log_2 n$. Then there exists a matching in $\{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m\}$.*

Proof. We will outline a convenient way of finding a matching in Π. For this purpose, choose a color $P_1 \in \mathcal{P}_1$ with $d_1 = |P_1| > 1$. Evidently, $Q_2 = P_1^{(2)}$ is a disjoint union of colors in $\mathcal{P}_2$. Choose a smallest color $P_2 \in \mathcal{P}_2$ with $P_2 \subset Q_2$. Then by the compatibility of Π, we have

$$\pi_1^2(P_2) = \pi_2^2(P_2) = Q_2 \ .$$

Moreover, by the antisymmetry of Π, we have

$$d_2 := \frac{|P_2|}{|P_1|} \leq \frac{\frac{d_1(d_1-1)}{2}}{d_1} < \frac{d_1}{2} \ .$$

Evidently, if $d_2 = 1$, then P_2 is a matching. Otherwise, if $d_2 > 1$, then we proceed iteratively as follows: Suppose that, for some $2 < s < m$, we have already chosen $P_1 \in \mathcal{P}_1, ..., P_{s-1} \in \mathcal{P}_{s-1}$ such that $\pi^i_{i-1}(P_i) = \pi^i_i(P_i) = P_{i-1}$ and $1 < d_i := \frac{|P_i|}{|P_{i-1}|}$ $< \frac{d_{i-1}}{2}$ for every $2 \leq i \leq s-1$. Since $d_{s-1} > 1$, the set

$$Q_s := \{\bar{v} \in V^{(s)} \mid \pi^s_{s-1}(\bar{v}), \pi^s_s(\bar{v}) \in P_{s-1}\}$$

is nonempty. Let P_s be a smallest color of $\mathcal{P}_s$ such that $P_s \subset Q_s$. Then again by the antisymmetry of Π we have

$$d_s := \frac{|P_s|}{|P_{s-1}|} < \frac{d_{s-1}}{2} \ .$$

Evidently, if $d_s = 1$, then P_s is a matching. Otherwise, if $d_s > 1$, we proceed to level $s+1$ and further halve the subdegree. This procedure finds a matching in at most $\log_2 d_1 < \log_2 n$ rounds. □

3.5 The Schemes Conjecture

As it was shown in Lemma 3.5, every antisymmetric m-scheme on n points (for large enough m) contains a matching somewhere between level 1 and $\log_2 n$. In this section, we ask if there exists a constant $c \geq 4$ that could replace the above $\log_2 n$-bound. This is the subject of the so-called *Schemes Conjecture*:

Schemes Conjecture. *There exists a constant $m \geq 4$ such that every homogeneous, antisymmetric m-scheme contains a matching.*

It will be shown in Chapter 5 that, under GRH, the correctness of the Schemes Conjecture would result in the first polynomial-time algorithm for the factorization of polynomials over finite fields (see Theorem 5.4). We are therefore much interested in making progress towards a proof. However, current efforts have led only to partial results; we list them below.

So far, the Schemes Conjecture has been proven for orbit schemes:

Theorem 3.6 (Schemes Conjecture for Orbit m-Schemes)**.** *For $m \geq 4$, every homogeneous, antisymmetric orbit m-scheme contains a matching.*

Proof. This is shown in [16], Sec. 4. □

Concerning the general case of the schemes conjecture, the following constant-factor improvement of Lemma 3.5 has been achieved:

Lemma 3.7. *Let $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m\}$ be an m-scheme on $V = \{v_1, v_2, ..., v_n\}$. Assume that Π is antisymmetric at the first three levels. Moreover, assume that $|\mathcal{P}_1| < n$ and $m \geq \frac{2}{3}\log_2 n$. Then there exists a matching in $\{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m\}$.*

Proof. This is shown in [16], Sec. 6. □

The bound $m \geq \frac{2}{3}\log_2 n$ of Lemma 3.7 is currently the nearest we can come to the Schemes Conjecture.

4 A Topological Interpretation of m-Schemes

In this chapter, we discuss the theory of m-schemes from a topological viewpoint. We show that m-schemes belong to a special class of combinatorial objects called Δ-sets (also called *simplicial sets*, see [15], [27]), which are commonly studied in algebraic topology. From this duality, we draw new insights into the algebraic properties and the geometry of m-schemes. Our goal is to create a link between the theory of m-schemes and the world of combinatorial algebraic topology.

Since we introduce all relevant definitions along the way, no previous knowledge of algebraic topology is required. For a rigorous introduction to (combinatorial) algebraic topology, the reader is referred to the standard texts [18], [20].

4.1 Preliminaries

In this section, we introduce the prerequisites for our topological discussion of m-schemes. The following preliminary remarks concern the *topological standard n-simplex*.

Let $n \geq 0$ and let $e_0, ..., e_n$ be the standard basis of $\mathbb{R}^{n+1}$. We define the standard n-simplex ∇^n as the convex hull of the set $\{e_0, ..., e_n\}$,

$$\nabla^n := \{(t_0, ..., t_n) \in \mathbb{R}^{n+1} \mid t_0 \geq 0, \ \sum t_i = 1\} \ .$$

In the lower dimensions, the standard simplices can be interpreted geometrically:

$$\begin{aligned} \nabla^3 \subset \mathbb{R}^4 &\quad \text{is a tetrahedron} \\ \nabla^2 \subset \mathbb{R}^3 &\quad \text{is a triangle} \\ \nabla^1 \subset \mathbb{R}^2 &\quad \text{is a line segment} \\ \nabla^0 \subset \mathbb{R}^1 &\quad \text{is a singleton} \end{aligned}$$

Topologically, we consider the standard simplex ∇^n as a subspace of $\mathbb{R}^{n+1}$ (i.e. it is given the subspace topology). In each dimension n, we have $(n+1)$ embeddings $\delta_0^n, ..., \delta_n^n : \nabla^n \longrightarrow \nabla^{n+1}$ (often abbreviated $\delta_0, ..., \delta_n$),

$$\delta_i : (t_0, ..., t_n) \longrightarrow (t_0, ..., \underset{\substack{\uparrow \\ i\text{-th coordinate}}}{t_{i-1}}, 0, t_i, ..., t_n) \ ,$$

whose respective images $\delta_0(\nabla^n), ..., \delta_n(\nabla^n)$ are called the *faces* of the standard simplex ∇^{n+1}. As an example: The faces of the tetrahedron $\nabla^3 \subset \mathbb{R}^4$ are the four triangles dividing its surface. The maps $\delta_0, \delta_1, \delta_2, \delta_3$ represent the corresponding ways in which the triangle $\nabla^2 \subset \mathbb{R}^3$ can be embedded in ∇^3. Similarly, the faces of the triangle $\nabla^2 \subset \mathbb{R}^3$ are its three sides, and the maps $\delta_0, \delta_1, \delta_2$ represent the corresponding ways in which the line segment $\nabla^1 \subset \mathbb{R}^2$ can be embedded in ∇^2.

Note that the composites of the above embeddings

$$\delta_i \delta_j : \nabla^n \xrightarrow{\delta_j} \nabla^{n+1} \xrightarrow{\delta_i} \nabla^{n+2}$$

satisfy the important relation

$$\delta_i \delta_j = \delta_j \delta_{i-1} \ , \quad \text{if} \ \ j < i \ . \tag{1}$$

4.2 Δ-Sets

In this section, we discuss the notion of Δ-sets and look at notable examples. Δ-sets are set sequences of a certain type which have an underlying combinatorial structure; they appear frequently in contexts of algebraic topology. Our central insight is that m-schemes can be characterized as Δ-sets in a natural way (see Example 4.4). The latter observation gives rise to a topological discussion of m-schemes.

Definition 4.1 (Δ-Set)**.** *A Δ-Set X consists of a sequence of sets*

$$X_0, X_1, X_2, ...$$

and (for each n) a system of maps d_i^n (often abbreviated d_i)

$$d_i^n : X_n \longrightarrow X_{n-1} \ , \quad i = 0, ..., n \ ,$$

such that the composite maps (when $n \geq 2$)

$$d_j d_i : X_n \longrightarrow X_{n-1} \longrightarrow X_{n-2}$$

satisfy the relation

$$d_j d_i = d_{i-1} d_j \ , \quad \text{if} \ \ j < i \ .$$

Note that the sequence of sets $X_0, X_1, X_2, ...$ is allowed to be both finite or infinite. For each n, we call the elements of X_n as the n-simplices of X. Moreover, we call the maps $(d_i^n)_{n,i}$ as the structure maps of X.

The first example of Δ-sets we consider is the singular complex of a topological space (see below). In the following example, we use the notation introduced in Section (4.1) for the standard simplex ∇^n and the associated embeddings $\delta_0, ..., \delta_n : \nabla^n \longrightarrow \nabla^{n+1}$.

Example 4.2 (Singular Complex of a Topological Space)**.** *Let Y be a topological space. For each $k \geq 0$, let $S(Y)_k$ denote the set of all continous functions $\nabla^k \longrightarrow Y$. We define structure maps $d_0, ..., d_k : S(Y)_k \longrightarrow S(Y)_{k-1}$ as follows: Given a function*

$$f \in S(Y)_k \ , \quad f : \nabla^k \longrightarrow Y \ ,$$

we put $d_i(f) \in S(Y)_{k-1}$ as the composite map

$$f\delta_i : \quad \nabla^{k-1} \xrightarrow{\delta_i} \nabla^k \xrightarrow{f} Y \ .$$

Then the sequence of sets

$$S(Y)_0, S(Y)_1, S(Y)_2, ...$$

together with the structure maps in each dimension k,

$$d_0, ..., d_k : S(Y)_k \longrightarrow S(Y)_{k-1} \ ,$$

constitute a Δ-Set. To verify this, note that the composite maps (when $k \geq 2$)

$$d_j d_i : S(Y)_k \longrightarrow S(Y)_{k-1} \longrightarrow S(Y)_{k-2}$$

satisfy the required relation

$$d_j d_i = d_{i-1} d_j \ , \quad \text{if} \ \ j < i \ .$$

More precisely: For $f \in S(Y)_k$ and $j < i$, the identity (1) from Section (4.1) yields

$$d_j d_i(f) = d_j(f\delta_i) = f\delta_i\delta_j = f\delta_j\delta_{i-1} = d_{i-1}(f\delta_j) = d_{i-1}d_j(f) \ .$$

We denote the above Δ*-set by*

$$S(Y) := \big((S(Y)_k)_{k\geq 0},\ (d_i^k)_{k\geq 0,\ 0\leq i\leq k}\big)\ .$$

We call $S(Y)$ *the singular complex of* Y*.* □

The singular complex is an important topic which we come back to at a later point in this chapter. Now, before we proceed to the characterization of m-schemes as Δ-sets, we show that the sets of tuples from the preceding chapter can also be characterized as Δ-sets. This is subject of the next example.

Example 4.3 (Sets of Tuples)**.** *We use the same terminology as in Chapter 3. Let* $V = \{v_1, v_2, ..., v_n\}$ *be an arbitrary set of* n *distinct elements. Then the sets of tuples*

$$V^{(1)}, V^{(2)}, V^{(3)}, ...$$

together with the projections at each level s*,*

$$\pi_1^s, \pi_2^s, ..., \pi_s^s : V^{(s)} \longrightarrow V^{(s-1)}$$
$$\pi_i^s : (v_1, ..., v_{i-1}, v_i, v_{i+1}, ..., v_s) \longrightarrow (v_1, ..., v_{i-1}, v_{i+1}, ..., v_s)$$

constitute a Δ*-set. To verify this, note that the composite maps (when* $s \geq 3$*)*

$$\pi_j\pi_i : V^{(s)} \longrightarrow V^{(s-1)} \longrightarrow V^{(s-2)}$$

satisfy the relation

$$\pi_j\pi_i = \pi_{i-1}\pi_j\ , \quad \textit{if}\ \ j < i\ ,$$

where the level indices have been omitted. Notice that an index shift naturally occurs in the definition of this Δ*-set, as the* 0*-simplices are actually the elements of* $V^{(1)}$*, the* 1*-simplices are actually the elements of* $V^{(2)}$*, etc. We have to keep this in mind for future applications.* □

In the next example, we show that m-schemes can be regarded as Δ-sets in a natural way. The main idea is to regard the colors of an m-scheme at level $(n+1)$ as n-simplices. The characterization of m-schemes as Δ-sets will help us draw new insights into the algebraic properties and the geometry of m-schemes.

Example 4.4 (m-Schemes)**.** *If* $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m\}$ *is an* m*-scheme on* V*, then*

$$\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m$$

together with the maps $\overline{\pi_1^s}, \overline{\pi_2^s}..., \overline{\pi_s^s}$ *at each level* s*,*

$$\begin{aligned} \overline{\pi_1^s}, \overline{\pi_2^s}, ..., \overline{\pi_s^s} : \mathcal{P}_s &\longrightarrow \mathcal{P}_{s-1} \\ \overline{\pi_i^s} : P &\longrightarrow \pi_i^s(P) \end{aligned}$$

constitute a Δ*-set; this follows from Example 4.3 and the* m*-scheme axioms. We denote the above* Δ*-set also by* Π*,*

$$\Pi = \big((\mathcal{P}_s)_s, (\ \overline{\pi_i^s}\ )_{s,i}\big)\ .$$

As in the preceding example, notice that an index shift naturally occurs in the definition of this Δ*-set, as the* 0*-simplices are actually the elements of* $\mathcal{P}_1$*, the* 1*-simplices are actually the elements of* $\mathcal{P}_2$*, etc. We have to keep this in mind for future applications.* □

In the following sections, we discuss how the above characterization of m-schemes as Δ-sets will benefit us in obtaining a geometric picture of m-schemes, and further, how this enables us to study their combinatorial properties through methods of algebraic topology.

4.3 Geometric Realization

In this section, we discuss the *geometric realization* of a Δ-set $X = ((X_i)_i, (d_i^n)_{n,i})$, denoted $Real(X)$. The geometric realization $Real(X)$ is a topological space which describes the set-theoretic structure of X in simple geometric terms. It provides us with an intuitive picture of the combinatorial data of Δ-sets.

Formally, $Real(X)$ is defined as a quotient space of the disjoint union

$$\dot{\cup}_n\ X_n \times \nabla^n\ ,$$

which one might think of as a disjoint union of standard simplices ∇^n indexed by the simplices of X. We impose an equivalence relation " $\sim$ " on this disjoint union

as follows: For all n and for each point

$$(x,t) \in X_n \times \nabla^{n-1} \ ,$$

we identify the point

$$\ni (d_i(x),t) \in X_{n-1} \times \nabla^{n-1} \quad \text{with} \quad (x,\delta_i(t)) \in X_n \times \nabla^n \ .$$

Now the geometric realization $Real(X)$ of the Δ-set X is defined as

$$Real(X) := \dot{\cup}_n \ X_n \times \nabla^n \ / \ \sim \ .$$

From this definition, we see that each n-simplex $x \in X_n$ corresponds to exactly one standard n-simplex ∇^n in $Real(X)$. Moreover, the i-th face of the standard n-simplex corresponding to x is identified with the standard $(n-1)$-simplex corresponding to $d_i^n(x)$. This is the core idea of geometric realization: Each n-simplex $x \in X_n$ is interpreted as a standard n-simplex ∇^n, and the $(n-1)$-simplices $d_0(x), ..., d_n(x) \in X_{n-1}$ are interpreted as the faces of x.

The construction of $Real(X)$ constitutes the starting point for considerations of algebraic-topological nature; it puts the combinatorial information of X in a topological context. As a space, the geometric realization $Real(X)$ has very pleasant properties: It can be classified as a *CW-complex*, which means it has a well-understood and easy-to-work-with topological structure (see [15], [27]). In the following, we discuss how the concept of geometric realization applies to the study of m-schemes.

For this purpose, let $V = \{v_1, v_2, ..., v_n\}$ be an arbitrary set of n distinct elements and let $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m\}$ be an m-scheme on V. Let $X = \big((V^{(s)})_{1 \le s \le m}, (\pi_i^s)_{s,i}\big)$ be the Δ-set from Example 4.3 (the sets of tuples), "cut off" at level m. Taking into account the index shift that naturally occurs in the definition of this Δ-set, the geometric realization of X is

$$Real(X) = \dot{\cup}_s \ V^{(s+1)} \times \nabla^s \ / \ \sim \ ,$$

where " $\sim$ " denotes the equivalence relation defined above. We want to color the space $Real(X)$ according to the information given by the m-scheme Π; we use the fact that every point in $Real(X)$ has a unique representative

$$(\bar{u},t) \in V^{(s+1)} \times \nabla^s$$

such that s is minimal (see [27]). The coloring is defined as follows: If the point $x \in \mathit{Real}(X)$ is minimally represented by $(\bar{u}, t) \in V^{s+1} \times \nabla^s$, we say that x *has color* $P \in \mathcal{P}_{s+1}$ if $\bar{u} \in P$. That way, the partitions $\mathcal{P}_s$ of $V^{(s)}$ $(1 \leq s \leq m)$ which color the tuples naturally induce a coloring on the interlaced standard simplices in $\mathit{Real}(X)$. The space $\mathit{Real}(X)$ together with the coloring induced by Π we call the *color complex associated with* Π.

One might think of the color complex associated with Π as a higher-dimensional analog of a graph, colored according to the combinatorial information of the m-scheme Π. Importantly, the color complex contains *all* the combinatorial information that Π contains, but in addition, it allows us to use topological tools to study the underlying m-scheme invariants like regularity or matchings. Note that the above idea of translating combinatorial data into topological cell complexes is not new; in fact, it has been used extensively in recent years and has led to a number of important advances for combinatorial problems (see [18], [20]). Most prominently, this approach has led to a proof of the Kneser Conjecture by L. Lovász (see [19]). The search for cell complexes that describe certain combinatorial problems constitutes a central method in combinatorial algebraic topology.

Regarding the above definition, an interesting question is how the color complex associated with Π relates to the geometric realization $\mathit{Real}(\Pi)$ of the m-scheme Π regarded as a Δ-set. In comparison, the space $\mathit{Real}(\Pi)$ seems to "lack" the information of the subdegrees of the colors of Π. An interesting observation is that $\mathit{Real}(\Pi)$ is indeed a quotient space of the color complex associated with Π: If we canonically identify standard simplices of the same color in the color complex, we obtain $\mathit{Real}(\Pi)$. To shorten the discussion, we will not specify the exact procedure at this point; instead we leave the details as an exercise to the reader.

To give an example of how topological methods can be used in the study of Δ-sets, we introduce the notion of homology in the following section. Especially, we discuss how the concept of homology applies to the Δ-sets introduced in Section (4.2). Our hope is that through the use of topological methods like homology, we will gain new insights into m-scheme properties that interest us in the context of polynomial factoring (see Chapter 5).

4.4 Homology Groups

For the following paragraph, let us fix some notation. If A is an abelian group and M is some arbitrary set, then we denote by $A[M]$ the free abelian group with basis M and coefficient group A. Namely, $A[M]$ is the abelian group whose elements consist of the formal finite sums

$$a_1x_1 + ... + a_kx_k \ , \quad a_i \in A \ , \quad x_i \in M \ ,$$

modulo the following equivalence relation:

(i) For each $a, a' \in A$ and $x \in M$, we identify $ax + a'x$ with $(a + a')x$,

(ii) For all $x \in M$, we identify the element $0 \cdot x$ with 0.

In the case of a Δ-set $X = ((X_i)_i, (d_i^n)_{i,n})$, applying the free abelian group construction to each of the sets $X_0, X_1, X_2, ...$, we obtain a sequence of abelian groups:

$$A[X_0], A[X_1], A[X_2], ...$$

In this situation, each of the maps $d_i : X_n \longrightarrow X_{n-1}$ induces a group homomorphism

$$\begin{aligned} A[X_n] &\longrightarrow A[X_{n-1}] \\ a_1x_1 + ... + a_kx_k &\longrightarrow a_1d_i(x_1) + ... + a_kd_i(x_k) \end{aligned}$$

which we also denote by d_i in the following. We define by

$$d^n := \sum_{i=0}^{n} (-1)^i d_i : A[X_n] \longrightarrow A[X_{n-1}]$$

the *n-th boundary operator* d^n of X over A (often abbreviated d).

The boundary operator has a very interesting and important property (see [27]):

Lemma 4.5. *In the above situation, for all n, the composition map $d^n d^{n+1}$ equals the trivial homomorphism. In other words: For all $n \geq 1$, we have*

$$Im(d^{n+1}) \subset Ker(d^n) \ .$$

Proof. We use the fact that $d_j d_i = d_{i-1} d_j$ for $j < i$. Evidently,

$$\begin{aligned} d^n d^{n+1} &= \sum_{j=0}^{n} (-1)^j d_j^n \sum_{i=0}^{n+1} (-1)^i d_i^n \\ &= \sum_{i,j} (-1)^{i+j} d_j d_i \\ &= \sum_{j \geq i} (-1)^{i+j} d_j d_i \; + \; \sum_{j<i} (-1)^{i+j} d_j d_i \\ &= \sum_{j \geq i} (-1)^{i+j} d_j d_i \; + \; \sum_{j<i} (-1)^{i+j} d_{i-1} d_j \; , \end{aligned}$$

where the above sums cancel each other. The assertion follows. □

Note that in the above lemma, $Im(d^{n+1})$ and $Ker(d^n)$ are both normal subgroups of $A[X_n]$. Therefore the above property of the boundary operator intuitively gives rise to the notion of *homology groups*:

Definition 4.6 (Homology Groups)**.** *Let $X = ((X_i)_i, (d_i^n)_{i,n})$ be a Δ-set. Let d^n denote the n-th boundary operator. We call the quotient group*

$$H_n(X, A) := Ker(d^n)/Im(d^{n+1}) \; .$$

the n-th homology group of X over the coefficient group A.

In algebraic topology, $A = \mathbb{Z}$ is an important special case for the coefficient group; we will restrict ourselves to this case in the following. Another important special case occurs if A is a field; in this case, the homology groups can be considered as vector spaces over A. The latter possibility will not play a role in the present discussion.

In the following, we discuss the importance of the notion of homology groups using the classic example of the singular complex of a topological space.

Example 4.7 (Singular Homology)**.** *Let Y be a topological space and let*

$$S(Y) := \big((S(Y)_k)_k, \; (d_i^k)_{k,i}\big)$$

be the singular complex of Y as defined in Example 4.2. Since $S(Y)$ can be characterized as a Δ-set, we may define the homology groups $H_n(S(Y), \mathbb{Z})$ $(n \geq 1)$ of $S(Y)$ following the procedure described above. In algebraic topology, the homology

groups $H_n(S(Y), \mathbb{Z})$ are called the singular homology groups of Y, and often they are denoted simply by $H_n(Y, \mathbb{Z})$. Singular homology is one of the major tools for classifying topological spaces, because two topological spaces Y, Y' having different singular homology groups cannot be topologically equivalent, and indeed cannot even have the same homotopy type (see [15], Cor. 2.11).

The original idea behind the definition of the singular homology groups $H_n(Y, \mathbb{Z})$ is the observation that a major invariant of a topological space are its holes. But because holes are not part of the topological space itself, the problem of defining holes and distinguishing between different kinds of holes (especially in terms of dimension) is nontrivial. The notion of singular homology offers a solution to this problem: It gives us a formal method for detecting and categorizing holes, which helps us to differentiate between topological spaces (see [15], Ch. 2, "The Idea of Homology"). □

In the following, we consider how the concept of homology applies to the sets of tuples (see Example 4.3), the Δ-set from which we constructed the color complex in the previous section. The theorem below specifies our intuition that the color complex of an m-scheme does not "contain any holes".

Lemma 4.8. *Let $V = \{v_1, v_2, ..., v_n\}$ be an arbitrary set of n distinct elements and let $X = \left((V^{(s)})_s, (\pi_i^s)_{s,i}\right)$ be the Δ-set from Example 4.3 (the sets of tuples). Then for all k, we have*

$$H_k(X, \mathbb{Z}) = 0 \ ,$$

where 0 denotes the trivial group. Especially, the sequence

$$\cdots \longrightarrow \mathbb{Z}\left[V^{(k)}\right] \xrightarrow{d} \mathbb{Z}\left[V^{(k-1)}\right] \xrightarrow{d} \mathbb{Z}\left[V^{(k-2)}\right] \longrightarrow \cdots \longrightarrow \mathbb{Z}\left[V^{(1)}\right]$$

is exact.

Proof. By [18], Th. 3.26, the homology groups $H_k(X, \mathbb{Z})$ and the singular homology groups $H_k(Real(X), \mathbb{Z})$ are isomorphic for each k. Thus, it suffices to show that

$$H_k(Real(X), \mathbb{Z}) = \{*\}$$

for all k. But $Real(X)$ is k-connected for every $k \geq 0$ (see [20], Prop. 4.4.2), so the assertion follows from [20], Th. 4.4.1. □

For an m-scheme $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m\}$ on a set $V = \{v_1, v_2, ..., v_n\}$ of n distinct elements, we do not know an equally general homology result at the moment. It is not clear which restrictions one can impose on the homology groups by the properties of the m-scheme, although it seems that most of the examples of m-schemes one might think of have geometric realizations which are k-connected for all $1 \leq k < m$ (in the sense of [20], Def. 4.3.1). Finding a theoretical foundation for the homology of m-schemes will be an important topic for further research.

Many more concepts could be discussed in the realm of combinatorial algebraic topology, but for now, we shall terminate our topological survey of m-schemes. If the reader is interested in learning more about (combinatorial) algebraic topology, she is referred to the standard texts [18], [20]. In the following (final) chapter, we discuss the application of m-scheme theory in polynomial factoring over finite fields.

5 Factoring Polynomials over Finite Fields

In this chapter, we discuss a new GRH-based algorithm for the factorization of polynomials over finite fields, suggested recently by Ivanyos, Karpinski and Saxena (see [16]). This new algorithm (called *IKS-algorithm* in the following) makes use of the theory of m-schemes, and it is known to have deterministic polynomial running time in the factorization of polynomials of prime degree p, where $(p-1)$ is a constant-smooth number. There is hope that the IKS-algorithm also factors arbitrary polynomials efficiently - and as we will see, this result would be implied by the Schemes Conjecture (see Chapter 3).

Note that the discussion below does not include a full introduction to polynomial factoring; for this purpose, the reader is referred to classical texts on the subject such as [2] and [30]. In the following, we discuss only the theory that is relevant for the understanding of the IKS-algorithm.

5.1 Algebraic Prerequisites

In this section, we introduce the necessary algebra for our study of the IKS-algorithm. The paper [16] will serve as our main reference. We start by recapitulating some fundamental concepts of polynomial factoring over finite fields:

Natural Associated Algebra $\mathcal{A}$: In order to solve polynomial factoring over finite fields (FPFF), it is enough to factor polynomials $f(x)$ of degree n over $\mathbb{F}_p$ that have n distinct roots $\alpha_1, ..., \alpha_n$ in $\mathbb{F}_p$ (see [2], [30]). Given such a polynomial $f(x)$, for any field extension $k \supseteq \mathbb{F}_p$, we have the *natural associated algebra*

$$\mathcal{A} := k[x]/(f(x)) \ .$$

In the following, we interpret $\mathcal{A}$ as the algebra of all functions

$$V =: \{\alpha_1, ..., \alpha_n\} \longrightarrow k \ .$$

The factors of $f(x)$ appear as zero divisors in $\mathcal{A}$: Assume $y(x)z(x) = 0$ for some nonzero polynomials $y(x), z(x) \in \mathcal{A}$. Then $f(x)|y(x) \cdot z(x)$, which implies $\gcd(f(x), z(x))$ factors $f(x)$ nontrivially. Since the gcd of polynomials can be computed by the Euclidean Algorithm in deterministic polynomial time, factoring $f(x)$ is - up to polynomial time reductions - equivalent to finding a zero divisor in $\mathcal{A}$.

Connection with GRH: As we already mentioned, the IKS-algorithm is based on the correctness of the generalized Riemann hypothesis. The formal statement of the hypothesis follows. Recall that a *Dirichlet character* is a completely multiplicative arithmetic function $\chi : \mathbb{Z} \longrightarrow \mathbb{C}$ such that there exists a positive integer k with $\chi(n+k) = \chi(n)$ for all n and $\chi(n) = 0$ whenever $\gcd(n,k) > 1$. If such a character is given, we define the corresponding *Dirichlet L-function* by

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

for every complex number s with real part > 1. By analytic continuation, this function can be extended to a meromorphic function defined on the whole complex plane. The generalized Riemann hypothesis now asserts that, for every Dirichlet character χ, the zeros of $L(\chi, s)$ in the *critical strip* $0 < \text{Re } s < 1$ all lie on the *critical line* $\text{Re } s = 1/2$.

Under the assumption of GRH, Rónyai showed in [24] that the knowledge of any explicit nontrivial automorphism $\sigma \in \text{Aut}(\mathcal{A})$ of the natural associated algebra $\mathcal{A}$ would immediately give us a nontrivial factor of $f(x)$. The latter result will play an important role in the routine of the IKS-algorithm (see Section 5.2).

Ideals of $\mathcal{A}$ and roots of $f(x)$: For an ideal I of $\mathcal{A}$, we define the *support* of I as

$$Supp(I) := V \setminus \{v \in V \mid a(v) = 0 \text{ for every } a \in I\} .$$

Via the support, ideal decompositions of $\mathcal{A}$ induce partitions on the set V. This is formulated in the following lemma:

Lemma 5.1. *If $I_1, ..., I_t$ are pairwise orthogonal ideals of $\mathcal{A}$ (i.e. $I_i I_j = 0$ for all $i \neq j$) such that $\mathcal{A} = I_1 + \cdots + I_t$, then*

$$V = Supp(I_1) \sqcup \cdots \sqcup Supp(I_t) .$$

Tensor powers of $\mathcal{A}$: For $1 \leq m \leq n$, we denote by $\mathcal{A}^{\otimes m}$ the m-th tensor power of $\mathcal{A}$. We may regard $\mathcal{A}^{\otimes m}$ as the algebra of all functions from V^m to k; in this interpretation, the rank one tensor element $h_1 \otimes \cdots \otimes h_m$ corresponds to a function that maps $(v_1, ..., v_m) \longrightarrow h_1(v_1) \cdots h_m(v_m)$.

Essential part of tensor powers: We define the *essential part* $\mathcal{A}^{(m)}$ of $\mathcal{A}^{\otimes m}$ to be the (unique) ideal of $\mathcal{A}^{\otimes m}$ consisting of the functions which vanish on all the m-tuples $(v_1, ..., v_m) \in V^m$ with $v_i = v_j$ for some $i \neq j$. Functionally interpreted, $\mathcal{A}^{(m)}$ is the algebra consisting of all functions $V^{(m)} \longrightarrow k$.

Ideals of $\mathcal{A}^{(m)}$ and roots of $f(x)$: Like in the case $m = 1$, we define the *support* of an ideal I of $\mathcal{A}^{(m)}$ as

$$Supp(I) := V^{(m)} \setminus \{\bar{v} \in V^{(m)} \,|\, a(\bar{v}) = 0 \ \text{ for every } a \in I\} \ .$$

Using this convention, Lemma 5.1 can be generalized as follows:

Lemma 5.2. *For $s \leq n$, if $I_{s,1}, ..., I_{s,t_s}$ are pairwise orthogonal ideals of $\mathcal{A}^{(s)}$ such that $\mathcal{A}^{(s)} = I_{s,1} + \cdots + I_{s,t_s}$, then*

$$V^{(s)} = Supp(I_{s,1}) \sqcup \cdots \sqcup Supp(I_{s,t_s}) \ .$$

This completes our discussion of the algebraic prerequisites. In the following sections, we give a description of the routine of the IKS-algorithm and discuss bounds for its running time.

Before we proceed, let me say one or two words about the current state of polynomial factoring over finite fields. As it has already been mentioned, we know that under GRH, the IKS-algorithm has deterministic polynomial running time in the factorization of polynomials of prime degree p, where $(p-1)$ is a constant-smooth number (see [16], Sec. 5). This result constitutes a novelty, because previous effort have yielded only polynomial-time randomized algorithms or polynomial-time deterministic algorithms for a less general class of polynomials than considered by the IKS-algorithm.

In practice, the most commonly used polynomial-time randomized algorithms for polynomial factoring are Berlekamp's algorithm and the Cantor-Zassenhaus algorithm (see [2], [5]). Regarding deterministic algorithms for a special class of polynomials, the work of Rónyai should be mentioned (see [24]), whose ideas have originated the line of research from which the IKS-algorithm sprouted.

5.2 Description of the IKS-Algorithm

In this section, we outline the routine of the IKS-Algorithm. We discuss how to compute the essential parts $\mathcal{A}^{(s)}$ $(1 \leq s \leq n)$ efficiently and how an m-scheme can be obtained from the ideal decompositions of these algebras. In the subsequent sections, we will show how to use this knowledge in the context of polynomial factoring over finite fields.

In the following, let $f(x)$ be a polynomial of degree n over $\mathbb{F}_p$ having n distinct roots $V = \{\alpha_1, ..., \alpha_n\}$ in $\mathbb{F}_p$. For some field extension $k \supseteq \mathbb{F}_p$, let $\mathcal{A} := k[x]/(f(x))$ be the natural associated algebra. With regards to the algorithm, we assume $\mathcal{A}$ is given by structure constants with respect to some basis $b_1, ..., b_n$.

The first thing we show is that the essential parts $\mathcal{A}^{(s)}$ $(1 \leq s \leq n)$ can be computed efficiently. This is subject of the next lemma (see [16], Sec. 3).

Lemma 5.3. *A basis for $\mathcal{A}^{(m)} = (k[X]/(f(X)))^{(m)}$ over $k \supseteq \mathbb{F}_p$ can be computed by a deterministic algorithm in time poly$(\log |k|, n^m)$.*

Proof. To see this, we define embeddings μ_i $(1 \leq i \leq m)$ of $\mathcal{A}$ into $\mathcal{A}^{\otimes m}$ as follows:

$$\mu_i : \mathcal{A} \longrightarrow \mathcal{A}^{\otimes m} \ , \quad a \longrightarrow \ 1 \otimes \cdots \otimes 1 \otimes \underset{\substack{\uparrow \\ i\text{-th factor}}}{a} \otimes 1 \otimes \cdots \otimes 1 \ .$$

In the functional interpretation, $\mu_i(\mathcal{A})$ corresponds to those functions on $V^{(m)}$ which depend only on the i-th coordinate of the tuples. For $1 \leq i < j \leq m$, we define

$$\Delta_{i,j}^m := \{b \in \mathcal{A}^{\otimes m} \,|\, (\mu_i(a) - \mu_j(a))b = 0 \ \text{ for every } a \in \mathcal{A}\} \ .$$

Observe that $\Delta_{i,j}^m$ is the ideal of $\mathcal{A}^{\otimes m}$ consisting of the functions which are zero on every tuple $(v_1, v_2, ..., v_m) \in V^m$ with $v_i \neq v_j$. A basis for $\Delta_{i,j}^m$ can be computed by solving a system of linear equations in time polynomial in the dimension of $\mathcal{A}^{\otimes m}$ over k (which is n^m). Since $\mathcal{A}^{(m)}$ is just the annihilating ideal of $\sum_{1 \leq i < j \leq m} \Delta_{i,j}^m$,

$$\mathcal{A}^{(m)} = \{c \in \mathcal{A}^{\otimes m} \,|\, bc = 0 \ \text{ for every } b \in \textstyle\sum_{1 \leq i < j \leq m} \Delta_{i,j}^m\} \ ,$$

we can compute $\mathcal{A}^{(m)}$ in $poly(n^m)$ field operations. The assertion follows. □

We will now proceed to give an overview of the routine of the IKS-algorithm. For referential purposes, let us quickly recapitulate the algorithmic data:

Input: A degree n polynomial $f(x)$ having n distinct roots $V = \{\alpha_1, ..., \alpha_n\}$ in $\mathbb{F}_p$.

Given $1 < m \leq n$, we can wlog assume that we also have the smallest field extension $k \supseteq \mathbb{F}_p$ having s-th nonresidues for all $1 \leq s \leq m$ (computing k will take $poly(\log p, m^m)$ time under GRH).

Output: A nontrivial factor of $f(x)$ or a homogeneous, antisymmetric m-scheme on $V = \{\alpha_1, ..., \alpha_n\}$.

Description of the Algorithm: We define $\mathcal{A}^{(1)} = \mathcal{A} = k[x]/(f(x))$ and compute the essential parts $\mathcal{A}^{(s)}$ $(1 < s \leq m)$ of the tensor powers of $\mathcal{A}$; this takes $poly(\log p, n^m)$ time by Lemma 5.3.

Automorphisms and Ideal Decompositions of $\mathcal{A}^{(s)}$ $(1 < s \leq m)$: Observe that for each $\tau \in Symm_s$, the map defined by

$$\tau : \mathcal{A}^{(s)} \longrightarrow \mathcal{A}^{(s)} \ , \quad (b_{i_1} \otimes \cdots \otimes b_{i_s})^{\tau} \longrightarrow b_{i_{1^\tau}} \otimes \cdots \otimes b_{i_{s^\tau}}$$

is an algebra automorphism of $\mathcal{A}^{(s)}$. By [24], this knowledge of explicit automorphisms of $\mathcal{A}^{(s)}$ can be used to efficiently decompose $\mathcal{A}^{(s)}$ under GRH: Namely, one can compute mutually orthogonal ideals $I_{s,1}, ..., I_{s,t_s}$ $(t_s \geq 2)$ of $\mathcal{A}^{(s)}$ such that

$$\mathcal{A}^{(s)} = I_{s,1} + \cdots + I_{s,t_s} \ .$$

By Lemma 5.2, the above decomposition induces a partition $\mathcal{P}_s$ on the set V:

$$\mathcal{P}_s : \quad V^{(s)} = Supp(I_{s,1}) \sqcup \cdots \sqcup Supp(I_{s,t_s}) \ .$$

Thus, together with $\mathcal{P}_1 := \{V\}$, we have an m-collection $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m\}$ on V.

Algebra Embeddings $\mathcal{A}^{(s-1)} \longrightarrow \mathcal{A}^{(s)}$: For $1 < s \leq m$, consider the s embeddings $\iota_j^s : \mathcal{A}^{\otimes(s-1)} \longrightarrow \mathcal{A}^{\otimes s}$ mapping $b_{i_1} \otimes \cdots \otimes b_{i_{s-1}}$ to $b_{i_1} \otimes \cdots \otimes b_{i_{j-1}} \otimes 1 \otimes b_{i_j} \otimes \cdots \otimes b_{i_{s-1}}$. By restricting ι_j^s to $\mathcal{A}^{(s-1)}$ and multiplying its image by the identity element of $\mathcal{A}^{(s)}$, we obtain algebra embeddings $\mathcal{A}^{(s-1)} \longrightarrow \mathcal{A}^{(s)}$ denoted also by $\iota_1^s, ..., \iota_s^s$. In the following, we interpret $\iota_j^s(\mathcal{A}^{(s-1)})$ as the set of functions $V^{(s)} \longrightarrow k$ which do not depend on the j-th coordinate.

The algorithm is now best described through the following refinement procedures:

R1 (Compatibility): If for any $1 < s \leq m$, for any pair of ideals $I_{s-1,i}$ and $I_{s,i'}$ in the decomposition of $\mathcal{A}^{(s-1)}$ and $\mathcal{A}^{(s)}$ respectively, and for any $j \in \{1, ..., s\}$, the ideal $\iota_j^s(I_{s-1,i})I_{s,i'}$ is neither zero nor $I_{s,i'}$, then we can efficiently compute a subideal of $I_{s,i'}$ and thus, refine $I_{s,i'}$ and the m-collection Π.

Note that R1 fails to refine Π *only when* Π *is a compatible collection.*

R2 (Regularity): If for any $1 < s \leq m$, for any pair of ideals $I_{s-1,i}$ and $I_{s,i'}$ in the decomposition of $\mathcal{A}^{(s-1)}$ and $\mathcal{A}^{(s)}$ respectively, and for any $j \in \{1, ..., s\}$, $\iota_j^s(I_{s-1,i})I_{s,i'}$ is not a free module over $\iota_j^s(I_{s-1,i})$, then by trying to find a free basis, we can efficiently compute a zero divisor in $I_{s-1,i}$ and thus, refine $I_{s-1,i}$ and the m-collection Π.

Note that R2 fails to refine Π *only when* Π *is a regular collection.*

R3 (Invariance): If for some $1 < s \leq m$ and some $\tau \in Symm_s$ the decomposition of $\mathcal{A}^{(s)}$ is not τ-invariant, then we can find two ideals $I_{s,i}$ and $I_{s,i'}$ such that $I_{s,i}^{\tau}I_{s,i'}$ is neither zero nor $I_{s,i'}$; hence, we can efficiently refine $I_{s,i'}$ and the m-collection Π.

Note that R3 fails to refine Π *only when* Π *is an invariant collection.*

R4 (Antisymmetry): If for some $1 < s \leq m$, for some ideal $I_{s,i}$ and for some $\tau \in Symm_s \setminus \{id\}$, we have $I_{s,i}^{\tau} = I_{s,i}$, then τ is an algebra automorphism of $I_{s,i}$. By [24], this means we can find a subideal of $I_{s,i}$ efficiently under GRH and hence, refine $I_{s,i}$ and the m-collection Π.

Note that R4 fails to refine Π *only when* Π *is an antisymmetric collection.*

R5 (Homogeneity): If the algebra $\mathcal{A}^{(1)} = \mathcal{A}$ is in a known decomposed form, then we can trivially find a nontrivial factor of $f(x)$ from that decomposition.

Note that R5 fails to refine Π *only when* Π *is a homogeneous collection.*

Summary: The algorithm executes the ideal operations R1-R5 described above on $\mathcal{A}^{(s)}$ $(1 \leq s \leq m)$ until either we get a nontrivial factor of $f(x)$ or the underlying m-collection Π becomes a homogeneous, antisymmetric m-scheme on V. It is routine to verify that the time complexity of the IKS-algorithm is $poly(\log p, n^m)$.

5.3 From m-Schemes to Factoring

In the following, we explain how to deal with the "bad case" of the IKS-algorithm, when we get a homogeneous, antisymmetric m-scheme instead of a nontrivial factor. As it turns out, factorization can be forced even in this case by augmenting m to a larger value in the algorithm - but this might come at the cost of efficiency.

The next theorem is of much importance (see [16], Th. 7).

Theorem 5.4. *Let $f(x)$ be a polynomial of degree n over $\mathbb{F}_p$ having n distinct roots $V = \{\alpha_1, ..., \alpha_n\}$ in $\mathbb{F}_p$. Assuming GRH, we either find a nontrivial factor of $f(x)$ or we construct a homogeneous, antisymmetric m-scheme on V having no matchings, deterministically in time poly$(\log p, n^m)$.*

Proof. We apply the algorithm from Section (5.2); suppose it yields a homogeneous, antisymmetric m-scheme $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m\}$ on V. For the sake of contradiction, assume that some color $P \in \mathcal{P}_s$ is a matching: Let $1 \leq i < j \leq s$ such that $\pi_i^s(P) = \pi_j^s(P)$ and $|\pi_i^s(P)| = |P|$. Then $\pi_i^s(\pi_j^s)^{-1}$ is a nontrivial permutation of $\pi_j^s(P)$. For the corresponding orthogonal ideals decomposition of $\mathcal{A}^{(1)}, ..., \mathcal{A}^{(m)}$, this means that the embeddings ι_i^s and ι_j^s both give isomorphisms $I_{s-1,l'} \longrightarrow I_{s,l}$, where the ideals $I_{s-1,l'}$ and $I_{s,l}$ correspond to $\pi_j^s(P)$ and P, respectively. Hence, the map $(\iota_i^s)^{-1}\iota_j^s$ is a nontrivial automorphism of $I_{s-1,l'}$. By [24], this means we can find a subideal of $I_{s-1,l'}$ efficiently under GRH and thus, refine the m-scheme Π. □

Combining the above result with Lemma 3.5, we conclude that one can completely factor $f(x)$ in time *poly*$(\log p, n^{\log n})$ under GRH. Furthermore, any progress towards the Schemes Conjecture (see Chapter 3) will directly result in an improvement of the time complexity of the IKS-algorithm. Should we be able to resolve the Schemes Conjecture completely, the total time taken for the factorization of $f(x)$ would improve to *poly*$(\log p, n^c)$, where $c \geq 4$ is a constant. In the latter case, we have the first deterministic polynomial time algorithm for the factorization of polynomials over finite fields (assuming GRH).

As a special case, if $f(x)$ is a polynomial of prime degree, we can circumvent the involvement of the Schemes Conjecture and instead use the results about association schemes from Chapter 2 to show that $f(x)$ can be factored by the IKS-algorithm in polynomial time (assuming GRH). This will be discussed in the following section.

5.4 Factoring Polynomials of Prime Degree

In this section, we show that the IKS-algorithm has polynomial running time in the factorization of polynomials of prime degree n, where $(n-1)$ is a constant-smooth number. For the proof, we need Hanaki and Uno's classification results for association schemes of prime order (see Chapter 2).

The following nonexistence lemma is of much importance (taken from [16], Sec. 1).

Lemma 5.5. *Let $r > 1$ be a divisor of n. Then for $m \geq r$ there does not exist a homogeneous and antisymmetric m-scheme on n points.*

Proof. For any $m \geq r$, clearly every m-scheme contains an r-scheme. Therefore, it suffices to prove the above statement for $m = r$. Suppose for the sake of contradiction that there exists a homogeneous and antisymmetric r-scheme $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_r\}$ on $V = \{v_1, v_2, ..., v_n\}$. By definition, $\mathcal{P}_r$ partitions $n(n-1)\cdots(n-r+1)$ tuples of $V^{(r)}$ into, say t_r colors. By antisymmetricity, every such color P has $r!$ associated colors, namely $\{P^\tau \,|\, \tau \in Symm_r\}$. Moreover, by homogeneity, the size of every color at level r is divisible by n. Hence, $r!n|n(n-1)\cdots(n-r+1)$. But this implies $r!|(n-1)\cdots(n-r+1)$, which contradicts $r|n$. Therefore, Π cannot exist. □

We can now prove the main theorem of this section (see [16], Sec. 5).

Theorem 5.6. *If $n > 2$ is a prime, r is the largest prime factor of $(n-1)$ and $f(x)$ is a polynomial of degree n over $\mathbb{F}_p$, then we can find a nontrivial factor of $f(x)$ deterministically in time poly$(\log p, n^r)$ under GRH.*

Proof. It suffices to consider the case that $f(x)$ has n distinct roots $V = \{\alpha_1, ..., \alpha_n\}$ in $\mathbb{F}_p$. We apply the algorithm from Section (5.2); suppose it yields a homogeneous, antisymmetric $(r+1)$-scheme $\{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_{r+1}\}$ on V. As in Section (3.2), we will regard $\{\mathcal{P}_1, \mathcal{P}_2 \cup \{1\}\}$ as an association scheme, where 1 denotes the trivial relation. Since $\{\mathcal{P}_1, \mathcal{P}_2 \cup \{1\}\}$ is an association scheme of prime order, there exists $d|(n-1)$ such that $|P| = dn$ for all $P \in \mathcal{P}_2$ (see Theorem 2.28). We distinguish between the following two cases:

<u>*First Case : $d = 1$.*</u> Evidently, if $d = 1$, then every color in $\mathcal{P}_2$ has subdegree 1; in particular, $\mathcal{P}_2$ contains a matching. By the proof of Theorem 5.4, this gives us a nontrivial factor of $f(x)$ in a total time of *poly*$(\log p, n^r)$.

Second Case : $d > 1$. If $d > 1$, then the colors in $\{\mathcal{P}_2, ..., \mathcal{P}_{r+1}\}$ can be used to define a homogeneous, antisymmetric r-scheme on d points as follows: Pick $P_0 \in \mathcal{P}_2$ and define $V' := \{\alpha \in V \,|\, (\alpha_1, \alpha) \in P_0\}$. Furthermore, define an r-collection $\Pi' = \{\mathcal{P}'_1, ..., \mathcal{P}'_r\}$ on V' such that for all $1 \leq s \leq r$ and for each color $P \in \mathcal{P}_{i+1}$, we put a color $P' \in \mathcal{P}'_i$ such that

$$P' := \{\bar{v} \in V'^{(i)} \,|\, (\alpha_1, \bar{v}) \in P\} \ .$$

Then $|V'| = d$, and $\Pi' = \{\mathcal{P}'_1, ..., \mathcal{P}'_r\}$ is a homogeneous, antisymmetric r-scheme on d points. But d has a prime divisor which is at most r; therefore, such a Π' cannot exist by Lemma 5.5.

We conclude that the second case cannot occur. The assertion follows. □

References

[1] R. Bailey, Association Schemes: Designed Experiments, Algebra and Combinatorics, Cambrige University Press (2004).

[2] E. R. Berlekamp *Factoring Polynomials over Finite Fields*, Bell System Technical Journal 46 (1967), 1853-1859.

[3] S. Bosch, Algebra, Springer (2006).

[4] E. Bannai, T. Ito, Algebraic Combinatorics I: Association Schemes, Benjamin-Cummings (1984).

[5] D. G. Cantor, H. Zassenhaus, *A new Algorithm for Factoring Polynomials over Finite Fields*, Mathematics of Computation 36/154 (1981), 587-592.

[6] C. W. Curtis, I. Reiner, Representation Theory of Finite Groups and Associative Algebras, Wiley Classics Library (1988).

[7] J. S. Frame *The Double Cosets of a Finite Group*, Bulletin of the American Mathematical Society 47/6 (1941), 458-467.

[8] D. M. Goldschmidt, Lectures on Character Theory, Publish or Perish (1980).

[9] C. Godsil, G. Royle, Algebraic Graph Theory, Springer (2001).

[10] A. Hanaki, *Locality of a Modular Adjacency Algebra of an Association Scheme of Prime Power Order*, Archiv der Mathematik 79 (2002), 167-170.

[11] A. Hanaki, *Representations of Finite Association Schemes*, European Journal of Combinatorics 30 (2009), 1477-1496.

[12] A. Hanaki, E-mail Correspondence (2010).

[13] A. Hanaki, K. Uno, *Algebraic Structure of Association Schemes of Prime Order*, Journal of Algebraic Combinatorics 23/2 (2006), 189-195.

[14] A. Hanaki, K. Uno, *A Remark on our Paper: "Algebraic Structure of Association Schemes of Prime Order"*, Preprint (2007).

[15] A. Hatcher, Algebraic Topology, Cambridge University Press (2002).

[16] G. Ivanyos, M. Karpinski, N. Saxena, *Schemes for Deterministic Polynomial Factoring*, 34th International Symposium on Symbolic and Algebraic Computation (2009).

[17] J. Jacob, *Representation Theory of Association Schemes*, Fakultät für Mathematik, Informatik und Naturwissenschaften der RTWH Aachen (2004).

[18] D. Kozlov, Combinatorial Algebraic Topology, Springer (2007).

[19] L. Lovász, *Kneser's Conjecture, Chromatic Number, and Homotopy*, Journal of Combinatorial Theory Ser. A 25 (1978), 319-324.

[20] J. Matousek, Using the Borsuk-Ulam Theorem: Lectures on Topological Methods in Combinatorics and Geometry, Springer (2007).

[21] H. Matsumura, Commutative Ring Theory, Cambridge University Press (2006).

[22] G. Michler, Theory of Finite Simple Groups, Cambridge University Press (2006).

[23] H. Nagao, Y. Tsushima, Representations of Finite Groups, Academic Press (1989).

[24] L. Rónyai *Galois Groups and Factoring Polynomials over Finite Fields*, SIAM Journal on Discrete Mathematics 5/3 (1992), 345-365.

[25] H. Sachs, *Über selbstkomplementäre Graphen*, Publicationes Mathematicae Debrecen 9 (1962), 270-288.

[26] J. D. H. Smith, *Association Schemes, Superschemes, and Relations Invariant Under Permutation Groups*, European Journal of Combinatorics 15 (1994), 285-291.

[27] F. Waldhausen, Skript zur Vorlesung Algebraische Topologie, Fakultät für Mathematik der Universität Bielefeld (2002).

[28] B. Weisfeiler, *On Construction and Identification of Graphs*, Lecture Notes in Mathematics 558 (1976), 219-225.

[29] Z. X. Wan, Geometry of Matrices, World Scientific (1996).

[30] H. Zassenhaus, *On Hensel Factorization I*, Lecture Notes in Mathematics 1 (1969), 291-311.

[31] P. H. Zieschang, Theory of Association Schemes, Springer (2005).

[32] P. H. Zieschang, An Algebraic Approach to Association Schemes, Lecture Notes in Mathematics 1628 (1996).