

FernUniversität in Hagen
Fakultät für Mathematik und Informatik

Diplomarbeit

Über die Kombinatorik der
Galoiszahlen

von
Steffen Hitzemann

betreut von
Prof. Dr. Winfried Hochstättler

Karlsruhe, den 2. Oktober 2008

Erklärung

Ich versichere, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt sowie Zitate kenntlich gemacht habe.

Karlsruhe, den 2. Oktober 2008

Steffen Hitzemann

Inhaltsverzeichnis

1	Einleitung	1
2	Grundlagen	2
2.1	Endliche Körper	2
2.1.1	Ringe	2
2.1.2	Mächtigkeit endlicher Körper	6
2.1.3	Existenz und Eindeutigkeit endlicher Körper	8
2.2	Verbände	14
2.2.1	Definition von Verbänden	14
2.2.2	Eigenschaften von Verbänden	19
2.2.3	Lineare Verbände	25
3	Gauß'sche Koeffizienten und Galoiszahlen	27
3.1	Kombinatorische Definition	27
3.2	Versuch einer geometrischen Interpretation	33
4	Graphentheorie	37
4.1	Grundbegriffe der Graphentheorie	37
4.2	Matchings in bipartiten k -regulären Graphen	40
4.3	Weitere wichtige Resultate	45
4.3.1	Flüsse in Netzwerken	45
4.3.2	Satz von König	48
4.3.3	Heiratssatz von Hall	49
5	Intervallzerlegungen linearer Verbände	51
5.1	Allgemeine Sätze	51
5.2	Die Fälle $\mathcal{L}(n, GF(2))$ und $\mathcal{L}(n, GF(3))$	59
5.3	Mächtigere Körper und höhere Dimensionen	68
6	Schlusswort und Ausblick	77
A	Strukturierte Intervallzerlegungen von $\mathcal{L}(4, GF(3))$	78
B	Strukturierte Intervallzerlegungen von $\mathcal{L}(5, GF(3))$	81

Abbildungsverzeichnis

1	Hasse-Diagramm des Teilverbands von 12	22
2	Hasse-Diagramm des Verbandes (\mathbb{N}, \leq)	23
3	Hasse-Diagramm des Teilmengenverbandes von $\{1, 2, 3\}$	24
4	Hasse-Diagramm des linearen Verbandes $\mathcal{L}(3, GF(2))$	24
5	Anschauliche Vorstellung eines Graphen	37
6	Intervallzerlegungsproblem in $\mathcal{L}(3, GF(2))$	39
7	Beispiel für G und G'	43
8	Netzwerk und Fluss	46
9	Verbesserung eines Matchings durch einen augmentierenden Weg	48
10	Beispiel für die Konstruktion von U	49

Tabellenverzeichnis

1	Intervallzerlegung von $\mathcal{L}(3, GF(3))$	56
2	Intervallzerlegung von $\mathcal{L}(3, GF(2))$	62
3	Intervallzerlegung von $\mathcal{L}(4, GF(2))$	63
4	Versuch einer Intervallzerlegung von $\mathcal{L}(5, GF(2))$	65
5	Strukturierte Intervallzerlegungen von $\mathcal{L}(3, GF(3))$, S_1 bis S_3	66
6	Strukturierte Intervallzerlegungen von $\mathcal{L}(4, GF(3))$, S_1 , S_3 und S_6	67
7	Strukturierte Intervallzerlegungen von $\mathcal{L}(5, GF(3))$, S_1	68
8	Übersicht über die Existenz von Intervallzerlegungen	77

Algorithmenverzeichnis

1	Allgemeine Suche nach Intervallzerlegungen	60
2	Suche nach Intervallzerlegungen über reines Ausprobieren	70
3	Suche nach Intervallzerlegungen über Projektionen	71
4	Suche nach Intervallzerlegungen ohne Satz 5.7	72

1 Einleitung

Betrachtet man die Mächtigkeit $G_{n,q}$ des Verbandes der Unterräume eines n -dimensionalen Vektorraums über einem endlichen Körper mit q Elementen, so kommt man auf die Rekursionsformel der Galoiszahlen

$$G_{n,q} = 2G_{n-1,q} + (q^{n-1} - 1)G_{n-2,q}$$

für $n \geq 2$. Faigle [4] hat die Frage gestellt, ob sich diese Rekursionsformel für $n \geq 3$ geometrisch interpretieren lässt, d.h. ob sich ein solcher Verband, der kurz mit $\mathcal{L}(n, GF(q))$ bezeichnet wird, disjunkt in zwei Teilverbände isomorph zu $\mathcal{L}(n-1, GF(q))$ und $q^{n-1} - 1$ Teilverbände isomorph zu $\mathcal{L}(n-2, GF(q))$ zerlegen lässt. Daraus ergibt sich ein kombinatorisches Problem, das sogenannte Intervallzerlegungsproblem.

In einer vorausgehenden Arbeit [13] wurde dieses Problem unter Verwendung symmetrischer Kettenzerlegungen untersucht. Dort wurde gezeigt, dass ein spezielles Verfahren, der Algorithmus von Vogt und Voigt, eine entsprechende Intervallzerlegung von $\mathcal{L}(n, GF(2))$ mit $n \leq 4$ liefert, dies aber für $n \geq 5$ nicht kann.

In dieser Diplomarbeit wird gezeigt, dass es für $n \geq 5$ keine solche Intervallzerlegung von $\mathcal{L}(n, GF(2))$ gibt; ein Resultat, das auf Hochstättler [8] zurückgeht. Über Körpern mit mehr als zwei Elementen hat das Intervallzerlegungsproblem eine deutlich komplexere Struktur. Neben dem Beweis einiger allgemeiner Aussagen werden insbesondere Intervallzerlegungen von $\mathcal{L}(n, GF(3))$ gesucht. Das zentrale Resultat ist, dass eine Intervallzerlegung von $\mathcal{L}(5, GF(3))$ existiert.

Da Verbände über endlichen Körpern untersucht werden, sollten zunächst einige Grundlagen zu endlichen Körpern und Verbänden vorgestellt werden. Dies wird in Kapitel 2 getan.

Anschließend werden in Kapitel 3 Gauß'sche Koeffizienten und Galoiszahlen behandelt. Über die Rekursionsformel der Galoiszahlen kann dann auch das kombinatorische Problem formuliert werden, das in dieser Arbeit untersucht wird.

Um zu dieser Untersuchung voranzuschreiten, werden noch einige Resultate aus der Graphentheorie, die sich auf die Existenz von Matchings beziehen, als nützlich erachtet. Diese sind Inhalt von Kapitel 4.

Danach kann in Kapitel 5 das Intervallzerlegungsproblem genauer betrachtet werden.

2 Grundlagen

Zuerst werden endliche Körper und dann Verbände behandelt.

2.1 Endliche Körper

In diesem Abschnitt soll untersucht werden, welche endlichen Körper es gibt. Dazu wird der Weg gegangen, der auch in anderen Schriften wie [9] oder [6] zu finden ist: Zuerst werden Ringe im Allgemeinen betrachtet und Ergebnisse herausgearbeitet, die sich dann konkret auf Körper anwenden lassen. Danach wird gezeigt, dass die Mächtigkeit eines endlichen Körpers stets eine Primzahlpotenz ist und dass auch zu jeder Primzahlpotenz ein bis auf Isomorphie eindeutiger Körper existiert, dessen Mächtigkeit eben diese Primzahlpotenz ist.

Vorausgesetzt werden grundlegende Resultate der Gruppentheorie, insbesondere die über Gruppenhomomorphismen sowie endliche und zyklische Gruppen.

2.1.1 Ringe

Zuerst werden die Definitionen von Ring und Unterring rekapituliert.

Definition 2.1. Eine algebraische Struktur $(R, +, \cdot)$ heißt **Ring**, wenn R eine nichtleere Menge ist und $+$ und \cdot zwei binäre Verknüpfungen sind, sodass gilt:

1. $(R, +)$ ist eine abelsche Gruppe.
2. (R, \cdot) ist eine Halbgruppe mit neutralem Element.
3. Für alle $a, b, c \in R$ gelten die Distributivgesetze

$$\begin{aligned}a \cdot (b + c) &= a \cdot b + a \cdot c \\(a + b) \cdot c &= a \cdot c + b \cdot c\end{aligned}$$

Erfüllt R zusätzlich noch die Bedingung

4. Für alle $a, b \in R$ gilt $a \cdot b = b \cdot a$,

so heißt $(R, +, \cdot)$ **kommutativer Ring**.

Definition 2.2. Sei $(R, +, \cdot)$ ein Ring und $R' \subseteq R$. Ist $(R', +, \cdot)$ ein Ring und $1 \in R'$, so heißt R' **Unterring** von R .

Anstatt $(R, +, \cdot)$ schreibt man auch einfach R , sofern klar ist, dass der Ring und nicht die Menge R gemeint ist. Außerdem ist es üblich, das neutrale Element der Addition mit 0 und das der Multiplikation wahlweise mit 1 oder e zu bezeichnen. Für das zu einem Element $a \in R$

additiv inverse Element schreibt man $-a$, für das multiplikativ Inverse a^{-1} . Außerdem wird $b - a$ anstatt $b + (-a)$, ab anstatt $a \cdot b$, na anstatt $a + \dots + a$ (n Summanden) und a^n anstatt $a \cdot \dots \cdot a$ (n Faktoren) verwendet.

Bekannte Beispiele für Ringe sind die Restklassenringe von \mathbb{Z} modulo n . Man führt diese üblicherweise ein, indem man auf dem Ring $(\mathbb{Z}, +, \cdot)$ durch $a \equiv b \Leftrightarrow a = b \pmod{n}$, $a, b \in \mathbb{Z}$ eine Äquivalenzrelation definiert und bezüglich dieser den Quotientenring betrachtet.

Eine Verallgemeinerung dieses Vorgehens auf beliebige Ringe stellen die Ideale dar.

Definition 2.3. Sei $(R, +, \cdot)$ ein Ring. Eine Untergruppe I von $(R, +)$ heißt **Ideal** in R , wenn für alle $a \in I$ und alle $r \in R$ auch $ar, ra \in I$ gilt. Ist I ein Ideal in R , so schreibt man $I \triangleleft R$.

Beispiel 2.4. Die Ideale in \mathbb{Z} sind genau die $m\mathbb{Z}$ mit $m \in \mathbb{N}_0$.

Beweis. Trivialerweise sind $\{0\}$ und \mathbb{Z} Ideale in \mathbb{Z} . Sei nun $I \neq \{0\}$ ein Ideal in \mathbb{Z} und $0 \neq k \in I$. Da $(I, +)$ eine Gruppe ist, liegt auch $-k$ in I , sodass I mindestens eine positive Zahl enthält. Sei m die kleinste positive Zahl in I . Man zeigt nun $m\mathbb{Z} \subseteq I$ und $I \subseteq m\mathbb{Z}$:

- $m\mathbb{Z} \subseteq I$:

Da $(\mathbb{Z}, +)$ zyklisch, ist dies auch $(I, +)$ als Untergruppe von $(\mathbb{Z}, +)$, was aus der Gruppentheorie bekannt ist. Also ist $\{mn \mid n \in \mathbb{Z}\} = m\mathbb{Z} \subseteq I$.

- $I \subseteq m\mathbb{Z}$:

Sei $y \in I$. Teilt man y durch m mit Rest, so erhält man $y = xm + r$ mit $y, r \in \mathbb{Z}$ und $0 \leq r < m$. Ist $r \neq 0$, so folgt $y - xm = r \in I$. Dies ist ein Widerspruch, denn m war als kleinste positive Zahl in I angenommen. Also ist $r = 0$ und demzufolge $y \in m\mathbb{Z}$.

Insgesamt folgt $I = m\mathbb{Z}$ für ein $m \in \mathbb{N}_0$. □

Analog zur Kongruenz modulo einer natürlichen Zahl wird die Kongruenz modulo eines Ideals definiert.

Definition 2.5. Sei R ein Ring und $I \triangleleft R$. Dann heißen zwei Elemente $a, b \in R$ **kongruent modulo I** , wenn $a - b \in I$ ist. Man schreibt in diesem Fall $a \equiv b \pmod{I}$.

Es lässt sich leicht zeigen, dass dies auch eine Äquivalenzrelation auf R definiert. Die Nebenklassen bezeichne man mit

$$[r] := \{r + k \mid k \in I\}$$

für $r \in R$ und R/I sei die Menge der Nebenklassen. Definiert man Operationen $+$ und \cdot auf R/I durch

$$[a] + [b] = [a + b]$$

und

$$[a] \cdot [b] = [a \cdot b]$$

auf R/I , so sind diese wohldefiniert. Eine standardmäßige Überprüfung der Axiome aus Definition 2.1 zeigt, dass $(R/I, +, \cdot)$ damit ein Ring ist.

Definition 2.6. Sei R ein Ring und $I \triangleleft R$. Der Ring $(R/I, +, \cdot)$ wird **Restklassenring von R modulo I** genannt.

Als nächstes soll der Primring eines Ringes eingeführt werden und es wird gezeigt, dass dieser isomorph zu $\mathbb{Z}/m\mathbb{Z}$ für ein $m \in \mathbb{N}_0$ ist. Dazu werden zunächst Ringhomomorphismen benötigt.

Definition 2.7. Seien R, R' Ringe. Eine Abbildung $\phi : R \rightarrow R'$ heißt ein **Ringhomomorphismus**, wenn für alle $a, b \in R$ gilt:

1. $\phi(a + b) = \phi(a) + \phi(b)$,
2. $\phi(ab) = \phi(a)\phi(b)$,
3. $\phi(1) = 1$.

Ist ϕ bijektiv, so heißt ϕ **Ringisomorphismus**. Existiert ein Ringisomorphismus $\phi : R \rightarrow R'$, so bezeichnet man R und R' als **isomorph** und schreibt $R \cong R'$.

Definition 2.8. Seien R, R' Ringe und $\phi : R \rightarrow R'$ ein Ringhomomorphismus. Dann ist das **Bild** von ϕ als

$$\text{Bild}(\phi) := \{r' \in R' \mid \exists r \in R : \phi(r) = r'\}$$

und der **Kern** von ϕ als

$$\text{Kern}(\phi) := \{r \in R \mid \phi(r) = 0\}$$

definiert.

Bild und Kern eines Ringhomomorphismus erfüllen bestimmte algebraische Eigenschaften, wie die folgende Proposition zeigt.

Proposition 2.9. *Seien R, R' Ringe und $\phi : R \rightarrow R'$ ein Ringhomomorphismus. Dann ist $\text{Bild}(\phi)$ ein Unterring von R' und $\text{Kern}(\phi)$ ein Ideal in R .*

Beweis. Es werden beide Aussagen gezeigt:

- **Bild(ϕ) ist ein Unterring von R' :**

Aus der Gruppentheorie ist bekannt, dass $(\text{Kern}(\phi), +)$ eine Untergruppe von $(R, +)$ und $(\text{Bild}(\phi), +)$ eine Untergruppe von $(R', +)$ ist.

Da R' ein Ring ist, ist $(R', +)$ abelsch, und damit ist auch die Untergruppe $(\text{Bild}(\phi), +)$ von $(R', +)$ abelsch. Seien nun $a', b' \in \text{Bild}(\phi)$, d.h. es gibt $a, b \in R$ mit $a' = \phi(a)$ und $b' = \phi(b)$. Dann folgt

$$a'b' = \phi(a)\phi(b) = \phi(ab) \in \text{Bild}(\phi),$$

also ist $\text{Bild}(\phi)$ bezüglich der Multiplikation abgeschlossen. Da das Assoziativgesetz der Multiplikation in R' gilt, gilt es insbesondere auch in $\text{Bild}(\phi)$, womit $(\text{Bild}(\phi), \cdot)$ ein Halbgruppe ist. Außerdem ist $\phi(1) = 1 \in \text{Bild}(\phi)$, d.h. das neutrale Element von (R', \cdot) liegt in $\text{Bild}(\phi)$ und ist damit auch neutrales Element von $(\text{Bild}(\phi), \cdot)$. Schließlich bleibt festzustellen, dass die Distributivgesetze in R' , also insbesondere in $\text{Bild}(\phi)$ gelten. Also ist $\text{Bild}(\phi)$ ein Unterring von R' .

• **Kern(ϕ) ist ein Ideal in R :**

Mit der Vorbemerkung ist also $(\text{Kern}(\phi), +)$ eine Untergruppe von $(R, +)$. Sei nun $a \in \text{Kern}(\phi)$ und $r \in R$. Dann gilt

$$\begin{aligned}\phi(ar) &= \phi(a)\phi(r) = 0 \cdot \phi(r) = 0 \text{ und} \\ \phi(ra) &= \phi(r)\phi(a) = \phi(r) \cdot 0 = 0,\end{aligned}$$

also $ar, ra \in \text{Kern}(\phi)$. Somit ist $\text{Kern}(\phi) \triangleleft R$.

Insgesamt ist die Proposition bewiesen. □

Es wird jetzt der Homomorphiesatz für Ringe bewiesen, der Kern und Bild eines Ringhomomorphismus in Verbindung bringt.

Satz 2.10 (Homomorphiesatz für Ringe). *Seien R, R' Ringe und $\phi : R \rightarrow R'$ ein Ringhomomorphismus. Dann ist die Abbildung*

$$\begin{aligned}\Phi : R/\text{Kern}(\phi) &\rightarrow \text{Bild}(\phi), \\ [r] &\mapsto \phi(r)\end{aligned}$$

ein Ringisomorphismus, insbesondere gilt also $R/\text{Kern}(\phi) \cong \text{Bild}(\phi)$.

Beweis. Die Abbildung Φ ist wohldefiniert, denn für $[a] = [b]$, also $a - b \in \text{Kern}(\phi)$, gilt $\phi(a) - \phi(b) = \phi(a - b) = 0$ und damit $\phi(a) = \phi(b)$.

Um zu zeigen, dass Φ ein Ringhomomorphismus ist, werden die Axiome aus Definition 2.7 überprüft.

1. $\Phi([a] + [b]) = \Phi([a + b]) = \phi(a + b) = \phi(a) + \phi(b) = \Phi([a]) + \Phi([b]),$
2. $\Phi([a][b]) = \Phi([ab]) = \phi(ab) = \phi(a)\phi(b) = \Phi([a])\Phi([b]),$
3. $\Phi([1]) = \phi(1) = 1.$

Man kann nun die Injektivität des Homomorphismus durch $\text{Kern}(\Phi) = \{[0]\}$ zeigen, was aus der Gruppentheorie bekannt ist und sich ebenso auf Ringhomomorphismen anwenden lässt. Für $[r] \in \text{Kern}(\Phi)$ gilt $\phi(r) = 0$, d.h. $r = r - 0 \in \text{Kern}(\phi)$. Damit ist $[r] = [0]$ bezüglich dem Ideal $\text{Kern}(\Phi)$. Die Surjektivität von Φ folgt daraus, dass für jedes $\phi(r) \in \text{Bild}(\phi)$ durch $[r]$ ein Urbild unter Φ gegeben ist.

Insgesamt handelt es sich bei Φ also um einen bijektiven Ringhomomorphismus, d.h. um einen Ringisomorphismus. □

Besonderes Interesse gilt dem Bild $\mathbb{Z}e$ von $\phi : \mathbb{Z} \rightarrow R$ mit $\phi(n) = ne$, das nach Proposition 2.9 ein Ring ist.

Definition 2.11. Sei $(R, +, \cdot)$ ein Ring und e das neutrale Element von (R, \cdot) . Der Unterring $\mathbb{Z}e$ von R wird **Primring** von R genannt und mit $P(R)$ bezeichnet.

Man kann den Primring eines Ringes als dessen kleinsten Unterring ansehen. Betrachtet man nämlich einen anderen Unterring $S \subseteq R$, so gilt per Definition $e \in S$, und S ist bezüglich der Addition abgeschlossen. Daraus folgt aber schon $ne \in S$ für alle $n \in \mathbb{Z}$, also $\mathbb{Z}e \subseteq S$.

Mit Hilfe des Homomorphiesatzes kann man nun schließen, wie der Primring eines Ringes auszusehen hat.

Proposition 2.12. *Sei R ein Ring. Der Primring $P(R)$ von R ist entweder isomorph zu \mathbb{Z} oder zu $\mathbb{Z}/m\mathbb{Z}$ für ein $m \in \mathbb{N}$. Gilt letzteres, so ist m die kleinste positive Zahl mit $me = 0$.*

Beweis. Nach dem Homomorphiesatz gilt $P(R) \cong \mathbb{Z}/\text{Kern}(\phi)$ und nach Proposition 2.9 ist $\text{Kern}(\phi)$ ein Ideal in \mathbb{Z} . Die Ideale in \mathbb{Z} sind nach Beispiel 2.4 genau die $m\mathbb{Z}$ mit $m \in \mathbb{N}^0$. Ist $m = 0$, so gilt also $P(R) \cong \mathbb{Z}$, andernfalls $P(R) \cong \mathbb{Z}/m\mathbb{Z}$ mit $m \in \mathbb{N}$.

Ist $\text{Kern}(\phi) = m\mathbb{Z}$ und Φ der zu ϕ zugehörige Isomorphismus aus dem Homomorphiesatz, so folgt $\Phi([a]) = ae \neq 0$ für $a \in \{1, \dots, m-1\}$ und $\Phi([m]) = \Phi([0]) = me = 0$. Somit ist m die kleinste positive Zahl mit $me = 0$. \square

Dies ist die Grundlage für den folgenden Begriff.

Definition 2.13. Sei R ein Ring und $P(R)$ sein Primring. Ist $P(R) \simeq \mathbb{Z}$, so sagt man, dass R die **Charakteristik 0** hat und schreibt kurz $\text{char}(R) = 0$. Ist $P(R) \simeq \mathbb{Z}/m\mathbb{Z}$ mit $m \in \mathbb{N}$, so sagt man, dass R die **Charakteristik m** hat und schreibt kurz $\text{char}(R) = m$.

Für den Ring, der ausschließlich aus einem Nullelement besteht, wird keine Charakteristik definiert.

Mit Hilfe dieser Erkenntnisse ist es nun möglich, endliche Körper über ihre Mächtigkeit zu charakterisieren.

2.1.2 Mächtigkeit endlicher Körper

Eingangs werden Schiefkörper und Körper definiert.

Definition 2.14. Ein Ring $(R, +, \cdot)$ heißt **Schiefkörper**, wenn $(R \setminus \{0\}, \cdot)$ eine Gruppe ist.

Beispiel 2.15. Die Menge der Quaternionen \mathbb{H} ist definiert durch $\mathbb{H} := \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$. Auf dieser Menge definiert man die Addition $+$ durch

$$\begin{aligned} & (a_1 + b_1i + c_1j + d_1k) + (a_2 + b_2i + c_2j + d_2k) \\ &= a_1 + a_2 + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k \end{aligned}$$

und die Multiplikation \cdot durch

$$\begin{aligned} & (a_1 + b_1i + c_1j + d_1k) \cdot (a_2 + b_2i + c_2j + d_2k) \\ &= (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) + (a_1b_2 + a_2b_1 + c_1d_2 - c_2d_1)i \\ &+ (a_1c_2 - b_1d_2 + a_2c_1 + b_2d_1)j + (a_1d_2 + b_1c_2 - b_2c_1 + a_2d_1)k, \end{aligned}$$

also indem man die Distributivgesetze wie gewohnt auf die beiden Faktoren anwendet und die Beziehungen $i^2 = j^2 = k^2 = ijk = -1$ beachtet.

Dann ist $(\mathbb{H}, +, \cdot)$ ein Schiefkörper; die entsprechenden Axiome können routinemäßig überprüft werden.

Der Schiefkörper $(\mathbb{H}, +, \cdot)$ ist nicht kommutativ, dann man erhält $k = ij$, wenn man die Beziehung $k^2 = ijk$ von rechts mit k^{-1} multipliziert, aber $-k = ji$, wenn man $i^2 = ijk$ von links mit ji^{-1} multipliziert und $j^2 = -1$ verwendet.

Bei einem Körper wird so etwas ausgeschlossen.

Definition 2.16. Ein Schiefkörper heißt **Körper**, wenn er kommutativ ist.

Man erhält also die Körperaxiome, indem man in den Ringaxiomen aus Definition 2.1 das 2. Axiom durch

2.' $(R \setminus \{0\}, \cdot)$ ist eine kommutative Gruppe.

ersetzt.

Bei der Definition eines **Körperhomomorphismus** wird Definition 2.7 unverändert übernommen, nur dass es sich bei den Ringen R, R' um Körper handeln muss. Ist dieser bijektiv, heißt er auch **Körperisomorphismus**.

Als nächstes wird die Charakteristik endlicher Körper untersucht. Es sei aber noch erwähnt, dass es äquivalent wäre, endliche Schiefkörper zu betrachten, denn es gilt der Satz von Wedderburn, für dessen insgesamt recht umfangreichen Beweis auf die einschlägige Literatur (z.B. [9], S. 453f.) verwiesen wird.

Satz 2.17 (Satz von Wedderburn). *Jeder endliche Schiefkörper ist ein Körper.*

Es wird jetzt noch folgende Aussage benötigt.

Proposition 2.18. *Sei R ein Schiefkörper. Dann folgt für $a, b \in R$ aus $ab = 0$ stets $a = 0$ oder $b = 0$.*

Beweis. Zunächst einmal gilt $r \cdot 0 = 0$ für alle $r \in R$, was man aus $r \cdot 0 = r \cdot (0 + 0) = r \cdot 0 + r \cdot 0$ durch Subtraktion von $r \cdot 0$ auf beiden Seiten erhält.

Seien nun $a, b \in R$ mit $ab = 0$. Ist $a = 0$, so ist die Behauptung erfüllt, also sei $a \neq 0$. Multipliziert man $ab = 0$ auf beiden Seiten mit a^{-1} , so folgt $a^{-1}ab = b = 0$, und die Behauptung ist auch in diesem Fall erfüllt. \square

Insbesondere gilt diese Proposition dann in Körpern, und in Körpern ist per Definition $1 \neq 0$, da ja 1 das neutrale Element der Gruppe $(R \setminus \{0\}, \cdot)$ ist. Ringe, in denen $1 \neq 0$ ist und für $a, b \in R$ aus $ab = 0$ stets $a = 0$ oder $b = 0$ folgt, bezeichnet man auch als **Integritätsbereiche**.

Damit ist es möglich, etwas über die Charakteristik endlicher Körper auszusagen.

Lemma 2.19. *Ist K ein endlicher Körper, so ist $\text{char}(K) = p$, wobei p eine Primzahl ist.*

Beweis. Da in einem Körper $1 \neq 0$ ist und diese Elemente auch in jedem Unterring von K liegen, hat der Primring $P(K)$ von K mindestens zwei Elemente, also ist $p \geq 2$. Ist p keine Primzahl, so gibt es Teiler $t_1, t_2 \in \mathbb{N}$ von p mit $1 < t_1, t_2 < p$ und $p = t_1 t_2$. Mit dem neutralen Element e von (K, \cdot) gilt

$$0 = pe = (t_1 t_2)e = (t_1 e)(t_2 e),$$

woraus wegen Proposition 2.18 $t_1 e = 0$ oder $t_2 e = 0$ folgt. Dies ist ein Widerspruch, denn nach Proposition 2.12 ist p die kleinste positive Zahl mit $pe = 0$. Somit ist p eine Primzahl. \square

Damit ist der Primring eines Körpers ebenso ein Körper und man spricht auch vom **Primkörper** des Körpers. Allgemein ist ein Primkörper, analog zum Primring, ein Körper, der keine echten Unterkörper enthält. Dies ist hier natürlich auch erfüllt, da der Primring eines Ringes mit dem Nachsatz zu Definition 2.11 keine echten Unterringe enthält, also erst recht keine echten Unterkörper.

Es folgt das Hauptresultat dieses Teilabschnittes.

Satz 2.20. *Ist K ein endlicher Körper, so hat K p^n Elemente, wobei p eine Primzahl und $n \in \mathbb{N}$ ist.*

Beweis. Nach Lemma 2.19 ist $\text{char}(K) = p$ für eine Primzahl p , sodass der Primring von K isomorph zu $\mathbb{Z}/p\mathbb{Z}$ und damit ein Körper mit p Elementen ist. Man kann K als Vektorraum endlicher Dimension über $P(K)$ auffassen, da K endlich ist; sei $\dim_{P(K)}(K) = n$. Damit gibt es $b_i \in K$, sodass die Elemente $b \in K$ genau die sind, die sich als $b = \sum_{j=1}^n a_j b_j$, $a_j \in P(K)$, darstellen lassen. Für jedes a_i gibt es p Möglichkeiten, also gibt es insgesamt p^n verschiedene Elemente von K . \square

2.1.3 Existenz und Eindeutigkeit endlicher Körper

Nachdem geklärt ist, dass es nur endliche Körper mit p^n Elementen geben kann, wird jetzt gezeigt, dass zu jeder Primzahlpotenz p^n auch ein bis auf Isomorphie eindeutiger Körper mit p^n Elementen existiert.

Dazu wird erst mal der Begriff der Körpererweiterung benötigt.

Definition 2.21. Sei L ein Körper. Dann heißt eine Teilmenge $\emptyset \neq K \subseteq L$ **Unterkörper** von L , wenn $(K, +, \cdot)$ ein Körper ist, und L heißt eine **Körpererweiterung** von K . Für eine Körpererweiterung L von K schreibt man dann auch $L : K$.

Wie im Beweis von Satz 2.20 für $K : P(K)$ schon getan, lässt sich eine Körpererweiterung $L : K$ als Vektorraum über K auffassen. In diesem Sinne definiert man den Grad einer Körpererweiterung.

Definition 2.22. Sei $L : K$ eine Körpererweiterung. Dann heißt

$$[L : K] := \dim_K L$$

Grad der Körpererweiterung. Ist $[L : K] < \infty$, so heißt $[L : K]$ **endlich**, sonst **unendlich**.

Es folgen einige einfache Beispiele für Körpererweiterungen.

Beispiele 2.23.

1. Wie schon gesehen, ist ein Körper mit p^n Elementen eine Körpererweiterung seines Primkörpers $\mathbb{Z}/p\mathbb{Z}$ vom Grad n .
2. Die komplexen Zahlen \mathbb{C} sind eine Körpererweiterung von \mathbb{R} . Dabei ist $[\mathbb{C} : \mathbb{R}] = 2$. Ebenso sind die Zahlen $\mathbb{Q}(i) := \{a + bi \mid a, b \in \mathbb{Q}\}$ mit der üblichen Addition und Multiplikation von komplexen Zahlen eine Körpererweiterung von \mathbb{Q} vom Grad 2.
3. \mathbb{R} ist eine Körpererweiterung von \mathbb{Q} . Bekanntermaßen ist diese unendlich.

Ein wichtiges Resultat über den Grad endlicher Körpererweiterungen ist der folgende Satz.

Satz 2.24 (Gradsatz). *Seien $M : L$ und $L : K$ endliche Körpererweiterungen. Dann ist auch $M : K$ eine endliche Körpererweiterung und es gilt*

$$[M : K] = [M : L][L : K].$$

Beweis. Sei (w_1, \dots, w_m) eine Basis von M über L und (v_1, \dots, v_n) eine Basis von L über K , also $[M : L] = m$ und $[L : K] = n$. Es wird nun gezeigt, dass

$$(v_1w_1, \dots, v_1w_m, v_2w_1, \dots, v_2w_m, \dots, v_nw_1, \dots, v_nw_m)$$

eine Basis von M über K und somit $[M : K] = mn$ ist.

Sei also a ein beliebiges Element aus M . Dann lässt sich a über L als Linearkombination

$$a = \sum_{j=1}^m \alpha_j w_j$$

mit $\alpha_1, \dots, \alpha_m \in L$ darstellen. Diese $\alpha_j, j = 1, \dots, m$ lassen sich wiederum über K als Linearkombinationen

$$\alpha_j = \sum_{i=1}^n \beta_{ij} v_i$$

mit $\beta_{ij} \in K, i = 1, \dots, n, j = 1, \dots, m$ darstellen. Insgesamt ist also

$$a = \sum_{j=1}^m \left(\sum_{i=1}^n \beta_{ij} v_i \right) w_j = \sum_{j=1}^m \sum_{i=1}^n \beta_{ij} v_i w_j,$$

d.h. a lässt sich als Linearkombination der $v_i w_j, i = 1, \dots, n, j = 1, \dots, m$ darstellen. Somit erzeugen diese Elemente den Körper M über K .

Schließlich wird nun noch gezeigt, dass die $v_i w_j, i = 1, \dots, n, j = 1, \dots, m$ auch linear unabhängig sind, sich in K also nur trivial zum Nullvektor kombinieren lassen.

Seien also $\gamma_{ij} \in K, i = 1, \dots, n, j = 1, \dots, m$ so gewählt, dass

$$\sum_{j=1}^m \sum_{i=1}^n \gamma_{ij} v_i w_j = \sum_{j=1}^m \left(\sum_{i=1}^n \gamma_{ij} v_i \right) w_j = 0$$

gilt, wobei die $\sum_{i=1}^n \gamma_{ij} v_i, j = 1, \dots, m$ natürlich Koeffizienten aus L sind. Da die w_1, \dots, w_m linear unabhängig über L sind, sind all diese Koeffizienten null, denn sonst ließen sich die w_1, \dots, w_m über L nichttrivial zum Nullvektor kombinieren. Außerdem sind die v_1, \dots, v_n linear unabhängig über K , sodass auch alle $\gamma_{ij}, i = 1, \dots, n, j = 1, \dots, m$ null sein müssen. Damit ist die lineare Unabhängigkeit der

$$(v_1 w_1, \dots, v_1 w_m, v_2 w_1, \dots, v_2 w_m, \dots, v_n w_1, \dots, v_n w_m)$$

über K gezeigt, womit eine Basis von M über K mit mn Elementen gegeben ist.

Also ist $[M : K] = mn$. □

Es werden nun die Körper vorgestellt, die sich als Repräsentanten der Isomorphieklassen endlicher Körper herausstellen werden.

Definition 2.25. Sei $L : K$ eine Körpererweiterung und $\{a_1, \dots, a_n\} \subseteq L$ eine endliche Teilmenge von L . Dann wird der Schnitt aller Unterkörper von L , die sowohl K als auch die a_1, \dots, a_n enthalten, mit $K(a_1, \dots, a_n)$ bezeichnet.

Definition 2.26. Sei $L : K$ eine Körpererweiterung und $f \in K[T]$ nicht konstant. Man sagt, f **zerfällt** über L , wenn f über L als Produkt von Linearfaktoren geschrieben werden kann, d.h.

$$f = a \prod_{i=1}^n (T - a_i) \text{ mit } a, a_i \in L.$$

L heißt **Zerfällungskörper** von f , wenn f über L zerfällt und $L = K(a_1, \dots, a_n)$ gilt.

Ohne Beweis wird das folgende Resultat über die Existenz und Eindeutigkeit von Zerfällungskörpern verwendet. Für einen Beweis müsste man etwas weiter ausholen und Kenntnisse über algebraische Körpererweiterungen verwenden; hierfür wird auf [9], S. 225f., oder [6], S. 280, verwiesen.

Lemma 2.27. *Sei K ein Körper und $f \in K[T]$ ein nichtkonstantes Polynom. Dann existiert ein bis auf Isomorphie eindeutiger Zerfällungskörper $L : K$ von f .*

Damit wird nun auf das zentrale Resultat dieses Teilabschnittes hingearbeitet. Dazu müssen noch ein paar kleinere Hilfspropositionen bewiesen werden; zuerst eine Aussage über Polynome über K .

Proposition 2.28. *Sei K ein Körper und $f \in K[T]$. Ist $\lambda \in K$ eine mehrfache Nullstelle von f , so ist λ auch eine Nullstelle von f' .*

Beweis. Sei λ eine Nullstelle von f mit Vielfachheit $\alpha(\lambda) \geq 2$. Dann hat f die Form

$$f = (T - \lambda)^{\alpha(\lambda)} q$$

mit einem Polynom $q \in K[T]$, und mit der Produktregel der Differentialrechnung folgt

$$f' = \alpha(\lambda)(T - \lambda)^{\alpha(\lambda)-1} q + (T - \lambda)^{\alpha(\lambda)} q'.$$

Somit ist λ auch eine Nullstelle von f' . □

Beispiel 2.29. Sei K ein Körper mit q Elementen. Dann hat das Polynom $f = T^q - T \in K[T]$ keine mehrfachen Nullstellen, denn es ist

$$f' = (T^q - T)' = qT^{q-1} - 1 = -1,$$

womit f' keine Nullstellen hat.

Wie die nächste Proposition zeigt, ist eine Körpererweiterung stets ein Zerfällungskörper des Polynoms aus dem Beispiel.

Proposition 2.30. Sei $L : K$ eine Körpererweiterung mit q Elementen und $f = T^q - T \in K[T]$. Dann ist L ein Zerfällungskörper von f über K .

Beweis. Zu zeigen sind nach Definition 2.26 die folgenden Aussagen:

- **f zerfällt über L :**

Da L ein Körper ist, ist aus der Gruppentheorie bekannt, dass $(L \setminus \{0\}, \cdot)$ eine zyklische Gruppe ist, und damit folgt aus dem Satz von Lagrange $a^{q-1} - 1 = 0$, also auch $a^q - a = 0$ für alle $a \in L \setminus \{0\}$. Auch für $a = 0$ gilt natürlich $a^q - a = 0$. Damit sind q Nullstellen von f gefunden, und das sind bereits alle, da $\text{Grad}(f) = q$ ist. Somit ist

$$f = \prod_{a \in L} (T - a)$$

und f zerfällt über L .

- **L enthält keinen echten Unterkörper, der sowohl K als auch alle Nullstellen von f enthält:**

In Beispiel 2.29 war bereits zu sehen, dass f keine mehrfachen Nullstellen besitzt, und damit muss jeder Körper, in dem f zerfällt, mindestens die q verschiedenen Nullstellen als Elemente haben. Natürlich kann so ein Körper dann nicht kleiner als L sein.

Insgesamt ist die Proposition also bewiesen. □

Benötigt wird auch die folgende Aussage.

Proposition 2.31. Sei K ein Körper und $\{0\} \neq J \subseteq K$ eine nichtleere Teilmenge von K . Gilt für alle $a, b \in J$ mit $b \neq 0$ sowohl $a - b \in J$ als auch $ab^{-1} \in J$, so ist J ein Körper.

Beweis. Es gelte für alle $a, b \in J$ mit $b \neq 0$ sowohl $a - b \in J$ als auch $ab^{-1} \in J$. Dann kann man zeigen, dass die Körperaxiome für J gelten:

1. **$(J, +)$ ist eine abelsche Gruppe:**

Da J eine Teilmenge von K ist, gilt das Assoziativgesetz der Addition. Für ein beliebiges $b \in J$ folgt mit $a := b$ sofort $a - b = b - b = 0 \in J$, sodass das neutrale Element der Addition von K in J liegt. Mit $a := 0$ erhält man zudem $a - b = -b \in J$, also liegt das additiv Inverse eines Elements aus J auch in J . Die Kommutativität bezüglich der Addition folgt wieder daraus, dass J eine Teilmenge von K ist. Schließlich folgt die Abgeschlossenheit von $(J, +)$ daraus, dass, wie gezeigt, mit b auch $-b \in J$ ist und daraus $a - (-b) = a + b \in J$ folgt. Insgesamt ist also $(J, +)$ eine abelsche Gruppe.

2. **$(J \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe:**

Da $J \setminus \{0\}$ eine Teilmenge von K ist, gilt das Assoziativgesetz der Multiplikation. Für ein beliebiges $b \in J \setminus \{0\}$ folgt mit $a := b$ sofort $ab^{-1} = bb^{-1} = 1 \in J \setminus \{0\}$, sodass das neutrale Element der Multiplikation von K in $J \setminus \{0\}$ liegt. Mit $a := 1$ erhält man zudem $ab^{-1} = b^{-1} \in J \setminus \{0\}$, also liegt das multiplikativ Inverse eines Elements aus $J \setminus \{0\}$ auch in $J \setminus \{0\}$. Die Kommutativität bezüglich der Multiplikation folgt wieder daraus, dass $J \setminus \{0\}$ eine Teilmenge von K ist. Schließlich folgt die Abgeschlossenheit von $(J \setminus \{0\}, \cdot)$ daraus, dass, wie gezeigt, mit b auch $b^{-1} \in J \setminus \{0\}$ ist und daraus $a(b^{-1})^{-1} = ab \in J \setminus \{0\}$ folgt. Insgesamt ist also $(J \setminus \{0\}, \cdot)$ eine abelsche Gruppe.

3. **Für alle $a, b, c \in J$ gelten die Distributivgesetze:**

Dies ist wiederum der Fall, da J eine Teilmenge von K ist.

Somit wurde gezeigt, dass J ein Körper ist. □

Als letztes folgt noch eine Rechenregel, in deren Beweis verwendet wird, dass in einem kommutativen Ring R die binomische Formel

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$$

für alle $a, b \in R$ und $n \in \mathbb{N}$ gilt.

Proposition 2.32. *In einem kommutativen Ring R mit $\text{char}(R) = p > 0$ gilt die binomische Formel*

$$(a + b)^{p^n} = a^{p^n} + b^{p^n}$$

für alle $a, b \in R$ und $n \in \mathbb{N}$.

Beweis. Der Beweis wird durch Induktion nach n geführt.

• **Induktionsanfang:**

Für $n = 1$ gilt

$$(a + b)^p = \sum_{k=0}^p \binom{p}{k} a^k b^{p-k} = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k} + b^p$$

unter Anwendung der binomischen Formel. Da per Definition $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ gilt und da $p \mid p!$, aber $p \nmid k!$ und $p \nmid (p-k)!$ für $k \in \{1, \dots, p-1\}$ gilt, gilt auch $p \mid \binom{p}{k}$ für $k \in \{1, \dots, p-1\}$. Mit der Nachbemerkung von Proposition 2.12 sind diese $\binom{p}{k}$ also alle null, womit die Proposition für $n = 1$ folgt.

• **Induktionsschritt:**

Die Behauptung gelte nun für $n \geq 1$:

$$(a + b)^{p^n} = a^{p^n} + b^{p^n}$$

Potenziert man beide Seiten mit p , so erhält man

$$(a + b)^{p^{n+1}} = a^{p^{n+1}} + b^{p^{n+1}},$$

wobei die linke Seite klar ist und die rechte Seite aus der Behauptung dieser Proposition folgt, die ja, wie schon gezeigt wurde, für $n = 1$ gilt.

Insgesamt folgt die Behauptung für alle $n \in \mathbb{N}$. □

Unter Verwendung dieser Kenntnisse kann nun der Satz über die Existenz und Eindeutigkeit endlicher Körper formuliert und bewiesen werden.

Satz 2.33. *Ein endlicher Körper mit q Elementen existiert genau dann, wenn $q = p^n$ ist. Ferner ist jeder Körper mit $q = p^n$ isomorph zum Zerfällungskörper von $T^q - T$ über $\mathbb{Z}/p\mathbb{Z}$.*

Beweis. In Satz 2.20 wurde bewiesen, dass es höchstens endliche Körper mit $q = p^n$ Elementen gibt, wobei p eine Primzahl und $n \in \mathbb{N}$ ist. Jetzt wird gezeigt, dass es zu jeder Primzahlpotenz $q = p^n$ auch einen Körper mit q Elementen gibt, nämlich den Zerfällungskörper K von $T^q - T$ über $\mathbb{Z}/p\mathbb{Z}$. Sei dazu $L := \{a \in K \mid a^q - a = 0\}$. Dann ist L nach Proposition 2.31 ein Körper, denn es gilt $(a - b)^q = (a - b)^{p^n} = a^{p^n} - b^{p^n} = a^q - b^q = a - b$ sowie $(ab^{-1})^q = a^q b^{-q} = ab^{-1}$ unter Anwendung von 2.32 und dem Satz von Lagrange und damit $a - b, ab^{-1} \in L$. Da L alle Nullstellen von $T^q - T$ enthält und dieses Polynom keine mehrfachen Nullstellen hat, folgt $L = K$ und dieser Körper hat q Elemente.

Nach Proposition 2.30 ist ein Körper, als Erweiterung seines Primkörpers betrachtet, isomorph zu einem Zerfällungskörper von $T^q - T$ über $\mathbb{Z}/p\mathbb{Z}$. Dieser ist aber nach Lemma 2.27 bis auf Isomorphie eindeutig, und damit auch der hier betrachtete Körper mit q Elementen. □

Man kann somit berechtigterweise von dem Körper mit q Elementen sprechen. Dieser wird auch kurz als $GF(q)$ bezeichnet (von englisch „Galois field“).

Abschließend soll noch geklärt werden, welche Unterkörper ein Körper mit p^n Elementen besitzt.

Satz 2.34. *Sei $n \in \mathbb{N}$ und p prim. $GF(p^n)$ hat einen Unterkörper mit p^m Elementen genau dann, wenn m ein Teiler von n ist. Gegebenenfalls ist dieser Unterkörper der einzige Unterkörper von $GF(p^n)$ mit p^m Elementen.*

Beweis. Unter Anwendung des Gradsatzes 2.24 ist sofort klar, dass m wegen

$$\begin{aligned}n &= [GF(p^n) : GF(p)] \\ &= [GF(p^n) : GF(p^m)][GF(p^m) : GF(p)] \\ &= [GF(p^n) : GF(p^m)] \cdot m\end{aligned}$$

ein Teiler von n ist.

Sei nun m ein Teiler von n . Dann ist

$$\frac{p^n - 1}{p^m - 1} = p^{n-m} + p^{n-2m} + \dots + p^m + 1,$$

also gilt $(p^m - 1) \mid (p^n - 1)$. Aus $a^{p^m - 1} = 1$ für alle $a \in GF(p^m) \setminus \{0\}$ folgt damit auch $a^{p^n - 1} = 1$, was auch $a^{p^n} - a = 0$ bedeutet, sodass a Nullstelle von $T^{p^n} - T$ und somit Element von $GF(p^n)$ ist. Also ist $GF(p^m)$ Unterkörper von $GF(p^n)$. Würde $GF(p^n)$ zwei verschiedene zu $GF(p^m)$ isomorphe Unterkörper enthalten, so enthielte $GF(p^n)$ mehr als p^m Nullstellen von $T^{p^m} - T$, was nicht sein kann. \square

Mit den Begriffen des nächsten Abschnitts könnte man sagen, dass die Unterkörper eines endlichen Körpers zusammen mit der Unterkörperbeziehung einen Verband bilden, der isomorph zum entsprechenden Teilverband ist.

Einige Grundlagen der Verbandstheorie, inklusive der soeben benutzten Begriffe, werden nun vorgestellt.

2.2 Verbände

Verbände lassen sich als partiell geordnete Mengen oder als algebraische Strukturen definieren. Wie auch in [5] oder [7] werden beide Definitionen vorgestellt und es wird gezeigt, dass sie in einem bestimmten Sinne äquivalent sind. Anschließend werden wichtige Eigenschaften von Verbänden behandelt, bevor speziell lineare Verbände betrachtet werden.

2.2.1 Definition von Verbänden

Zuerst werden also Halbordnungen eingeführt.

Definition 2.35. Eine Relation \leq auf einer Menge M heißt **Halbordnung**, wenn für alle $a, b, c \in M$

1. $a \leq a$ (Reflexivität),
2. $a \leq b$ und $b \leq a \Rightarrow a = b$ (Antisymmetrie) und
3. $a \leq b$ und $b \leq c \Rightarrow a \leq c$ (Transitivität)

gilt.

Ist \leq eine Halbordnung auf M , so heißt das Paar (M, \leq) **partiell geordnete Menge**.

In einer partiell geordneten Menge (M, \leq) ist es, anders als bei einer total geordneten Menge, möglich, dass für zwei verschiedene Elemente $a, b \in M$ weder $a \leq b$ noch $b \leq a$ gilt. Dies führt zu folgender Definition.

Definition 2.36. Sei (M, \leq) eine partiell geordnete Menge. Dann heißen zwei Elemente $a, b \in M$ **vergleichbar**, falls $a \leq b$ oder $b \leq a$ gilt, sonst **unvergleichbar**. Eine Teilmenge $N \subseteq M$ heißt **Kette**, wenn je zwei Elemente aus N vergleichbar sind, und **Antikette**, wenn je zwei Elemente aus N unvergleichbar sind.

Die folgenden Begriffe Filter, Ideal und Intervall werden in dieser Arbeit noch eine sehr zentrale Rolle spielen.

Definition 2.37. Sei (M, \leq) eine partiell geordnete Menge und $a \in M$. Die Menge $\text{Filter}(a) := \{c \in M \mid c \geq a\}$ heißt **Filter** von a , die Menge $\text{Ideal}(a) := \{c \in M \mid c \leq a\}$ heißt **Ideal** von a .

Ist $b \in M$ mit $a \leq b$, so wird $[a, b] := \{c \in M \mid a \leq c \leq b\}$ als **Intervall** bezeichnet.

Dieser Idealbegriff ist nicht mit dem aus der Ringtheorie zu verwechseln. Auch Schranken kommt in partiell geordneten Mengen eine große Bedeutung zu.

Definition 2.38. Sei (M, \leq) eine partiell geordnete Menge und $N \subseteq M$. Ein Element \underline{s} bzw. $\bar{s} \in M$ heißt **untere** bzw. **obere Schranke** von N , wenn $\underline{s} \leq c$ bzw. $\bar{s} \geq c$ für alle $c \in N$ gilt. Eine untere bzw. obere Schranke \underline{s}^* bzw. \bar{s}^* von N heißt **Infimum** bzw. **Supremum** von N , falls $\underline{s}^* \geq \underline{s}$ für alle unteren Schranken \underline{s} von N bzw. $\bar{s}^* \leq \bar{s}$ für alle oberen Schranken \bar{s} von N gilt.

Die Eindeutigkeit von Infimum und Supremum ist per Definition gegeben, die Existenz jedoch nicht. Besitzt eine partiell geordnete Menge als ganze ein Infimum oder Supremum, so erhält dieses eine eigene Bezeichnung.

Definition 2.39. Sei (M, \leq) eine partiell geordnete Menge. Besitzt M ein Infimum, so heißt dieses **Nullelement** von M ; besitzt M ein Supremum, so heißt dieses **Einselement** von M .

Das Null- bzw. Einselement einer partiell geordneten Menge ist nicht mit dem neutralen Element eines Ringes bezüglich der Addition bzw. Multiplikation zu verwechseln. Wenn klar ist, dass das Nullelement bzw. das Einselement eines Verbandes gemeint ist, so schreibt man auch einfach 0 bzw. 1.

Mit Hilfe von Halbordnungen können nun Verbände definiert werden.

Definition 2.40. Eine partiell geordnete Menge $\mathcal{L} = (L, \leq)$ heißt **Verband**, wenn L eine nichtleere Menge ist und $\inf\{a, b\}$ sowie $\sup\{a, b\}$ für alle $a, b \in L$ existieren.

Liegt nun ein solcher Verband $\mathcal{L} = (L, \leq)$ vor, so definiert man, zunächst ohne genauere Absichten, zwei binäre Operationen \wedge_a und \vee_a auf L durch

$$a \wedge_a b := \inf\{a, b\}$$

und

$$a \vee_a b := \sup\{a, b\}$$

für $a, b \in L$. Diese Operationen sind wegen der Existenz und Eindeutigkeit von Infimum und Supremum wohldefiniert. Man nennt $a \wedge_a b$ den Schnitt und $a \vee_a b$ die Verbindung von a und b . Zu dem Verband \mathcal{L} definiert man jetzt $\mathcal{L}^a := (L, \vee_a, \wedge_a)$ als algebraische Struktur mit diesen beiden Operationen.

Es ist auch durchaus üblich, einen Verband von vornherein als algebraische Struktur mit diesen beiden Operationen einzuführen. Dies wird nun auch gemacht; anschließend wird gezeigt, dass die beiden Definitionen eines Verbandes miteinander in Einklang stehen.

Definition 2.41. Eine algebraische Struktur $\mathcal{L} = (L, \wedge, \vee)$ heißt **Verband**, wenn L eine nichtleere Menge ist und \vee und \wedge zwei binäre Operationen auf L sind, sodass für alle $a, b, c \in L$ die folgenden Bedingungen erfüllt sind:

1. $a \wedge b = b \wedge a$, $a \vee b = b \vee a$ (Kommutativität)
2. $(a \wedge b) \wedge c = a \wedge (b \wedge c)$, $(a \vee b) \vee c = a \vee (b \vee c)$ (Assoziativität)
3. $a \wedge (a \vee b) = a$, $a \vee (a \wedge b) = a$ (Absorptionsregeln)

Aus den Axiomen folgen außerdem die Idempotenzregeln:

Proposition 2.42. Sei $\mathcal{L} = (L, \wedge, \vee)$ ein Verband. Dann gilt für alle $a, b \in L$

$$a \wedge a = a, a \vee a = a,$$

d.h. die **Idempotenz** von \wedge und \vee .

Beweis. Aus der zweiten Absorptionsregel folgt $a \wedge a = a \wedge (a \vee (a \wedge b))$, und aus der ersten Absorptionsregel folgt $a \wedge (a \vee (a \wedge b)) = a$. Die Idempotenzregel $a \vee a = a$ zeigt man dual. \square

Anhand der zweiten Definition eines Verbandes kann man sich leicht klarmachen, was man unter **Dualität** in Verbänden versteht. In den Axiomen treten die beiden Operationen \wedge und \vee gleichberechtigt auf, d.h. wenn man in einem der Axiome \wedge durch \vee und \vee durch \wedge ersetzt, dann gehört die so entstehende Aussage auch zu den Verbandsaxiomen. Die aus einer Aussage durch eine solche Ersetzung entstehende Aussage nennt man die zu dieser Aussage **duale Aussage**. Man kann auf Grund der Ausführungen direkt schließen, dass auch für alle weiteren gültigen Aussagen, die aus den Axiomen folgen, auch die zu diesen dualen Aussagen gültig sind.

Auch die Definition eines Teilverbandes ist mit dieser zweiten Definition leicht möglich.

Definition 2.43. Ist $\mathcal{L} = (L, \wedge, \vee)$ ein Verband und $M \subseteq L$, so heißt $\mathcal{M} = (M, \wedge, \vee)$ Teilverband von \mathcal{L} , wenn M bezüglich \wedge und \vee abgeschlossen ist.

Jedoch soll jetzt gezeigt werden, dass die Definitionen 2.40 und 2.41 tatsächlich einander entsprechen. Zu einem Verband $\mathcal{L} = (L, \wedge, \vee)$ definiere man eine Relation \leq_p auf L durch

$$a \leq_p b :\Leftrightarrow a \wedge b = a$$

für $a, b \in L$. Äquivalent dazu wäre $a \leq_p b :\Leftrightarrow b \vee a = b$, denn wenn man $a \wedge b = a$ mit b vereinigt und die Kommutativität sowie die zweite Absorptionsregel anwendet, so erhält man genau $b \vee a = b$; analog kommt man auch wieder zurück.

Man setzt zudem $\mathcal{L}^p := (L, \leq_p)$. Der folgende Satz spezifiziert nun, in wiefern die beiden angegebenen Definitionen von Verbänden als äquivalent anzusehen sind.

Satz 2.44. *Ist $\mathcal{L}_1 = (L_1, \leq)$ ein Verband, so auch \mathcal{L}_1^a . Ist $\mathcal{L}_2 = (L_2, \wedge, \vee)$ ein Verband, so auch \mathcal{L}_2^p . Zudem ist $(\mathcal{L}_1^a)^p = \mathcal{L}_1$ und $(\mathcal{L}_2^p)^a = \mathcal{L}_2$.*

Beweis. Seien $\mathcal{L}_1 = (L_1, \leq)$ und $\mathcal{L}_2 = (L_2, \wedge, \vee)$ Verbände. Man beweist dann:

1. **\mathcal{L}_1^a ist ein Verband:**

Es ist zu zeigen, dass \wedge_a und \vee_a , wie in Anschluss an Definition 2.40 eingeführt, kommutativ und assoziativ sind und die Absorptionsregeln erfüllen. Kommutativität und Assoziativität sind klar, denn es ist

$$a \wedge_a b = \inf\{a, b\} = b \wedge_a a$$

und

$$a \vee_a b = \sup\{a, b\} = b \vee_a a$$

sowie

$$\begin{aligned} (a \wedge_a b) \wedge_a c &= \inf\{\inf\{a, b\}, c\} = \inf\{a, b, c\} \\ &= \inf\{a, \inf\{b, c\}\} = a \wedge_a (b \wedge_a c) \end{aligned}$$

und

$$\begin{aligned} (a \vee_a b) \vee_a c &= \sup\{\sup\{a, b\}, c\} = \sup\{a, b, c\} \\ &= \sup\{a, \sup\{b, c\}\} = a \vee_a (b \vee_a c). \end{aligned}$$

Um zu zeigen, dass die Absorptionsregeln gelten, muss man sich zunächst klarmachen, dass per Definition von Infimum und Supremum $a \leq b$ äquivalent zu $\inf\{a, b\} = a$ und zu $\sup\{a, b\} = b$ ist. Also sind auch $a \wedge_a b = a$ und $a \vee_a b = b$ äquivalent dazu.

Natürlich ist $a \leq \sup\{a, b\} = a \vee_a b$ und $a \wedge_a b = \inf\{a, b\} \leq a$, deshalb lassen sich die eben hergeleiteten Beziehungen auf a und $a \vee_a b$ sowie auf $a \wedge_a b$ und a anwenden und man erhält

$$a \wedge_a (a \vee_a b) = a$$

sowie

$$(a \wedge_a b) \vee_a a = a.$$

Unter Beachtung der Kommutativität von \vee_a , die schon gezeigt wurde, sind damit auch die Absorptionsregeln erfüllt.

2. \mathcal{L}_2^p ist ein Verband:

Es ist zu zeigen, dass die auf L_2 entsprechend der Nachbemerkung zu Definition 2.41 definierte Relation \leq_p eine Halbordnung, sie also reflexiv, antisymmetrisch und transitiv ist. Auf Grund der Idempotenz von \wedge gilt $a \wedge a = a$, also $a \leq_p a$ für alle $a \in L_2$, womit \leq_p reflexiv ist. Gilt $a \leq_p b$ und $b \leq_p a$ für zwei beliebige Elemente aus L_2 , also $a \wedge b = a$ und $b \wedge a = b$, so folgt wegen der Kommutativität von \wedge sofort $a = b$. Damit ist \leq_p auch antisymmetrisch. Außerdem folgt aus $a \leq_p b$ und $b \leq_p c$, also $a \wedge b = a$ und $b \wedge c = b$, für beliebige $a, b, c \in L_2$ auch

$$a = a \wedge b = a \wedge (b \wedge c) = (a \wedge b) \wedge c = a \wedge c,$$

wobei die Assoziativität von \wedge entscheidend genutzt wurde. Damit ist auch die Transitivität von \leq_p gezeigt und (L_2, \leq_p) ist eine partiell geordnete Menge.

Es bleibt zu zeigen, dass $\inf_p\{a, b\}$ und $\sup_p\{a, b\}$, also Infimum und Supremum bezüglich der Halbordnung \leq_p , für alle $a, b \in L_2$ existieren; es wird sogar $\inf_p\{a, b\} = a \wedge b$ und $\sup_p\{a, b\} = a \vee b$ gezeigt, was erstgenannte Aussage impliziert, da L_2 bezüglich \wedge und \vee abgeschlossen ist:

Aus

$$(a \wedge b) \wedge a = a \wedge (b \wedge a) = a \wedge (a \wedge b) = (a \wedge a) \wedge b = a \wedge b$$

folgt $a \wedge b \leq_p a$ und analog $a \wedge b \leq_p b$. Gilt nun $c \leq_p a$ und $c \leq_p b$, also $c \wedge a = c$ und $c \wedge b = c$, so folgt $c \wedge (a \wedge b) = (c \wedge a) \wedge b = c \wedge b = c$, also $c \leq_p a \wedge b$, und somit ist $\inf_p\{a, b\} = a \wedge b$ für alle $a, b \in L_2$.

Verwendet man $a \geq_p b \Leftrightarrow a \vee b = a$, so erhält man $\sup_p\{a, b\} = a \vee b$ ganz analog.

3. $(\mathcal{L}_1^a)^p = \mathcal{L}_1$ und $(\mathcal{L}_2^p)^a = \mathcal{L}_2$:

Hier ist nachzuweisen, dass die Halbordnung auf L_1 in $(\mathcal{L}_1^a)^p$ dieselbe ist wie in \mathcal{L}_1 und dass die binären Operationen auf L_2 in $(\mathcal{L}_2^p)^a$ dieselben sind wie in \mathcal{L}_2 .

Ersteres folgt leicht ersichtlich aus den entsprechenden Definitionen:

$$\begin{aligned} a \leq b &\Leftrightarrow a \wedge_a b = a \\ &\Leftrightarrow \inf_{a_p}\{a, b\} = a \\ &\Leftrightarrow a \leq_{a_p} b. \end{aligned}$$

Und auch die zweite Aussage folgt aus den entsprechenden Definitionen:

$$\begin{aligned} c \wedge (a \wedge b) = c &\Leftrightarrow c \wedge a = c \text{ und } c \wedge b = c \\ &\Leftrightarrow c \leq_p a \text{ und } c \leq_p b \\ &\Leftrightarrow \inf_p\{a, c\} = c \text{ und } \inf_p\{b, c\} = c \\ &\Leftrightarrow a \wedge_{p_a} c = c \text{ und } b \wedge_{p_a} c = c \\ &\Leftrightarrow (a \wedge_{p_a} b) \wedge_{p_a} c = c, \end{aligned}$$

zusammen mit der Kommutativität von \wedge_{p_a} , und für \vee folgt die Aussage dual.

Insgesamt ist der Satz bewiesen. □

Dementsprechend werden ab jetzt Verbände $\mathcal{L}_1 = (L_1, \leq)$ und \mathcal{L}^a bzw. $\mathcal{L}_2 = (L_2, \wedge, \vee)$ und \mathcal{L}_2^p als äquivalent betrachtet. Außerdem schreibe man anstatt \leq_p einfach \leq und statt \wedge_a und \vee_a einfach \wedge und \vee . Zudem schreibe man $a \in \mathcal{L}_1$ bzw. $b \in \mathcal{L}_2$ für $a \in L_1$ bzw. $b \in L_2$.

Die nun per Definition offensichtlich geltenden Äquivalenzen

$$a \leq b \Leftrightarrow a \wedge b = a \Leftrightarrow a \vee b = b$$

bezeichnet man auch als **Konsistenzgesetze**.

2.2.2 Eigenschaften von Verbänden

In diesem Teilabschnitt werden einige Eigenschaften vorgestellt, nach denen Verbände klassifiziert werden können. Insbesondere werden die wichtigen Begriffe des komplementären und des distributiven Verbandes eingeführt.

Doch zunächst werden verschiedene Endlichkeits- und Beschränkkeitsbegriffe betrachtet.

Definition 2.45. Die Anzahl

$$|\mathcal{L}| := |\{a \in \mathcal{L}\}|$$

der Elemente eines Verbandes \mathcal{L} nennt man **Mächtigkeit** von \mathcal{L} .

Definition 2.46. Ein Verband \mathcal{L} heißt **endlich**, wenn $|\mathcal{L}| < \infty$ ist.

In einem endlichen Verband hat natürlich auch jede Kette eine endliche Mächtigkeit. Dies ist eine schwächere Eigenschaft als die Endlichkeit des Verbandes.

Definition 2.47. Ein Verband \mathcal{L} heißt **von endlicher Länge**, wenn es ein $n < \infty$ gibt, sodass eine maximale Kette von \mathcal{L} maximal n Elemente hat.

Trivialerweise besitzt in einem Verband von endlicher Länge jede Teilmenge ein Infimum und Supremum. Diese Eigenschaft wird folgendermaßen bezeichnet.

Definition 2.48. Ein Verband \mathcal{L} heißt **vollständig**, wenn jede Teilmenge von \mathcal{L} ein Infimum und ein Supremum besitzt.

Ist ein Verband $\mathcal{L} = (L, \leq)$ vollständig, so besitzt insbesondere L Infimum und Supremum. Verbände mit dieser Eigenschaft erhalten auch eine Bezeichnung, auch wenn sie nicht vollständig sind.

Definition 2.49. Ein Verband $\mathcal{L} = (L, \leq)$ heißt **nach unten beschränkt**, wenn L ein Infimum besitzt, und **nach oben beschränkt**, wenn L ein Supremum besitzt.

Ein Verband heißt **beschränkt**, wenn er nach unten und nach oben beschränkt ist.

Diese letzte und schwächste der hier aufgeführten Eigenschaften ist deshalb interessant, da ein Verband ein Nullelement und ein Einselement besitzt, wenn er beschränkt ist. Dies macht die Definition von Komplementen möglich.

Definition 2.50. Sei \mathcal{L} ein beschränkter Verband und $a \in \mathcal{L}$. Ein Element $b \in \mathcal{L}$ heißt **Komplement** von a , wenn $a \wedge b = 0$ und $a \vee b = 1$ gilt.

Damit kommt man zum Begriff des komplementären Verbandes.

Definition 2.51. Ein beschränkter Verband \mathcal{L} heißt **komplementär**, wenn zu jedem Element $a \in \mathcal{L}$ mindestens ein Komplement existiert.

Ein anderer wichtiger Begriff ist der der Distributivität.

Definition 2.52. Ein Verband \mathcal{L} heißt **distributiv**, wenn die Distributivgesetze

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

und

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

für alle $a, b, c \in \mathcal{L}$ gelten.

Auch wenn die Distributivität eines Verbandes, wie üblich, über die Gültigkeit beider Distributivgesetze definiert wurde, genügt die Gültigkeit von

$$a \wedge (b \vee c) \leq (a \wedge b) \vee (a \wedge c),$$

damit ein Verband distributiv ist. Die Ungleichung $a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)$ gilt ohnehin, da $a \wedge b$ und $a \wedge c$ sowohl $\leq a$ als auch in $\leq b \vee c$ sind. Daraus folgt das erste Distributivgesetz; das zweite folgt durch Dualität.

Eine besondere Eigenschaft distributiver Verbände ist die folgende.

Proposition 2.53. *Sei \mathcal{L} ein distributiver Verband und $a \in \mathcal{L}$. Existiert ein Komplement von a , so ist dies eindeutig.*

Beweis. Sei \mathcal{L} ein distributiver Verband und seien $b, b' \in \mathcal{L}$ Komplemente zu einem beliebigen $a \in \mathcal{L}$, d.h. es gilt

$$a \wedge b = a \wedge b' = 0$$

und

$$a \vee b = a \vee b' = 1.$$

Daraus folgt

$$\begin{aligned} b &= b \vee (b \wedge a) \\ &= b \vee (a \wedge b') \\ &= (b \vee a) \wedge (b \vee b') \\ &= (a \vee b') \wedge (b \vee b') \\ &= (a \wedge b) \vee b' \\ &= (a \wedge b') \vee b' \\ &= b' \end{aligned}$$

unter Ausnutzung der Absorptionsregeln, der Kommutativität und der Distributivgesetze. Somit ist das Komplement eines beliebigen Elementes $a \in \mathcal{L}$, falls vorhanden, eindeutig bestimmt. \square

In distributiven Verbänden ist die Existenz eines Komplements nicht zwangsläufig für jedes Element gegeben, gegebenenfalls ist dieses aber eindeutig. Hingegen existiert in komplementären Verbänden zu jedem Element ein Komplement, welches aber nicht zwangsläufig eindeutig ist. Natürlich interessiert man sich auch für Verbände, in denen zu jedem Element ein eindeutiges Komplement existiert.

Definition 2.54. Ein Verband \mathcal{L} heißt **Boolescher Verband**, wenn er komplementär und distributiv ist.

Es werden in 2.58 Beispiele für Boolesche Verbände gegeben. Häufig treten auch Verbände auf, die nicht distributiv sind, sondern die folgende schwächere Eigenschaft haben.

Definition 2.55. Ein Verband \mathcal{L} heißt **modular**, wenn das modulare Gesetz

$$a \leq c \Rightarrow a \vee (b \wedge c) = (a \vee b) \wedge c$$

für alle $a, b, c \in \mathcal{L}$ gilt.

Proposition 2.56. *Ist ein Verband distributiv, so ist er auch modular.*

Beweis. Ist \mathcal{L} distributiv, so gilt insbesondere

$$c \wedge (a \vee b) = (c \wedge a) \vee (c \wedge b)$$

für alle $a, b, c \in \mathcal{L}$. Da $a \leq c$ gleichbedeutend mit $c \wedge a = a \wedge c = a$ ist, folgt in diesem Fall sofort

$$c \wedge (a \vee b) = a \vee (c \wedge b).$$

Durch die Kommutativität von \wedge ist damit das modulare Gesetz erfüllt und \mathcal{L} ist modular. \square

Zum Abschluss dieses Teilabschnittes werden nun noch einige Verbände beispielhaft vorgestellt. Dazu ist es zunächst noch nützlich zu wissen, wann zwei Verbände als im wesentlichen gleich, also isomorph, anzusehen sind.

Definition 2.57. Seien $\mathcal{L} = (L, \leq)$ und $\mathcal{L}' = (L', \leq')$ Verbände. Eine bijektive Abbildung $\phi : L \rightarrow L'$ heißt ein **Verbandsisomorphismus**, wenn für alle $a, b \in L$

$$a \leq b \Leftrightarrow \phi(a) \leq' \phi(b)$$

gilt.

Existiert ein Verbandsisomorphismus $\phi : L \rightarrow L'$, so heißen \mathcal{L} und \mathcal{L}' **isomorph**; man schreibt $\mathcal{L} \cong \mathcal{L}'$.

Man kann sich leicht davon überzeugen, dass die eingeführten Eigenschaften unter einem Verbandsisomorphismus erhalten bleiben.

Es folgen nun die Beispiele, wobei jeder Verband auch grafisch als Hasse-Diagramm vorgestellt wird, wie es allgemein für Halbordnungen üblich ist. Mit den Begriffen aus Kapitel 4 ist das Hasse-Diagramm eines Verbandes $\mathcal{L} = (L, \leq)$ ein Graph mit Knotenmenge L und Kantenmenge E , die durch

$$\{a, b\} \in E \Leftrightarrow a \leq b, a \neq b \text{ und } \nexists c \in L : a \leq c \leq b$$

definiert wird.

Beispiele 2.58.

1. Sei $n \in \mathbb{N}$ und $T(n)$ die Menge der Teiler von n . Dann ist $(T(n), |)$ ein Verband, wobei $|$ die Teilbarkeitsrelation ist. Man kann sich leicht klarmachen, dass $(T(n), |)$ eine partiell

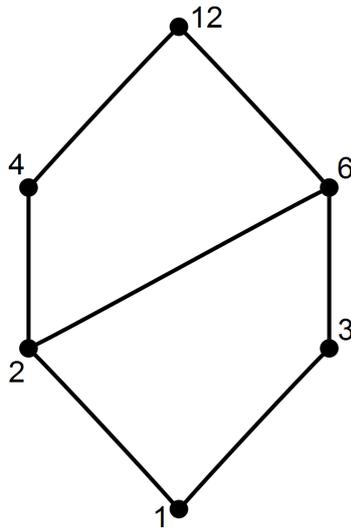


Abbildung 1: Hasse-Diagramm des Teilverbands von 12

geordnete Menge ist und dass für $t_1, t_2 \in T(n)$ insbesondere $\inf\{t_1, t_2\} = ggT(t_1, t_2)$ und $\sup\{t_1, t_2\} = kgV(t_1, t_2)$ ist. Natürlich sind dann $ggT(t_1, t_2), kgV(t_1, t_2) \in T(n)$. Der so definierte Verband wird Teilverband von n genannt.

Ein Teilverband per Definition endlich. Da für ggT und kgV das Distributivgesetz

$$ggT(a, kgV(b, c)) = kgV(ggT(a, b), ggT(a, c))$$

gilt, teilt insbesondere der linke Term den rechten und jeder Teilverband ist distributiv. Die Frage, ob ein Teilverband komplementär ist, lässt sich wie folgt beantworten: Ist n quadratfrei, d.h. in der Primfaktorzerlegung $n = p_1^{k_1} \cdot \dots \cdot p_j^{k_j}$ von n sind alle $k_i = 1$, so ist $b := \frac{n}{a}$ das Komplement zu a . Ist n nicht quadratfrei, so sei a ein Element mit $a^2 \in T(n)$. Wenn für ein $b \in T(n)$ dann $ggT(a, b) = 1$ ist, so ist a kein Teiler von b , und damit ist $kgV(a, b) = a \cdot b \neq n$, da a^2 ein Teiler von n , aber nicht von $a \cdot b$ ist. Damit existiert kein Komplement zu a . Insgesamt ist ein Teilverband also genau dann komplementär (und damit Boolesch), wenn n quadratfrei ist.

2. Sei $K := GF(p^n)$ ein endlicher Körper und $U(K)$ die Menge der Unterkörper von K . Dann ist $(U(K), \subseteq)$ ein Verband, wobei $K_1 \subseteq K_2$ hier für $K_1, K_2 \in U(K)$ bedeuten soll, dass K_1 ein Unterkörper von K_2 ist. Nach Satz 2.34 ist dieser Verband isomorph zum Teilerverband von n ; ein Isomorphismus ist durch

$$\begin{aligned}\phi : T(n) &\rightarrow U(GF(p^n)) \\ k &\mapsto GF(p^k)\end{aligned}$$

gegeben. Die Eigenschaften dieses Verbandes entsprechen damit denen des isomorphen Teilerverbandes.

3. Die Menge der natürlichen Zahlen \mathbb{N} ist mit der gewöhnlichen Ordnung \leq ein Verband. Dieser Verband (\mathbb{N}, \leq) ist nicht nach oben beschränkt, also auch nicht beschränkt. Damit



Abbildung 2: Hasse-Diagramm des Verbandes (\mathbb{N}, \leq)

kann dieser Verband auch nicht komplementär sein, aber er ist distributiv, da für \min und \max das Distributivgesetz

$$\min(a, \max(b, c)) = \max(\min(a, b), \min(a, c))$$

gilt und der hier betrachtete Verband äquivalent zu (\mathbb{N}, \min, \max) ist.

4. Sei M eine Menge und $\mathcal{P}(M)$ die Potenzmenge von M . Dann ist $(\mathcal{P}(M), \subseteq)$ ein Verband, wobei \subseteq die übliche Enthaltenseinsrelation ist. Ein solcher Teilmengenverband ist, unabhängig von der Menge M , distributiv, denn für \cap und \cup gilt das Distributivgesetz

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

und der betrachtete Verband ist äquivalent zu $(\mathcal{P}(M), \cap, \cup)$. Außerdem ist der Teilmengenverband von M auch komplementär, da durch $M \setminus A$ das (eindeutige) Komplement zu $A \in \mathcal{P}(M)$ gegeben ist. Es handelt sich dann also um einen Booleschen Verband.

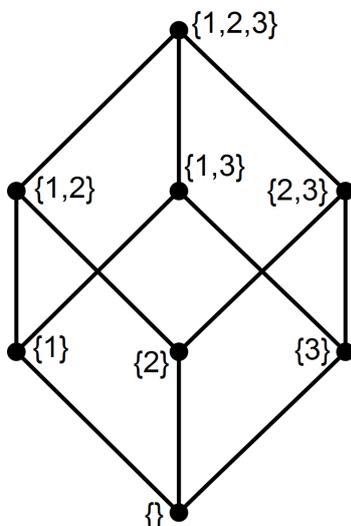


Abbildung 3: Hasse-Diagramm des Teilmengenverbands von $\{1, 2, 3\}$

5. Sei K ein Körper und $L(n, K)$ die Menge aller Unterräume eines n -dimensionalen Vektorraums ($n < \infty$). Dann ist $\mathcal{L}(n, K) := (L(n, K), \cap, +)$ ein Verband, wobei die Verknüpfung $+$ für $U_1, U_2 \in L(n, K)$ durch

$$U_1 + U_2 := \{u_1 + u_2 \mid u_1 \in U_1, u_2 \in U_2\}$$

definiert ist und \cap der übliche Schnitt zweier Vektorräume ist. Das Hasse-Diagramm

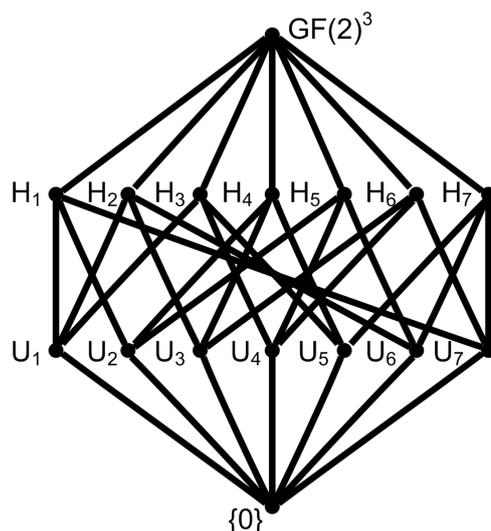


Abbildung 4: Hasse-Diagramm des linearen Verbands $\mathcal{L}(3, GF(2))$

eines solchen Verbands mit $n = 3$ und $K = GF(2)$ ist in Abbildung 4 zu sehen, wenn man die 1-dimensionalen Unterräume U_1, \dots, U_7 und die Hyperebenen H_1, \dots, H_7 dementsprechend durchnummeriert.

Die Eigenschaften dieser letzten Verbände werden im Folgenden analysiert.

2.2.3 Lineare Verbände

Zuerst wird definiert:

Definition 2.59. Der Verband $\mathcal{L}(n, K)$ heißt n -dimensionaler **linearer Verband** über K .

Es ist sofort klar, dass lineare Verbände von endlicher Länge sind, denn eine maximale Kette besteht aus einem Unterraum jeder Dimension, d.h. n Elementen. Ist K sogar ein endlicher Körper, so ist der lineare Verband über diesem natürlich auch endlich.

Im Verlauf dieser Arbeit wird besonders die folgende Eigenschaft linearer Verbände noch von Relevanz sein.

Proposition 2.60. *Lineare Verbände sind komplementär.*

Beweis. Sei $U_1 \in \mathcal{L}(n, K)$. Man betrachte die Menge

$$\{U \in \mathcal{L}(n, K) \mid U_1 \cap U = 0\}$$

der Unterräume, deren Schnitt mit U_1 das Nullelement ist. Diese ist auf Grund der Verbands-eigenschaften halbgeordnet und besitzt eine obere Schranke, weshalb sie nach dem Lemma von Zorn einen maximalen Unterraum enthält; sei dies U_2 . Ist nun $v \in K^n$ ein beliebiger Vektor, so liegt er natürlich in $U_1 + U_2$, wenn er in U_2 liegt, also sei $v \notin U_2$ angenommen. Dann muss $U_1 \cap (U_2 + Kv) \neq 0$ sein, da U_2 bereits der größte Unterraum mit $U_1 \cap U_2 = 0$ ist. Somit existieren $u_1 \in U_1$, $u_2 \in U_2$, $\alpha \in K \setminus \{0\}$ mit $u_1 = u_2 + \alpha v \neq 0$.

Damit folgt

$$v = \frac{1}{\alpha}(u_1 - u_2) \in U_1 + U_2$$

und es ist $U_1 + U_2 = K^n$ gezeigt, womit U_2 ein Komplement zu U_1 ist. Da U_2 beliebig war, ist $\mathcal{L}(n, K)$ komplementär. \square

Beispiel 2.61. Man betrachte den Unterraum $U := \left\langle \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \right\rangle$ im Verband $\mathcal{L}(3, GF(2))$,

wobei mit $\langle \cdot \rangle$ ab jetzt das lineare Erzeugnis eines Punktes oder einer Menge von Punkten notiert wird. Dann sind $\left\langle \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\rangle$, $\left\langle \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\rangle$ und $\left\langle \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \right\rangle$ die Komplemente von U . Dies sind genau die 2-dimensionalen Unterräume von $GF(2)^3$, die U nicht enthalten.

Wie man gesehen hat, ist das Komplement eines Elementes von $\mathcal{L}(3, GF(2))$ nicht eindeutig bestimmt, also können lineare Verbände im Allgemeinen nicht distributiv sein. Es lässt sich aber die nach 2.56 schwächere Eigenschaft der Modularität nachweisen.

Proposition 2.62. *Lineare Verbände sind modular.*

Beweis. Sei $U_1 \subseteq U_3$. Dann gilt:

- $U_1 + (U_2 \cap U_3) \subseteq (U_1 + U_2) \cap U_3$:
Da $U_1 \subseteq U_3$ ist, gilt $U_1 + (U_2 \cap U_3) = (U_1 \cap U_3) + (U_2 \cap U_3) \subseteq (U_1 + U_2) \cap U_3$.
- $(U_1 + U_2) \cap U_3 \subseteq U_1 + (U_2 \cap U_3)$:
Sei $w \in (U_1 + U_2) \cap U_3$ mit $w = u_1 + u_2$, $u_1 \in U_1$ und $u_2 \in U_2$. Dann sind $w, u_1 \in U_3$, also muss auch $u_2 = w - u_1 \in U_3$ sein. Damit ist $w = u_1 + u_2 \in U_1 + (U_2 \cap U_3)$.

Zusammen folgt $U_1 + (U_2 \cap U_3) = (U_1 + U_2) \cap U_3$. □

Die linearen Verbände wurden somit anhand der im letzten Teilabschnitt eingeführten Eigenschaften klassifiziert. Noch nicht beantwortet wurde die Frage nach der Mächtigkeit solcher Verbände. Klar ist, dass ein linearer Verband über einem unendlichen Körper für $n \geq 2$ auch unendliche Mächtigkeit hat. Mit der Mächtigkeit linearer Verbände über endlichen Körpern befasst sich das nächste Kapitel.

3 Gauß'sche Koeffizienten und Galoiszahlen

Wenn man die Mächtigkeit des n -dimensionalen linearen Verbandes über einem endlichen Körper bestimmen möchte, so wird man sich zunächst überlegen, wie viele k -dimensionale Unterräume in diesem Verband für jedes $k \in \{1, \dots, n\}$ vorhanden sind, womit man zu den Gauß'schen Koeffizienten kommt. Anschließend wird man die Teilergebnisse über diese k aufsummieren und erhält die so bezeichneten Galoiszahlen.

Es folgt nun eine kombinatorische Einführung in diese Thematik, wie sie auch in [1], S. 76-79 und S. 94, oder [13] erfolgt. Danach soll das kombinatorische Problem, das in dieser Arbeit behandelt wird, formuliert werden.

3.1 Kombinatorische Definition

Definition 3.1. Man betrachte $GF(q)^n$, den n -dimensionaler Vektorraum über dem endlichen Körper mit q Elementen. Dann schreibt man

$$\binom{n}{k}_q$$

für die Anzahl an verschiedenen k -dimensionalen Unterräumen von $GF(q)^n$ für $k \in \{1, \dots, n\}$. Allgemein, wie in [1], S. 69, werden die Zahlen $\binom{n}{k}_q$ als **Gauß'sche Koeffizienten** bezeichnet.

Der folgende Satz gibt an, wie man Gauß'sche Koeffizienten berechnen kann.

Satz 3.2. Für $n \in \mathbb{N}$ und $k \in \{1, \dots, n\}$ gilt

$$\binom{n}{k}_q = \frac{\prod_{l=0}^{k-1} (q^{n-l} - 1)}{\prod_{l=0}^{k-1} (q^{k-l} - 1)}.$$

Beweis. Zunächst wird die Anzahl $U_{n,k}$ an geordneten k -Tupeln von linear unabhängigen Vektoren in $GF(q)^n$ bestimmt. Für die erste Komponente eines solchen Tupels kommen alle $q^n - 1$ Vektoren $v_1 \neq 0$ in Frage. Der Vektor v_1 spannt einen 1-dimensionalen Unterraum auf, welcher dementsprechend q Vektoren enthält. Für die zweite Komponente des Tupels bleiben damit die $q^n - q$ von v_1 linear unabhängigen Vektoren übrig. Wählt man $v_2 \notin \langle v_1 \rangle$ als zweiten Vektor, so spannen v_1 und v_2 einen 2-dimensionalen Unterraum auf, welcher dementsprechend q^2 Vektoren enthält. Dies kann man so fortsetzen; für die l -te Komponente kommen jeweils $q^n - q^{l-1} = q^{l-1}(q^{n-(l-1)} - 1)$ in Frage. Insgesamt erhält man

$$U_{n,k} = \prod_{l=1}^k q^{l-1} (q^{n-(l-1)} - 1).$$

Jedes dieser Tupel spannt einen k -dimensionalen Unterraum auf. Jeder k -dimensionale Unterraum hat aber $U_{k,k}$ geordnete Basen, also gilt für die Anzahl $\binom{n}{k}_q$ an k -dimensionalen

Unterräumen

$$\binom{n}{k}_q = \frac{U_{n,k}}{U_{k,k}} = \frac{\prod_{l=1}^k q^{l-1}(q^{n-(l-1)} - 1)}{\prod_{l=1}^k q^{l-1}(q^{k-(l-1)} - 1)} = \frac{\prod_{l=1}^k (q^{n-(l-1)} - 1)}{\prod_{l=1}^k (q^{k-(l-1)} - 1)} = \frac{\prod_{l=0}^{k-1} (q^{n-l} - 1)}{\prod_{l=0}^{k-1} (q^{k-l} - 1)}.$$

□

Gauß'sche Koeffizienten für ein festes $n \in \mathbb{N}$ haben bestimmte Eigenschaften, die man auch von anderen endlichen Zahlenfolgen kennt. Diese beschreibt die folgende Proposition.

Proposition 3.3. *Sei $n \in \mathbb{N}$. Dann gilt für die Gauß'schen Koeffizienten*

$$\binom{n}{k}_q = \binom{n}{n-k}_q, \quad 0 \leq k \leq n \text{ und}$$

$$\binom{n}{0}_q < \binom{n}{1}_q < \cdots < \binom{n}{\lfloor \frac{n}{2} \rfloor}_q = \binom{n}{\lceil \frac{n}{2} \rceil}_q > \cdots > \binom{n}{n-1}_q > \binom{n}{n}_q.$$

Beweis. Durch einfache Umformungen erhält man

$$\begin{aligned} \binom{n}{k}_q &= \frac{\prod_{l=0}^{k-1} (q^{n-l} - 1)}{\prod_{l=0}^{k-1} (q^{k-l} - 1)} \\ &= \frac{\prod_{l=0}^{n-k-1} (q^{n-l} - 1) \prod_{l=n-k}^{k-1} (q^{n-l} - 1)}{\prod_{l=0}^{2k-n-1} (q^{k-l} - 1) \prod_{l=2k-n}^{k-1} (q^{k-l} - 1)} \\ &= \frac{\prod_{l=0}^{n-k-1} (q^{n-l} - 1) \prod_{l=0}^{2k-n-1} (q^{k-l} - 1)}{\prod_{l=0}^{2k-n-1} (q^{k-l} - 1) \prod_{l=0}^{n-k-1} (q^{n-k-l} - 1)} \\ &= \frac{\prod_{l=0}^{n-k-1} (q^{n-l} - 1)}{\prod_{l=0}^{n-k-1} (q^{n-k-l} - 1)} \\ &= \binom{n}{n-k}_q \end{aligned}$$

und

$$\begin{aligned}
 \binom{n}{k+1}_q &= \frac{\prod_{l=0}^k (q^{n-l} - 1)}{\prod_{l=0}^k (q^{k+1-l} - 1)} \\
 &= \frac{(q^{n-k} - 1) \prod_{l=0}^{k-1} (q^{n-l} - 1)}{(q^{k+1} - 1) \prod_{l=1}^k (q^{k+1-l} - 1)} \\
 &= \frac{q^{n-k} - 1}{q^{k+1} - 1} \frac{\prod_{l=0}^{k-1} (q^{n-l} - 1)}{\prod_{l=0}^{k-1} (q^{k-l} - 1)} \\
 &= \frac{(q^{n-k} - 1)}{(q^{k+1} - 1)} \binom{n}{k}_q.
 \end{aligned}$$

Also ist

$$\binom{n}{k}_q < \binom{n}{k+1}_q$$

genau dann, wenn $\frac{(q^{n-k}-1)}{(q^{k+1}-1)} > 1$ ist, also $q^{n-2k-1} < 1$. Dies ist genau dann der Fall, wenn $n - 2k - 1 < 0$ ist, was gleichbedeutend mit $k \leq \lfloor \frac{n}{2} \rfloor$ ist, da $n \in \mathbb{N}$ ist. Ansonsten gilt $\frac{(q^{n-k}-1)}{(q^{k+1}-1)} < 1$, womit die Aussage bewiesen ist. \square

Insbesondere ist die Folge $(\binom{n}{k}_q)_{k \in \{0, \dots, n\}}$ also unimodal (eine endliche Folge (a_n) heißt unimodal, wenn es ein k gibt mit $a_1 \leq a_2 \leq \dots \leq a_k$ und $a_k \geq a_{k+1} \geq \dots \geq a_n$).

Wie man sehen konnte, haben die Gauß'schen Koeffizienten Eigenschaften, die man auch von den Binomialkoeffizienten kennt. Tatsächlich kann man zeigen, dass

$$\lim_{q \rightarrow 1} \binom{n}{k}_q = \binom{n}{k}$$

ist, wenn man $\binom{n}{k}_q$ als Funktion $\binom{n}{k}_q :]1, \infty[\rightarrow \mathbb{R}$ mit der Abbildungsvorschrift aus Satz 3.2 auffasst (siehe dazu [13], S. 63f.). In diesem Sinne verallgemeinern die Gauß'schen Koeffizienten die Binomialkoeffizienten. Daher kommt auch die analoge Schreibweise.

Nachdem die geschlossene Form für die Gauß'schen Koeffizienten schon bestimmt wurde, wird jetzt eine Rekursion gesucht. Bekannt ist ja, dass für die Binomialkoeffizienten $\binom{n}{0} = 1$ und

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

für $1 \leq k \leq n$ gilt. Die Rekursion für Gauß'sche Koeffizienten ist ähnlich.

Satz 3.4. Für $n \in \mathbb{N}$ gilt

$$\binom{n}{0}_q = 1 \text{ und}$$

$$\binom{n}{k}_q = \binom{n-1}{k-1}_q + q^k \binom{n-1}{k}_q$$

für alle $k \in \{1, \dots, n\}$.

Beweis. Wieder ergibt sich dies durch einige Umformungen:

$$\begin{aligned} \binom{n}{k}_q &= \frac{\prod_{l=0}^{k-1} (q^{n-l} - 1)}{\prod_{l=0}^{k-1} (q^{k-l} - 1)} \\ &= \frac{(q^n - 1) \prod_{l=0}^{k-2} (q^{n-l-1} - 1)}{\prod_{l=0}^{k-1} (q^{k-l} - 1)} \\ &= \frac{(q^k - 1) \prod_{l=0}^{k-2} (q^{n-l-1} - 1) + q^k (q^{n-k} - 1) \prod_{l=0}^{k-2} (q^{n-l-1} - 1)}{\prod_{l=0}^{k-1} (q^{k-l} - 1)} \\ &= \frac{(q^k - 1) \prod_{l=0}^{k-2} (q^{n-l-1} - 1) + q^k \prod_{l=0}^{k-1} (q^{n-l-1} - 1)}{\prod_{l=0}^{k-1} (q^{k-l} - 1)} \\ &= \frac{(q^k - 1) \prod_{l=0}^{k-2} (q^{n-l-1} - 1)}{\prod_{l=0}^{k-1} (q^{k-l} - 1)} + \frac{q^k \prod_{l=0}^{k-1} (q^{n-l-1} - 1)}{\prod_{l=0}^{k-1} (q^{k-l} - 1)} \\ &= \frac{\prod_{l=0}^{k-2} (q^{n-l-1} - 1)}{\prod_{l=1}^{k-1} (q^{k-l} - 1)} + \frac{q^k \prod_{l=0}^{k-1} (q^{n-l-1} - 1)}{\prod_{l=0}^{k-1} (q^{k-l} - 1)} \\ &= \frac{\prod_{l=0}^{k-2} (q^{n-l-1} - 1)}{\prod_{l=0}^{k-2} (q^{k-l-1} - 1)} + \frac{q^k \prod_{l=0}^{k-1} (q^{n-l-1} - 1)}{\prod_{l=0}^{k-1} (q^{k-l} - 1)} \\ &= \binom{n-1}{k-1}_q + q^k \binom{n-1}{k}_q. \end{aligned}$$

□

Damit ist die Rekursion für die Gauß'schen Koeffizienten gefunden und es werden die Galoiszahlen entsprechend [1], S. 69, vorgestellt.

Definition 3.5. Sei $\mathcal{L}(n, GF(q))$ der n -dimensionale lineare Verband über dem endlichen Körper mit q Elementen. Dann schreibt man

$$G_{n,q} := |\mathcal{L}(n, GF(q))| = \sum_{k=0}^n \binom{n}{k}_q$$

für die Mächtigkeit von $\mathcal{L}(n, GF(q))$.

Allgemein werden die Zahlen $G_{n,q}$ als **Galoiszahlen** bezeichnet.

Wieder soll auch eine Rekursion gefunden werden. Sieht man die Gauß'schen Koeffizienten als Verallgemeinerung der Binomialkoeffizienten an, so sollte man die Galoiszahlen konsequenterweise als Verallgemeinerung der Zweierpotenzen ansehen, da ja

$$\sum_{k=0}^n \binom{n}{k} = 2^n$$

gilt. Die Rekursion der Zweierpotenzen ist trivialerweise durch

$$2^n = 2 \cdot 2^{n-1}$$

gegeben. Die Rekursion der Galoiszahlen ist ähnlich in dem Sinne, dass sich

$$G_{n,q} = 2G_{n-1,q}$$

ergibt, wenn man $q = 1$ einsetzt, wie der folgende Satz zeigt.

Satz 3.6. Für alle $q \in \mathbb{N}$, $n \in \mathbb{N}_0$ ist durch

$$G_{0,q} = 1, G_{1,q} = 2 \text{ und} \\ G_{n,q} = 2G_{n-1,q} + (q^{n-1} - 1)G_{n-2,q}, \text{ falls } n \geq 2$$

eine Rekursionsformel gegeben.

Beweis. Zunächst wird gezeigt, dass bei gegebenem $n \geq 2$ und $0 \leq k \leq n - 2$ die Beziehung

$$(q^{k+1} - 1) \binom{n-1}{k+1}_q = (q^{n-1} - 1) \binom{n-2}{k}_q$$

gilt:

- **1. Fall:** $k = 0$:

Es ist

$$(q^{k+1} - 1) \binom{n-1}{k+1}_q = (q-1) \frac{q^{n-1} - 1}{q-1} = q^{n-1} - 1 = (q^{n-1} - 1) \binom{n-2}{k}_q.$$

• **2. Fall:** $k \geq 1$:

Dann ist $n \geq 3$ und damit

$$\begin{aligned}
 (q^{k+1} - 1) \binom{n-1}{k+1}_q &= (q^{k+1} - 1) \frac{\prod_{l=0}^k (q^{n-1-l} - 1)}{\prod_{l=0}^k (q^{k+1-l} - 1)} \\
 &= (q^{k+1} - 1) \frac{(q^{n-1} - 1) \prod_{l=1}^k (q^{n-1-l} - 1)}{(q^{k+1} - 1) \prod_{l=1}^k (q^{k+1-l} - 1)} \\
 &= (q^{n-1} - 1) \frac{\prod_{l=0}^{k-1} (q^{n-2-l} - 1)}{\prod_{l=0}^{k-1} (q^{k-l} - 1)} \\
 &= (q^{n-1} - 1) \binom{n-2}{k}_q.
 \end{aligned}$$

Da $\mathcal{L}(0, K)$ nur aus dem Nullraum besteht und $\mathcal{L}(1, K)$ aus dem Nullraum und K , ist $G_{0,q} = 1$ und $G_{1,q} = 2$. Für $\mathcal{L}(0, K)$, $n \geq 2$ gilt schließlich

$$\begin{aligned}
 G_{n,q} &= \sum_{k=0}^n \binom{n}{k}_q = \binom{n}{0}_q + \sum_{k=1}^{n-1} \binom{n}{k}_q + \binom{n}{n}_q \\
 &= 1 + \sum_{k=1}^{n-1} \left(\binom{n-1}{k-1}_q + q^k \binom{n-1}{k}_q \right) + 1 \\
 &= 1 + \sum_{k=1}^{n-1} \left(\binom{n-1}{k-1}_q + (q^k - 1) \binom{n-1}{k}_q + \binom{n-1}{k}_q \right) + 1 \\
 &= \binom{n-1}{n-1}_q + \sum_{k=0}^{n-2} \binom{n-1}{k}_q + \binom{n-1}{0}_q + \sum_{k=1}^{n-1} \binom{n-1}{k}_q + \sum_{k=1}^{n-1} (q^k - 1) \binom{n-1}{k}_q \\
 &= 2 \sum_{k=0}^{n-1} \binom{n-1}{k}_q + \sum_{k=0}^{n-2} (q^{k+1} - 1) \binom{n-1}{k+1}_q \\
 &= 2 \sum_{k=0}^{n-1} \binom{n-1}{k}_q + \sum_{k=0}^{n-2} (q^{n-1} - 1) \binom{n-2}{k}_q \\
 &= 2G_{n-1,q} + (q^{n-1} - 1)G_{n-2,q},
 \end{aligned}$$

womit der Beweis vollständig ist. □

Im nächsten Abschnitt wird nun versucht, dieser Rekursion eine bestimmte geometrische Interpretation zu verleihen.

3.2 Versuch einer geometrischen Interpretation

Es soll nun versucht werden, die soeben bewiesene Rekursionsformel für Galoiszahlen geometrisch zu interpretieren, wie es Faigle vorgeschlagen hat [4]. Um zu verstehen, was mit so einer Interpretation gemeint ist, ist das nächste Beispiel hilfreich. Dabei bezieht sich dieses auf Mengen, weshalb von einer mengentheoretischen Interpretation die Rede ist.

Beispiel 3.7. Für die Binomialkoeffizienten $\binom{n}{k}$ gilt bekanntermaßen die Rekursion

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

für $n \in \mathbb{N}$ und $k \in \{0, \dots, n\}$.

Diese lässt sich folgendermaßen geometrisch interpretieren: $\binom{n}{k}$ ist ja die Anzahl an k -Teilmengen einer n -elementigen Menge N . Sei jetzt $a \in N$ ein beliebiges, aber fest ausgewähltes Element. Dann kann man die k -Teilmengen von N in zwei Klassen partitionieren: Die eine besteht aus allen k -Teilmengen, die a enthalten, die andere aus allen, die a nicht enthalten. Jetzt kann man die Anzahl der k -Teilmengen der beiden Klassen zählen. In jeder k -Teilmenge der ersten Klasse ist a enthalten, also sind dies genau die $(k-1)$ -Teilmengen von $N \setminus \{a\}$ vereinigt mit a , d.h. $\binom{n-1}{k-1}$ Mengen. In jeder k -Teilmenge der zweiten Klasse ist a nicht enthalten, also sind dies genau die k -Teilmengen von $N \setminus \{a\}$, d.h. $\binom{n-1}{k}$ Mengen. Man sieht also, dass die Rekursionsformel eine mengentheoretische Interpretation besitzt.

Analog zu diesem Beispiel könnte man also versuchen, die Rekursionsformel für Galoiszahlen

$$G_{n,q} = 2G_{n-1,q} + (q^{n-1} - 1)G_{n-2,q}$$

für $n \geq 3$ zu interpretieren. Dementsprechend müsste sich ein Verband $\mathcal{L}(n, GF(q))$ in zwei Teilverbände isomorph zu $\mathcal{L}(n-1, GF(q))$ und $q^{n-1} - 1$ Teilverbände isomorph zu $\mathcal{L}(n-2, GF(q))$ disjunkt zerlegen lassen, damit eine geometrische Interpretation existiert. Von vornherein ist klar, dass es sich bei diesen Teilverbänden um den Filter eines 1-dimensionalen Unterraums, das Ideal einer Hyperebene und $q^{n-1} - 1$ Intervallen aus 1-dimensionalen Unterräumen und Hyperebenen handeln muss, da andere Konstellationen nicht ohne Überschneidungen möglich sind.

Dementsprechend definiert man eine Intervallzerlegung.

Definition 3.8. Eine Menge

$$\{U_0, U_1, \dots, U_{q^{n-1}-1}, H_0, H_1, \dots, H_{q^{n-1}-1}\}$$

aus 1-dimensionalen Unterräumen $U_0, U_1, \dots, U_{q^{n-1}-1}$ und Hyperebenen $H_0, H_1, \dots, H_{q^{n-1}-1}$ heißt **Intervallzerlegung** des linearen Verbandes $\mathcal{L}(n, GF(q))$, $n \geq 3$ genau dann, wenn

$$\mathcal{L}(n, GF(q)) = \text{Filter}(U_0) \cup \text{Ideal}(H_0) \cup [U_1, H_1] \cup \dots \cup [U_{q^{n-1}-1}, H_{q^{n-1}-1}]$$

gilt.

Die Disjunktheit der Mengen muss hier nicht explizit gefordert werden, denn wären diese nicht alle disjunkt, so enthielte ihre Vereinigung weniger Elemente als der lineare Verband und die Gleichheit könnte nicht gelten.

Zur Illustration dient eine Intervallzerlegung von $\mathcal{L}(3, GF(3))$.

Beispiele 3.9. Es sei $U' := \left\langle \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \right\rangle$ und $H' := \left\langle \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\rangle$. Zusammen mit den restlichen Intervallen

$$\begin{aligned} & \left[\left\langle \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} \right\rangle \right], \left[\left\langle \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \right\rangle \right], \\ & \left[\left\langle \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \right\rangle \right], \left[\left\langle \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix} \right\rangle \right], \\ & \left[\left\langle \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \right\rangle \right], \left[\left\langle \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix} \right\rangle \right], \\ & \left[\left\langle \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \right\rangle \right], \left[\left\langle \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} \right\rangle \right] \end{aligned}$$

liegt dann eine Intervallzerlegung von $\mathcal{L}(3, GF(3))$ vor.

Die nächste Proposition beschreibt die Struktur der Unterräume.

Proposition 3.10. *Sei U ein k -dimensionaler Unterraum in $\mathcal{L}(n, GF(q))$. Dann hat U genau $\binom{k}{l}_q$ l -dimensionale Unterräume und $\binom{n-k}{m-k}_q$ m -dimensionale Oberräume in $\mathcal{L}(n, GF(q))$.*

Beweis. Die l -dimensionalen Unterräume von U sind genau die l -dimensionalen Unterräume in $\text{Ideal}(U)$. Da U selbst ein k -dimensionaler Vektorraum ist, ist $\text{Ideal}(U) \cong \mathcal{L}(k, GF(q))$ und nach Definition 3.1 gibt es $\binom{k}{l}_q$ l -dimensionale Unterräume in $\mathcal{L}(k, GF(q))$.

Die m -dimensionalen Oberräume von U sind genau die m -dimensionalen Unterräume in $\text{Filter}(U)$. Nun ist $\text{Filter}(U) \cong \mathcal{L}(n-k, GF(q))$ und nach Definition 3.1 gibt es $\binom{n-k}{m-k}_q$ m -dimensionale Unterräume in $\mathcal{L}(n-k, GF(q))$. \square

Jetzt erhält man Aufschluss darüber, wie U' und H' zu wählen sind.

Proposition 3.11. *Sei U ein 1-dimensionaler Unterraum und H eine Hyperebene in $\mathcal{L}(n, GF(q))$. Genau dann sind $\text{Filter}(U)$ und $\text{Ideal}(H)$ disjunkt, wenn U und H komplementär sind.*

Beweis. Seien U und H nicht komplementär. Dann gilt $U \cap H \neq \{0\}$ oder $U + H \neq GF(q)^n$. Ist $U + H \neq GF(q)^n$, so müssen die Vektoren aus U und H linear abhängig sein, denn sonst würden sie $GF(q)^n$ aufspannen. Damit liegt U in H und es ist auch hier $U \cap H \neq \{0\}$. Damit folgt sofort $U \in \text{Filter}(U) \cap \text{Ideal}(H)$.

Seien nun U und H komplementär. Angenommen, $\text{Filter}(U)$ und $\text{Ideal}(H)$ sind nicht disjunkt und es ist $V \in \text{Filter}(U) \cap \text{Ideal}(H)$. Dann gilt nach Definition von Filter und Ideal $U \subseteq V \subseteq H$, womit $U \cap H = U \neq \{0\}$ ist, ein Widerspruch, da U und H komplementär sind. \square

Damit ist klar, dass es unproblematisch ist, bei der Intervallzerlegung eines linearen Verbandes U_0 und H_0 auszuwählen: Nach Proposition 3.10 macht es prinzipiell keinen Unterschied, welcher eindimensionale Unterraum als U_0 gewählt wird, und nach Proposition 3.11 ist H_0 komplementär dazu zu wählen. Da nach Proposition 2.60 lineare Verbände komplementär sind, existiert eine solche Hyperebene.

Diese ist jedoch im Allgemeinen nicht eindeutig bestimmt (siehe Beispiel 2.61). In der nächsten Proposition wird die vorliegende Situation deshalb noch etwas genauer quantifiziert und man sieht, dass die Wahl der komplementären Hyperebene keine Rolle spielt.

Proposition 3.12. *Sei U ein 1-dimensionaler Unterraum und H eine dazu komplementäre Hyperebene in $\mathcal{L}(n, GF(q))$, außerdem $1 \leq k_1 < k_2 \leq n - 1$. Dann gibt es*

$$\binom{n}{k_1}_q - \binom{n-1}{k_1-1}_q - \binom{n-1}{k_1}_q \text{ bzw. } \binom{n}{k_2}_q - \binom{n-1}{k_2-1}_q - \binom{n-1}{k_2}_q$$

k_1 - bzw. k_2 -dimensionale Unterräume in $\mathcal{L}(n, GF(q))$, die nicht in $\text{Filter}(U) \cup \text{Ideal}(H)$ liegen. Jeder dieser k_1 - bzw. k_2 -dimensionalen Unterräume liegt in bzw. über

$$\binom{n-k_1}{k_2-k_1}_q - \binom{n-k_1-1}{k_2-k_1-1}_q \text{ bzw. } \binom{k_2}{k_1}_q - \binom{k_2-1}{k_1}_q$$

k_2 - bzw. k_1 -dimensionalen Unterräumen, die nicht in $\text{Filter}(U) \cup \text{Ideal}(H)$ liegen.

Beweis. Per Definition gibt es $\binom{n}{k_1}_q$ k_1 -dimensionale Unterräume in $\mathcal{L}(n, GF(q))$. Davon sind diese zu subtrahieren, die in $\text{Filter}(U)$ oder $\text{Ideal}(H)$ liegen. Da $\text{Filter}(U) \cong \mathcal{L}(n-1, GF(q))$ und $\text{Ideal}(H) \cong \mathcal{L}(n-1, GF(q))$ ist und die gesuchten Unterräume genau die (k_1-1) -dimensionalen Unterräume in $\text{Filter}(U)$ und die k_1 -dimensionalen Unterräume in $\text{Ideal}(H)$ sind, ist die Anzahl der zu subtrahierenden Unterräume genau $\binom{n-1}{k_1-1}_q + \binom{n-1}{k_1}_q$. Für k_2 gilt dies analog.

Sei nun U_{k_1} ein k_1 -dimensionaler Unterraum des Verbandes, der nicht in $\text{Filter}(U) \cup \text{Ideal}(H)$ liegt. Dann ist U_{k_1} genau in den Unterräumen seines Filters enthalten, und dieser ist isomorph zu $\mathcal{L}(n-k_1, GF(q))$. Die k_2 -dimensionalen Unterräume in $\mathcal{L}(n, GF(q))$, die in diesem Filter liegen, sind genau die (k_2-k_1) -dimensionalen Unterräume von $\text{Filter}(U_{k_1})$, und deren Anzahl ist somit $\binom{n-k_1}{k_2-k_1}_q$. Davon sind nun diese zu subtrahieren, die auch in $\text{Filter}(U)$ liegen (in $\text{Ideal}(H)$ liegt keiner, da sonst auch $U_{k_1} \in \text{Ideal}(H)$ wäre). Da U nicht in U_{k_1} liegt, ist $U+U_{k_1}$ ein (k_1+1) -dimensionaler Unterraum, und gesucht sind die k_2 -dimensionalen Unterräume, die in $\text{Filter}(U+U_{k_1})$ liegen, die also bezüglich dieses Filters (k_2-k_1-1) -dimensional sind. Da $\text{Filter}(U+U_{k_1}) \cong \mathcal{L}(n-k_1-1, GF(q))$ ist, sind genau $\binom{n-k_1-1}{k_2-k_1-1}_q$ Unterräume zu subtrahieren.

Die letzte Aussage wird analog (dual dazu) bewiesen, soll aber ausformuliert werden. Sei also U_{k_2} ein k_2 -dimensionaler Unterraum des Verbandes, der nicht in $\text{Filter}(U) \cup \text{Ideal}(H)$ liegt. Dann enthält U_{k_2} genau die Unterräume seines Ideals, und dieses ist isomorph zu $\mathcal{L}(k_2, GF(q))$. Die k_1 -dimensionalen Unterräume in $\mathcal{L}(n, GF(q))$, die in diesem Ideal liegen, sind auch genau die k_1 -dimensionalen Unterräume von $\text{Ideal}(U_{k_2})$, und deren Anzahl ist somit $\binom{k_2}{k_1}_q$. Davon sind diese zu subtrahieren, die auch in $\text{Ideal}(H)$ liegen (in $\text{Filter}(U)$ liegt keiner, da sonst auch $U_{k_2} \in \text{Filter}(U)$ wäre). Da U_{k_2} nicht in H liegt, ist $U_{k_2} \cap H$ ein (k_2-1) -dimensionaler Unterraum, und gesucht sind die k_1 -dimensionalen Unterräume, die in $\text{Ideal}(U_{k_2} \cap H)$ liegen, welche auch bezüglich dieses Ideals k_1 -dimensional sind. Da $\text{Ideal}(U_{k_2} \cap H) \cong \mathcal{L}(k_2-1, GF(q))$ ist, sind genau $\binom{k_2-1}{k_1}_q$ Unterräume zu subtrahieren. \square

Offensichtlich war der Beweis nicht von der Auswahl des 1-dimensionalen Unterraums und der komplementären Hyperebene abhängig.

Somit reduziert sich die Frage nach einer Intervallzerlegung eines linearen Verbandes auf die Bestimmung der restlichen Intervalle

$$[U_1, H_1], \dots, [U_{q^{n-1}-1}, H_{q^{n-1}-1}],$$

wobei die Unterräume aus $\text{Filter}(U_0)$ und $\text{Ideal}(H_0)$ in keinem dieser Intervalle enthalten sein dürfen.

Dieser Fragestellung wird in Kapitel 5 weiter nachgegangen. Vorher werden aber noch einige Grundlagen der Graphentheorie, insbesondere über die Existenz von perfekten Matchings in bipartiten k -regulären Graphen, vorgestellt. Diese werden sich dann später in zweierlei Hinsicht auf das betrachtete Problem anwenden lassen.

4 Graphentheorie

Nach Vorstellung einiger Grundbegriffe der Graphentheorie, wie sie auch etwa in [3] zu finden sind, wird nun bewiesen, dass jeder bipartite k -reguläre Graph ein perfektes Matching besitzt, was König bereits 1916 gelang, siehe [11]. Nach Erreichen dieses Resultats werden die Ausführungen zu diesem Gebiet allerdings nicht sofort beendet; vielmehr sollen die Beziehung solcher Aussagen zu Flüssen in Netzwerken, der Satz von König sowie der Heiratssatz von Hall zur Abrundung vorgestellt werden, da dies sehr populäre Resultate sind und sich das Resultat über bipartite k -reguläre Graphen wiederum einfach aus diesen folgern lässt.

4.1 Grundbegriffe der Graphentheorie

In Teilabschnitt 2.2.2 wurden die Beispiele 2.58 für Verbände als Hasse-Diagramme dargestellt. Diese sind nichts anderes als Graphen. Anschaulich gesprochen besteht ein Graph aus

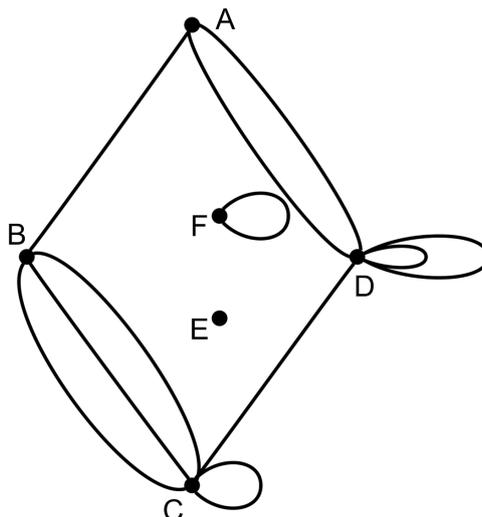


Abbildung 5: Anschauliche Vorstellung eines Graphen

einer Menge von Punkten und einer Menge von Linien, die zwischen diesen Punkten verlaufen (siehe Abbildung 5). Die Punkte werden auch Knoten genannt, die Linien werden Kanten genannt. Prinzipiell ist es denkbar, dass eine Kante von einem Knoten zu sich selbst verläuft („Schleifen“, wie etwa bei Punkt C in Abbildung 5), und auch mehrere Kanten zwischen zwei Knoten sind möglich („Mehrfachkanten“, wie etwa die Kanten zwischen B und C in Abbildung 5).

Graphen sollen nun aber so formal eingeführt werden, dass Schleifen nicht möglich sind, Mehrfachkanten aber schon. Dazu wird zunächst ein Begriff benötigt, der eine Verallgemeinerung gewöhnlicher Mengen darstellt.

Definition 4.1. Sei M eine Menge. Dann bezeichnet man M zusammen mit einer Abbildung $r : M \rightarrow \mathbb{N}$ als **Multimenge** über M .

Bildlich gesprochen ist eine Multimenge eine Menge, die dasselbe Element mehr als einmal enthalten kann; die Abbildung r gibt dann seine Vielfachheit an. Ist $r(a) = 1$ für alle $a \in M$, so handelt es sich um eine normale Menge.

Damit kann man nun Graphen definieren.

Definition 4.2. Ein ungerichteter Graph G , im Folgenden nur **Graph** genannt, ist ein Paar (V, E) , wobei V eine nichtleere Menge und E eine Multimenge über der Menge aller 2-elementigen Teilmengen von V ist. Die Elemente $v \in V$ werden **Knoten** genannt, die Elemente $e \in E$ **Kanten**.

Nach dieser Definition ist sofort klar, dass die hier behandelten Graphen keine Schleifen besitzen. Solche „Kanten“ $\{a, a\}$ mit gleichem Anfangs- und Endknoten $a \in V$ können hier nicht zur Kantenmenge gehören, da $\{a, a\}$ lediglich eine 1-elementige Menge ist.

Mehrfachkanten sind erlaubt, da die Kanten Elemente einer Multimenge sind. Manchmal werden Graphen mit Mehrfachkanten „Multigraphen“ genannt. Hier wird es umgekehrt gemacht und der Fall, dass ein Graph keine Mehrfachkanten besitzt, bekommt eine besondere Bezeichnung.

Definition 4.3. Ein Graph $G = (V, E)$ heißt **schlicht**, wenn E eine gewöhnliche Menge ist.

Im Folgenden werden aber allgemeine Graphen betrachtet, ohne die Schlichtheit vorauszusetzen. Beziehungen zwischen Knoten und Kanten eines Graphen werden folgendermaßen beschrieben.

Definition 4.4. Ein Knoten $v \in V$ heißt mit einer Kante $e \in E$ **inzident**, wenn $v \in e$ ist. Zwei Knoten $v, w \in V$ heißen **adjazent**, wenn $\{v, w\} \in E$ ist. Zwei Kanten heißen **adjazent**, wenn sie einen Knoten gemeinsam enthalten, d.h. $e_1 \cap e_2 \neq \emptyset$.

Definition 4.5. Sei $G = (V, E)$ ein Graph und $U \subseteq V$ eine Knotenmenge sowie $D \subseteq E$ eine Kantenmenge. Man sagt, U **überdeckt** D , falls jede Kante $d \in D$ mindestens einen Knoten $u \in U$ enthält. Man sagt, D **überdeckt** U , falls jeder Knoten $u \in U$ mit mindestens einer Kante $d \in D$ inzident ist.

Definition 4.6. Sei $G = (V, E)$ ein Graph. Dann bezeichnet man eine Knotenmenge $U \subseteq V$ als **Knotenüberdeckung** von G , falls U E überdeckt. Eine Kantenmenge $D \subseteq E$ heißt **Kantenüberdeckung** von G , falls D V überdeckt. Eine Knotenüberdeckung U von G heißt **minimal**, wenn es keine Knotenüberdeckung U' von G mit $|U'| < |U|$ gibt.

Wichtige Begriffe zur Charakterisierung von Knoten in einem Graphen sind die der Nachbarschaft und des Knotengrads, die nun eingeführt werden.

Definition 4.7. Die Menge der zu einem Knoten $v \in V$ adjazenten Knoten heißt **Nachbarschaft** von v und wird mit $N(v)$ bezeichnet. Ist $S \subseteq V$ eine Knotenmenge, so wird die Nachbarschaft von S als $N(S) := \bigcup_{v \in S} N(v)$ definiert.

Definition 4.8. In einem Graphen $G = (V, E)$ bezeichnet man die Anzahl der Kanten, mit denen ein Knoten $v \in V$ inzident ist, als **Grad von v** ; man schreibt dafür $d_G(v)$ oder $d(v)$, wenn klar ist, dass $d_G(v)$ gemeint ist.

Anzumerken ist, dass die Nachbarschaft eines Knotens als Menge, nicht als Multimenge definiert ist. Deshalb gilt im Allgemeinen nicht $d(v) = |N(v)|$, was in schlichten Graphen der Fall ist, da es zu jedem Knoten $w \in N(v)$ genau eine Kante $\{v, w\}$ gibt.

Im Folgenden spielen bipartite k -reguläre Graphen eine zentrale Rolle.

Definition 4.9. Ein Graph $G = (V, E)$ heißt **regulär**, wenn alle $v \in V$ den gleichen Grad besitzen. Ist $k = d(v)$ für ein (und damit für alle) $v \in V$, so heißt G **k -regulär**.

Ein Graph ist also regulär, wenn mit jedem Knoten gleich viele Kanten inzident sind. Bipartit ist er, wenn sich die Knotenmenge in zwei Teile aufteilen lässt, sodass die Kanten ausschließlich zwischen diesen beiden Teilen verlaufen.

Definition 4.10. Ein Graph $G = (V, E)$ heißt **bipartit**, wenn es zwei Knotenmengen V_1 und V_2 mit $V_1 \cap V_2 = \emptyset$ und $V_1 \cup V_2 = V$ gibt, sodass für alle $\{v, w\} \in E$ entweder $v \in V_1$ und $w \in V_2$ oder $v \in V_2$ und $w \in V_1$ gilt. Anstatt $G = (V, E)$ schreibt man dann auch $G = (V_1 \cup V_2, E)$.

In bipartiten k -regulären Graphen ist $|V_1| = |V_2|$, da $k|V_1|$ Kanten mit den Knoten aus V_1 inzident sind, und diese auch genau die Kanten sind, die mit den Knoten aus V_2 inzident sind. Mit jedem Knoten aus V_2 sind ebenso k Kanten inzident, also ist $k|V_1| = k|V_2|$. Das folgende Beispiel verdeutlicht die Begriffe k -regulär und bipartit.

Beispiel 4.11. Man betrachte das Intervallzerlegungsproblem im Verband $\mathcal{L}(3, GF(2))$ und ziehe dazu das Hasse-Diagramm heran. Wählt man Filter(U_1) und Ideal(H_7) aus (siehe Abbildung 6, dunkelgrau), so bleiben U_2, U_3 und U_4 sowie H_4, H_5 und H_6 zur Bildung der Intervalle übrig.

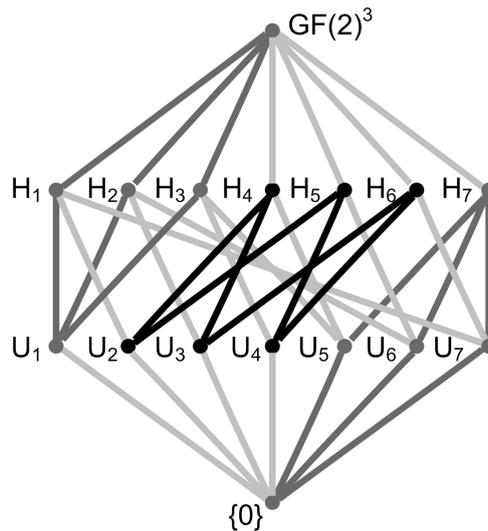


Abbildung 6: Intervallzerlegungsproblem in $\mathcal{L}(3, GF(2))$

Aus dem restlichen Teilgraphen (siehe Abbildung 6, schwarz) sind dann drei Kanten so auszuwählen, dass mit jedem Knoten genau eine Kante inzidiert (jede dieser Kanten stellt dann ein Intervall der Intervallzerlegung dar). Wie man unschwer erkennen kann, führt dieses spezielle

Intervallzerlegungsproblem hier auf einen 2-regulären bipartiten Graphen, in dem eben solche drei Kanten gesucht werden.

Entsprechendes gilt auch allgemein für Verbände $\mathcal{L}(3, GF(q))$, denn laut Proposition 3.12 (für $k_1 = 1$ und $k_2 = 2$) besteht der restliche Teilgraph aus $\binom{3}{1}_q - \binom{2}{0}_q - \binom{2}{1}_q = \binom{3}{2}_q - \binom{2}{1}_q - \binom{2}{2}_q$ 1-dimensionalen Unterräumen und Hyperebenen, und jeder 1-dimensionale Unterraum bzw. jede Hyperebene liegt in bzw. über $\binom{2}{1}_q - \binom{1}{0}_q = \binom{2}{1}_q - \binom{1}{1}_q$ Hyperebenen bzw. 1-dimensionalen Unterräumen. Im allgemeinen 3-dimensionalen Fall führt die Frage nach einer Intervallzerlegung also auf einen bipartiten $(\binom{2}{1}_q - 1)$ -regulären Graphen.

Formal beschrieben sucht man dann das, was nun als perfektes Matching bezeichnet wird.

Definition 4.12. Sei $G = (V, E)$ ein Graph und $M \subseteq E$. Dann heißt M **Matching** von G , wenn alle Kanten $e_1, e_2 \in M$ paarweise disjunkt sind.

Ein Matching M von G heißt **maximal**, wenn es kein Matching N von G gibt mit $|N| > |M|$. Überdeckt M jeden Knoten $v \in V$, so heißt M **perfektes Matching**.

Selbstverständlich sind Matchings damit gewöhnliche Mengen und keine echten Multimengen. In einem bipartiten regulären Graphen $G = (V_1 \cup V_2, E)$ ist ein Matching der Mächtigkeit $|V_1|$ perfekt, da dies alle Knoten aus V_1 und wegen $|V_1| = |V_2|$ auch alle Knoten aus V_2 überdeckt. Liegt ein Intervallzerlegungsproblem vor, das wie in Beispiel 4.11 auf ein einfaches Matchingproblem führt, so wird dies in [13] auch sinnvollerweise als **Matching-Intervallzerlegungs-Problem** bezeichnet.

4.2 Matchings in bipartiten k -regulären Graphen

In diesem Abschnitt wird jetzt gezeigt, dass jeder bipartite k -reguläre Graph ein perfektes Matching besitzt. Dieses Resultat lässt sich dann nicht nur auf das Matching-Intervallzerlegungs-Problem anwenden, sondern kann auch bei Intervallzerlegungen im Allgemeinen auf andere Art und Weise hilfreich sein (siehe Proposition 5.13).

Wege und deren Länge spielen im Folgenden eine zentrale Rolle; diese Begriffe werden nun definiert.

Definition 4.13. Eine Folge von Knoten $W = (v_0, v_1, v_2, \dots, v_r)$, bei der v_i und v_{i+1} für alle $i \in \{0, \dots, r-1\}$ adjazent sind, heißt **Weg** von v_0 nach v_r . Sind alle Knoten v von W paarweise verschieden, so heißt W **Pfad**. Ist W ein Pfad und v_0 und v_r adjazent, so bezeichnet man $(v_0, v_1, v_2, \dots, v_r, v_0)$ als **Kreis**.

Aus Einfachheitsgründen interpretiere man einen Weg als Menge von Knoten, wenn man einen Mengenoperator anwenden möchte, z.B. schreibe man einfach $(v_0, v_1, v_2, \dots, v_r) \cap \{v_1, w, v_r\} = \{v_1, v_r\}$. Wenn ein Knoten $v \in V$ an einen Weg angefügt wird, so notiere man den daraus entstehenden Weg mit Wv .

Eine wichtige Eigenschaft von Graphen ist folgende:

Definition 4.14. Ein Graph $G = (V, E)$ heißt **zusammenhängend**, wenn es für alle $v, w \in V$ einen Weg von v nach w in G gibt.

Es ist unmittelbar klar, dass ein nicht zusammenhängender Graph in zusammenhängende Teilgraphen zerfällt, welche **Zusammenhangskomponenten** des Graphen heißen. Im Folgenden wird stets vorausgesetzt, dass die betrachteten Graphen zusammenhängend sind. Ein Resultat für zusammenhängende Graphen gilt natürlich auch für die einzelnen Zusammenhangskomponenten eines nicht zusammenhängenden Graphen als Teilgraphen, da dies zusammenhängende Graphen sind.

Man komme nun nochmal auf die Definition eines Weges zurück; dies ist also eine Folge von Knoten. Da zwei aufeinander folgende Knoten eines Weges adjazent sind, kann man ihn aber ebenso als Folge von Kanten $(\{v_0, v_1\}, \{v_1, v_2\}, \dots, \{v_{r-1}, v_r\})$ ansehen. Darauf baut die nächste Definition auf.

Definition 4.15. Die Anzahl an Kanten eines Weges W heißt **Länge** von W . Die Länge eines kürzesten Weges von einem Knoten $v \in V$ zu einem weiteren Knoten $w \in V$ wird als **Distanz** von v und w oder $d(v, w)$ bezeichnet.

Die Distanz zweier Knoten ist wohldefiniert, da die betrachteten Graphen zusammenhängend sind. Wie durch die Schreibweise schon angedeutet, ist die Distanz eine Metrik auf der Knotenmenge, wenn man der Vollständigkeit halber den kürzesten Weg von einem Knoten zu sich selbst als eine leere Folge von Knoten und deren Länge als 0 definiert. Damit ist dann nämlich $d(v, v) = 0$ für alle $v \in V$ und $d(v, w) > 0$ genau dann, wenn $v \neq w \in V$ ist. Die Symmetrie ist auch klar, und wenn (v, \dots, w) ein kürzester Weg von v nach w und (w, \dots, z) ein kürzester Weg von w nach z ist, so kann der kürzeste Weg von v nach z nicht länger als (v, \dots, w, \dots, z) sein, und die Dreiecksungleichung ist erfüllt.

Das folgende Lemma charakterisiert bipartite Graphen nun anhand der Länge ihrer Kreise.

Lemma 4.16. *Ein Graph ist genau dann bipartit, wenn er keinen Kreis ungerader Länge enthält.*

Beweis. Sei $G = (V_1 \cup V_2, E)$ ein bipartiter Graph. Ist $W = (v_0, v_1, v_2, \dots, v_r)$ ein Weg ungerader Länge in G , so ist $v_0 \in V_1$ und $v_r \in V_2$ oder $v_0 \in V_2$ und $v_r \in V_1$ und somit kann W kein Kreis sein, womit die eine Richtung gezeigt wurde.

Nun sei angenommen, es gäbe keinen Kreis ungerader Länge in G . Man konstruiert zwei Mengen V_1 und V_2 derart, dass sie die Voraussetzungen von Definition 4.10 erfüllen. Dazu sei $v \in V$ ein beliebiger, aber fester Knoten von G und

$$V_1 := \{w \in V \mid d(v, w) = 0 \text{ oder } d(v, w) \text{ ist gerade}\}$$

sowie

$$V_2 := \{w \in V \mid d(v, w) \text{ ist ungerade}\} = V \setminus V_1.$$

Per Definition ist $V_1 \cap V_2 = \emptyset$ und $V_1 \cup V_2 = V$, womit zu zeigen bleibt, dass jede Kante von G einen Knoten in V_1 und einen in V_2 besitzt. Dazu sei angenommen, dass es eine Kante $e = \{a, b\} \in E$ gibt mit $a, b \in V_1$ oder $a, b \in V_2$, wobei zunächst der Fall $a, b \in V_1$ betrachtet wird. Dann gibt es also einen kürzesten Weg W_1 gerader Länge von v nach a und einen kürzesten Weg W_2 gerader Länge von v nach b .

Unterschieden werden nun zwei Fälle:

1. W_1 und W_2 besitzen keinen gemeinsamen Knoten:

Dann bilden W_1 und W_2 zusammen mit e einen Kreis ungerader Länge, wodurch ein Widerspruch zur Voraussetzung entsteht.

2. W_1 und W_2 besitzen mindestens einen gemeinsamen Knoten:

Sei hier v^* von den gemeinsamen Knoten derjenige mit der größten Distanz zu v . Dann enthalten W_1 und W_2 je einen Weg von v nach v^* mit Länge $d(v, v^*)$. Damit gilt auch $d(v^*, a) = d(v, a) - d(v, v^*)$ und $d(v^*, b) = d(v, b) - d(v, v^*)$. Das heißt, dass $d(v^*, a)$ und $d(v^*, b)$ entweder beide gerade oder beide ungerade sein müssen.

Somit starten aber zwei kürzeste Wege bei v^* , die entweder beide gerade oder beide ungerade Länge haben. Zusammen mit e bilden diese wiederum einen Kreis ungerader Länge, sodass auch in diesem Fall ein Widerspruch zur Voraussetzung entsteht.

Somit können nicht beide Knoten a, b in V_1 liegen. Der Fall $a, b \in V_2$ kann ganz analog widerlegt werden, denn zwei Wege ungerader Länge haben zusammen genommen gerade Länge, und wenn sie durch eine Kante e zu einem Kreis ergänzt werden, hat dieser natürlich ungerade Länge.

Insgesamt wurde also gezeigt, dass a und b nicht in derselben Menge V_1 oder V_2 liegen, womit G bipartit ist. \square

Unter Verwendung dieses Lemmas lässt sich ein Satz beweisen, der auf Denes König [11] zurückgeht und aus dem das in diesem Abschnitt angestrebte Resultat direkt folgt. Es wird hier zunächst der Beweis vorgestellt, wie er auch von König geführt wurde.

Satz 4.17. Sei $G = (V, E)$ ein bipartiter Graph mit $d_G(v) \leq k$ für ein $k \in \mathbb{N}$ und alle $v \in V$. Dann gibt es k paarweise disjunkte Matchings M_1, \dots, M_k von G mit $\bigcup_{l=1}^k M_l = E$.

Beweis. Der Satz wird durch Induktion nach der Kantenanzahl $|E|$ bewiesen. Ist $|E| \leq k$, so ist die Aussage trivialerweise richtig. Sei also angenommen, der Satz gilt stets für Graphen mit $|E| \leq n$. Wir betrachten nun einen beliebigen Graphen $G = (V, E)$ mit $|E| = n + 1$. Bildet man daraus den Graphen $G' = (V, E')$ mit $E' := E \setminus \{e\}$ durch Weglassen einer beliebigen Kante $e = \{v_0, w\} \in E$, so ist dieser ebenfalls bipartit und es ist $|E'| = n$, sodass der Satz für diesen nach Voraussetzung gilt.

Seien also M_1, \dots, M_k die entsprechenden Matchings. Gibt es ein $i \in \{1, \dots, k\}$ mit $u \notin E_i$ für alle $u \in E'$ mit $v_0 \in u$ oder $w \in u$, d.h. in dieser Kantenmenge M_i liegt keine der mit den Knoten von e inzidenten Kanten, so sind durch $M_i \cup e$ zusammen mit den anderen Matchings k Matchings von G gegeben.

Sei also angenommen, es gibt kein solches i . Da $d_{G'}(v_0) \leq k - 1$ und $d_{G'}(w) \leq k - 1$ gilt, gibt es $i \neq j \in \{1, \dots, k\}$, sodass keine mit v_0 inzidente Kante in E_i liegt, es aber eine mit w inzidente Kante in E_i gibt, und sodass keine mit w inzidente Kante in E_j liegt, es aber eine mit v_0 inzidente Kante in E_j gibt. O.B.d.A. sei $i=1$ und $j=2$ angenommen, sonst vertausche man die Indizes.

Sei also $\{v_0, v_1\} \in M_2$. Es wird nun von $\{v_0, v_1\}$ aus ein möglichst langer alternierender Weg $W = (v_0, v_1, \dots, v_r)$ gebildet, wobei „alternierend“ hier heißt, dass $\{v_{m-1}, v_m\} \in M_2$ ist für ungerades $m \in \{1, \dots, r - 1\}$ und $\{v_{m-1}, v_m\} \in M_1$ für gerades $m \in \{1, \dots, r - 1\}$ ist.

Existiert also kein v_2 mit $\{v_1, v_2\} \in M_1$, so ist $W := (v_0, v_1)$, andernfalls wird v_2 betrachtet. Existiert kein v_3 mit $\{v_2, v_3\} \in M_2$, so ist $W := (v_0, v_1, v_2)$, andernfalls gehört v_3 zu W und die Erweiterung von W wird von dort aus analog fortgesetzt. Zur Erläuterung dient Abbildung

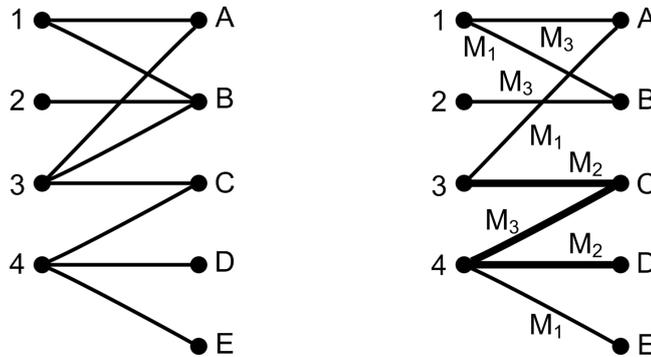


Abbildung 7: Beispiel für G (links) und G' (rechts)

7: Der linke Graph sei $G = (V, E)$ und es gilt $d_G(v) \leq 3$ für alle $v \in V$. Der rechte Graph ist demnach $G' = (V, E')$ mit $E' := E \setminus \{3, B\}$. Die disjunkten Matchings bestehen aus den Kanten, die entsprechend beschriftet sind. Es gibt dann keine mit dem Knoten 3 inzidente Kante in M_3 , aber eine mit B inzidente Kante in M_3 ; es gibt keine mit B inzidente Kante in M_2 , aber eine mit 3 inzidente Kante in M_2 . Der konstruierte „alternierende“ Weg ist dann $(3, C, 4, D)$ und fett eingezeichnet.

Ein solcher Weg W hat folgende Eigenschaften:

- **W ist eindeutig bestimmt:**
Dies ist per Definition von W klar.
- **W ist ein Pfad:**
Für $1 \leq m \leq r$ kann v_m nicht doppelt erreicht werden, denn wäre v_i der erste dieser Knoten, der doppelt erreicht wird, so gibt es drei verschiedene mit v_i inzidente Kanten aus $E_1 \cup E_2$, also zwei aus E_1 oder aus E_2 , was nicht sein kann. Und auch v_0 kann nicht doppelt erreicht werden, da keine mit v_0 inzidente Kante in M_1 existiert und $\{v_0, v_1\}$ die einzige zu v_0 inzidente Kante in M_2 ist. Demnach müsste v_1 doppelt erreicht werden, was bereits widerlegt wurde. Also enthält W keinen Knoten doppelt und ist damit ein Pfad.
- **W enthält w nicht:**
Der Knoten w könnte nur über eine Kante aus M_1 erreicht werden, und dann würde der Weg von v nach w eine gerade Anzahl an Kanten enthalten. Nimmt man e wieder dazu, ergäbe sich also ein Kreis in G mit ungerader Kantenzahl, was nicht sein kann, da G bipartit ist.

Hilfswise werden $\widetilde{W}_1 := W \cap M_1$ und $\widetilde{W}_2 := W \cap M_2$ definiert. Nun setzt man $\widetilde{M}_1 := M_1 \setminus \widetilde{W}_1 \cup \widetilde{W}_2$ und $\widetilde{M}_2 := M_2 \setminus \widetilde{W}_2 \cup \widetilde{W}_1$, d.h. \widetilde{M}_1 enthält alle Kanten von M_1 außer denen, die zu W gehören, und zusätzlich die Kanten von W aus M_2 ; für \widetilde{M}_2 gilt das gleiche umgekehrt. Die Mengen $\widetilde{M}_1, \widetilde{M}_2, M_3, \dots, M_k$ besitzen die folgenden Eigenschaften:

- $\widetilde{M}_1, \widetilde{M}_2, M_3, \dots, M_k$ sind paarweise disjunkt und ergeben vereinigt E' :
Dies ist per Definition von \widetilde{M}_1 und \widetilde{M}_2 klar.
- **Bezüglich $\widetilde{M}_1, \widetilde{M}_2, M_3, \dots, M_k$ liegen zwei adjazente Kanten stets in unterschiedlichen Kantenmengen:**
Außer der Kante $\{v_0, v_1\}$ gibt es keine mit v inzidente Kante, die in \widetilde{M}_1 liegt, da in M_1 überhaupt keine zu v inzidente Kante liegt. Weil für gerades $m \in \{1, \dots, r-1\}$ nur $\{v_{m-1}, v_m\}$ aus M_1 und nur $\{v_m, v_{m+1}\}$ aus M_2 mit v_m inzident sind und für ungerades $m \in \{1, \dots, r-1\}$ nur $\{v_{m-1}, v_m\}$ aus M_2 und nur $\{v_m, v_{m+1}\}$ aus E_1 , sind ebenso für gerades $m \in \{1, \dots, r-1\}$ nur $\{v_{m-1}, v_m\}$ aus \widetilde{M}_1 und nur $\{v_m, v_{m+1}\}$ aus \widetilde{M}_2 mit v_m inzident und für ungerades $m \in \{1, \dots, r-1\}$ nur $\{v_{m-1}, v_m\}$ aus \widetilde{M}_2 und nur $\{v_m, v_{m+1}\}$ aus \widetilde{M}_1 . Mit v_r gibt es entweder genau eine inzidente Kante in E_1 oder in E_2 , da v_r zu W gehört, aber v_r der letzte Knoten von W ist. Damit gibt es auch höchstens eine mit v_r inzidente Kante in \widetilde{M}_1 und \widetilde{M}_2 . Für die Kanten, die mit keinem Knoten von W inzident sind, gilt die Aussage, da sie bezüglich M_1, M_2, \dots, M_k auf Grund der Matchingeigenschaft gilt.
- **Es gibt keine mit v_0 oder w inzidente Kante in \widetilde{M}_2 :**
Für w ist dies klar, denn es gibt keine mit w inzidente Kante in M_2 und damit auch nicht in \widetilde{M}_2 , da $w \notin W$ ist. Für v_0 liegt genau die Kante $\{v_0, v_1\}$ in \widetilde{M}_2 , aber keine in M_1 . Durch Konstruktion von \widetilde{M}_1 und \widetilde{M}_2 ist dann genau $\{v_0, v_1\} \in \widetilde{M}_1$, aber es gibt keine mit v_0 inzidente Kante in \widetilde{M}_2 .

Damit kann man wieder den ursprünglichen Graphen G betrachten und die weggelassene Kante e mit \widetilde{M}_2 vereinigen. Man erhält dadurch k Kantenmengen $\widetilde{M}_1, \widetilde{M}_2 \cup \{e\}, M_3, \dots, M_k$ derart, dass zwei adjazente Kanten von G in unterschiedlichen Kantenmengen liegen. Somit ist der Induktionsschritt vollzogen und der Beweis erbracht. \square

Korollar 4.18. *Jeder bipartite k -reguläre Graph besitzt k disjunkte perfekte Matchings.*

Beweis. Ein bipartiter k -regulärer Graph $G = (V_1 \cup V_2, E)$ erfüllt die Voraussetzungen von Satz 4.17. Zudem muss jedes der k Matchings zu jedem Knoten $v \in V_1 \cup V_2$ genau eine mit diesem inzidente Kante enthalten, da ansonsten ein anderes Matching zwei mit v inzidente Kanten enthalten würde, ein Widerspruch. Somit ist jedes der k Matchings perfekt. \square

Äquivalent zu diesem Korollar ist die Aussage, dass ein bipartiter k -regulärer Graph ein perfektes Matching besitzt. Besitzt er nämlich ein solches, so erhält man einen bipartiten $(k-1)$ -regulären Graphen, indem man die Kanten dieses Matchings aus dem ursprünglichen Graphen entfernt. Dieser besitzt dann wiederum ein perfektes Matching, und das Korollar folgt so induktiv.

4.3 Weitere wichtige Resultate

Wie angekündigt, werden nun noch einige weitere Resultate auf diesem Gebiet vorgestellt.

4.3.1 Flüsse in Netzwerken

Die Formulierung eines Matchingproblems als äquivalentes Flussproblem ist vor allem in der Praxis nützlich, da effiziente Algorithmen existieren, um die Stärke eines maximalen Flusses in einem Netzwerk zu bestimmen, siehe z.B. [10], Kapitel 7. Man kann aber aus den Erkenntnissen über Flussprobleme auch sehr elegant nochmals die Existenz eines perfekten Matchings in einem k -regulären Graphen folgern.

Hier werden nun gerichtete Graphen verwendet.

Definition 4.19. Ein gerichteter Graph G , auch **Digraph** genannt, ist ein Paar (V, E) , wobei V eine nichtleere Menge und E eine Multimenge über $V \times V$ ist. Die Elemente $v \in V$ werden auch hier **Knoten** genannt, die Elemente $e \in E$ (gerichtete) **Kanten**.

In einem Digraphen sind also auch Schleifen erlaubt, da (v, v) ein Element von $V \times V$ ist. Ähnlich wie bei Wegen ist es hier ebenso oft praktisch, Mengenoperatoren auf ein Element $(v, w) \in V \times V$ anzuwenden. Damit ist dann ebenfalls die Anwendung auf die zugehörige Menge $\{v, w\}$ gemeint.

Die Begriffe Adjazenz und Inzidenz sind analog zu ungerichteten Graphen zu verwenden. Man unterscheidet hier aber bei den mit einem Knoten $v \in V$ inzidenten Kanten die Multimenge der in v **eingehenden Kanten** $A^+(v)$ von der Menge der aus v **ausgehenden Kanten** $A^-(v)$. Ersteres sind alle Kanten, die sich als (w, v) schreiben lassen, letzteres die, die sich als (v, w) schreiben lassen, mit $w \in V$.

Jetzt wird definiert, was ein Netzwerk ist, wozu der Begriff der Kapazitätsfunktion benötigt wird.

Definition 4.20. Sei $G = (V, E)$ ein Digraph. Dann heißt eine Funktion $c : E \rightarrow \mathbb{R}$ **Kapazitätsfunktion** auf G . Nimmt c nur Werte aus \mathbb{N} an, so heißt c **ganzzahlig**.

Definition 4.21. Ein **Netzwerk** N ist ein Tupel (V, E, s, t, c) , wobei $G = (V, E)$ ein Digraph ist, $s, t \in V$ zwei ausgezeichnete Knoten sind c eine Kapazitätsfunktion auf G ist. Man nennt s **Quelle** und t **Senke** von N .

In einem solchen Netzwerk betrachtet man nun Flüsse. Dieser Begriff hat eine sehr bildliche Interpretation: Von der Quelle s fließen gewisse Einheiten über die Kanten des Netzwerks zur Senke t . Dabei müssen die Kapazitätsbeschränkungen der Kanten eingehalten werden, und außer bei Quelle und Senke müssen an einem Knoten gleich viele Einheiten ein- und ausgehen. Diese Vorstellung wird jetzt formal beschrieben.

Definition 4.22. Ein **Fluss** in einem Netzwerk $N = (V, E, s, t, c)$ ist eine Funktion $f : E \rightarrow \mathbb{R}$, die die folgenden Bedingungen erfüllt:

1. Für jede Kante $e \in E$ gilt: $f(e) \leq c(e)$

2. Für alle Knoten $v \in V \setminus \{s, t\}$ gilt: $\sum_{e \in A^+(v)} f(e) = \sum_{e \in A^-(v)} f(e)$

Nimmt f nur Werte aus \mathbb{N} an, so heißt f **ganzzahlig**.

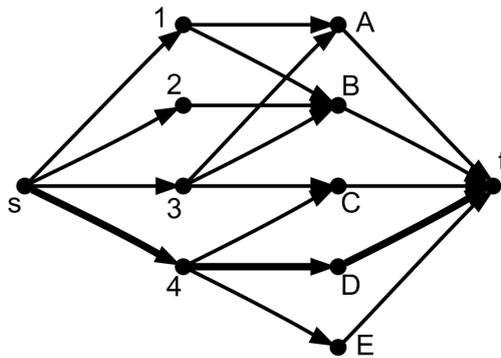


Abbildung 8: Netzwerk und Fluss

Das in Abbildung 8 skizzierte Netzwerk habe eine Kapazitätsfunktion, die jeder Kante die Kapazität 1 zuweist, wodurch es dann auch tatsächlich zu einem Netzwerk nach der Definition wird. Ein Beispiel für einem Fluss in diesem Netzwerk ist eine Funktion, die den fett eingezeichneten Kanten den Wert 1 und allen anderen Kanten den Wert 0 zuweist.

Interessant ist oft, wie viele Einheiten auf einem Fluss von der Quelle zur Senke fließen, um in der bildlichen Interpretation zu bleiben.

Definition 4.23. Sei f ein Fluss in einem Netzwerk $N = (V, E, s, t, c)$. Dann nennt man

$$|f| := \sum_{e \in A^+(t)} f(e) - \sum_{e \in A^-(t)} f(e)$$

die **Stärke** von f .

f heißt ein **Fluss maximaler Stärke** oder **maximaler Fluss**, wenn es keinen Fluss g in N gibt mit $|g| > |f|$.

Sucht man in einem Graphen ein maximales Matching, so spricht man auch von einem Matchingproblem. Sucht man in einem Netzwerk einen maximalen Fluss, so spricht man auch von einem Flussproblem. Etwas schwammig bezeichnet man das Netzwerk selbst dann auch als Flussproblem. Zu einem Matchingproblem in bipartiten Graphen kann man ein (wie man noch sehen wird) äquivalentes Flussproblem formulieren.

Definition 4.24. Sei $G = (V_1 \cup V_2, E)$ ein bipartiter Graph. Das dazu **äquivalente Flussproblem** ist ein Netzwerk $N := (V', E', s, t, c)$ mit

- Knotenmenge $V' := V_1 \cup V_2 \cup \{s, t\}$, wobei s und t zwei Knoten sind, die nicht in $V_1 \cup V_2$ enthalten sind,

- Kantenmenge $E' := \{(a, b) \mid \{a, b\} \in E\} \cup \{(s, a) \mid a \in V_1\} \cup \{(b, t) \mid b \in V_2\}$, wobei E' ebenso wie E eine Multimenge ist und (a, b) in E' die gleiche Vielfachheit hat wie $\{a, b\}$ in E ; die Vielfachheiten der Kanten (s, a) und (b, t) , $a \in V_1$, $b \in V_2$ sind eins, und
- Kapazitätsfunktion c mit $c(e) = 1$ für alle $e \in E'$.

Das in Abbildung 8 beschriebene Netzwerk ist das äquivalente Flussproblem zum linken Graphen aus Abbildung 7.

Um die tatsächliche Äquivalenz beider Probleme zu zeigen, wird die nächste Proposition verwendet, für deren Beweis auf [3], Seite 155f., verwiesen wird.

Proposition 4.25. *Sei $N = (V, E, s, t, c)$ ein Netzwerk und c ganzzahlig. Dann gibt es einen maximalen Fluss f in N , der ganzzahlig ist.*

Nun kann der Beweis der Äquivalenzaussage folgen.

Satz 4.26. *Sei $G = (V_1 \cup V_2, E)$ ein bipartiter Graph und $N = (V', E', s, t, c)$ das dazu äquivalente Flussproblem. Dann ist die Mächtigkeit eines maximalen Matchings von G gleich der Stärke eines maximalen Flusses in N .*

Beweis. Sei M ein maximales Matching. Dann ist durch

$$f_M(e) := \begin{cases} 1, & \text{falls } e \in M \text{ oder } e = (s, a) \text{ oder } e = (a, t) \text{ mit } a \in e^* \text{ für ein } e^* \in M; \\ 0, & \text{sonst.} \end{cases}$$

ein Fluss in N definiert. Dieser hat die Stärke $|M|$, wie man leicht sieht. Also ist die Stärke eines maximalen Flusses in N größer oder gleich der Mächtigkeit eines maximalen Matchings in G .

Sei nun f ein maximaler Fluss in N . Dann existiert nach Proposition 4.25 ein ganzzahliger Fluss g derselben Stärke, welcher in diesem Fall also nur die Werte 0 und 1 annehmen kann, da $0 \leq c(e) \leq 1$ für alle $e \in E'$ ist. Man betrachte die Kantenmenge M_g mit

$$M_g := \{e \in E \mid g(e) = 1, s \notin e, t \notin e\}.$$

Dies ist ein Matching von G , da auf Grund der Kapazitätsfunktion von N jeder Knoten aus $V' \setminus \{s, t\}$ höchstens eine ein- bzw. ausgehende Kante e mit $f(e) = 1$ haben kann. Damit ist die Mächtigkeit eines maximalen Matchings in G größer oder gleich der Stärke eines maximalen Flusses in N .

Insgesamt ist also die Gleichheit bewiesen. □

Aus diesem Satz kann man wiederum folgern, dass in bipartiten k -regulären Graphen ein perfektes Matching existiert. Man betrachte dazu im äquivalenten Flussproblem den Fluss f mit

$$f(e) := \begin{cases} 1, & \text{wenn } s \in e \text{ oder } t \in e; \\ \frac{1}{k}, & \text{sonst.} \end{cases}$$

Dieser hat die Stärke $|V_1| \cdot k \cdot \frac{1}{k} = |V_1|$, also ist die Mächtigkeit eines maximalen Matchings mindestens $|V_1|$ und damit gleich $|V_1|$.

4.3.2 Satz von König

Nun wird der sehr bekannte Satz von König bewiesen, dessen Beweis im Original in [12], S. 248f., und in der hier präsentierten Fassung beispielsweise in [3], S. 39, zu finden ist. Dabei spielen die folgenden Begriffe eine wichtige Rolle.

Definition 4.27. Sei G ein Graph. Ein Weg $W = (v_0, v_1, v_2, \dots, v_r)$ in G heißt **alternierend** bezüglich eines Matchings M von G , wenn v_0 nicht von M überdeckt wird und $\{v_{m-1}, v_m\} \notin M$ für ungerades $m \in \{1, \dots, r\}$ sowie $\{v_{m-1}, v_m\} \in M$ für gerades $m \in \{1, \dots, r\}$ gilt. W heißt **augmentierend**, wenn zusätzlich auch v_r nicht von M überdeckt wird.

Der alternierende Weg aus dieser Definition ist natürlich nicht zu verwechseln mit dem speziellen „alternierenden“ Weg, der im Beweis von Satz 4.17 verwendet wurde. In der folgenden Abbildung links ist $(2, B, 3, C)$ ein augmentierender Weg bezüglich des fett eingezeichneten Matchings. Existiert in einem Graphen ein augmentierender Weg W bezüglich eines Mat-

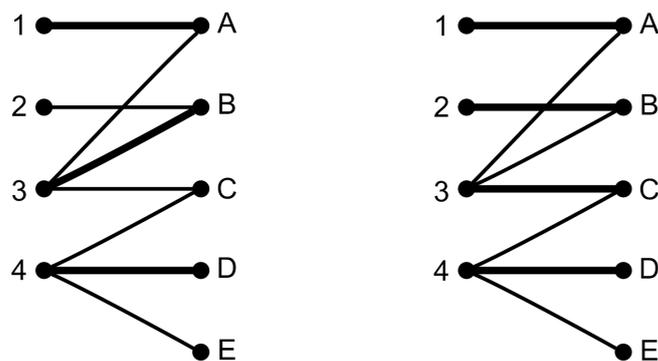
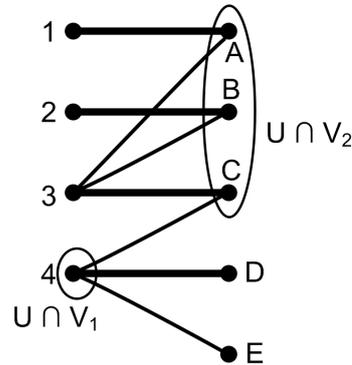


Abbildung 9: Verbesserung eines Matchings durch einen augmentierenden Weg

chings M , so kann M zu einem Matching N von G mit $|N| > |M|$ „verbessert“ werden. Man erhält dieses, indem man die Kanten $\{v_{m-1}, v_m\}$ von W mit geradem $m \in \{1, \dots, r\}$ aus M entfernt und die Kanten $\{v_{m-1}, v_m\}$ von W mit ungeradem $m \in \{1, \dots, r\}$ zu M hinzufügt, wie es auch in der Abbildung gemacht wurde. Dies wird im Beweis des Satzes von König verwendet. In Abbildung 9 entsteht dadurch das rechts fett eingezeichnete Matching.

Satz 4.28 (Satz von König). *In einem bipartiten Graphen ist die Mächtigkeit eines maximalen Matchings gleich der Mächtigkeit einer minimalen Knotenüberdeckung.*

Beweis. Sei M ein maximales Matching von $G = (V_1 \cup V_2, E)$. Es werde folgendermaßen eine Knotenmenge U gebildet: Von jeder Kante $e \in M$ wird der Knoten ausgewählt, der in V_2 liegt, falls es einen alternierenden Weg bezüglich M gibt, der in diesem Knoten endet, und sonst der Knoten, der in V_1 liegt. Abbildung 10 illustriert die Konstruktion von U für den rechten Graphen aus Abbildung 9. Nun wird gezeigt, dass U eine minimale Knotenüberdeckung von G ist: Sei $\{v, w\} \in E$ eine beliebige Kante. Ist $\{v, w\} \in M$, so liegt nach Definition von U entweder v oder w in U , also wird $\{v, w\}$ durch U überdeckt. Sei also $\{v, w\} \notin M$. Da M maximal ist, muss M eine Kante $\{a, b\}$ mit $a = v$ oder $b = w$ enthalten. Wird v nicht von M überdeckt, so ist $\{v, w\} \notin M$ und damit $b = w \in U$, da in $b = w$ der alternierende Weg (v, w)

Abbildung 10: Beispiel für die Konstruktion von U

endet. Wird v von M überdeckt und ist $v \notin U$, so muss $b \in U$ sein und ein alternierender Weg W_1 endet in b . Ebenso endet aber auch ein alternierender Weg W_2 in w , für den entweder $W_2 = W_1w$ (falls $w \in W_1$) oder $W_2 = W_1baw$ gilt. Da M ein maximales Matching ist, kann W_2 nicht augmentierend sein. Somit wird w von M überdeckt und es ist $w \in U$. Damit ist U eine Knotenüberdeckung von G . Diese ist minimal, denn eine Knotenüberdeckung von G muss zu jeder Kante $e \in M$ einen Knoten enthalten, der mit dieser inzident ist. \square

Daraus folgt der Satz über k -reguläre Graphen auch direkt: Ist U eine Knotenüberdeckung von G , so überdeckt U maximal $k|U|$ Kanten, da jeder Knoten genau k Kanten überdeckt und es Überschneidungen geben kann (deshalb überdeckt U nicht immer genau $k|U|$ Kanten). Als bipartiter k -regulärer Graph hat G insgesamt $k|V_1|$ Kanten, also muss eine kleinste Knotenüberdeckung mindestens $|V_1|$ Knoten enthalten. Nach dem Satz von König überdeckt das größte Matching also mindestens V_1 Knoten, und da es nicht mehr sein können, genau V_1 Knoten.

4.3.3 Heiratssatz von Hall

Zuletzt wird jetzt der Heiratssatz von Hall bewiesen. Der Beweis wird häufig durch Induktion nach der Knotenanzahl geführt, ist aber auch über den Satz von König möglich (siehe [3], S. 40f.).

Satz 4.29 (Heiratssatz). *Sei $G = (V_1 \cup V_2, E)$ ein bipartiter Graph. Es existiert genau dann ein Matching M von G der Mächtigkeit $|V_1|$, wenn die Hall-Bedingung*

$$\forall S \subseteq V_1 : |S| \leq |N(S)|$$

erfüllt ist.

Beweis. Die eine Richtung ist klar, denn wenn es eine Knotenmenge $S \subseteq V_1$ mit $|S| > |N(S)|$ gibt, so kann nicht jeder Knoten aus V_1 zu einem Matching von G gehören.

Existiert kein Matching von G der Mächtigkeit V_1 , so hat G nach dem Satz von König eine Knotenüberdeckung U durch weniger als $|V_1|$ Knoten. Sei $U = U_1 \cup U_2$ mit $U_1 \subseteq V_1$ und

$U_2 \subseteq V_2$, es gelte also $|U_1| + |U_2| = |U| < |V_1|$, d.h. umgeformt $|U_2| < |V_1| - |U_1| = |V_1 \setminus U_1|$. Nach Definition von U hat G aber keine Kante zwischen $|V_1 \setminus U_1|$ und $|V_2 \setminus U_2|$. Also gilt

$$|N(V_1 \setminus U_1)| \leq |U_2| < |V_1 \setminus U_1|.$$

Für $S := V_1 \setminus U_1$ ist die Hall-Bedingung also nicht erfüllt. □

Hieraus folgt das Resultat über perfekte Matchings in bipartiten k -regulären Graphen nochmal: Mit den Knoten jeder Menge $S \subseteq V_1$ sind $k|S|$ Kanten inzident. Diese gehören natürlich zu den $k|N(S)|$ Kanten, die mit den Knoten aus $N(S)$ inzident sind, also gilt $k|S| \leq k|N(S)|$, d.h. $|S| \leq |N(S)|$. Die Hall-Bedingung ist damit erfüllt und es existiert ein Matching der Mächtigkeit $|V_1|$, das damit perfekt ist.

5 Intervallzerlegungen linearer Verbände

In diesem Kapitel steht nun die Suche nach Intervallzerlegungen linearer Verbände an. Der einfachste Fall wurde im letzten Kapitel schon geklärt: Nach Beispiel 4.11 führt die Frage nach einer Intervallzerlegung in $\mathcal{L}(3, GF(q))$ auf das Matching-Intervallzerlegungs-Problem, d.h. auf die Frage nach einem perfekten Matching in einem regulären Graphen, und Korollar 4.18 beantwortet diese Frage positiv. Eine Folgerung aus dem letzten Kapitel ist also:

Korollar 5.1. *Für jeden endlichen Körper $GF(q)$ existiert eine Intervallzerlegung des Verbandes $\mathcal{L}(3, GF(q))$.*

Nun sollen auch Verbände $\mathcal{L}(n, GF(q))$ mit $n \geq 4$ betrachtet werden. Dazu werden zuerst einige allgemeingültige Aussagen hergeleitet, bevor konkret Verbände über $GF(2)$ und $GF(3)$ angesehen werden. Abschließend folgen noch einige Bemerkungen zu dem Problem über mächtigeren endlichen Körpern.

5.1 Allgemeine Sätze

Das am Ende von Kapitel 3 formulierte Intervallzerlegungsproblem soll zunächst etwas umformuliert werden, um es anschließend besser untersuchen zu können. Ist

$$\{U_0, U_1, \dots, U_{q^{n-1}-1}, H_0, H_1, \dots, H_{q^{n-1}-1}\}$$

eine Intervallzerlegung von $\mathcal{L}(n, GF(q))$, so sei p_0 ein Repräsentant des 1-dimensionalen Vektorraums U_0 . Außerdem seien p_1, \dots, p_s , $s := \frac{q^{n-1}-1}{q-1}$ Repräsentanten der 1-dimensionalen Unterräume von H_0 .

Zuerst wird gezeigt:

Proposition 5.2. *Für alle $i, j \in \{1, \dots, s\}$ sind p_0, p_i und p_j linear unabhängig.*

Beweis. Seien $\lambda_0, \lambda_i, \lambda_j \in GF(q)$ mit $\lambda_0 p_0 + \lambda_i p_i + \lambda_j p_j = 0$. Dann folgt $\lambda_0 p_0 = -(\lambda_i p_i + \lambda_j p_j)$ und, da $p_0 \in U_0$ ist und $p_i, p_j \in H_0$ sind, $\lambda_0 p_0 \in U_0 \cap H_0 = \{0\}$. Da p_i und p_j linear unabhängig sind, folgt auch $\lambda_i = \lambda_j = 0$. \square

Damit kommt man zu einer weiteren Unabhängigkeitsaussage.

Proposition 5.3. *Für alle $i, j \in \{1, \dots, s\}$ und $\beta, \beta' \in GF(q)^*$ mit $(i, \beta) \neq (j, \beta')$ sind $p_i + \beta p_0$ und $p_j + \beta' p_0$ linear unabhängig.*

Beweis. Seien $\lambda_1, \lambda_2 \in GF(q)$ mit

$$0 = \lambda_1(p_i + \beta p_0) + \lambda_2(p_j + \beta' p_0) = \lambda_1 p_i + \lambda_2 p_j + (\lambda_1 \beta + \lambda_2 \beta') p_0.$$

Dann folgt $\lambda_1 = \lambda_2 = 0$ nach Proposition 5.2, womit $p_i + \beta p_0$ und $p_j + \beta' p_0$ linear unabhängig sind. \square

Somit werden $(q-1)s = q^{n-1} - 1$ verschiedene 1-dimensionale Unterräume von den $p_i + \beta p_0$, $i \in \{1, \dots, s\}$, $\beta \in GF(q)^*$, aufgespannt. Diese liegen zudem nicht in $\text{Filter}(U_0)$ und nicht in $\text{Ideal}(H_0)$, wie die folgende Proposition zeigt.

Proposition 5.4. *Für alle $i \in \{1, \dots, s\}$ und $\beta \in GF(q)^*$ gilt $\langle p_i + \beta p_0 \rangle \notin \text{Filter}(U_0)$ und $\langle p_i + \beta p_0 \rangle \notin \text{Ideal}(H_0)$.*

Beweis. Natürlich ist $\langle p_i + \beta p_0 \rangle \notin \text{Filter}(U_0)$, da $p_i + \beta p_0$ kein Vielfaches von p_0 ist. Aus $\langle p_i + \beta p_0 \rangle \in \text{Ideal}(H_0)$ würde, da $p_i \in H_0$ ist, auch $\beta^{-1}(p_i + \beta p_0 - p_i) = p_0 \in H_0$ folgen. Dies ist jedoch ein Widerspruch, womit die Aussage folgt. \square

Nach Proposition 3.12 (für $k_1 = 1$) gibt es genau $\binom{n}{1}_q - \binom{n-1}{0}_q - \binom{n-1}{1}_q = \frac{q^n-1}{q-1} - 1 - \frac{q^{n-1}-1}{q-1} = q^{n-1} - 1$ 1-dimensionale Unterräume, die nicht in $\text{Filter}(U_0)$ und nicht in $\text{Ideal}(H_0)$ liegen, und damit sind durch die $p_i + \beta p_0$ bereits alle abgedeckt.

Es ist häufig sinnvoll, Hyperebenen von $GF(q)^n$ mit den Kernen von Linearformen aus $GF(q)^{n*}$ zu identifizieren. Hier definiere man $\sigma_{i,\beta} : GF(q)^n \rightarrow GF(q)$ durch

$$\sigma_{i,\beta}(p) := \begin{cases} 0, & \text{falls } p \in H_{i,\beta} \cap H_0, \\ 0, & \text{falls } p = p_i + \beta p_0, \\ \beta, & p = p_i. \end{cases}$$

Da p_i kein Vielfaches von $p_i + \beta p_0$ ist und aus $p_i \in H_0$ und $p_0 \notin H_0$ sowie $p_i + \beta p_0 \in H_{i,\beta}$ auch $p_i + \beta p_0 \notin H_{i,\beta} \cap H_0$ und $p_i \notin H_{i,\beta} \cap H_0$ folgt, sind diese auf $GF(q)^n = \langle H_{i,\beta} \cap H_0, p_i + \beta p_0, p_i \rangle$ wohldefiniert.

Es folgt dann:

Lemma 5.5. *Für alle $p_j \in H_0$ gilt*

$$p_j + \beta' p_0 \in H_{i,\beta} \Leftrightarrow \sigma_{i,\beta}(p_j) = \beta'.$$

Beweis. Per Definition gilt

$$\sigma_{i,\beta}(p_0) = \sigma_{i,\beta}(\beta^{-1}(p_i + \beta p_0 - p_i)) = \beta^{-1}(\sigma_{i,\beta}(p_i + \beta p_0) - \sigma_{i,\beta}(p_i)) = \beta^{-1}(-\beta) = -1$$

und

$$0 = \sigma_{i,\beta}(p_j + \beta' p_0) = \sigma_{i,\beta}(p_j) - \beta',$$

woraus die Behauptung folgt. \square

Wie man sehen wird, weist die Menge von Linearformen, die durch eine Intervallzerlegung definiert wird, bestimmte Eigenschaften auf. Diese sollen zunächst definiert werden.

Definition 5.6. Eine Menge $S = \{\sigma_{i,\beta} \mid i \in \{1, \dots, s\}, \beta \in GF(q)^*\}$ von Linearformen $\sigma_{i,\beta} : GF(q)^n \rightarrow GF(q)$ heißt **punktweise irreflexiv** auf H_0 , wenn $\sigma_{i,\beta}(p_i) \neq 0$ für alle $i \in \{1, \dots, s\}$ und $\beta \in GF(q)^*$ gilt. S heißt **punktweise antisymmetrisch** auf H_0 , wenn

$$\sigma_{j,\beta'}(p_i) = \sigma_{i,\beta}(p_i) \Rightarrow \sigma_{i,\beta}(p_j) \neq \sigma_{j,\beta'}(p_j)$$

für alle $i, j \in \{1, \dots, s\}$ und $\beta, \beta' \in GF(q)^*$ mit $(i, \beta) \neq (j, \beta')$ gilt.

Es folgt der Nachweis dieser Eigenschaften und man kommt sogar zu einer Äquivalenzaussage.

Satz 5.7. *Sei U ein 1-dimensionaler Unterraum von $GF(q)^n$, H eine dazu komplementäre Hyperebene von $GF(q)^n$ und p_0 ein Repräsentant von U . Es existiert eine Intervallzerlegung von $\mathcal{L}(n, GF(q))$ mit $U_0 := U$ und $H_0 := H$ genau dann, wenn eine Menge $S = \{\sigma_{i,\beta} \mid i \in \{1, \dots, s\}, \beta \in GF(q)^*\}$ von Linearformen $\sigma_{i,\beta} : GF(q)^n \rightarrow GF(q)$ existiert, die punktweise irreflexiv und antisymmetrisch auf H_0 ist.*

Beweis. Es werden beide Richtungen einzeln gezeigt:

• **Intervallzerlegung \Rightarrow Menge von Linearformen:**

Sei

$$\{U_0, U_1, \dots, U_{q^n-1-1}, H_0, H_1, \dots, H_{q^n-1-1}\}$$

eine Intervallzerlegung. Dann gilt per Definition $\sigma_{i,\beta}(p_i) = \beta \neq 0$. Sei nun

$$\sigma_{j,\beta'}(p_i) = \sigma_{i,\beta}(p_i) = \beta \text{ und } \sigma_{i,\beta}(p_j) = \sigma_{j,\beta'}(p_j) = \beta'.$$

Dann gilt nach Lemma 5.5

$$p_i + \beta p_0, p_j + \beta' p_0 \in H_{i,\beta} \text{ und } p_j + \beta' p_0, p_i + \beta p_0 \in H_{j,\beta'}.$$

Damit wäre

$$\langle p_i + \beta p_0, p_j + \beta' p_0 \rangle \in [p_i + \beta p_0, H_{i,\beta}] \cap [p_j + \beta' p_0, H_{j,\beta'}]$$

und somit sind diese beiden Intervalle nicht disjunkt, was nicht sein kann, da eine Intervallzerlegung vorliegt. Insgesamt ist gezeigt, dass durch die Linearformen eine Menge S wie gefordert vorliegt, die punktweise irreflexiv und antisymmetrisch auf H_0 ist.

• **Intervallzerlegung \Leftarrow Menge von Linearformen:**

Sei $S = \{\sigma_{i,\beta} \mid i \in \{1, \dots, s\}, \beta \in GF(q)^*\}$ eine Menge von Linearformen, die punktweise irreflexiv und antisymmetrisch auf H_0 ist. Man definiere

$$H_{i,\beta} := \langle p_i + \beta p_0, H_0 \cap \text{Kern}(\sigma_{i,\beta}) \rangle$$

und betrachte die Intervalle $[p_i + \beta p_0, H_{i,\beta}]$. Angenommen, es gibt ein $W \neq \emptyset$ und $(i, \beta) \neq (j, \beta')$ mit

$$W \in [p_i + \beta p_0, H_{i,\beta}] \cap [p_j + \beta' p_0, H_{j,\beta'}].$$

Dann sind $p_i + \beta p_0, p_j + \beta' p_0 \in W$, also auch $p_i + p_j + (\beta + \beta')p_0 \in W$. Da $p_0 \notin W$ ist, existiert ein $p_k \in H_0$ und $\lambda \in GF(q)^*$ mit $\lambda p_k = p_i + p_j$ und nach Lemma 5.5 ist $\sigma_{i,\beta}(p_k) = \lambda^{-1}(\beta + \beta') = \sigma_{j,\beta'}(p_k)$. Wegen $\sigma_{i,\beta}(p_k) = \lambda^{-1}(\sigma_{i,\beta}(p_i) + \sigma_{i,\beta}(p_j)) = \lambda^{-1}(\beta + \sigma_{i,\beta}(p_j))$ und $\sigma_{j,\beta'}(p_k) = \lambda^{-1}(\sigma_{j,\beta'}(p_i) + \sigma_{j,\beta'}(p_j)) = \lambda^{-1}(\sigma_{j,\beta'}(p_i) + \beta')$ ergibt sich $\sigma_{i,\beta}(p_j) = \beta'$ und $\sigma_{j,\beta'}(p_i) = \beta$. Damit wäre aber

$$\sigma_{j,\beta'}(p_i) = \sigma_{i,\beta}(p_i) = \beta \text{ und } \sigma_{i,\beta}(p_j) = \sigma_{j,\beta'}(p_j) = \beta',$$

ein Widerspruch dazu, dass S punktweise asymmetrisch auf H_0 ist. Somit folgt

$$[p_i + \beta p_0, H_{i,\beta}] \cap [p_j + \beta' p_0, H_{j,\beta'}] = \emptyset$$

für alle $(i, \beta) \neq (j, \beta')$, und die Intervalle sind zusammen mit $\text{Filter}(U)$ und $\text{Ideal}(H)$ eine Intervallzerlegung von $\mathcal{L}(n, GF(q))$.

Insgesamt ist der Satz aus Anzahlgründen bewiesen. \square

Damit ist es gleichgültig, ob eine Menge von Intervallen oder die entsprechende Menge von Linearformen betrachtet wird. Da die Linearformen ab jetzt bevorzugt verwendet werden, wird eine Intervallzerlegung neu definiert, wobei, ähnlich wie bei den beiden Definitionen von Verbänden, auch Definition 3.8 ihre Gültigkeit behalten soll.

Definition 5.8. Sei $n \geq 3$, $U_0 = \langle p_0 \rangle$ ein 1-dimensionaler Unterraum von $GF(q)^n$ und H_0 eine dazu komplementäre Hyperebene. Dann heißt eine Menge

$$S = \{\sigma_{i,\beta} \mid i \in \{1, \dots, s\}, \beta \in GF(q)^*\}$$

von linearen Abbildungen $\sigma_{i,\beta} : GF(q)^n \rightarrow GF(q)$ **Intervallzerlegung** des linearen Verbandes $\mathcal{L}(n, GF(q))$, wenn S punktweise irreflexiv und antisymmetrisch auf H_0 ist.

Ab jetzt nimmt man $U_0 = \langle p_0 \rangle$ und H_0 als gegeben an. Ein wichtiger Bestandteil der weiteren Suche nach Intervallzerlegungen ist der folgende Satz.

Satz 5.9. *Existiert eine Intervallzerlegung von $\mathcal{L}(n, GF(q))$, $n \geq 4$, so existiert auch eine Intervallzerlegung des Verbandes $\mathcal{L}(n-1, GF(q))$.*

Beweis. Sei S eine Intervallzerlegung von $\mathcal{L}(n, GF(q))$. Weiter sei W_0 ein $(n-2)$ -dimensionaler Unterraum von H_0 . Zusammen mit p_0 spannt W_0 dann einen $(n-1)$ -dimensionalen Unterraum von $GF(q)^n$ auf, der isomorph zu $GF(q)^{n-1}$ ist. Für $p_i \in W_0$ und $p \in \langle p_0, W_0 \rangle$ definiere man dann

$$\widetilde{\sigma}_{i,\beta}(p) := \begin{cases} 0, & \text{falls } p \in H_{i,\beta} \cap W_0, \\ 0, & \text{falls } p = p_i + \beta p_0, \\ \beta, & p = p_i. \end{cases}$$

und $\widetilde{S} := \{\widetilde{\sigma}_{i,\beta} \mid i \in \{1, \dots, \widetilde{s}\}, \beta \in GF(q)^*\}$ mit $\widetilde{s} := \frac{q^{n-2}-1}{q-1}$. Dann gilt für alle $p \in W_0$ auch $\widetilde{\sigma}_{i,\beta}(p) = \sigma_{i,\beta}(p)$, da genau dann $p \in H_{i,\beta} \cap W_0$ gilt, wenn $p \in H_{i,\beta} \cap H_0$ gilt. Damit wäre S nicht punktweise irreflexiv und antisymmetrisch auf H_0 , wenn \widetilde{S} nicht punktweise irreflexiv und antisymmetrisch auf W_0 ist. Also erhält man eine Intervallzerlegung von $\mathcal{L}(n-1, GF(q))$. \square

Die im Beweis konstruierte Menge \widetilde{S} , die aus einer Mischung von Restriktion und Projektion von S auf W_0 hervorgegangen ist, wird nun als $S|_{W_0}$ geschrieben und bekommt eine eigene Bezeichnung.

Definition 5.10. Sei $S = \{\sigma_{i,\beta} \mid i \in \{1, \dots, s\}, \beta \in GF(q)^*\}$ eine Menge von Linearformen $\sigma_{i,\beta} : GF(q)^n \rightarrow GF(q)$, $n \geq 4$ und W_0 ein $(n-2)$ -dimensionaler Unterraum von H_0 . Dann heißt die Menge $S|_{W_0}$ **Projektion** von S bezüglich W_0 . Ist S eine Intervallzerlegung von $\mathcal{L}(n, GF(q))$, so heißt die Intervallzerlegung $S|_{W_0}$ von $\mathcal{L}(n-1, GF(q))$ **projizierte Intervallzerlegung** von S bezüglich W_0 .

Es sei betont, dass die Linearformen einer projizierten Intervallzerlegung $S|_{W_0}$ entsprechend dem Beweis von Satz 5.9 formal auf $\langle p_0, W_0 \rangle$ als Teilmenge von $\langle p_0, H_0 \rangle$ definiert sind, und nicht auf dem dazu isomorphen Raum $GF(q)^{n-1}$.

Unter Verwendung der Projektionen ergibt sich sofort folgendes Korollar.

Korollar 5.11. *Eine Menge $S = \{\sigma_{i,\beta} \mid i \in \{1, \dots, s\}, \beta \in GF(q)^*\}$ von Linearformen $\sigma_{i,\beta} : GF(q)^n \rightarrow GF(q)$ ist eine Intervallzerlegung von $\mathcal{L}(n, GF(q))$ genau dann, wenn die Projektion $S|_{W_0}$ bezüglich jedes $(n-2)$ -dimensionalen Unterraums $W_0 \subset H_0$ eine Intervallzerlegung von $\mathcal{L}(n-1, GF(q))$ ist.*

Beweis. Ist S eine Intervallzerlegung und $W_0 \subset H_0$ ein $(n-2)$ -dimensionaler Unterraum, so ist $S|_{W_0}$ nach dem Beweis von Satz 5.9 eine Intervallzerlegung von $\mathcal{L}(n-1, GF(q))$.

Sei nun S eine Menge von Linearformen, die keine Intervallzerlegung von $\mathcal{L}(n, GF(q))$ ist, d.h. S ist nicht punktweise irreflexiv oder nicht punktweise antisymmetrisch auf H_0 . Es gibt also $i, j \in \{1, \dots, s\}$ und $\beta, \beta' \in GF(q)^*$ mit $\sigma_{i,\beta}(p_i) \neq 0$ oder

$$\sigma_{j,\beta'}(p_i) = \sigma_{i,\beta}(p_i) = \beta \text{ und } \sigma_{i,\beta}(p_j) = \sigma_{j,\beta'}(p_j) = \beta'.$$

Wählt man dann einen $(n-2)$ -dimensionalen Unterraum W_0 von H_0 , der p_i und p_j enthält (was immer möglich ist, da $n-2 \geq 2$ ist und $p_i, p_j \in H_0$ sind), so ist $S|_{W_0}$ keine Intervallzerlegung von $\mathcal{L}(n-1, GF(q))$, da $\widetilde{\sigma_{i,\beta}}(p) = \sigma_{i,\beta}(p)$ auf W_0 gilt. \square

Es ist jetzt klar, wie die Projektionen und das letzte Korollar bei der Suche von Intervallzerlegungen eines Verbandes $\mathcal{L}(n, GF(q))$ für $n \geq 4$ helfen können, wenn man (alle) Intervallzerlegungen des Verbandes $\mathcal{L}(n-1, GF(q))$ kennt: Man durchläuft für die $(n-2)$ -dimensionalen Unterräume $W \subset H_0$ alle Kombinationen von Intervallzerlegungen von $\mathcal{L}(n-1, GF(q))$. Zu beachten ist lediglich noch, dass die ausgewählten Intervallzerlegungen miteinander **verträglich** sein müssen, d.h. sind $S|_{W_1}$ und $S|_{W_2}$ die projizierten Intervallzerlegungen auf zwei Unterräumen W_1 und W_2 , so müssen diese auf $W_1 \cap W_2$ gleich sein, also $(S|_{W_1})|_{W_1 \cap W_2} = (S|_{W_2})|_{W_1 \cap W_2}$. In der praktischen Anwendung ist es oft sinnvoll, nicht die Projektionen bezüglich aller $(n-2)$ -dimensionalen Unterräume in H_0 zu verwenden, sondern die Verwendung von Projektionen mit der Überprüfung der Bedingungen aus Definition 5.6 zu kombinieren. Dies wird in den Abschnitten 5.2 und 5.3 genauer ausgeführt. Die Grundlage dafür ist das folgende Korollar, dessen Beweis sich sofort aus dem bereits Geschriebenen ergibt.

Korollar 5.12. *Seien W_1, \dots, W_k $(n-2)$ -dimensionale Unterräume in H_0 . Eine Menge $S = \{\sigma_{i,\beta} \mid i \in \{1, \dots, s\}, \beta \in GF(q)^*\}$ von Linearformen $\sigma_{i,\beta} : GF(q)^n \rightarrow GF(q)$ ist eine Intervallzerlegung von $\mathcal{L}(n, GF(q))$ genau dann, wenn die Projektionen $S|_{W_l}$, $l \in \{1, \dots, k\}$ Intervallzerlegungen von $\mathcal{L}(n-1, GF(q))$ sind und $\sigma_{i,\beta}(p_i) \neq 0$ sowie*

$$\sigma_{j,\beta'}(p_i) = \sigma_{i,\beta}(p_i) \Rightarrow \sigma_{i,\beta}(p_j) \neq \sigma_{j,\beta'}(p_j)$$

für alle $p_i, p_j \in H_0$, für die es kein $l \in \{1, \dots, k\}$ mit $p_i, p_j \in W_l$ gibt, gilt.

Bevor ein auf diesem Korollar basierendes Verfahren in die Tat umgesetzt wird, kann man die $\sigma_{i,\beta}$ einer Intervallzerlegung S noch auf eine bestimmte Art und Weise ordnen.

Proposition 5.13. *Ist $S = \{\sigma_{i,\beta} \mid i \in \{1, \dots, s\}, \beta \in GF(q)^*\}$ eine Intervallzerlegung von $\mathcal{L}(n, GF(q))$, so existiert eine Partition M_1, \dots, M_{q-1} von S derart, dass*

$$i \neq j \text{ und } \text{Kern}(\sigma_{i,\beta}) \cap H_0 \neq \text{Kern}(\sigma_{j,\beta'}) \cap H_0$$

für alle $\sigma_{i,\beta}, \sigma_{j,\beta'} \in M_\alpha$, $\alpha \in GF(q)^*$, mit $(i, \beta) \neq (j, \beta')$ gilt.

Beweis. Man betrachte den bipartiten Graphen $G = (V_1 \cup V_2, E)$ mit

$$V_1 := \{1, \dots, s\}, V_2 := \{\text{Kern}(\sigma_{i,\beta}) \cap H_0 \mid i \in \{1, \dots, s\}\}$$

und

$$E := \{\{i, \text{Kern}(\sigma_{i,\beta}) \cap H_0\} \mid i \in \{1, \dots, s\}, \beta \in GF(q)^*\}.$$

Dieser ist $(q - 1)$ -regulär, denn jedem $i \in \{1, \dots, s\}$ ist genau für jedes $\beta \in GF(q)^*$ ein $\text{Kern}(\sigma_{i,\beta}) \cap H_0$ zuordnet, und genau bei den $q - 1$ Vielfachen einer Linearform $\sigma_{i,\beta}$ ist $\text{Kern}(\sigma_{i,\beta}) \cap H_0$ gleich. Nach Korollar 4.18 existieren also $q - 1$ perfekte Matchings M_1, \dots, M_{q-1} von G , und dies ist genau die Aussage der Proposition. □

Dadurch lässt sich eine Intervallzerlegung S also in $q - 1$ im Sinne der Proposition gleichartige Teilmengen aufteilen. Man weiß dann beispielsweise, dass in jeder Teilmenge M_α genau ein Vielfaches jeder Linearform $\sigma_{i,\beta}$ vorkommt. Dies kann vorteilhaft sein, wenn man eine Intervallzerlegung eines linearen Verbandes sucht.

Eine solche soll nun auch aufgeschrieben werden, und zwar von $\mathcal{L}(3, GF(3))$; die Existenz ist ja inzwischen bekannt. Dazu sei $\{p_0, e_1, e_2\}$ eine Basis von $GF(3)^3$ und $\{d_0, d_1, d_2\}$ die dazu duale Basis. Außerdem wird, immer wenn die Punkte bezüglich einer Basis dargestellt werden, die Indizierung der Linearformen etwas verändert: Für $p \in H_0$ schreibt man $\sigma_{p,\beta}$. Damit ist die Linearform $\sigma_{i,\beta}$ gemeint mit $p_i = p$.

Beispiel 5.14. In der folgenden Tabelle ist eine Intervallzerlegung nach Definition 5.8 von $\mathcal{L}(3, GF(3))$ zu sehen. Genauer gesagt wird die Menge

$p_i \in H_0$	$\sigma_{i,1} \in S$	$\sigma_{i,2} \in S$
e_1	d_1	$2d_1 + 2d_2$
e_2	$2d_1 + d_2$	$d_1 + 2d_2$
$e_1 + e_2$	d_2	$d_1 + d_2$
$e_1 + 2e_2$	$2d_2$	$2d_1$

Tabelle 1: Intervallzerlegung von $\mathcal{L}(3, GF(3))$

$$S = \{\sigma_{e_1,1} = d_1, \sigma_{e_2,1} = 2d_1 + d_2, \sigma_{e_1+e_2,1} = d_2, \sigma_{e_1+2e_2,1} = 2d_2, \\ \sigma_{e_1,2} = 2d_1 + 2d_2, \sigma_{e_2,2} = d_1 + 2d_2, \sigma_{e_1+e_2,2} = d_1 + d_2, \sigma_{e_1+2e_2,2} = 2d_1\}$$

durch Tabelle 1 dargestellt, und diese ist punktweise irreflexiv und antisymmetrisch auf $H_0 = \langle e_1, e_2 \rangle$. Jede der Linearformen steht für ein Intervall der zugehörigen Intervallzerlegung nach Definition 3.8.

Ist beispielsweise $p_0 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, $e_1 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ und $e_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$, so konstruiert man zum

Beispiel zu $\sigma_{e_2,1} = 2d_1 + d_2$, wie im Beweis von Satz 5.7 beschrieben, zuerst

$$\begin{aligned} H_{(0,0,1)^T,1} &= \left\langle \left(\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} + 1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \left\langle \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\rangle \cap \left\langle \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \right\rangle \right\rangle \\ &= \left\langle \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \right\rangle \end{aligned}$$

und erhält daraus das Intervall

$$\left[\left\langle \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \right\rangle \right].$$

Durch Satz 5.7 ist klar, dass die so konstruierten Intervalle zusammen mit $\text{Filter}(\langle p_0 \rangle)$ und $\text{Ideal}(H_0)$ eine Intervallzerlegung im Sinne der ursprünglichen Definition 3.8 darstellen.

Im Übrigen ist durch

$$\begin{aligned} M_1 &= \{\sigma_{e_1,1} = d_1, \sigma_{e_2,2} = d_1 + 2d_2, \sigma_{e_1+e_2,2} = d_1 + d_2, \sigma_{e_1+2e_2,1} = 2d_2\} \text{ und} \\ M_2 &= \{\sigma_{e_1,2} = 2d_1 + 2d_2, \sigma_{e_2,1} = 2d_1 + d_2, \sigma_{e_1+e_2,1} = d_2, \sigma_{e_1+2e_2,2} = 2d_1\} \end{aligned}$$

eine Partition von S wie in Proposition 5.13 gegeben.

Wie man außerdem sieht, erfüllen die Linearformen aus M_1 die Eigenschaft

$$\sigma_{e_j, \beta_j}(e_k) = 0 \Leftarrow k > j,$$

$k, j \in \{1, 2\}$, wenn sie zur Basis $\{e_1, e_2\}$ dargestellt werden und man β_1, β_2 so wählt, dass $\sigma_{e_j, \beta_j} \in M_1$ für $j \in \{1, 2\}$ gilt. Dass es für jedes M_α , $\alpha \in GF(q)^*$ eine solche Basis gibt, zeigt das folgende Lemma.

Lemma 5.15. *Sei $S = \{\sigma_{i,\beta} \mid i \in \{1, \dots, s\}, \beta \in GF(q)^*\}$ eine Intervallzerlegung von $\mathcal{L}(n, GF(q))$ und M_1, \dots, M_{q-1} eine Partition von S wie in Proposition 5.13. Dann gibt es für jedes $\alpha \in GF(q)^*$ Punkte $e_1, \dots, e_{n-1} \in H_0$ und $\beta_1, \dots, \beta_{n-1} \in GF(q)^*$, sodass alle $\sigma_{e_k, \beta_k} \in M_\alpha$ sind, $\{p_0, e_1, \dots, e_{n-1}\}$ eine Basis von $GF(q)^n$ ist und*

$$\sigma_{e_j, \beta_j}(e_k) = 0 \Leftarrow k > j$$

für $j, k \in \{1, \dots, n-1\}$ gilt.

Beweis. Sei $\alpha \in GF(q)^*$ beliebig. Es wird durch Induktion nach i gezeigt, dass es für jedes $i \in \{1, \dots, n-1\}$ linear unabhängige Punkte $e_1, \dots, e_{i-1} \in H_0$ sowie $\beta_1, \dots, \beta_{i-1} \in GF(q)^*$ gibt, dass $\sigma_{e_k, \beta_k} \in M_\alpha$ und $\sigma_{e_j, \beta_j}(e_k) = 0 \Leftarrow k > j$ für alle $j, k \in \{1, \dots, i-1\}$ gilt, und dass $b_i, \dots, b_{n-1} \in H_0 \cap \bigcap_{j=1}^{i-1} \text{Kern}(\sigma_{e_j, \beta_j})$ existieren, sodass $\{p_0, e_1, \dots, e_{i-1}, b_i, \dots, b_{n-1}\}$ eine Basis von $GF(q)^n$ ist.

Der Induktionsanfang ($i = 1$) ist trivial, denn die Menge $\{e_1, \dots, e_{i-1}\}$ ist dann leer, und

natürlich gibt es $b_1, \dots, b_{n-1} \in H_0$, sodass $\{p_0, b_1, \dots, b_{n-1}\}$ eine Basis von $GF(q)^n$ ist. Sei nun angenommen, die Aussage gelte für ein $i \in \{1, \dots, n-2\}$. Dann setze man $e_i := b_i$ und wähle $\beta_i \in GF(q)^*$ so aus, dass $\sigma_{e_i, \beta_i} \in M_\alpha$ ist. Dann sind e_1, \dots, e_i linear unabhängig und so beschaffen, dass $\sigma_{e_j, \beta_j}(e_k) = 0 \Leftrightarrow k > j$ für $j, k \in \{1, \dots, i\}$ gilt. Zudem setze man

$$\widehat{b}_k := b_k - \sigma_{e_i, \beta_i}(b_k)(\sigma_{e_i, \beta_i}(e_i))^{-1}e_i.$$

Da

$$\sigma_{e_j, \beta_j}(b_k) = \sigma_{e_j, \beta_j}(e_i) = 0$$

für $j \in \{1, \dots, i-1\}$ und

$$\sigma_{e_i, \beta_i}(b_k - \sigma_{e_i, \beta_i}(b_k)(\sigma_{e_i, \beta_i}(e_i))^{-1}e_i) = \sigma_{e_i, \beta_i}(b_k) - \sigma_{e_i, \beta_i}(b_k)(\sigma_{e_i, \beta_i}(e_i))^{-1}\sigma_{e_i, \beta_i}(e_i) = 0$$

gilt, liegen $\widehat{b}_{i+1}, \dots, \widehat{b}_{n-1}$ in $H_0 \cap \bigcap_{j=1}^i \text{Kern}(\sigma_{e_j, \beta_j})$ und $\{p_0, e_1, \dots, e_i, \widehat{b}_{i+1}, \dots, \widehat{b}_{n-1}\}$ ist eine

Basis von $GF(q)^{n-1}$, womit der Induktionsschritt vollzogen ist.

Damit ist die Aussage bewiesen. \square

Man kommt damit zu folgendem Begriff:

Definition 5.16. Eine Intervallzerlegung $S = \{\sigma_{i, \beta} \mid i \in \{1, \dots, s\}, \beta \in GF(q)^*\}$ heißt **normiert** durch eine Basis $\{p_0, e_1, \dots, e_{n-1}\}$ von $GF(q)^n$, wenn es ein $\alpha \in GF(q)^*$ und $\beta_1, \dots, \beta_{n-1} \in GF(q)^*$ gibt, sodass $\sigma_{e_k, \beta_k} \in M_\alpha$ und

$$\sigma_{e_j, \beta_j}(e_k) = 0 \Leftrightarrow k > j$$

für $j, k \in \{1, \dots, n-1\}$ gilt.

Im Folgenden soll aber eine Art von Intervallzerlegungen im Vordergrund stehen, die besonders einfach ist, sodass dort die Aussage von Proposition 5.13 trivial ist.

Definition 5.17. Eine Intervallzerlegung $S = \{\sigma_{i, \beta} \mid i \in \{1, \dots, s\}, \beta \in GF(q)^*\}$ heißt **strukturiert**, wenn

$$\text{Kern}(\sigma_{i, \beta}) \cap H_0 = \text{Kern}(\sigma_{i, \beta'}) \cap H_0$$

für alle $\beta, \beta' \in GF(q)^*$ gilt.

Trivialerweise ist jede Intervallzerlegung eines linearen Verbandes über $GF(2)$ strukturiert. Im allgemeinen Fall einer strukturierten Intervallzerlegung ist beispielsweise durch

$$M_\alpha := \{\sigma_{i, \beta} \mid i \in \{1, \dots, s\}, \beta = \alpha\}$$

eine Partition der Linearformen wie in Proposition 5.13 gegeben.

Bei der Notation von strukturierten Intervallzerlegungen genügt es, für jedes $i \in \{1, \dots, s\}$ eine Linearform $\sigma_{i, \beta}$ anzugeben, da alle $\sigma_{i, \beta}$, $\beta \in GF(q)^*$ Vielfache voneinander sind. Das β im Index wird dann auch weggelassen; es ergibt sich aus $\sigma_i(p_i)$. Dementsprechend macht es auch keinen Unterschied, welches Vielfache angegeben wird, da dies auf die gleichen Linearformen $\sigma_{i, \beta}$, $\beta \in GF(q)^*$ führt. Folgende Proposition zeigt, wie die Bedingungen der punktwisen Irreflexivität und Antisymmetrie auf H_0 für eine strukturierte Intervallzerlegung im Speziellen aussehen.

Proposition 5.18. *Eine Menge $S = \{\gamma\sigma_i \mid i \in \{1, \dots, s\}, \gamma \in GF(q)^*\}$ von Linearformen $\sigma_i : GF(q)^n \rightarrow GF(q)$ ist eine Intervallzerlegung genau dann, wenn $\sigma_i(p_i) \neq 0$ für alle $i \in \{1, \dots, s\}$ sowie*

$$\gamma\sigma_j(p_i) = \sigma_i(p_i) \Rightarrow \sigma_i(p_j) \neq \gamma\sigma_j(p_j)$$

für alle $i \neq j \in \{1, \dots, s\}$ und $\gamma \in GF(q)^*$ gilt.

Beweis. Es gilt $\sigma_i(p_i) \neq 0$ für alle $i \in \{1, \dots, s\}$ genau dann, wenn dies auch für alle Vielfachen $\delta\sigma_i$, $\delta \in GF(q)^*$ gilt. Zudem ist die Gültigkeit von $\delta'\sigma_j(p_i) = \delta\sigma_i(p_i) \Rightarrow \delta\sigma_i(p_j) \neq \delta'\sigma_j(p_j)$ für alle $i, j \in \{1, \dots, s\}$ und $\delta, \delta' \in GF(q)^*$ mit $(i, \delta) \neq (j, \delta')$ gleichbedeutend mit der von $(\delta^{-1}\delta')\sigma_j(p_i) = \sigma_i(p_i) \Rightarrow \sigma_i(p_j) \neq (\delta^{-1}\delta')\sigma_j(p_j)$ für alle $i \neq j \in \{1, \dots, s\}$ und $\gamma = (\delta^{-1}\delta') \in GF(q)^*$, denn für $i = j \in \{1, \dots, s\}$ und $\delta \neq \delta' \in GF(q)^*$ gilt die Bedingung per Definition immer.

Daraus folgt zusammen mit Definition 5.6 die Aussage. \square

Im nächsten Abschnitt wird nun nach Intervallzerlegungen, insbesondere strukturierten, der linearen Verbände $\mathcal{L}(n, GF(2))$ und $\mathcal{L}(n, GF(3))$ für $n \geq 4$ gesucht.

5.2 Die Fälle $\mathcal{L}(n, GF(2))$ und $\mathcal{L}(n, GF(3))$

Zur Suche von strukturierten Intervallzerlegungen wird Korollar 5.12 in ein konkretes Verfahren umgesetzt, das sich als Algorithmus formulieren lässt. Dieser Algorithmus wird auf lineare Verbände über $GF(2)$ manuell angewendet und für lineare Verbände über $GF(3)$ als Computerprogramm implementiert.

Sei $\{p_0, e_1, \dots, e_{n-1}\}$ eine Basis von $GF(q)^n$ und $\{d_0, d_1, \dots, d_{n-1}\}$ die dazu duale Basis sowie $H_0 = \langle e_1, \dots, e_{n-1} \rangle$. Angenommen, man kennt alle Intervallzerlegungen von $\mathcal{L}(n-1, GF(q))$. Seien $W_1, \dots, W_k \subset H_0$ $(n-2)$ -dimensionale Unterräume in $\mathcal{L}(n, GF(q))$. Man kann dann wie folgt vorgehen, um nach Intervallzerlegungen von $\mathcal{L}(n, GF(q))$ zu suchen: Man durchläuft für die W_l , $l \in \{1, \dots, k\}$ alle Kombinationen an Intervallzerlegungen von $\mathcal{L}(n-1, GF(q))$, und zwar isomorph abgebildet auf $\langle p_0, W_l \rangle$.

Beispiel 5.19. Aus der Intervallzerlegung S aus Beispiel 5.14 isomorph abgebildet auf $\langle p_0, e_2, e_3 \rangle$ erhält man

$$S = \{\sigma_{e_2,1} = d_2, \sigma_{e_3,1} = 2d_2 + d_3, \sigma_{e_2+e_3,1} = d_3, \sigma_{e_2+2e_3,1} = 2d_3, \\ \sigma_{e_2,2} = 2d_2, \sigma_{e_3,2} = 2d_2 + 2d_3, \sigma_{e_2+e_3,2} = d_2 + d_3, \sigma_{e_2+2e_3,2} = d_2 + 2d_3\}$$

Eine solche Kombination wird als k -Tupel (S_1, \dots, S_k) dargestellt. Dann überprüft man, ob die S_l paarweise miteinander verträglich sind. Gegebenenfalls betrachtet man alle Mengen S , für die $S|_{W_l} = S_l$ für alle $l \in \{1, \dots, k\}$ gilt, und überprüft für alle $p_i, p_j \in H_0$, für die $\langle p_i, p_j \rangle \not\subset W_l$ für alle $l \in \{1, \dots, k\}$ gilt, die Bedingungen aus Definition 5.6.

Nach Korollar 5.12 findet man durch diese Vorgehensweise genau die Intervallzerlegungen von $\mathcal{L}(n, GF(q))$. Dieses Verfahren ist in Pseudocode als Algorithmus 1 aufgeschrieben, wobei mit

Algorithmus 1 Allgemeine Suche nach Intervallzerlegungen

```

for all  $(S_1, \dots, S_k) \in Z^k$  do {Schleife 1}
  iszerlegung  $\leftarrow true$ ;
  for all  $i < j \in \{1, \dots, k\}$  do {Schleife 2}
    if  $S_i|_{W_i \cap W_j} \neq S_j|_{W_i \cap W_j}$  then {Verträglichkeit}
      iszerlegung  $\leftarrow false$ ;
      break;
    end if
  end for
  if iszerlegung = true then
    for all  $S$  mit  $S|_{W_l} = S_l$  für alle  $l \in \{1, \dots, k\}$  do {Schleife 3}
      iszerlegung  $\leftarrow true$ ;
      for all  $p_i, p_j$  mit  $\langle p_i, p_j \rangle \notin W_l$  für alle  $l \in \{1, \dots, k\}$ ,
       $\beta, \beta' \in GF(q)^*$  do {Schleife 4}
        if  $\sigma_{i,\beta}(p_i) = 0$  OR  $\sigma_{j,\beta'}(p_i) = \sigma_{i,\beta}(p_i)$  AND  $\sigma_{i,\beta}(p_j) = \sigma_{j,\beta'}(p_j)$  then
          {Irreflexivität und Antisymmetrie}
          iszerlegung  $\leftarrow false$ ;
          break;
        end if
      end for
      if iszerlegung = true then
        print  $S$ ;
      end if
    end for
  end if
end for

```

Z die Menge an Intervallzerlegungen von $\mathcal{L}(n-1, GF(q))$ bezeichnet wird und dementsprechend Z^k die Menge aller k -Tupel solcher Intervallzerlegungen ist.

In dieser allgemeinen Form ist der Algorithmus nicht auf bestimmte Arten von Intervallzerlegungen, etwa auf strukturierte, beschränkt. Konkreter betrachte man nun aber nur strukturierte Intervallzerlegungen betrachtet und als weitere Einschränkung nur solche, die durch $\{p_0, e_1, \dots, e_{n-1}\}$ normiert sind. Dazu wird Algorithmus 1 in einer speziellen Form verwendet.

Algorithmus 1'. Als $(n-2)$ -dimensionale Unterräume verwende man genau diejenigen, die von je $n-2$ Vektoren aus $\{e_1, \dots, e_{n-1}\}$ aufgespannt werden, also $W_l := \langle e_1, \dots, e_{l-1}, e_{l+1}, \dots, e_{n-1} \rangle$ für $l \in \{1, \dots, n-1\}$. Mit dieser Wahl wende man Algorithmus 1 an.

Dass nur strukturierte Intervallzerlegungen gesucht werden, bringt den Vorteil mit sich, dass auch nur die strukturierten Intervallzerlegungen von $\mathcal{L}(n-1, GF(q))$ durchlaufen werden müssen, denn es gilt:

Proposition 5.20. *Sei S eine strukturierte Intervallzerlegung von $\mathcal{L}(n, GF(q))$, $n \geq 4$ und $W \subset H_0$ ein $(n-2)$ -dimensionaler Unterraum in $\mathcal{L}(n, GF(q))$. Dann ist $S|_W$ eine strukturierte Intervallzerlegung von $\mathcal{L}(n-1, GF(q))$.*

Der Beweis folgt direkt aus der Definition der projizierten Intervallzerlegungen. Zusätzlich dazu bringt die konkrete Wahl der $(n-2)$ -dimensionalen Unterräume einen weiteren Vorteil mit sich:

Proposition 5.21. *Seien die W_l , $l \in \{1, \dots, n-1\}$ wie soeben definiert und S eine Intervallzerlegung von $\mathcal{L}(n, GF(q))$, $n \geq 4$. Ist S normiert durch $\{p_0, e_1, \dots, e_{n-1}\}$, so ist $S|_{W_l}$ normiert durch $\{p_0, e_1, \dots, e_{l-1}, e_{l+1}, \dots, e_{n-1}\}$ für alle $l \in \{1, \dots, n-1\}$.*

Wiederum folgt der Beweis unmittelbar aus der Definition. Bei der Wahl anderer $(n-2)$ -dimensionaler Unterräume scheitert eine solche Aussage daran, dass sich diese nicht durch $n-2$ Vektoren aus $\{e_1, \dots, e_{n-1}\}$ aufspannen lassen. Zusätzlich dazu, dass nur strukturierte Intervallzerlegungen durchlaufen werden müssen, müssen nun also auch nur durch eine feste Basis normierte Intervallzerlegungen durchlaufen werden.

Außerdem werden dann auch nur normierte Intervallzerlegungen gefunden, wie man jetzt sieht.

Proposition 5.22. *Seien die W_l , $l \in \{1, \dots, n-1\}$ wie soeben definiert und S eine Intervallzerlegung von $\mathcal{L}(n, GF(q))$, $n \geq 4$. Sind alle $S|_{W_l}$, $l \in \{1, \dots, n-1\}$ durch $\{p_0, e_1, \dots, e_{l-1}, e_{l+1}, \dots, e_{n-1}\}$ normiert, so ist S durch $\{p_0, e_1, \dots, e_{n-1}\}$ normiert.*

Beweis. Sei S nicht normiert, es gebe also $j < k \in \{1, \dots, n-1\}$ mit $\sigma_{e_j}(e_k) \neq 0$. Wählt man W_l so, dass $\{e_j, e_k\} \in W_l$ ist (was immer möglich ist), so ist $S|_{W_l}$ ebenfalls nicht normiert. \square

Der letzte Schritt zur Konkretisierung des Algorithmus besteht darin, dass geklärt wird, welche Mengen von Linearformen S in Schleife 3 genau durchprobiert werden.

Lemma 5.23. *Seien die W_l und S_l , $l \in \{1, \dots, n-1\}$ wie soeben definiert und paarweise miteinander verträglich; für $S = \{\gamma\sigma_{p_i} \mid i \in \{1, \dots, s\}, \gamma \in GF(q)^*\}$ gelte $S|_{W_l} = S_l$ für alle $l \in \{1, \dots, n-1\}$.*

Gibt es $l_1 \neq l_2 \in \{1, \dots, n-1\}$ mit $p_i \in W_{l_1} \cap W_{l_2}$, so ist σ_{p_i} durch S_{l_1} und S_{l_2} bereits wohldefiniert. Gibt es genau ein $l \in \{1, \dots, n-1\}$ mit $p_i \in W_l$, so gilt $\sigma_{p_i} = \rho_{p_i} + \gamma d_l$ für ein $\gamma \in GF(q)$, wenn $S_l = \{\gamma\rho_{p_i} \mid i \in \{1, \dots, s_l\}, \gamma \in GF(q)^\}$ ist.*

Beweis. Gibt es $l_1 \neq l_2 \in \{1, \dots, n-1\}$ mit $p_i \in W_{l_1} \cap W_{l_2}$ und gilt $S|_{W_{l_1}} = S_{l_1}$ und $S|_{W_{l_2}} = S_{l_2}$, so muss $\sigma_{p_i}|_{W_{l_1}} = \rho_{p_i}$ und $\sigma_{p_i}|_{W_{l_2}} = \tau_{p_i}$ gelten, wenn $S_{l_1} = \{\gamma\rho_{p_i} \mid i \in \{1, \dots, s_{l_1}\}, \gamma \in GF(q)^*\}$ und $S_{l_2} = \{\gamma\tau_{p_i} \mid i \in \{1, \dots, s_{l_2}\}, \gamma \in GF(q)^*\}$ ist. Da $W_{l_1} + W_{l_2} = H_0$ ist, ist σ_{p_i} durch die Linearität vollständig wohldefiniert.

Gibt es genau ein $l \in \{1, \dots, n-1\}$ mit $p_i \in W_l$, so ist σ_{p_i} auf W_l definiert, aber auf $\langle e_l \rangle$ beliebig. Also gilt $\sigma_{p_i} = \rho_{p_i} + \gamma d_l$ für ein $\gamma \in GF(q)$. \square

Bei solchen p_i , die in keinem der W_l liegen, ist für σ_{p_i} natürlich überhaupt nichts vorgegeben.

Durch die Definition der W_l liegt p_i in keinem der W_l , wenn $p_i = \sum_{k=1}^{n-1} \gamma_k e_k$ mit $\gamma_k \in GF(q)^*$ für alle $k \in \{1, \dots, n-1\}$ ist; es gibt $(q-1)^{n-2}$ solcher p_i , die paarweise voneinander linear unabhängig sind. Ein p_i liegt in genau einem der W_l , wenn $p_i = \sum_{k=1}^{n-1} \gamma_k e_k$ mit $\gamma_{k^*} = 0$ für ein

$k^* \in \{1, \dots, n-1\}$ und $\gamma_k \in GF(q)^*$ für $k \in \{1, \dots, n-1\} \setminus k^*$ ist; davon gibt es $(n-1)(q-1)^{n-3}$ paarweise linear unabhängige p_i .

Damit kann die Suche nach Intervallzerlegungen von $\mathcal{L}(n, GF(2))$ beginnen.

Für $\mathcal{L}(2, GF(2))$ ist das Intervallzerlegungsproblem nicht definiert, deshalb können keine Intervallzerlegungen von $\mathcal{L}(2, GF(2))$ verwendet werden; zur Suche nach Intervallzerlegungen von $\mathcal{L}(3, GF(2))$ kann der Algorithmus also keine Anwendung finden. Anstattdessen hilft aber reines Ausprobieren.

Proposition 5.24. *Es existiert genau eine Intervallzerlegung von $\mathcal{L}(3, GF(2))$, die durch $\{p_0, e_1, e_2\}$ normiert ist.*

Beweis. Für eine durch $\{p_0, e_1, e_2\}$ normierte Intervallzerlegung $S = \{\sigma_i \mid i \in \{1, \dots, s\}\}$ von $\mathcal{L}(3, GF(2))$ gilt nach Definition 5.16 $\sigma_{e_1} = d_1$. Damit kann nicht auch $\sigma_{e_1+e_2} = d_1$ gelten, und es bleibt $\sigma_{e_1+e_2} = d_2$ oder $\sigma_{e_1+e_2} = d_1 + d_2$. Wäre $\sigma_{e_1+e_2} = d_1 + d_2$, so wäre $\sigma_{e_1+e_2}(e_1 + e_2) = 1 + 1 = 0$, womit S nicht punktweise irreflexiv auf H_0 wäre, was nicht sein darf. Es folgt $\sigma_{e_1+e_2} = d_2$ und damit bleibt für σ_{e_2} nur $\sigma_{e_2} = d_1 + d_2$.

$p_i \in H_0$	$\sigma_i \in S$
e_1	d_1
e_2	$d_1 + d_2$
$e_1 + e_2$	d_2

Tabelle 2: Intervallzerlegung von $\mathcal{L}(3, GF(2))$

Überprüft man die Bedingungen aus Definition 5.6 für die so konstruierte Menge S , die in Tabelle 2 nochmals aufgeschrieben ist, so erkennt man, dass diese tatsächlich punktweise irreflexiv und antisymmetrisch auf H_0 und damit eine Intervallzerlegung von $\mathcal{L}(3, GF(2))$ ist. \square

Für $\mathcal{L}(4, GF(2))$ kann jetzt Algorithmus 1' verwendet werden. Das Ergebnis wird hier manuell ermittelt, indem die Schleifen logisch ausgewertet und nicht wie bei einem Computerprogramm einfach nacheinander durchlaufen werden.

Proposition 5.25. *Es existiert genau eine Intervallzerlegung von $\mathcal{L}(4, GF(2))$, die durch $\{p_0, e_1, e_2, e_3\}$ normiert ist.*

Beweis. Dies ist das Ergebnis der Anwendung von Algorithmus 1'. Da nur genau eine Intervallzerlegung von $\mathcal{L}(3, GF(2))$ existiert, wird Schleife 1 genau einmal durchlaufen und die projizierten Intervallzerlegungen einer möglichen Intervallzerlegung S von $\mathcal{L}(4, GF(2))$ bezüglich der W_l sind durch

$$\begin{aligned} S_1 &= \{\sigma_{e_2} = d_2, \sigma_{e_3} = d_2 + d_3, \sigma_{e_2+e_3} = d_3\}, \\ S_2 &= \{\sigma_{e_1} = d_1, \sigma_{e_3} = d_1 + d_3, \sigma_{e_1+e_3} = d_3\} \text{ und} \\ S_3 &= \{\sigma_{e_1} = d_1, \sigma_{e_2} = d_1 + d_2, \sigma_{e_1+e_2} = d_2\} \end{aligned}$$

vorgegeben. Offensichtlich stimmen die Linearformen dieser Mengen auf $\langle e_1 \rangle$, $\langle e_2 \rangle$ und $\langle e_3 \rangle$ überein, sodass die Verträglichkeit gegeben ist; dies ist das Ergebnis von Schleife 2. Damit kommt man zu den nächsten Schleifen.

• **Schleife 3:**

Nach Lemma 5.23 sind σ_{e_1} , σ_{e_2} und σ_{e_3} durch die Projektionen bereits wohldefiniert. Damit gilt $\sigma_{e_1} = d_1$, $\sigma_{e_2} = d_1 + d_2$ und $\sigma_{e_3} = d_1 + d_2 + d_3$.

Für die Linearformen $\sigma_{e_1+e_2}$, $\sigma_{e_1+e_3}$ und $\sigma_{e_2+e_3}$ gilt nach Lemma 5.23

$$\begin{aligned}\sigma_{e_1+e_2} &= d_2 + \gamma_1 d_3, \\ \sigma_{e_1+e_3} &= d_3 + \gamma_2 d_2 \text{ und} \\ \sigma_{e_2+e_3} &= d_3 + \gamma_3 d_1\end{aligned}$$

mit $\gamma_1, \gamma_2, \gamma_3 \in GF(2)$. Lediglich für $\sigma_{e_1+e_2+e_3}$ ist durch die Projektionen nichts vorgegeben, sodass dafür prinzipiell alle Möglichkeiten in Frage kommen.

• **Schleife 4:**

Schleife 4 überprüft nun, welche der zu durchlaufenden Mengen von Linearformen tatsächlich die Bedingungen aus Definition 5.6 erfüllen. Für $\sigma_{e_1+e_2+e_3}$ sind d_1 , d_2 , d_3 und $d_1 + d_2 + d_3$ möglich, um Irreflexivität zu erreichen; davon fallen d_1 und $d_1 + d_2 + d_3$ weg, da diese Linearformen schon anderen Punkten zugeordnet wurden. Also bleibt $\sigma_{e_1+e_2+e_3} = d_2$ oder $\sigma_{e_1+e_2+e_3} = d_3$. Nimmt man $\sigma_{e_1+e_2+e_3} = d_3$ an, so folgt $\sigma_{e_1+e_2+e_3}(e_3) = \sigma_{e_3}(e_3) = \sigma_{e_1+e_2+e_3}(e_1 + e_2 + e_3) = \sigma_{e_3}(e_1 + e_2 + e_3) = 1$, was nicht sein darf. Also muss $\sigma_{e_1+e_2+e_3} = d_2$ sein und aus den anderen Bedingungen folgt sofort $\sigma_{e_1+e_2} = d_2 + d_3$, $\sigma_{e_1+e_3} = d_3$ und $\sigma_{e_2+e_3} = d_1 + d_3$.

$p_i \in H_0$	$\sigma_i \in S$
e_1	d_1
e_2	$d_1 + d_2$
e_3	$d_1 + d_2 + d_3$
$e_1 + e_2$	$d_2 + d_3$
$e_1 + e_3$	d_3
$e_2 + e_3$	$d_1 + d_3$
$e_1 + e_2 + e_3$	d_2

Tabelle 3: Intervallzerlegung von $\mathcal{L}(4, GF(2))$

Durch eine abschließende Überprüfung stellt man fest, dass S (siehe auch Tabelle 3) tatsächlich punktweise irreflexiv und antisymmetrisch auf H_0 ist und damit eine Intervallzerlegung.

Insgesamt ist die Aussage als Ergebnis von Algorithmus 1' bewiesen. □

Genauso kann man bei $\mathcal{L}(5, GF(2))$ vorgehen. Man kommt dort aber auf ein anderes Ergebnis.

Proposition 5.26. *Es existiert keine Intervallzerlegung von $\mathcal{L}(5, GF(2))$.*

Beweis. Wie man gesehen hat, existiert auch nur genau eine Intervallzerlegung von $\mathcal{L}(4, GF(2))$, also wird Schleife 1 auch hier genau einmal durchlaufen. Die projizierten Intervallzerlegungen einer möglichen Intervallzerlegung S von $\mathcal{L}(5, GF(2))$ bezüglich der W_l sind durch

$$\begin{aligned} S_1 &= \{\sigma_{e_2} = d_2, \sigma_{e_3} = d_2 + d_3, \sigma_{e_4} = d_2 + d_3 + d_4, \\ &\quad \sigma_{e_2+e_3} = d_3 + d_4, \sigma_{e_2+e_4} = d_4, \sigma_{e_3+e_4} = d_2 + d_4, \sigma_{e_2+e_3+e_4} = d_3\}, \\ S_2 &= \{\sigma_{e_1} = d_1, \sigma_{e_3} = d_1 + d_3, \sigma_{e_4} = d_1 + d_3 + d_4, \\ &\quad \sigma_{e_1+e_3} = d_3 + d_4, \sigma_{e_1+e_4} = d_4, \sigma_{e_3+e_4} = d_1 + d_4, \sigma_{e_1+e_3+e_4} = d_3\}, \\ S_3 &= \{\sigma_{e_1} = d_1, \sigma_{e_2} = d_1 + d_2, \sigma_{e_4} = d_1 + d_2 + d_4, \\ &\quad \sigma_{e_1+e_2} = d_2 + d_4, \sigma_{e_1+e_4} = d_4, \sigma_{e_2+e_4} = d_1 + d_4, \sigma_{e_1+e_2+e_4} = d_2\} \text{ und} \\ S_4 &= \{\sigma_{e_1} = d_1, \sigma_{e_2} = d_1 + d_2, \sigma_{e_3} = d_1 + d_2 + d_3, \\ &\quad \sigma_{e_1+e_2} = d_2 + d_3, \sigma_{e_1+e_3} = d_3, \sigma_{e_2+e_3} = d_1 + d_3, \sigma_{e_1+e_2+e_3} = d_2\} \end{aligned}$$

vorgegeben. Wieder sind diese Projektionen miteinander verträglich, denn die Linearformen der Mengen stimmen auf $\langle e_1, e_2 \rangle$, $\langle e_1, e_3 \rangle$ und $\langle e_2, e_3 \rangle$ überein. Jetzt folgen die Schleifen 3 und 4.

- **Schleife 3:**

Nach Lemma 5.23 sind σ_{e_1} , σ_{e_2} , σ_{e_3} , σ_{e_4} , $\sigma_{e_1+e_2}$, $\sigma_{e_1+e_3}$, $\sigma_{e_1+e_4}$, $\sigma_{e_2+e_3}$, $\sigma_{e_2+e_4}$ und $\sigma_{e_3+e_4}$ durch die Projektionen wohldefiniert. Damit gilt $\sigma_{e_1} = d_1$, $\sigma_{e_2} = d_1 + d_2$, $\sigma_{e_3} = d_1 + d_2 + d_3$, $\sigma_{e_4} = d_1 + d_2 + d_3 + d_4$, $\sigma_{e_1+e_2} = d_2 + d_3 + d_4$, $\sigma_{e_1+e_3} = d_3 + d_4$, $\sigma_{e_1+e_4} = d_4$, $\sigma_{e_2+e_3} = d_1 + d_3 + d_4$, $\sigma_{e_2+e_4} = d_1 + d_4$ und $\sigma_{e_3+e_4} = d_1 + d_2 + d_4$.

Für die Linearformen $\sigma_{e_1+e_2+e_3}$, $\sigma_{e_1+e_2+e_4}$, $\sigma_{e_1+e_3+e_4}$ und $\sigma_{e_2+e_3+e_4}$ gilt nach Lemma 5.23

$$\begin{aligned} \sigma_{e_1+e_2+e_3} &= d_2 + \gamma_1 d_4, \\ \sigma_{e_1+e_2+e_4} &= d_2 + \gamma_2 d_3, \\ \sigma_{e_1+e_3+e_4} &= d_3 + \gamma_3 d_2 \text{ und} \\ \sigma_{e_2+e_3+e_4} &= d_3 + \gamma_4 d_1 \end{aligned}$$

mit $\gamma_1, \gamma_2, \gamma_3, \gamma_4 \in GF(2)$. Für $\sigma_{e_1+e_2+e_3+e_4}$ ist durch die Projektionen hier nichts vorgegeben.

- **Schleife 4:**

Nun kommen wieder die Bedingungen aus Definition 5.6 ins Spiel. Wählt man $\sigma_{e_1+e_3+e_4} = d_3$, so folgt $\sigma_{e_1+e_3+e_4}(e_2 + e_3) = \sigma_{e_2+e_3}(e_2 + e_3) = \sigma_{e_1+e_3+e_4}(e_1 + e_3 + e_4) = \sigma_{e_2+e_3}(e_1 + e_3 + e_4) = 1$, was nicht sein darf. Auch die Wahl von $\sigma_{e_2+e_3+e_4} = d_1 + d_3$ führt wegen $\sigma_{e_2+e_3+e_4}(e_1 + e_2) = \sigma_{e_1+e_2}(e_1 + e_2) = \sigma_{e_2+e_3+e_4}(e_2 + e_3 + e_4) = \sigma_{e_1+e_2}(e_2 + e_3 + e_4)$ zum Widerspruch. Also folgt $\sigma_{e_1+e_3+e_4} = d_2 + d_3$ und $\sigma_{e_2+e_3+e_4} = d_3$ und aus den anderen Bedingungen $\sigma_{e_1+e_2+e_3} = d_2 + d_4$ sowie $\sigma_{e_1+e_2+e_4} = d_2$.

Es bleibt nun nur noch eine Linearform übrig und es folgt $\sigma_{e_1+e_2+e_3+e_4} = d_1 + d_3$. Aber auch das kann nicht sein, denn dann wäre $\sigma_{e_1+e_2+e_3+e_4}(e_1 + e_2 + e_3 + e_4) = 1 + 1 = 0$.

Damit existiert in diesem Fall keine Intervallzerlegung, was durch Tabelle 4 nochmals illustriert wird. \square

$p_i \in H_0$	$\sigma_i \in S$
e_1	d_1
e_2	$d_1 + d_2$
e_3	$d_1 + d_2 + d_3$
e_4	$d_1 + d_2 + d_3 + d_4$
$e_1 + e_2$	$d_2 + d_3 + d_4$
$e_1 + e_3$	$d_3 + d_4$
$e_1 + e_4$	d_4
$e_2 + e_3$	$d_1 + d_3 + d_4$
$e_2 + e_4$	$d_1 + d_4$
$e_3 + e_4$	$d_1 + d_2 + d_4$
$e_1 + e_2 + e_3$	d_2 oder $d_2 + d_4$
$e_1 + e_2 + e_4$	d_2 oder $d_2 + d_3$
$e_1 + e_3 + e_4$	d_3 oder $d_2 + d_3$
$e_2 + e_3 + e_4$	d_3 oder $d_1 + d_3$
$e_1 + e_2 + e_3 + e_4$?

 Tabelle 4: Versuch einer Intervallzerlegung von $\mathcal{L}(5, GF(2))$

Zusammengefasst erhält man also:

Satz 5.27. *Eine Intervallzerlegung von $\mathcal{L}(n, GF(2))$ existiert genau dann, wenn $n \leq 4$ ist.*

Beweis. Nach den Propositionen 5.24, 5.25 und 5.26 gibt es Intervallzerlegungen von $\mathcal{L}(3, GF(2))$ und $\mathcal{L}(4, GF(2))$, aber nicht von $\mathcal{L}(5, GF(2))$. Aus Satz 5.9 folgt, dass keine Intervallzerlegung von $\mathcal{L}(n, GF(2))$ mit $n \geq 5$ existiert. □

Einen Beweis dieses Satzes hat Hochstättler bereits im Vorfeld dieser Diplomarbeit erbracht [8], allerdings ohne Projektionen zu verwenden. Darauf wird in Abschnitt 5.3 noch eingegangen.

Mit der gleichen Vorgehensweise wurden auch strukturierte, normierte Intervallzerlegungen von $\mathcal{L}(n, GF(3))$ gesucht. Den Anfang machen die Intervallzerlegungen von $\mathcal{L}(3, GF(3))$, die wieder durch reines Ausprobieren zu ermitteln sind.

Proposition 5.28. *Es existieren genau 3 strukturierte Intervallzerlegungen von $\mathcal{L}(3, GF(3))$, die durch $\{p_0, e_1, e_2\}$ normiert sind.*

Beweis. Für eine durch $\{p_0, e_1, e_2\}$ normierte strukturierte Intervallzerlegung $S = \{\sigma_i \mid i \in \{1, \dots, s\}\}$ von $\mathcal{L}(3, GF(3))$ gilt nach Definition 5.16 $\sigma_{e_1} = d_1$. Wählt man außerdem $\sigma_{e_2} = d_2$, so bleiben für $\sigma_{e_1+e_2}$ die Möglichkeiten $\sigma_{e_1+e_2} = d_1 + d_2$ und $\sigma_{e_1+e_2} = d_1 + 2d_2$. Wäre $\sigma_{e_1+e_2} = d_1 + 2d_2$, so würde dies $\sigma_{e_1+e_2}(e_1 + e_2) = 1 + 2 = 0$ bedeuten, womit S nicht punktweise irreflexiv auf H_0 wäre, was nicht sein darf. Damit folgt $\sigma_{e_1+e_2} = d_1 + d_2$ und dann $\sigma_{e_1+2e_2} = d_1 + 2d_2$. Überprüft man die Bedingungen aus Definition 5.6, so sieht man, dass die

so konstruierte Menge S tatsächlich eine Intervallzerlegung von $\mathcal{L}(3, GF(3))$ ist; da es nicht die einzige ist, wird sie ab jetzt mit S_1 bezeichnet.

Man hat nämlich auch die Möglichkeit, $\sigma_{e_2} = d_1 + d_2$ zu wählen, und auf analoge Art und Weise folgen $\sigma_{e_1+e_2} = d_2$ sowie $\sigma_{e_1+2e_2} = d_1 + 2d_2$, wodurch man die Intervallzerlegung S_2 erhält. Schließlich erhält man die dritte Intervallzerlegung S_3 , wenn man $\sigma_{e_2} = d_1 + 2d_2$ wählt und dann $\sigma_{e_1+e_2} = d_1 + d_2$ sowie $\sigma_{e_1+2e_2} = d_2$ folgert.

$p_i \in H_0$	$\sigma_i \in S_1$	$\sigma_i \in S_2$	$\sigma_i \in S_3$
e_1	d_1	d_1	d_1
e_2	d_2	$d_1 + d_2$	$d_1 + 2d_2$
$e_1 + e_2$	$d_1 + d_2$	d_2	$d_1 + d_2$
$e_1 + 2e_2$	$d_1 + 2d_2$	$d_1 + 2d_2$	d_2

Tabelle 5: Strukturierte Intervallzerlegungen von $\mathcal{L}(3, GF(3))$, S_1 bis S_3

Die in Tabelle 5 nochmals aufgeschriebenen Mengen S_1 , S_2 und S_3 sind tatsächlich punktweise irreflexiv und antisymmetrisch auf H_0 und damit Intervallzerlegungen. \square

Für die Suche nach strukturierten, normierten Intervallzerlegungen von $\mathcal{L}(4, GF(3))$ und $\mathcal{L}(5, GF(3))$ wurde Algorithmus 1' als Computerprogramm implementiert. Da es 3 verschiedene Intervallzerlegungen von $\mathcal{L}(3, GF(3))$ gibt, muss nämlich Schleife 1 des Algorithmus schon $3^3 = 27$ mal durchlaufen werden, was einen beträchtlichen Aufwand darstellt. Es wäre zwar prinzipiell noch möglich, diesen manuell zu bewältigen, aber spätestens bei den, wie man sehen wird, $26^4 = 456.976$ Schleifendurchläufen bei der Suche nach Intervallzerlegungen von $\mathcal{L}(5, GF(3))$ wird dies unmöglich.

Für $\mathcal{L}(4, GF(3))$ erhält man dann:

Proposition 5.29. *Es existieren genau 26 strukturierte Intervallzerlegungen von $\mathcal{L}(4, GF(3))$, die durch $\{p_0, e_1, e_2, e_3\}$ normiert sind.*

Beweis. Die Implementierung von Algorithmus 1' folgt zur Ausgabe genau der 26 strukturierten und durch $\{p_0, e_1, e_2, e_3\}$ normierten Intervallzerlegungen S_1, \dots, S_{26} , von denen S_1 , S_3 und S_6 in Tabelle 6

$p_i \in H_0$	$\sigma_i \in S_1$	$\sigma_i \in S_3$	$\sigma_i \in S_6$
e_1	d_1	d_1	d_1
e_2	d_2	d_2	d_2
e_3	d_3	d_3	d_3
$e_1 + e_2$	$d_1 + d_2 + 2d_3$	$d_1 + d_2 + d_3$	$d_1 + d_2$
$e_1 + 2e_2$	$d_1 + 2d_2 + d_3$	$d_1 + 2d_2 + d_3$	$d_1 + 2d_2$
$e_1 + e_3$	$d_1 + d_2 + d_3$	$d_1 + d_3$	$d_1 + 2d_2 + d_3$
$e_1 + 2e_3$	$d_1 + 2d_2 + 2d_3$	$d_1 + 2d_3$	$d_1 + 2d_2 + 2d_3$
$e_2 + e_3$	$d_2 + d_3$	$2d_1 + d_2 + d_3$	$d_1 + d_2 + d_3$
$e_2 + 2e_3$	$d_2 + 2d_3$	$d_1 + d_2 + 2d_3$	$d_1 + d_2 + 2d_3$
$e_1 + e_2 + e_3$	$d_1 + d_2$	$d_2 + d_3$	$d_1 + d_3$
$e_1 + e_2 + 2e_3$	$d_1 + 2d_3$	$d_1 + d_2$	$d_1 + 2d_3$

$e_1 + 2e_2 + e_3$	$d_1 + d_3$	$d_2 + 2d_3$	$d_2 + 2d_3$
$e_1 + 2e_2 + 2e_3$	$d_1 + 2d_2$	$d_1 + 2d_2$	$d_2 + d_3$

 Tabelle 6: Strukturierte Intervallzerlegungen von $\mathcal{L}(4, GF(3))$, S_1 , S_3 und S_6

und die restlichen Intervallzerlegungen in Anhang A zu finden sind. \square

Setzt man den Computer auf die gleiche Art und Weise zur Suche nach Intervallzerlegungen von $\mathcal{L}(5, GF(3))$ ein, so wird man auch hier fündig.

Proposition 5.30. *Es existieren genau 52 strukturierte Intervallzerlegungen von $\mathcal{L}(5, GF(3))$, die durch $\{p_0, e_1, e_2, e_3, e_4\}$ normiert sind.*

Beweis. Die Implementierung von Algorithmus 1' folgt zur Ausgabe genau der 52 strukturierten und durch $\{p_0, e_1, e_2, e_3, e_4\}$ normierten Intervallzerlegungen S_1, \dots, S_{52} , von denen S_1 in Tabelle 7

$p_i \in H_0$	$\sigma_i \in S_1$
e_1	d_1
e_2	d_2
e_3	d_3
e_4	d_4
$e_1 + e_2$	$d_1 + d_2 + 2d_3 + d_4$
$e_1 + 2e_2$	$d_1 + 2d_2 + d_3 + d_4$
$e_1 + e_3$	$d_1 + d_2 + d_3 + d_4$
$e_1 + 2e_3$	$d_1 + 2d_2 + 2d_3 + d_4$
$e_1 + e_4$	$d_1 + d_4$
$e_1 + 2e_4$	$d_1 + 2d_4$
$e_2 + e_3$	$d_2 + d_3$
$e_2 + 2e_3$	$d_2 + 2d_3$
$e_2 + e_4$	$d_1 + 2d_2 + d_3 + 2d_4$
$e_2 + 2e_4$	$d_1 + d_2 + 2d_3 + 2d_4$
$e_3 + e_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$
$e_3 + 2e_4$	$d_1 + d_2 + d_3 + 2d_4$
$e_1 + e_2 + e_3$	$d_1 + d_2 + 2d_4$
$e_1 + e_2 + 2e_3$	$d_1 + 2d_3 + 2d_4$
$e_1 + 2e_2 + e_3$	$d_1 + d_3 + 2d_4$
$e_1 + 2e_2 + 2e_3$	$d_1 + 2d_2 + 2d_4$
$e_1 + e_2 + e_4$	$d_2 + d_3 + d_4$
$e_1 + e_2 + 2e_4$	$d_1 + d_2 + d_3$
$e_1 + 2e_2 + e_4$	$d_2 + d_3 + 2d_4$
$e_1 + 2e_2 + 2e_4$	$d_1 + 2d_2 + 2d_3$
$e_1 + e_3 + e_4$	$d_2 + 2d_3 + 2d_4$
$e_1 + e_3 + 2e_4$	$d_1 + 2d_2 + d_3$
$e_1 + 2e_3 + e_4$	$d_2 + 2d_3 + d_4$
$e_1 + 2e_3 + 2e_4$	$d_1 + d_2 + 2d_3$

$e_2 + e_3 + e_4$	$d_1 + d_2 + d_4$
$e_2 + e_3 + 2e_4$	$d_1 + 2d_2 + d_4$
$e_2 + 2e_3 + e_4$	$d_1 + 2d_3 + d_4$
$e_2 + 2e_3 + 2e_4$	$d_1 + d_3 + d_4$
$e_1 + e_2 + e_3 + e_4$	$d_1 + d_3$
$e_1 + e_2 + e_3 + 2e_4$	$d_3 + 2d_4$
$e_1 + e_2 + 2e_3 + e_4$	$d_1 + d_2$
$e_1 + e_2 + 2e_3 + 2e_4$	$d_2 + 2d_4$
$e_1 + 2e_2 + e_3 + e_4$	$d_1 + 2d_2$
$e_1 + 2e_2 + e_3 + 2e_4$	$d_2 + d_4$
$e_1 + 2e_2 + 2e_3 + e_4$	$d_1 + 2d_3$
$e_1 + 2e_2 + 2e_3 + 2e_4$	$d_3 + d_4$

Tabelle 7: Strukturierte Intervallzerlegungen von $\mathcal{L}(5, GF(3))$, S_1

und die restlichen Intervallzerlegungen in Anhang B zu finden sind. \square

Anders als beim 5-dimensionalen linearen Verband über $GF(2)$ konnten beim 5-dimensionalen linearen Verband über $GF(3)$ sehr wohl Intervallzerlegungen gefunden werden, wenn man den durch den Computer ermittelten Ergebnissen denn vertrauen kann.

Dem stehen natürlich die gleichen Bedenken gegenüber, die auch gegenüber Computerbeweisen bestehen. Zentral ist hier aber im Wesentlichen, dass überhaupt eine Intervallzerlegung von $\mathcal{L}(5, GF(3))$ existiert, und man kann sich durch manuelle Überprüfung noch einmal davon überzeugen: Dazu sollte man zunächst verifizieren, dass S_1 , S_3 und S_6 aus Tabelle 6 tatsächlich Intervallzerlegungen sind, da sie die Bedingungen aus Definition 5.6 erfüllen. Anschließend kann man mithilfe von Korollar 5.12 verifizieren, dass auch S_1 aus Tabelle 7 eine Intervallzerlegung ist. Die Projektionen bezüglich $\langle e_1, e_2, e_3 \rangle$, $\langle e_1, e_2, e_4 \rangle$, $\langle e_1, e_3, e_4 \rangle$ und $\langle e_2, e_3, e_4 \rangle$ führen genau auf die Intervallzerlegungen S_1 , S_3 , S_3 und S_6 aus Tabelle 6. Zusätzlich sind für die $p_i, p_j \in H_0$, für die es kein $l \in \{1, \dots, k\}$ mit $p_i, p_j \in W_l$ gibt, die Bedingungen aus Definition 5.6 zu überprüfen. Mit einiger Geduld kommt man zu der Erkenntnis, dass diese stets erfüllt sind und somit durch S_1 tatsächlich eine Intervallzerlegung von $\mathcal{L}(5, GF(3))$ gefunden wurde. Dieses wichtige Resultat, das in deutlichem Gegensatz zu Satz 5.27 steht, soll auch als Satz formuliert werden.

Satz 5.31. *Es existiert eine strukturierte Intervallzerlegung von $\mathcal{L}(5, GF(3))$.*

5.3 Mächtigere Körper und höhere Dimensionen

Abschließend soll noch analysiert werden, wie gut sich der erstellte Algorithmus für das Intervallzerlegungsproblem über mächtigeren Körpern und höheren Dimensionen eignet. Zunächst werden aber die Unterschiede zwischen dem Intervallzerlegungsproblem über $GF(2)$ und $GF(q)$ für $q \geq 3$ noch genauer untersucht. Man hat gesehen, dass die Antwort auf die Existenz von Intervallzerlegungen (und deren Anzahl) über $GF(2)$ und $GF(3)$ sehr unterschiedlich ausfällt: Für lineare Verbände $\mathcal{L}(n, GF(2))$ gibt es für $n \leq 4$ genau eine Intervallzerlegung

und für $n \geq 5$ keine; für lineare Verbände $\mathcal{L}(n, GF(3))$ existieren für alle $n \leq 5$ Intervallzerlegungen, und zwar für jedes n mehrere. Dieser Unterschied soll nun weiter beleuchtet werden. Dazu bemerkt man zunächst, dass sich die punktweise Irreflexivität und Antisymmetrie aus Definition 5.6 sowie das Lemma 5.15 für den Fall $q = 2$ etwas anders formulieren lassen.

Proposition 5.32. *Eine Menge $S = \{\sigma_i \mid i \in \{1, \dots, s\}\}$ von Linearformen $\sigma_i : GF(2)^n \rightarrow GF(2)$ ist genau dann punktweise irreflexiv auf H_0 , wenn $\sigma_i(p_i) = 1$ für alle $i \in \{1, \dots, s\}$ gilt, und punktweise antisymmetrisch auf H_0 genau dann, wenn*

$$\sigma_j(p_i) = 1 \Leftrightarrow \sigma_i(p_j) = 0$$

für alle $i, j \in \{1, \dots, s\}$ gilt.

Beweis. Die Aussage $\sigma_i(p_i) = 1$ folgt aus Definition 5.6, denn 1 ist in $GF(2)$ das einzige Element ungleich 0. Ebenso ist die Richtung $\sigma_j(p_i) = 1 \Rightarrow \sigma_i(p_j) = 0$ genau der Inhalt von Definition 5.6 für $GF(2)$. Demnach kann für $p_i, p_j \in H_0$ entweder $\sigma_j(p_i) = 1$ oder $\sigma_i(p_j) = 1$ sein, aber nicht beides, also ist

$$|\{(i, j) \mid i \neq j \in H_0 \text{ und } \sigma_i(p_j) = 1\}| \leq 2 \binom{2^{n-1} - 1}{2} \cdot \frac{1}{2}.$$

Zählt man diese Menge anders ab, nämlich anhand der Tatsache, dass $|\{p_j \neq p_i \in H_0 \mid \sigma_i(p_j) = 1\}| = |\text{Kern}(\sigma_i(p_j) + 1) \cap H_0| - 1 = 2^{n-2} - 1$ für alle $p_i \in H_0$ gilt, so erhält man

$$|\{(i, j) \mid p_i \neq p_j \in H_0 \text{ und } \sigma_i(p_j) = 1\}| = (2^{n-1} - 1)(2^{n-2} - 1) = \binom{2^{n-1} - 1}{2}$$

und damit ist in der obigen Ungleichung stets Gleichheit erfüllt. Also gilt für $p_i, p_j \in H_0$ immer entweder $\sigma_j(p_i) = 1$ oder $\sigma_i(p_j) = 1$, womit der Beweis erbracht ist. \square

Für Körper $GF(q)$ mit $q \geq 3$ gilt nur die eine Richtung: es kann nur entweder $\sigma_{i,\beta}(p_j) = \sigma_{j,\beta'}(p_j)$ oder $\sigma_{j,\beta'}(p_i) = \sigma_{i,\beta}(p_i)$ sein und nicht beides. Betrachtet man die gesamte Anzahl an Tupeln (i, β, j, β') mit $(i, \beta) \neq (j, \beta')$, so erhält man $2(q-1)^2 \binom{q^{n-1}-1}{2}$. Es folgt

$$|\{(i, \beta, j, \beta') \mid (i, \beta) \neq (j, \beta') \text{ und } \sigma_{i,\beta}(p_j) = \sigma_{j,\beta'}(p_j)\}| \leq 2(q-1)^2 \binom{q^{n-1}-1}{2} \cdot \frac{1}{2}.$$

Über die andere Abzählmethode erhält man hier nun aber

$$|\{(i, \beta, j, \beta') \mid (i, \beta) \neq (j, \beta') \text{ und } \sigma_{i,\beta}(p_j) = \sigma_{j,\beta'}(p_j)\}| = 2(q-1)^2 \binom{q^{n-1}-1}{2} \cdot \frac{1}{q}$$

und für $q \geq 3$ lässt sich keine analoge Folgerung vornehmen. Damit folgt aus $\sigma_{i,\beta}(p_j) \neq \sigma_{j,\beta'}(p_j)$ hier nicht zwingend oder $\sigma_{j,\beta'}(p_i) = \sigma_{i,\beta}(p_i)$.

Lemma 5.33. *Sei S eine Intervallzerlegung von $\mathcal{L}(n, GF(2))$. Dann gibt es Punkte $e_1, \dots, e_{n-1} \in H_0$, sodass $\{p_0, e_1, \dots, e_{n-1}\}$ eine Basis von $GF(2)^n$ ist und*

$$\sigma_{e_j}(e_k) = 0 \Leftrightarrow k > j$$

für $j, k \in \{1, \dots, n-1\}$ gilt.

Beweis. Die Richtung $\sigma_{e_j}(e_k) = 0 \Leftrightarrow k > j$ ist genau die Aussage von Lemma 5.15, und die andere Richtung folgt direkt aus Proposition 5.32. \square

Man betrachte jetzt nochmals das Intervallzerlegungsproblem in $\mathcal{L}(n, GF(2))$ mit $n \geq 5$. Verwendet man Proposition 5.32 und eine Basis $\{p_0, e_1, \dots, e_{n-1}\}$ entsprechend Lemma 5.33, so erhält man $\sigma_{e_k}(e_1 + e_2) = 0 \Leftrightarrow k \geq 2$ und deshalb

$$\sigma_{e_1+e_2}(e_k) = 1 \Leftrightarrow k \geq 2.$$

Außerdem erhält man auch $\sigma_{e_k}(e_1 + e_2 + e_3 + e_4) = 0 \Leftrightarrow k = 2 \vee k \geq 4$ und damit

$$\sigma_{e_1+e_2+e_3+e_4}(e_k) = 1 \Leftrightarrow k = 2 \vee k \geq 4.$$

Daraus folgt aber auf Grund der Linearität $\sigma_{e_1+e_2+e_3+e_4}(e_1 + e_2) = \sigma_{e_1+e_2}(e_1 + e_2) = \sigma_{e_1+e_2+e_3+e_4}(e_1 + e_2 + e_3 + e_4) = \sigma_{e_1+e_2}(e_1 + e_2 + e_3 + e_4) = 1$, was nicht sein darf. Damit liegt ein alternativer Beweis dafür vor, dass keine Intervallzerlegung von $\mathcal{L}(n, GF(2))$ mit $n \geq 5$ existiert. Dieser entspricht dem Beweis, den Hochstättler in [8] geführt hat und ist offensichtlich um einiges kompakter als der Beweis von Satz 5.27 über die Verwendung von Projektionen. Allerdings lässt sich diese Beweismethode nicht auf Körper $GF(q)$ mit $q \geq 3$ übertragen, die Verwendung von Projektionen aber schon, weshalb Satz 5.27 hier zunächst dadurch bewiesen wurde.

Wie angekündigt, folgt nun eine Laufzeitanalyse von Algorithmus 1' für größere q und n . Um Vergleichsmaßstäbe zu haben, wird zusätzlich dazu ein Algorithmus betrachtet, der Intervallzerlegungen durch reines Ausprobieren sucht, und einer, der ausschließlich Projektionen verwendet, was durch Korollar 5.11 möglich ist. Diese beiden Algorithmen können als Spezialfälle von Algorithmus 1 angesehen werden: Verwendet man keine $(n - 2)$ -dimensionalen Unterräume, so passiert in den Schleifen 1 und 2 nichts und man kommt direkt in Schleife 3, wo dann alle möglichen Mengen von Linearformen durchlaufen werden. Somit erhält man Algorithmus 2.

Algorithmus 2 Suche nach Intervallzerlegungen über reines Ausprobieren

```

for all  $S = \{\sigma_{i,\beta} \mid i \in \{1, \dots, s\}, \beta \in GF(q)^*\}$  do {Schleife 3}
  iszerlegung  $\leftarrow true$ ;
  for all  $p_i, p_j \in H_0, \beta, \beta' \in GF(q)^*$  do {Schleife 4}
    if  $\sigma_{i,\beta}(p_i) = 0$  OR  $\sigma_{j,\beta'}(p_i) = \sigma_{i,\beta}(p_i)$  AND  $\sigma_{i,\beta}(p_j) = \sigma_{j,\beta'}(p_j)$  then
      {Irreflexivität und Antisymmetrie}
      iszerlegung  $\leftarrow false$ ;
      break;
    end if
  end for
  if iszerlegung = true then
    print  $S$ ;
  end if
end for

```

Verwendet man alle s $(n-2)$ -dimensionalen Unterräume von $\mathcal{L}(n, GF(q))$ aus H_0 , so werden Schleifen 1 und 2 dementsprechend durchlaufen. Sind diese alle paarweise miteinander verträglich, so ist nach Korollar 5.12 eine Intervallzerlegung gefunden, welche dann ausgegeben werden kann. Damit werden hier die Schleifen 3 und 4 nicht mehr durchlaufen und man erhält Algorithmus 3.

Algorithmus 3 Suche nach Intervallzerlegungen über Projektionen

```

for all  $(S_1, \dots, S_s) \in Z^s$  do {Schleife 1}
  iszerlegung  $\leftarrow$  true;
  for all  $i < j \in \{1, \dots, s\}$  do {Schleife 2}
    if  $S_i|_{W_i \cap W_j} \neq S_j|_{W_i \cap W_j}$  then {Verträglichkeit}
      iszerlegung  $\leftarrow$  false;
      break;
    end if
  end for
  if iszerlegung = true then
    print  $S$  mit  $S|_{W_l} = S_l$  für alle  $l \in \{1, \dots, s\}$ ;
  end if
end for

```

Außerdem kann man noch einen Algorithmus heranziehen, der die Erkenntnisse aus Kapitel 5, insbesondere Satz 5.7, nicht verwendet. Man muss allerdings anmerken, dass dann auch die Begriffe der strukturierten und normierten Intervallzerlegung nicht verwendet werden können und nur ein Algorithmus konstruiert werden kann, der nach allen Intervallzerlegungen eines linearen Verbandes sucht. Dadurch ist die Vergleichbarkeit mit den anderen hier betrachteten Algorithmen nur eingeschränkt gegeben.

Dieser Algorithmus also würde dann, bei fest gewähltem 1-dimensionalen Unterraum U_0 und dazu komplementärer Hyperebene H_0 , die Intervalle aus den 1-dimensionalen Unterräumen und Hyperebenen aus $\mathcal{L}(n, GF(q)) \setminus (\text{Filter}(U_0) \cup \text{Ideal}(H_0))$ willkürlich zusammensetzen und dann prüfen, ob dadurch eine Intervallzerlegung gefunden wurde. Dazu kann man die 1-dimensionalen Unterräume aus $\mathcal{L}(n, GF(q)) \setminus (\text{Filter}(U_0) \cup \text{Ideal}(H_0))$ in eine beliebige Reihenfolge bringen und diese den Hyperebenen, die in einer festen Reihenfolge bleiben, zuordnen (siehe Algorithmus 4, Schleife 1). Die Menge an Tupeln aus 1-dimensionalen Unterräumen, die dabei durchlaufen wird, wird mit $A^{q^{n-1}-1}$ bezeichnet. Dann muss zuerst überprüft werden, ob jede Hyperebene H_i , $i \in \{1, \dots, q^{n-1} - 1\}$, wirklich den ihr zugeordneten Unterraum U_i enthält, also ob es sich tatsächlich um Intervalle handelt. Dies wird in Schleife 2 getan. Ist dies der Fall, so ist für jeden Unterraum in $\mathcal{L}(n, GF(q))$, der nicht schon in $\text{Filter}(U_0)$ oder $\text{Ideal}(H_0)$ liegt und kein 1-dimensionaler Unterraum und keine Hyperebene ist, festzustellen, ob er in genau einem der Intervalle liegt, was in den Schleifen 3 und 4 passiert. Gegebenenfalls ist eine Intervallzerlegung gefunden, die ausgegeben werden kann.

Es wird jetzt ermittelt, wie viele (Un-)Gleichungen bei jedem der Algorithmen maximal auszuwerten sind, um alle Intervallzerlegungen eines linearen Verbandes zu ermitteln, wobei die Überprüfung einer Teilmengenbeziehung auch als eine (Un-)Gleichung gezählt wird. Es wird also die Anzahl an (Un-)Gleichungen gezählt, die ausgewertet würden, wenn jede untersuchte Menge an Linearformen bzw. Intervallen eine Intervallzerlegung darstellen würde. Zweifellos ist dies längst nicht der Fall, aber es lässt sich nicht von vornherein sagen, wann eine der

Schleifen vorzeitig verlassen wird, wenn keine Intervallzerlegung vorliegt. Deshalb ist dies die einzig sinnvolle Größe, die zur Analyse der Laufzeit verwendet werden kann.

Algorithmus 4 Suche nach Intervallzerlegungen ohne Satz 5.7

```

for all  $(U_1, \dots, U_{q^{n-1}-1}) \in A^{q^{n-1}-1}$  do {Schleife 1}
  iszerlegung  $\leftarrow true$ ;
  for all  $i \in \{1, \dots, q^{n-1} - 1\}$  do {Schleife 2}
    if  $U_i \not\subset H_i$  then  $\{U_i$  und  $H_i$  bilden kein Intervall $\}$ 
      iszerlegung  $\leftarrow false$ ;
      break;
    end if
  end for
  if iszerlegung = true then
    for all  $U \in \mathcal{L}(n, GF(q)) \setminus (\text{Filter}(U_0) \cup \text{Ideal}(H_0) \cup U_1 \cup \dots \cup U_{q^{n-1}-1} \cup H_1 \cup \dots \cup H_{q^{n-1}-1})$ 
    do {Schleife 3}
      isertes  $\leftarrow true$ ;
      for all  $i \in \{1, \dots, q^{n-1} - 1\}$  do {Schleife 4}
        if  $U_i \subset U$  AND  $U \subset H_i$  then
          if isertes = false then  $\{U$  liegt in zwei Intervallen $\}$ 
            iszerlegung  $\leftarrow false$ ;
            break;
          end if
          isertes  $\leftarrow false$ ;
        end if
      end for
      if isertes = true then  $\{U$  liegt in keinem Intervall $\}$ 
        iszerlegung  $\leftarrow false$ ;
      end if
      if iszerlegung = false then
        break;
      end if
    end for
    if iszerlegung = true then
      print  $[U_1, H_1], \dots, [U_{q^{n-1}-1}, H_{q^{n-1}-1}]$ ;
    end if
  end if
end for

```

Zudem wird für diese Auswertung angenommen, dass die Schleifen optimal implementiert sind, also keine überflüssigen Durchläufe gemacht werden.

Satz 5.34. Sei z die Anzahl an strukturierten Intervallzerlegungen von $\mathcal{L}(n-1, GF(q))$, z_{norm} die Anzahl an strukturierten, normierten Intervallzerlegungen von $\mathcal{L}(n-1, GF(q))$ und $s = \frac{q^{n-1}-1}{q-1}$. Die Anzahl an maximal auszuwertenden Gleichungen beträgt bei den verschiedenen Algorithmen:

- *Algorithmus 1'*:

$$z_{norm}^{n-1} \left(\binom{n-1}{2} + (n-1)(q-1)^{n-3} q((q-1)^{n-2})! ((q-1)^{n-2} + 2(q-1) \sum_{k=0}^{n-3} (-1)^k \binom{n-1}{k} \binom{\frac{q^{n-1-k}-1}{q-1}}{2} \right)$$

- *Algorithmus 2*: $\prod_{j=1}^{n-1} \left(\frac{q^j-1}{q-1} - (j-1) \right) (s - (n-1))! (2(q-1) \binom{s}{2} + s)$
- *Algorithmus 3*: $z_{norm}^{n-1} z^{s-(n-1)} \binom{s}{2}$
- *Algorithmus 4*: $(q^{n-1} - 1)! (q^{n-1} - 1) (1 + 2(G_{n-2,q} - 2)(q^{n-1} - 1))$.

Beweis. Die Anzahl an auszuwertenden (Un-)Gleichungen wird für die einzelnen Algorithmen abgezählt:

- **Algorithmus 1'**:

Die konkretisierte Form von Algorithmus 1 verwendet $n-1$ strukturierte, normierte Intervallzerlegungen von $\mathcal{L}(n-1, GF(q))$, was zu z_{norm}^{n-1} Durchläufen von Schleife 1 führt. In Schleife 2 wird dann ein Tupel von $n-1$ Intervallzerlegungen auf Verträglichkeit geprüft, wofür $\binom{n-1}{2}$ Durchläufe benötigt werden. Man kommt nun zu Schleife 3: Nach Lemma 5.23 gibt es $(n-1)(q-1)^{n-3}$ Punkte, für die q verschiedene Hyperebenen in Frage kommen, und zu $(q-1)^{n-2}$ Punkten können die dann noch verbleibenden Hyperebenen beliebig zugeordnet werden, damit $S|_{W_l} = S_l$ für alle $l \in \{1, \dots, n-1\}$ gilt. Daraus ergeben sich $(n-1)(q-1)^{n-3} q((q-1)^{n-2})!$ Durchläufe für Schleife 3. In Schleife 4 werden dann diejenigen Punkte auf Irreflexivität überprüft, die sich in keinem der W_l , $l \in \{1, \dots, n-1\}$ befinden, und das sind bekanntermaßen $(q-1)^{n-2}$ Punkte; bei den anderen Punkten ist die Bedingung auf Grund der Projektionen erfüllt. Die Antisymmetrie ist dann noch für p_i, p_j mit $\langle p_i, p_j \rangle \notin W_l$ für alle $l \in \{1, \dots, n-1\}$ zu überprüfen. Dies sind genau die $p_i, p_j \in H_0$, abzüglich der p_i, p_j , die beide in einem der W_l liegen; dabei wurden diejenigen doppelt abgezogen, die in zweien der W_l liegen, also müssen diese wieder hinzuaddiert werden; jetzt wurden aber diese doppelt hinzuaddiert, die in dreien der W_l liegen, diese müssen also wieder abgezogen werden, usw., bis $n-3$ erreicht ist, denn in $n-2$ verschiedenen W_l können nicht zwei linear unabhängige Punkte liegen. Zusammengefasst gibt es $\sum_{k=0}^{n-3} (-1)^k \binom{n-1}{k} \binom{\frac{q^{n-1-k}-1}{q-1}}{2}$ solcher ungeordneten p_i, p_j , und für alle müssen nach Proposition 5.18 dann $2(q-1)$ (Un-)Gleichungen ausgewertet werden. Insgesamt sind in Schleife 4 also $(q-1)^{n-2} + 2(q-1) \sum_{k=0}^{n-3} (-1)^k \binom{n-1}{k} \binom{\frac{q^{n-1-k}-1}{q-1}}{2}$ (Un-)Gleichungen auszuwerten.

Da sich Schleife 2 und Schleife 3 auf gleicher Stufe innerhalb von Schleife 1 befinden

und sich Schleife 4 innerhalb von Schleife 3 befindet, ergibt das insgesamt

$$z_{norm}^{n-1} \left(\binom{n-1}{2} + (n-1)(q-1)^{n-3} q ((q-1)^{n-2})! ((q-1)^{n-2} + 2(q-1) \sum_{k=0}^{n-3} (-1)^k \binom{n-1}{k} \binom{\frac{q^{n-1-k}-1}{q-1}}{2} \right)$$

(Un-)Gleichungen bei Algorithmus 1'.

• **Algorithmus 2:**

In Schleife 3 werden einfach alle möglichen verschiedenen Mengen an Linearformen durchlaufen, was $s!$ Durchläufen entspricht, denn es werden ja nur strukturierte Intervallzerlegungen gesucht. Man kann noch zusätzlich berücksichtigen, dass auch nur normierte Intervallzerlegungen gesucht werden: Dann kommt für σ_{e_1} nur $\sigma_{e_1} = d_1$ in Frage, für σ_{e_2} kommen nur $\sigma_{e_2} \in \langle d_1, d_2 \rangle \setminus \{0\} \setminus \langle \sigma_{e_1} \rangle$ in Frage, usw., d.h. allgemein kommen für σ_{e_j} dann $\frac{q^j-1}{q-1} - (j-1)$ linear unabhängige Möglichkeiten in Frage. Dies reduziert die $s!$ Durchläufe auf

$$\prod_{j=1}^{n-1} \left(\frac{q^j-1}{q-1} - (j-1) \right) (s - (n-1))!$$

In Schleife 4 wird dann die Irreflexivität für jedes p_i überprüft, was s (Un-)Gleichungen entspricht, und für die Überprüfung der Antisymmetrie ist die Auswertung von $2(q-1) \binom{s}{2}$ (Un-)Gleichungen notwendig; beides folgt aus Proposition 5.18. Somit sind dies $2(q-1) \binom{s}{2} + s$ (Un-)Gleichungen in Schleife 4 und da sich Schleife 4 innerhalb von Schleife 3 befindet insgesamt maximal

$$\prod_{j=1}^{n-1} \left(\frac{q^j-1}{q-1} - (j-1) \right) (s - (n-1))! (2(q-1) \binom{s}{2} + s)$$

(Un-)Gleichungen.

• **Algorithmus 3:**

Schleife 1 durchläuft alle geordneten s -Tupel an strukturierten Intervallzerlegungen von $\mathcal{L}(n-1, GF(q))$, was z^s Durchläufe sind. Man kann allerdings auch hier beachten, dass nur strukturierte, normierte Intervallzerlegungen gesucht werden und deshalb wie bei Algorithmus 1' auf den $\langle e_1, \dots, e_{l-1}, e_{l+1}, \dots, e_{n-1} \rangle$ nur strukturierte, normierte Intervallzerlegungen durchlaufen. Dadurch reduziert sich die Anzahl auf $z_{norm}^{n-1} z^{s-(n-1)}$. In Schleife 2 werden all diese Intervallzerlegungen auf Verträglichkeit miteinander überprüft. Dazu sind $\binom{s}{2}$ Durchläufe notwendig, da dies die Anzahl ungeordneter S_i, S_j ist. Da sich Schleife 2 innerhalb von Schleife 1 befindet und in jedem Durchlauf von Schleife 2 eine Ungleichung ausgewertet wird, kommt man auf $z_{norm}^{n-1} z^{s-(n-1)} \binom{s}{2}$ auszuwertende Ungleichungen im schlechtesten Fall.

• **Algorithmus 4:**

In Schleife 1 werden alle Tupel aus $A^{q^{n-1}-1}$ durchlaufen, was $(q^{n-1}-1)!$ Durchläufen entspricht. Schleife 2 wird offensichtlich $q^{n-1}-1$ mal durchlaufen, und jedes mal wird eine (Un-)Gleichung ausgewertet. Schleife 3 wird für jeden Unterraum aus

$\mathcal{L}(n, GF(q)) \setminus (\text{Filter}(U_0) \cup \text{Ideal}(H_0) \cup U_1 \cup \dots \cup U_{q^{n-1}-1} \cup H_1 \cup \dots \cup H_{q^{n-1}-1})$ einmal durchlaufen, und dies entspricht einer Anzahl von $G_{n,q} - 2G_{n-1,q} - 2(q^{n-1} - 1) = (q^{n-1} - 1)G_{n-2,q} - 2(q^{n-1} - 1) = (q^{n-1} - 1)(G_{n-2,q} - 2)$. Bei Schleife 4 sind es wieder offensichtlich $q^{n-1} - 1$ Durchläufe, und in jedem werden 2 (Un-)Gleichungen ausgewertet. Da sich Schleife 2 und Schleife 3 auf gleicher Stufe innerhalb von Schleife 1 befinden und Schleife 4 innerhalb von Schleife 3 liegt, kommt man auf

$$\begin{aligned}
 & (q^{n-1} - 1)!(q^{n-1} - 1 + (q^{n-1} - 1)(G_{n-2,q} - 2) \cdot 2(q^{n-1} - 1)) \\
 & = (q^{n-1} - 1)!(q^{n-1} - 1)(1 + 2(G_{n-2,q} - 2)(q^{n-1} - 1))
 \end{aligned}$$

auszuwertende (Un-)Gleichungen insgesamt.

Zusammen ergibt sich der Satz. □

Um die Laufzeit eines Algorithmus zu charakterisieren, verwendet man üblicherweise die sogenannte Landau-Notation (siehe z.B. [2], S. 90), wobei hier nur Abschätzungen nach unten benötigt werden.

Definition 5.35. Sei $f : \mathbb{N} \rightarrow \mathbb{R}$ eine Folge. Die Menge

$$\{g : \mathbb{N} \rightarrow \mathbb{R} \mid \exists k > 0, n_0 \in \mathbb{N} : n > n_0 \Rightarrow |g(n) \cdot k| \leq |f(n)|\}$$

wird mit $\Omega(f)$ bezeichnet.

Dadurch erhält man eine Einordnung der Laufzeiten der hier betrachteten Algorithmen.

Korollar 5.36. *Angenommen, z_{norm} ist konstant und größer als 1. Dann haben die Algorithmen 1', 2, 3 und 4 im schlechtesten Fall mindestens exponentielle Laufzeit in q und n , d.h. bei festem $n \geq 4$ ist die Laufzeit Element von $\Omega(c_n^q)$ mit $c_n > 1$ und bei festem $q \geq 3$ ist sie Element von $\Omega(c_q^n)$ mit $c_q > 1$.*

Beweis. Die Anzahl an auszuwertenden (Un-)Gleichungen aus Satz 5.34 kann recht rigoros abgeschätzt werden. Dabei wird die grobe Stirlingsche Abschätzung $n! > (\frac{n}{e})^n$ verwendet, siehe [2], S. 91.

Für Algorithmus 1' gilt

$$\begin{aligned}
 z_{norm}^{n-1} & \left(\binom{n-1}{2} + (n-1)(q-1)^{n-3} q ((q-1)^{n-2})! ((q-1)^{n-2}) \right. \\
 & \left. + 2(q-1) \sum_{k=0}^{n-3} (-1)^k \binom{n-1}{k} \binom{\frac{q^{n-1-k}-1}{q-1}}{2} \right) \\
 & > ((q-1)^{n-2})! > \left(\frac{(q-1)^{n-2}}{e} \right)^{(q-1)^{n-2}},
 \end{aligned}$$

wenn $q \geq 3$ und $n \geq 4$ ist und daraus folgt die Aussage für Algorithmus 1', da dann auch $(q-1)^{n-2} \geq q$, $(q-1)^{n-2} \geq n$ und deshalb auch $\frac{(q-1)^{n-2}}{e} > 1, 1$ gilt.

Für Algorithmus 2 gilt

$$\prod_{j=1}^{n-1} \left(\frac{q^j - 1}{q - 1} - (j - 1) \right) (s - (n - 1))! (2(q - 1) \binom{s}{2} + s) > (s - (n - 1))! > \left(\frac{s - (n - 1)}{e} \right)^{s - (n - 1)}$$

und für $q \geq 3$ und $n \geq 4$ ist $s - (n - 1) > q$, $s - (n - 1) > n$ und deshalb auch $\frac{s - (n - 1)}{e} > 1, 1$, weshalb die Aussage für diesen folgt, und analog gilt bei Algorithmus 4

$$(q^{n-1} - 1)!(q^{n-1} - 1)(1 + 2(G_{n-2,q} - 2)(q^{n-1} - 1)) > (q^{n-1} - 1)! > \left(\frac{q^{n-1} - 1}{e} \right)^{q^{n-1} - 1}$$

und $q^{n-1} - 1 > q$ sowie $q^{n-1} - 1 > n$ und deshalb auch $\frac{q^{n-1} - 1}{e} > 1, 1$ für $q \geq 3$ und $n \geq 4$, weshalb die Aussage auch für diesen gilt.

Für Algorithmus 3 schließlich ist

$$z_{norm}^{n-1} z^{s - (n - 1)} \binom{s}{2} > z_{norm}^s \geq 2^s,$$

woraus die Aussage folgt, da für $q \geq 3$ und $n \geq 4$ schon $s > q$ und $s > n$ bekannt ist. \square

Algorithmen mit exponentieller Laufzeit werden üblicherweise als wenig praxistauglich angesehen. Allerdings war auf Grund der Schwierigkeit des kombinatorischen Problems hier auch nicht zu erwarten, dass ein Algorithmus mit weniger als exponentieller Laufzeit existiert.

Die Frage ist, was denn dann überhaupt der Vorteil von Algorithmus 1' gegenüber den anderen Algorithmen ist. Dieser liegt darin, dass die dominierenden Terme in der Anzahl an (Un-)Gleichungen in der Regel kleiner sind, und deshalb tatsächlich weniger (Un-)Gleichungen auszuwerten sind. Beispielsweise stehen bei dem noch nicht untersuchten Fall $q = 3$ und $n = 6$, wo dann $z_{norm} = 52$ ist, den ungefähr $1,56 \cdot 10^{28}$ (Un-)Gleichungen bei Algorithmus 1' ungefähr $1,41 \cdot 10^{200}$ (Un-)Gleichungen bei Algorithmus 2 und mindestens $3,14 \cdot 10^{211}$ (Un-)Gleichungen bei Algorithmus 3 (wenn man zur Abschätzung $z \geq z_{norm}$ benutzt) gegenüber. Algorithmus 4 bringt es sogar auf etwa $5,84 \cdot 10^{480}$ (Un-)Gleichungen. Dies ist natürlich ein deutlicher Unterschied, auch für den Computer. Dementsprechend ist Satz 5.7 auch aus algorithmischer Sicht sehr bedeutend. Eine weitere entscheidende Verbesserung konnte erreicht werden, indem die Methoden aus den Algorithmen 2 und 3 geschickt zu Algorithmus 1' miteinander kombiniert wurden.

Zum Abschluss dieses Abschnitts kann man, wenn auch etwas salopp, sagen, dass die spezielle Eigenschaft von $GF(2)$, nur ein Element verschieden von 0 zu besitzen, bestimmte Folgen für das Intervallzerlegungsproblem hat, die im allgemeinen Fall nicht in der Form auftreten. Darin mag der Grund liegen, dass eine Intervallzerlegung von $\mathcal{L}(5, GF(3))$ existiert, nicht aber von $\mathcal{L}(5, GF(2))$. Der entwickelte Algorithmus ist dazu geeignet, sich über die Existenz von (strukturierten) Intervallzerlegungen für kleine q und n einen Eindruck zu verschaffen. Für größere q und n wird es selbst unter Computereinsatz schwierig, und einen eventuellen allgemeinen (Nicht-)Existenzbeweis kann der Algorithmus natürlich ohnehin nicht ersetzen.

6 Schlusswort und Ausblick

In folgender Tabelle befinden sich zusammengefasst die jetzt vorhandenen Antworten auf die Frage, ob eine Intervallzerlegung des n -dimensionalen linearen Verbandes über einem endlichen Körper $GF(q)$ existiert. In den Fällen, in denen die Existenz einer Intervallzerlegung

n	$GF(2)$	$GF(3)$	$GF(q), q \geq 4$
3	ja	ja	ja
4	ja	ja	?
5	nein	ja	?
≥ 6	nein	?	?

Tabelle 8: Übersicht über die Existenz von Intervallzerlegungen

nachgewiesen werden konnte, konnte auch stets eine strukturierte Intervallzerlegung gefunden werden, insbesondere für den Verband $\mathcal{L}(5, GF(3))$. Dies ist nur ein kleiner Teil der Lösung des allgemeinen Intervallzerlegungsproblems. Aber er ist als Resultat, zusammen mit den anderen Erkenntnissen dieser Arbeit, recht aussagekräftig. Man erkennt nämlich deutlich, dass das Intervallzerlegungsproblem über $GF(2)$ kaum mit dem über $GF(q)$ mit $q \geq 3$ zu vergleichen ist und dass sich wesentliche Aussagen, die für $GF(2)$ gelten, nicht verallgemeinern lassen. Dies war bei Vergabe dieser Arbeit keineswegs klar.

Zu den nicht geklärten Fällen kann man bisher nur Vermutungen anstellen. Wenn man Abschnitt 5.3 zugrunde legt, so kann dieser nur die Vermutung, dass sich das Intervallzerlegungsproblem über allen Körpern $GF(q)$ mit $q \geq 3$ ähnlich verhält, wirklich stützen. Denkbar wäre dann, dass es für jeden Körper $GF(q)$ ein k_q gibt, sodass für alle $n \geq k_q$ keine Intervallzerlegung von $\mathcal{L}(n, GF(q))$ existiert, oder aber, dass es stets eine Intervallzerlegung von $\mathcal{L}(n, GF(q))$ mit $q \geq 3$ gibt. In beiden Fällen ist nicht absehbar, wie einfach oder kompliziert ein etwaiger Beweis für die jeweilige Aussage wäre.

Ich als Autor vermute, dass es stets eine Intervallzerlegung von $\mathcal{L}(n, GF(q))$ mit $q \geq 3$ gibt. Möglicherweise ist immer die Konstruktion einer Intervallzerlegung möglich, die ähnlich zu den Intervallzerlegungen S_1 bis S_6 von $\mathcal{L}(4, GF(3))$ und S_1 bis S_{12} von $\mathcal{L}(5, GF(3))$ aussieht. Dies wurde im Rahmen dieser Arbeit aber nicht mehr untersucht. Die Gültigkeit einer solchen Aussage hätte zur Folge, dass sich die Rekursionsformel

$$G_{n,q} = 2G_{n-1,q} + (q^{n-1} - 1)G_{n-2,q}$$

der Galoiszahlen für $q, n \geq 3$ tatsächlich auf die diskutierte Art geometrisch interpretieren ließe. Bisher ist eine solche geometrische Interpretation nur für $q = 2$ und $3 \leq n \leq 4$, $q = 3$ und $3 \leq n \leq 5$ sowie $q \geq 4$ und $n = 3$ nachweislich möglich, und für $q = 2$ und $n \geq 5$ ist sie bewiesenermaßen nicht möglich.

Etwas abstrahiert kann man außerdem, wie auch schon in [13] angedeutet, das Intervallzerlegungsproblem in linearen Verbänden über unendlichen Körpern betrachten. Die Frage ist dann, ob sich ein solcher Verband $\mathcal{L}(n, K)$ in 2 Teilverbände isomorph zu $\mathcal{L}(n-1, K)$ und unendlich viele Teilverbände isomorph zu $\mathcal{L}(n-2, K)$ zerlegen lässt. Der Bezug zu einer Rekursionsformel ginge bei dieser Fragestellung auf Grund der Unendlichkeit der Verbände verloren, was aber nichts daran ändert, dass es sich dabei ebenso um ein interessantes Problem handelt.

A Strukturierte Intervallzerlegungen von $\mathcal{L}(4, GF(3))$

$p_i \in H_0$	$\sigma_i \in S_2$	$\sigma_i \in S_4$	$\sigma_i \in S_5$
e_1	d_1	d_1	d_1
e_2	d_2	d_2	d_2
e_3	d_3	d_3	d_3
$e_1 + e_2$	$d_1 + d_2 + d_3$	$d_1 + d_2 + 2d_3$	$d_1 + d_2$
$e_1 + 2e_2$	$d_1 + 2d_2 + 2d_3$	$d_1 + 2d_2 + 2d_3$	$d_1 + 2d_2$
$e_1 + e_3$	$d_1 + 2d_2 + d_3$	$d_1 + d_3$	$d_1 + d_2 + d_3$
$e_1 + 2e_3$	$d_1 + d_2 + 2d_3$	$d_1 + 2d_3$	$d_1 + d_2 + 2d_3$
$e_2 + e_3$	$d_2 + d_3$	$d_1 + d_2 + d_3$	$d_1 + 2d_2 + 2d_3$
$e_2 + 2e_3$	$d_2 + 2d_3$	$d_1 + 2d_2 + d_3$	$d_1 + 2d_2 + d_3$
$e_1 + e_2 + e_3$	$d_1 + d_3$	$d_1 + d_2$	$d_2 + d_3$
$e_1 + e_2 + 2e_3$	$d_1 + d_2$	$d_2 + 2d_3$	$d_2 + 2d_3$
$e_1 + 2e_2 + e_3$	$d_1 + 2d_2$	$d_1 + 2d_2$	$d_1 + d_3$
$e_1 + 2e_2 + 2e_3$	$d_1 + 2d_3$	$d_2 + d_3$	$d_1 + 2d_3$

$p_i \in H_0$	$\sigma_i \in S_7$	$\sigma_i \in S_8$	$\sigma_i \in S_9$
e_1	d_1	d_1	d_1
e_2	d_2	d_2	d_2
e_3	$d_1 + d_2 + d_3$	$d_1 + 2d_2 + d_3$	$d_1 + 2d_2 + 2d_3$
$e_1 + e_2$	$d_1 + d_2 + 2d_3$	$d_1 + d_2$	$d_1 + d_2$
$e_1 + 2e_2$	$d_1 + 2d_2$	$d_1 + 2d_2 + 2d_3$	$d_1 + 2d_2 + d_3$
$e_1 + e_3$	$d_2 + 2d_3$	$d_2 + d_3$	$d_1 + d_2 + d_3$
$e_1 + 2e_3$	$d_1 + 2d_2 + 2d_3$	$d_1 + d_2 + 2d_3$	$d_2 + 2d_3$
$e_2 + e_3$	$d_1 + 2d_3$	$d_1 + d_2 + d_3$	$d_1 + d_3$
$e_2 + 2e_3$	$d_1 + 2d_2 + d_3$	$d_1 + 2d_3$	$d_1 + d_2 + 2d_3$
$e_1 + e_2 + e_3$	$d_1 + d_2$	$d_1 + d_3$	$d_2 + d_3$
$e_1 + e_2 + 2e_3$	d_3	$d_2 + 2d_3$	$d_1 + 2d_3$
$e_1 + 2e_2 + e_3$	$d_1 + d_3$	$d_1 + 2d_2$	d_3
$e_1 + 2e_2 + 2e_3$	$d_2 + d_3$	d_3	$d_1 + 2d_2$

$p_i \in H_0$	$\sigma_i \in S_{10}$	$\sigma_i \in S_{11}$	$\sigma_i \in S_{12}$
e_1	d_1	d_1	d_1
e_2	d_2	$d_1 + d_2$	$d_1 + d_2$
e_3	$d_1 + d_2 + 2d_3$	$d_2 + d_3$	$d_2 + 2d_3$
$e_1 + e_2$	$d_1 + d_2 + d_3$	$d_2 + 2d_3$	$d_2 + d_3$
$e_1 + 2e_2$	$d_1 + 2d_2$	$d_1 + 2d_2 + 2d_3$	$d_1 + 2d_2 + d_3$
$e_1 + e_3$	$d_1 + 2d_2 + d_3$	$d_1 + d_2 + d_3$	$d_1 + d_3$
$e_1 + 2e_3$	$d_2 + d_3$	$d_1 + 2d_3$	$d_1 + d_2 + 2d_3$
$e_2 + e_3$	$d_1 + 2d_2 + 2d_3$	$d_1 + d_3$	$d_1 + d_2 + d_3$
$e_2 + 2e_3$	$d_1 + d_3$	$d_1 + d_2 + 2d_3$	$d_1 + 2d_3$
$e_1 + e_2 + e_3$	d_3	d_2	$d_1 + 2d_2 + 2d_3$
$e_1 + e_2 + 2e_3$	$d_1 + d_2$	$d_1 + 2d_2 + d_3$	d_2
$e_1 + 2e_2 + e_3$	$d_2 + 2d_3$	d_3	$d_1 + 2d_2$
$e_1 + 2e_2 + 2e_3$	$d_1 + 2d_3$	$d_1 + 2d_2$	d_3

$p_i \in H_0$	$\sigma_i \in S_{13}$	$\sigma_i \in S_{14}$	$\sigma_i \in S_{15}$
e_1	d_1	d_1	d_1
e_2	$d_1 + d_2$	$d_1 + d_2$	$d_1 + d_2$
e_3	$d_1 + d_3$	$d_1 + d_2 + d_3$	$d_1 + d_2 + d_3$
$e_1 + e_2$	d_2	$d_2 + d_3$	$d_2 + d_3$
$e_1 + 2e_2$	$d_1 + 2d_2 + d_3$	$d_1 + 2d_2 + 2d_3$	$d_1 + 2d_2$
$e_1 + e_3$	d_3	d_3	$d_2 + 2d_3$
$e_1 + 2e_3$	$d_1 + d_2 + 2d_3$	$d_1 + d_2 + 2d_3$	$d_1 + d_2 + 2d_3$
$e_2 + e_3$	$d_2 + d_3$	$d_1 + d_3$	d_3
$e_2 + 2e_3$	$d_2 + 2d_3$	$d_2 + 2d_3$	$d_1 + 2d_2 + d_3$
$e_1 + e_2 + e_3$	$d_1 + 2d_2 + 2d_3$	d_2	$d_1 + 2d_2 + 2d_3$
$e_1 + e_2 + 2e_3$	$d_1 + 2d_3$	$d_1 + 2d_2 + d_3$	d_2
$e_1 + 2e_2 + e_3$	$d_1 + 2d_2$	$d_1 + 2d_2$	$d_1 + d_3$
$e_1 + 2e_2 + 2e_3$	$d_1 + d_2 + d_3$	$d_1 + 2d_3$	$d_1 + 2d_3$

$p_i \in H_0$	$\sigma_i \in S_{16}$	$\sigma_i \in S_{17}$	$\sigma_i \in S_{18}$
e_1	d_1	d_1	d_1
e_2	$d_1 + d_2$	$d_1 + d_2$	$d_1 + d_2$
e_3	$d_1 + 2d_3$	$d_1 + d_2 + 2d_3$	$d_1 + d_2 + 2d_3$
$e_1 + e_2$	d_2	$d_2 + 2d_3$	$d_2 + 2d_3$
$e_1 + 2e_2$	$d_1 + 2d_2 + 2d_3$	$d_1 + 2d_2 + d_3$	$d_1 + 2d_2$
$e_1 + e_3$	$d_1 + d_2 + d_3$	$d_1 + d_2 + d_3$	$d_1 + d_2 + d_3$
$e_1 + 2e_3$	d_3	d_3	$d_2 + d_3$
$e_2 + e_3$	$d_2 + d_3$	$d_2 + d_3$	$d_1 + 2d_2 + 2d_3$
$e_2 + 2e_3$	$d_2 + 2d_3$	$d_1 + 2d_3$	d_3
$e_1 + e_2 + e_3$	$d_1 + d_3$	$d_1 + 2d_2 + 2d_3$	d_2
$e_1 + e_2 + 2e_3$	$d_1 + 2d_2 + d_3$	d_2	$d_1 + 2d_2 + d_3$
$e_1 + 2e_2 + e_3$	$d_1 + d_2 + 2d_3$	$d_1 + d_3$	$d_1 + d_3$
$e_1 + 2e_2 + 2e_3$	$d_1 + 2d_2$	$d_1 + 2d_2$	$d_1 + 2d_3$

$p_i \in H_0$	$\sigma_i \in S_{19}$	$\sigma_i \in S_{20}$	$\sigma_i \in S_{21}$
e_1	d_1	d_1	d_1
e_2	$d_1 + 2d_2$	$d_1 + 2d_2$	$d_1 + 2d_2$
e_3	$d_2 + d_3$	$d_2 + 2d_3$	$d_1 + d_3$
$e_1 + e_2$	$d_1 + d_2 + d_3$	$d_1 + d_2 + 2d_3$	$d_1 + d_2 + d_3$
$e_1 + 2e_2$	$d_2 + 2d_3$	$d_2 + d_3$	d_2
$e_1 + e_3$	$d_1 + d_3$	$d_1 + 2d_2 + d_3$	d_3
$e_1 + 2e_3$	$d_1 + 2d_2 + 2d_3$	$d_1 + 2d_3$	$d_1 + 2d_2 + 2d_3$
$e_2 + e_3$	$d_1 + 2d_3$	$d_1 + 2d_2 + 2d_3$	$d_2 + d_3$
$e_2 + 2e_3$	$d_1 + 2d_2 + d_3$	$d_1 + d_3$	$d_2 + 2d_3$
$e_1 + e_2 + e_3$	$d_1 + d_2$	d_3	$d_1 + d_2$
$e_1 + e_2 + 2e_3$	d_3	$d_1 + d_2$	$d_1 + 2d_2 + d_3$
$e_1 + 2e_2 + e_3$	$d_1 + d_2 + 2d_3$	d_2	$d_1 + d_2 + 2d_3$
$e_1 + 2e_2 + 2e_3$	d_2	$d_1 + d_2 + d_3$	$d_1 + 2d_3$

A STRUKTURIERTE INTERVALLZERLEGUNGEN VON $\mathcal{L}(4, GF(3))$

$p_i \in H_0$	$\sigma_i \in S_{22}$	$\sigma_i \in S_{23}$	$\sigma_i \in S_{24}$
e_1	d_1	d_1	d_1
e_2	$d_1 + 2d_2$	$d_1 + 2d_2$	$d_1 + 2d_2$
e_3	$d_1 + 2d_2 + d_3$	$d_1 + 2d_2 + d_3$	$d_1 + 2d_3$
$e_1 + e_2$	$d_1 + d_2 + 2d_3$	$d_1 + d_2$	$d_1 + d_2 + 2d_3$
$e_1 + 2e_2$	$d_2 + 2d_3$	$d_2 + 2d_3$	d_2
$e_1 + e_3$	d_3	$d_2 + d_3$	$d_1 + 2d_2 + d_3$
$e_1 + 2e_3$	$d_1 + 2d_2 + 2d_3$	$d_1 + 2d_2 + 2d_3$	d_3
$e_2 + e_3$	$d_2 + d_3$	$d_1 + d_2 + d_3$	$d_2 + d_3$
$e_2 + 2e_3$	$d_1 + d_3$	d_3	$d_2 + 2d_3$
$e_1 + e_2 + e_3$	$d_1 + d_2$	$d_1 + d_3$	$d_1 + 2d_2 + 2d_3$
$e_1 + e_2 + 2e_3$	$d_1 + 2d_3$	$d_1 + 2d_3$	$d_1 + d_2$
$e_1 + 2e_2 + e_3$	d_2	$d_1 + d_2 + 2d_3$	$d_1 + d_3$
$e_1 + 2e_2 + 2e_3$	$d_1 + d_2 + d_3$	d_2	$d_1 + d_2 + d_3$

$p_i \in H_0$	$\sigma_i \in S_{25}$	$\sigma_i \in S_{26}$
e_1	d_1	d_1
e_2	$d_1 + 2d_2$	$d_1 + 2d_2$
e_3	$d_1 + 2d_2 + 2d_3$	$d_1 + 2d_2 + 2d_3$
$e_1 + e_2$	$d_1 + d_2$	$d_1 + d_2 + d_3$
$e_1 + 2e_2$	$d_2 + d_3$	$d_2 + d_3$
$e_1 + e_3$	$d_1 + 2d_2 + d_3$	$d_1 + 2d_2 + d_3$
$e_1 + 2e_3$	$d_2 + 2d_3$	d_3
$e_2 + e_3$	d_3	$d_1 + 2d_3$
$e_2 + 2e_3$	$d_1 + d_2 + 2d_3$	$d_2 + 2d_3$
$e_1 + e_2 + e_3$	$d_1 + d_3$	$d_1 + d_3$
$e_1 + e_2 + 2e_3$	$d_1 + 2d_3$	$d_1 + d_2$
$e_1 + 2e_2 + e_3$	d_2	$d_1 + d_2 + 2d_3$
$e_1 + 2e_2 + 2e_3$	$d_1 + d_2 + d_3$	d_2

B Strukturierte Intervallzerlegungen von $\mathcal{L}(5, GF(3))$

$p_i \in H_0$	$\sigma_i \in S_2$	$\sigma_i \in S_3$
e_1	d_1	d_1
e_2	d_2	d_2
e_3	d_3	d_3
e_4	d_4	d_4
$e_1 + e_2$	$d_1 + d_2 + 2d_3 + 2d_4$	$d_1 + d_2 + d_3 + d_4$
$e_1 + 2e_2$	$d_1 + 2d_2 + d_3 + 2d_4$	$d_1 + 2d_2 + 2d_3 + d_4$
$e_1 + e_3$	$d_1 + d_2 + d_3 + 2d_4$	$d_1 + 2d_2 + d_3 + d_4$
$e_1 + 2e_3$	$d_1 + 2d_2 + 2d_3 + 2d_4$	$d_1 + d_2 + 2d_3 + d_4$
$e_1 + e_4$	$d_1 + d_4$	$d_1 + d_4$
$e_1 + 2e_4$	$d_1 + 2d_4$	$d_1 + 2d_4$
$e_2 + e_3$	$d_2 + d_3$	$d_2 + d_3$
$e_2 + 2e_3$	$d_2 + 2d_3$	$d_2 + 2d_3$
$e_2 + e_4$	$d_1 + d_2 + 2d_3 + d_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$
$e_2 + 2e_4$	$d_1 + 2d_2 + d_3 + d_4$	$d_1 + d_2 + d_3 + 2d_4$
$e_3 + e_4$	$d_1 + d_2 + d_3 + d_4$	$d_1 + d_2 + 2d_3 + 2d_4$
$e_3 + 2e_4$	$d_1 + 2d_2 + 2d_3 + d_4$	$d_1 + 2d_2 + d_3 + 2d_4$
$e_1 + e_2 + e_3$	$d_1 + d_2 + d_4$	$d_1 + d_3 + 2d_4$
$e_1 + e_2 + 2e_3$	$d_1 + 2d_3 + d_4$	$d_1 + d_2 + 2d_4$
$e_1 + 2e_2 + e_3$	$d_1 + d_3 + d_4$	$d_1 + 2d_2 + 2d_4$
$e_1 + 2e_2 + 2e_3$	$d_1 + 2d_2 + d_4$	$d_1 + 2d_3 + 2d_4$
$e_1 + e_2 + e_4$	$d_1 + d_2 + d_3$	$d_2 + 2d_3 + d_4$
$e_1 + e_2 + 2e_4$	$d_2 + d_3 + 2d_4$	$d_1 + d_2 + 2d_3$
$e_1 + 2e_2 + e_4$	$d_1 + 2d_2 + 2d_3$	$d_2 + 2d_3 + 2d_4$
$e_1 + 2e_2 + 2e_4$	$d_2 + d_3 + d_4$	$d_1 + 2d_2 + d_3$
$e_1 + e_3 + e_4$	$d_1 + 2d_2 + d_3$	$d_2 + d_3 + d_4$
$e_1 + e_3 + 2e_4$	$d_2 + 2d_3 + d_4$	$d_1 + d_2 + d_3$
$e_1 + 2e_3 + e_4$	$d_1 + d_2 + 2d_3$	$d_2 + d_3 + 2d_4$
$e_1 + 2e_3 + 2e_4$	$d_2 + 2d_3 + 2d_4$	$d_1 + 2d_2 + 2d_3$
$e_2 + e_3 + e_4$	$d_1 + 2d_2 + 2d_4$	$d_1 + d_3 + d_4$
$e_2 + e_3 + 2e_4$	$d_1 + d_2 + 2d_4$	$d_1 + 2d_3 + d_4$
$e_2 + 2e_3 + e_4$	$d_1 + d_3 + 2d_4$	$d_1 + d_2 + d_4$
$e_2 + 2e_3 + 2e_4$	$d_1 + 2d_3 + 2d_4$	$d_1 + 2d_2 + d_4$
$e_1 + e_2 + e_3 + e_4$	$d_3 + d_4$	$d_1 + d_2$
$e_1 + e_2 + e_3 + 2e_4$	$d_1 + d_3$	$d_2 + 2d_4$
$e_1 + e_2 + 2e_3 + e_4$	$d_2 + d_4$	$d_1 + 2d_3$
$e_1 + e_2 + 2e_3 + 2e_4$	$d_1 + d_2$	$d_3 + d_4$
$e_1 + 2e_2 + e_3 + e_4$	$d_2 + 2d_4$	$d_1 + d_3$
$e_1 + 2e_2 + e_3 + 2e_4$	$d_1 + 2d_2$	$d_3 + 2d_4$
$e_1 + 2e_2 + 2e_3 + e_4$	$d_3 + 2d_4$	$d_1 + 2d_2$
$e_1 + 2e_2 + 2e_3 + 2e_4$	$d_1 + 2d_3$	$d_2 + d_4$

B STRUKTURIERTE INTERVALLZERLEGUNGEN VON $\mathcal{L}(5, GF(3))$

$p_i \in H_0$	$\sigma_i \in S_4$	$\sigma_i \in S_5$
e_1	d_1	d_1
e_2	d_2	d_2
e_3	d_3	d_3
e_4	d_4	d_4
$e_1 + e_2$	$d_1 + d_2 + d_3 + 2d_4$	$d_1 + d_2 + d_3 + 2d_4$
$e_1 + 2e_2$	$d_1 + 2d_2 + 2d_3 + 2d_4$	$d_1 + 2d_2 + d_3 + d_4$
$e_1 + e_3$	$d_1 + 2d_2 + d_3 + 2d_4$	$d_1 + d_3$
$e_1 + 2e_3$	$d_1 + d_2 + 2d_3 + 2d_4$	$d_1 + 2d_3$
$e_1 + e_4$	$d_1 + d_4$	$d_1 + d_2 + d_3 + d_4$
$e_1 + 2e_4$	$d_1 + 2d_4$	$d_1 + 2d_2 + d_3 + 2d_4$
$e_2 + e_3$	$d_2 + d_3$	$d_1 + 2d_2 + 2d_3 + d_4$
$e_2 + 2e_3$	$d_2 + 2d_3$	$d_1 + d_2 + 2d_3 + 2d_4$
$e_2 + e_4$	$d_1 + d_2 + d_3 + d_4$	$d_2 + d_4$
$e_2 + 2e_4$	$d_1 + 2d_2 + 2d_3 + d_4$	$d_2 + 2d_4$
$e_3 + e_4$	$d_1 + 2d_2 + d_3 + d_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$
$e_3 + 2e_4$	$d_1 + d_2 + 2d_3 + d_4$	$d_1 + d_2 + 2d_3 + d_4$
$e_1 + e_2 + e_3$	$d_1 + d_3 + d_4$	$d_2 + d_3 + d_4$
$e_1 + e_2 + 2e_3$	$d_1 + d_2 + d_4$	$d_1 + d_2 + d_4$
$e_1 + 2e_2 + e_3$	$d_1 + 2d_2 + d_4$	$d_2 + 2d_3 + d_4$
$e_1 + 2e_2 + 2e_3$	$d_1 + 2d_3 + d_4$	$d_1 + 2d_2 + 2d_4$
$e_1 + e_2 + e_4$	$d_1 + d_2 + 2d_3$	$d_1 + d_2 + 2d_3$
$e_1 + e_2 + 2e_4$	$d_2 + 2d_3 + 2d_4$	$d_1 + 2d_3 + 2d_4$
$e_1 + 2e_2 + e_4$	$d_1 + 2d_2 + d_3$	$d_1 + 2d_3 + d_4$
$e_1 + 2e_2 + 2e_4$	$d_2 + 2d_3 + d_4$	$d_1 + 2d_2 + 2d_3$
$e_1 + e_3 + e_4$	$d_1 + d_2 + d_3$	$d_2 + 2d_3 + 2d_4$
$e_1 + e_3 + 2e_4$	$d_2 + d_3 + 2d_4$	$d_2 + d_3 + 2d_4$
$e_1 + 2e_3 + e_4$	$d_1 + 2d_2 + 2d_3$	$d_1 + 2d_2 + d_4$
$e_1 + 2e_3 + 2e_4$	$d_2 + d_3 + d_4$	$d_1 + d_2 + 2d_4$
$e_2 + e_3 + e_4$	$d_1 + 2d_3 + 2d_4$	$d_1 + d_2 + d_3$
$e_2 + e_3 + 2e_4$	$d_1 + d_3 + 2d_4$	$d_1 + d_3 + 2d_4$
$e_2 + 2e_3 + e_4$	$d_1 + 2d_2 + 2d_4$	$d_1 + 2d_2 + d_3$
$e_2 + 2e_3 + 2e_4$	$d_1 + d_2 + 2d_4$	$d_1 + d_3 + d_4$
$e_1 + e_2 + e_3 + e_4$	$d_2 + d_4$	$d_1 + d_4$
$e_1 + e_2 + e_3 + 2e_4$	$d_1 + d_2$	$d_1 + d_2$
$e_1 + e_2 + 2e_3 + e_4$	$d_3 + 2d_4$	$d_3 + 2d_4$
$e_1 + e_2 + 2e_3 + 2e_4$	$d_1 + 2d_3$	$d_2 + 2d_3$
$e_1 + 2e_2 + e_3 + e_4$	$d_3 + d_4$	$d_1 + 2d_2$
$e_1 + 2e_2 + e_3 + 2e_4$	$d_1 + d_3$	$d_1 + 2d_4$
$e_1 + 2e_2 + 2e_3 + e_4$	$d_2 + 2d_4$	$d_2 + d_3$
$e_1 + 2e_2 + 2e_3 + 2e_4$	$d_1 + 2d_2$	$d_3 + d_4$

$p_i \in H_0$	$\sigma_i \in S_6$	$\sigma_i \in S_7$
e_1	d_1	d_1
e_2	d_2	d_2
e_3	d_3	d_3
e_4	d_4	d_4
$e_1 + e_2$	$d_1 + d_2 + d_3 + d_4$	$d_1 + d_2 + 2d_3 + 2d_4$
$e_1 + 2e_2$	$d_1 + 2d_2 + d_3 + 2d_4$	$d_1 + 2d_2 + 2d_3 + d_4$
$e_1 + e_3$	$d_1 + d_3$	$d_1 + d_3$
$e_1 + 2e_3$	$d_1 + 2d_3$	$d_1 + 2d_3$
$e_1 + e_4$	$d_1 + 2d_2 + d_3 + d_4$	$d_1 + d_2 + 2d_3 + d_4$
$e_1 + 2e_4$	$d_1 + d_2 + d_3 + 2d_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$
$e_2 + e_3$	$d_1 + 2d_2 + 2d_3 + 2d_4$	$d_1 + d_2 + d_3 + 2d_4$
$e_2 + 2e_3$	$d_1 + d_2 + 2d_3 + d_4$	$d_1 + 2d_2 + d_3 + d_4$
$e_2 + e_4$	$d_2 + d_4$	$d_2 + d_4$
$e_2 + 2e_4$	$d_2 + 2d_4$	$d_2 + 2d_4$
$e_3 + e_4$	$d_1 + d_2 + 2d_3 + 2d_4$	$d_1 + d_2 + d_3 + d_4$
$e_3 + 2e_4$	$d_1 + 2d_2 + 2d_3 + d_4$	$d_1 + 2d_2 + d_3 + 2d_4$
$e_1 + e_2 + e_3$	$d_2 + d_3 + 2d_4$	$d_1 + d_2 + d_4$
$e_1 + e_2 + 2e_3$	$d_1 + d_2 + 2d_4$	$d_2 + 2d_3 + d_4$
$e_1 + 2e_2 + e_3$	$d_2 + 2d_3 + 2d_4$	$d_1 + 2d_2 + 2d_4$
$e_1 + 2e_2 + 2e_3$	$d_1 + 2d_2 + d_4$	$d_2 + d_3 + d_4$
$e_1 + e_2 + e_4$	$d_1 + 2d_3 + d_4$	$d_1 + d_2 + d_3$
$e_1 + e_2 + 2e_4$	$d_1 + d_2 + 2d_3$	$d_1 + d_3 + 2d_4$
$e_1 + 2e_2 + e_4$	$d_1 + 2d_2 + 2d_3$	$d_1 + d_3 + d_4$
$e_1 + 2e_2 + 2e_4$	$d_1 + 2d_3 + 2d_4$	$d_1 + 2d_2 + d_3$
$e_1 + e_3 + e_4$	$d_2 + d_3 + d_4$	$d_1 + 2d_2 + d_4$
$e_1 + e_3 + 2e_4$	$d_2 + 2d_3 + d_4$	$d_1 + d_2 + 2d_4$
$e_1 + 2e_3 + e_4$	$d_1 + d_2 + d_4$	$d_2 + d_3 + 2d_4$
$e_1 + 2e_3 + 2e_4$	$d_1 + 2d_2 + 2d_4$	$d_2 + 2d_3 + 2d_4$
$e_2 + e_3 + e_4$	$d_1 + d_3 + d_4$	$d_1 + 2d_2 + 2d_3$
$e_2 + e_3 + 2e_4$	$d_1 + d_2 + d_3$	$d_1 + 2d_3 + d_4$
$e_2 + 2e_3 + e_4$	$d_1 + d_3 + 2d_4$	$d_1 + d_2 + 2d_3$
$e_2 + 2e_3 + 2e_4$	$d_1 + 2d_2 + d_3$	$d_1 + 2d_3 + 2d_4$
$e_1 + e_2 + e_3 + e_4$	$d_1 + d_2$	$d_3 + d_4$
$e_1 + e_2 + e_3 + 2e_4$	$d_1 + 2d_4$	$d_2 + d_3$
$e_1 + e_2 + 2e_3 + e_4$	$d_2 + 2d_3$	$d_1 + d_4$
$e_1 + e_2 + 2e_3 + 2e_4$	$d_3 + d_4$	$d_1 + d_2$
$e_1 + 2e_2 + e_3 + e_4$	$d_1 + d_4$	$d_2 + 2d_3$
$e_1 + 2e_2 + e_3 + 2e_4$	$d_1 + 2d_2$	$d_3 + 2d_4$
$e_1 + 2e_2 + 2e_3 + e_4$	$d_3 + 2d_4$	$d_1 + 2d_2$
$e_1 + 2e_2 + 2e_3 + 2e_4$	$d_2 + d_3$	$d_1 + 2d_4$

B STRUKTURIERTE INTERVALLZERLEGUNGEN VON $\mathcal{L}(5, GF(3))$

$p_i \in H_0$	$\sigma_i \in S_8$	$\sigma_i \in S_9$
e_1	d_1	d_1
e_2	d_2	d_2
e_3	d_3	d_3
e_4	d_4	d_4
$e_1 + e_2$	$d_1 + d_2 + 2d_3 + d_4$	$d_1 + d_2$
$e_1 + 2e_2$	$d_1 + 2d_2 + 2d_3 + 2d_4$	$d_1 + 2d_2$
$e_1 + e_3$	$d_1 + d_3$	$d_1 + d_2 + d_3 + 2d_4$
$e_1 + 2e_3$	$d_1 + 2d_3$	$d_1 + d_2 + 2d_3 + d_4$
$e_1 + e_4$	$d_1 + 2d_2 + 2d_3 + d_4$	$d_1 + d_2 + d_3 + d_4$
$e_1 + 2e_4$	$d_1 + d_2 + 2d_3 + 2d_4$	$d_1 + d_2 + 2d_3 + 2d_4$
$e_2 + e_3$	$d_1 + d_2 + d_3 + d_4$	$d_1 + 2d_2 + 2d_3 + d_4$
$e_2 + 2e_3$	$d_1 + 2d_2 + d_3 + 2d_4$	$d_1 + 2d_2 + d_3 + 2d_4$
$e_2 + e_4$	$d_2 + d_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$
$e_2 + 2e_4$	$d_2 + 2d_4$	$d_1 + 2d_2 + d_3 + d_4$
$e_3 + e_4$	$d_1 + 2d_2 + d_3 + d_4$	$d_3 + d_4$
$e_3 + 2e_4$	$d_1 + d_2 + d_3 + 2d_4$	$d_3 + 2d_4$
$e_1 + e_2 + e_3$	$d_1 + d_2 + 2d_4$	$d_2 + d_3 + d_4$
$e_1 + e_2 + 2e_3$	$d_2 + 2d_3 + 2d_4$	$d_2 + 2d_3 + 2d_4$
$e_1 + 2e_2 + e_3$	$d_1 + 2d_2 + d_4$	$d_1 + d_3 + d_4$
$e_1 + 2e_2 + 2e_3$	$d_2 + d_3 + 2d_4$	$d_1 + 2d_3 + 2d_4$
$e_1 + e_2 + e_4$	$d_1 + d_3 + d_4$	$d_2 + 2d_3 + d_4$
$e_1 + e_2 + 2e_4$	$d_1 + d_2 + d_3$	$d_2 + d_3 + 2d_4$
$e_1 + 2e_2 + e_4$	$d_1 + 2d_2 + d_3$	$d_1 + 2d_3 + d_4$
$e_1 + 2e_2 + 2e_4$	$d_1 + d_3 + 2d_4$	$d_1 + d_3 + 2d_4$
$e_1 + e_3 + e_4$	$d_1 + d_2 + d_4$	$d_1 + 2d_2 + d_3$
$e_1 + e_3 + 2e_4$	$d_1 + 2d_2 + 2d_4$	$d_1 + 2d_2 + 2d_4$
$e_1 + 2e_3 + e_4$	$d_2 + 2d_3 + d_4$	$d_1 + 2d_2 + d_4$
$e_1 + 2e_3 + 2e_4$	$d_2 + d_3 + d_4$	$d_1 + 2d_2 + 2d_3$
$e_2 + e_3 + e_4$	$d_1 + 2d_3 + 2d_4$	$d_1 + d_2 + d_3$
$e_2 + e_3 + 2e_4$	$d_1 + 2d_2 + 2d_3$	$d_1 + d_2 + 2d_4$
$e_2 + 2e_3 + e_4$	$d_1 + 2d_3 + d_4$	$d_1 + d_2 + d_4$
$e_2 + 2e_3 + 2e_4$	$d_1 + d_2 + 2d_3$	$d_1 + d_2 + 2d_3$
$e_1 + e_2 + e_3 + e_4$	$d_2 + d_3$	$d_1 + d_4$
$e_1 + e_2 + e_3 + 2e_4$	$d_3 + 2d_4$	$d_1 + d_3$
$e_1 + e_2 + 2e_3 + e_4$	$d_1 + d_2$	$d_1 + 2d_3$
$e_1 + e_2 + 2e_3 + 2e_4$	$d_1 + 2d_4$	$d_1 + 2d_4$
$e_1 + 2e_2 + e_3 + e_4$	$d_3 + d_4$	$d_2 + 2d_4$
$e_1 + 2e_2 + e_3 + 2e_4$	$d_2 + 2d_3$	$d_2 + 2d_3$
$e_1 + 2e_2 + 2e_3 + e_4$	$d_1 + d_4$	$d_2 + d_3$
$e_1 + 2e_2 + 2e_3 + 2e_4$	$d_1 + 2d_2$	$d_2 + d_4$

$p_i \in H_0$	$\sigma_i \in S_{10}$	$\sigma_i \in S_{11}$
e_1	d_1	d_1
e_2	d_2	d_2
e_3	d_3	d_3
e_4	d_4	d_4
$e_1 + e_2$	$d_1 + d_2$	$d_1 + d_2$
$e_1 + 2e_2$	$d_1 + 2d_2$	$d_1 + 2d_2$
$e_1 + e_3$	$d_1 + d_2 + d_3 + d_4$	$d_1 + 2d_2 + d_3 + 2d_4$
$e_1 + 2e_3$	$d_1 + d_2 + 2d_3 + 2d_4$	$d_1 + 2d_2 + 2d_3 + d_4$
$e_1 + e_4$	$d_1 + d_2 + 2d_3 + d_4$	$d_1 + 2d_2 + d_3 + d_4$
$e_1 + 2e_4$	$d_1 + d_2 + d_3 + 2d_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$
$e_2 + e_3$	$d_1 + 2d_2 + 2d_3 + 2d_4$	$d_1 + d_2 + d_3 + 2d_4$
$e_2 + 2e_3$	$d_1 + 2d_2 + d_3 + d_4$	$d_1 + d_2 + 2d_3 + d_4$
$e_2 + e_4$	$d_1 + 2d_2 + d_3 + 2d_4$	$d_1 + d_2 + d_3 + d_4$
$e_2 + 2e_4$	$d_1 + 2d_2 + 2d_3 + d_4$	$d_1 + d_2 + 2d_3 + 2d_4$
$e_3 + e_4$	$d_3 + d_4$	$d_3 + d_4$
$e_3 + 2e_4$	$d_3 + 2d_4$	$d_3 + 2d_4$
$e_1 + e_2 + e_3$	$d_2 + d_3 + 2d_4$	$d_1 + d_3 + d_4$
$e_1 + e_2 + 2e_3$	$d_2 + 2d_3 + d_4$	$d_1 + 2d_3 + 2d_4$
$e_1 + 2e_2 + e_3$	$d_1 + d_3 + 2d_4$	$d_2 + 2d_3 + 2d_4$
$e_1 + 2e_2 + 2e_3$	$d_1 + 2d_3 + d_4$	$d_2 + d_3 + d_4$
$e_1 + e_2 + e_4$	$d_2 + d_3 + d_4$	$d_1 + 2d_3 + d_4$
$e_1 + e_2 + 2e_4$	$d_2 + 2d_3 + 2d_4$	$d_1 + d_3 + 2d_4$
$e_1 + 2e_2 + e_4$	$d_1 + d_3 + d_4$	$d_2 + d_3 + 2d_4$
$e_1 + 2e_2 + 2e_4$	$d_1 + 2d_3 + 2d_4$	$d_2 + 2d_3 + d_4$
$e_1 + e_3 + e_4$	$d_1 + 2d_2 + d_4$	$d_1 + d_2 + d_3$
$e_1 + e_3 + 2e_4$	$d_1 + 2d_2 + d_3$	$d_1 + d_2 + 2d_4$
$e_1 + 2e_3 + e_4$	$d_1 + 2d_2 + 2d_3$	$d_1 + d_2 + d_4$
$e_1 + 2e_3 + 2e_4$	$d_1 + 2d_2 + 2d_4$	$d_1 + d_2 + 2d_3$
$e_2 + e_3 + e_4$	$d_1 + d_2 + d_4$	$d_1 + 2d_2 + 2d_3$
$e_2 + e_3 + 2e_4$	$d_1 + d_2 + d_3$	$d_1 + 2d_2 + d_4$
$e_2 + 2e_3 + e_4$	$d_1 + d_2 + 2d_3$	$d_1 + 2d_2 + 2d_4$
$e_2 + 2e_3 + 2e_4$	$d_1 + d_2 + 2d_4$	$d_1 + 2d_2 + d_3$
$e_1 + e_2 + e_3 + e_4$	$d_1 + d_3$	$d_2 + d_4$
$e_1 + e_2 + e_3 + 2e_4$	$d_1 + 2d_4$	$d_2 + d_3$
$e_1 + e_2 + 2e_3 + e_4$	$d_1 + d_4$	$d_2 + 2d_3$
$e_1 + e_2 + 2e_3 + 2e_4$	$d_1 + 2d_3$	$d_2 + 2d_4$
$e_1 + 2e_2 + e_3 + e_4$	$d_2 + 2d_3$	$d_1 + d_4$
$e_1 + 2e_2 + e_3 + 2e_4$	$d_2 + d_4$	$d_1 + d_3$
$e_1 + 2e_2 + 2e_3 + e_4$	$d_2 + 2d_4$	$d_1 + 2d_3$
$e_1 + 2e_2 + 2e_3 + 2e_4$	$d_2 + d_3$	$d_1 + 2d_4$

B STRUKTURIERTE INTERVALLZERLEGUNGEN VON $\mathcal{L}(5, GF(3))$

$p_i \in H_0$	$\sigma_i \in S_{12}$	$\sigma_i \in S_{13}$
e_1	d_1	d_1
e_2	d_2	d_2
e_3	d_3	$d_1 + d_2 + d_3$
e_4	d_4	$d_1 + 2d_2 + d_4$
$e_1 + e_2$	$d_1 + d_2$	$d_1 + d_2 + 2d_3$
$e_1 + 2e_2$	$d_1 + 2d_2$	$d_1 + 2d_2 + 2d_4$
$e_1 + e_3$	$d_1 + 2d_2 + d_3 + d_4$	$d_2 + 2d_3$
$e_1 + 2e_3$	$d_1 + 2d_2 + 2d_3 + 2d_4$	$d_1 + 2d_2 + 2d_3 + d_4$
$e_1 + e_4$	$d_1 + 2d_2 + 2d_3 + d_4$	$d_2 + d_4$
$e_1 + 2e_4$	$d_1 + 2d_2 + d_3 + 2d_4$	$d_1 + d_2 + d_3 + 2d_4$
$e_2 + e_3$	$d_1 + d_2 + d_3 + d_4$	$d_1 + 2d_3$
$e_2 + 2e_3$	$d_1 + d_2 + 2d_3 + 2d_4$	$d_1 + 2d_2 + d_3 + d_4$
$e_2 + e_4$	$d_1 + d_2 + 2d_3 + d_4$	$d_1 + d_2 + d_3 + d_4$
$e_2 + 2e_4$	$d_1 + d_2 + d_3 + 2d_4$	$d_1 + 2d_4$
$e_3 + e_4$	$d_3 + d_4$	$d_3 + d_4$
$e_3 + 2e_4$	$d_3 + 2d_4$	$d_3 + 2d_4$
$e_1 + e_2 + e_3$	$d_1 + d_3 + 2d_4$	$d_1 + d_2$
$e_1 + e_2 + 2e_3$	$d_1 + 2d_3 + d_4$	d_3
$e_1 + 2e_2 + e_3$	$d_2 + 2d_3 + d_4$	$d_1 + d_3 + 2d_4$
$e_1 + 2e_2 + 2e_3$	$d_2 + d_3 + 2d_4$	$d_2 + d_3 + d_4$
$e_1 + e_2 + e_4$	$d_1 + d_3 + d_4$	$d_1 + 2d_3 + d_4$
$e_1 + e_2 + 2e_4$	$d_1 + 2d_3 + 2d_4$	$d_2 + 2d_3 + 2d_4$
$e_1 + 2e_2 + e_4$	$d_2 + 2d_3 + 2d_4$	$d_1 + 2d_2$
$e_1 + 2e_2 + 2e_4$	$d_2 + d_3 + d_4$	d_4
$e_1 + e_3 + e_4$	$d_1 + d_2 + d_4$	$d_1 + 2d_3 + 2d_4$
$e_1 + e_3 + 2e_4$	$d_1 + d_2 + d_3$	$d_1 + d_2 + 2d_4$
$e_1 + 2e_3 + e_4$	$d_1 + d_2 + 2d_3$	$d_1 + 2d_2 + 2d_3$
$e_1 + 2e_3 + 2e_4$	$d_1 + d_2 + 2d_4$	$d_1 + d_3 + d_4$
$e_2 + e_3 + e_4$	$d_1 + 2d_2 + 2d_4$	$d_1 + d_2 + d_4$
$e_2 + e_3 + 2e_4$	$d_1 + 2d_2 + 2d_3$	$d_2 + 2d_3 + d_4$
$e_2 + 2e_3 + e_4$	$d_1 + 2d_2 + d_3$	$d_2 + d_3 + 2d_4$
$e_2 + 2e_3 + 2e_4$	$d_1 + 2d_2 + d_4$	$d_1 + 2d_2 + d_3$
$e_1 + e_2 + e_3 + e_4$	$d_2 + d_3$	$d_1 + d_2 + 2d_3 + d_4$
$e_1 + e_2 + e_3 + 2e_4$	$d_2 + 2d_4$	$d_1 + d_2 + 2d_3 + 2d_4$
$e_1 + e_2 + 2e_3 + e_4$	$d_2 + d_4$	$d_1 + d_4$
$e_1 + e_2 + 2e_3 + 2e_4$	$d_2 + 2d_3$	$d_2 + 2d_4$
$e_1 + 2e_2 + e_3 + e_4$	$d_1 + d_3$	$d_1 + 2d_2 + d_3 + 2d_4$
$e_1 + 2e_2 + e_3 + 2e_4$	$d_1 + 2d_4$	$d_1 + d_3$
$e_1 + 2e_2 + 2e_3 + e_4$	$d_1 + d_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$
$e_1 + 2e_2 + 2e_3 + 2e_4$	$d_1 + 2d_3$	$d_2 + d_3$

$p_i \in H_0$	$\sigma_i \in S_{14}$	$\sigma_i \in S_{15}$
e_1	d_1	d_1
e_2	d_2	d_2
e_3	$d_1 + d_2 + d_3$	$d_1 + 2d_2 + d_3$
e_4	$d_1 + 2d_2 + 2d_4$	$d_1 + d_2 + d_4$
$e_1 + e_2$	$d_1 + d_2 + 2d_3$	$d_1 + d_2 + 2d_4$
$e_1 + 2e_2$	$d_1 + 2d_2 + d_4$	$d_1 + 2d_2 + 2d_3$
$e_1 + e_3$	$d_2 + 2d_3$	$d_2 + d_3$
$e_1 + 2e_3$	$d_1 + 2d_2 + 2d_3 + 2d_4$	$d_1 + d_2 + 2d_3 + d_4$
$e_1 + e_4$	$d_1 + d_2 + d_3 + d_4$	$d_2 + 2d_4$
$e_1 + 2e_4$	$d_2 + 2d_4$	$d_1 + 2d_2 + d_3 + 2d_4$
$e_2 + e_3$	$d_1 + 2d_3$	$d_1 + d_2 + d_3 + d_4$
$e_2 + 2e_3$	$d_1 + 2d_2 + d_3 + 2d_4$	$d_1 + 2d_3$
$e_2 + e_4$	$d_1 + d_4$	$d_1 + 2d_4$
$e_2 + 2e_4$	$d_1 + d_2 + d_3 + 2d_4$	$d_1 + 2d_2 + d_3 + d_4$
$e_3 + e_4$	$d_3 + d_4$	$d_3 + d_4$
$e_3 + 2e_4$	$d_3 + 2d_4$	$d_3 + 2d_4$
$e_1 + e_2 + e_3$	$d_1 + d_2$	$d_1 + d_3 + 2d_4$
$e_1 + e_2 + 2e_3$	d_3	$d_2 + 2d_3 + 2d_4$
$e_1 + 2e_2 + e_3$	$d_1 + d_3 + d_4$	$d_1 + 2d_2$
$e_1 + 2e_2 + 2e_3$	$d_2 + d_3 + 2d_4$	d_3
$e_1 + e_2 + e_4$	$d_2 + 2d_3 + d_4$	$d_1 + d_2$
$e_1 + e_2 + 2e_4$	$d_1 + 2d_3 + 2d_4$	d_4
$e_1 + 2e_2 + e_4$	d_4	$d_1 + 2d_3 + d_4$
$e_1 + 2e_2 + 2e_4$	$d_1 + 2d_2$	$d_2 + d_3 + d_4$
$e_1 + e_3 + e_4$	$d_1 + d_2 + d_4$	$d_1 + 2d_3 + 2d_4$
$e_1 + e_3 + 2e_4$	$d_1 + 2d_3 + d_4$	$d_1 + 2d_2 + 2d_4$
$e_1 + 2e_3 + e_4$	$d_1 + d_3 + 2d_4$	$d_1 + d_2 + 2d_3$
$e_1 + 2e_3 + 2e_4$	$d_1 + 2d_2 + 2d_3$	$d_1 + d_3 + d_4$
$e_2 + e_3 + e_4$	$d_2 + 2d_3 + 2d_4$	$d_1 + d_2 + d_3$
$e_2 + e_3 + 2e_4$	$d_1 + d_2 + 2d_4$	$d_2 + 2d_3 + d_4$
$e_2 + 2e_3 + e_4$	$d_1 + 2d_2 + d_3$	$d_2 + d_3 + 2d_4$
$e_2 + 2e_3 + 2e_4$	$d_2 + d_3 + d_4$	$d_1 + 2d_2 + d_4$
$e_1 + e_2 + e_3 + e_4$	$d_1 + d_2 + 2d_3 + d_4$	$d_1 + d_2 + d_3 + 2d_4$
$e_1 + e_2 + e_3 + 2e_4$	$d_1 + d_2 + 2d_3 + 2d_4$	$d_1 + d_3$
$e_1 + e_2 + 2e_3 + e_4$	$d_2 + d_4$	$d_1 + d_2 + 2d_3 + 2d_4$
$e_1 + e_2 + 2e_3 + 2e_4$	$d_1 + 2d_4$	$d_2 + 2d_3$
$e_1 + 2e_2 + e_3 + e_4$	$d_1 + d_3$	$d_1 + 2d_2 + 2d_3 + d_4$
$e_1 + 2e_2 + e_3 + 2e_4$	$d_1 + 2d_2 + d_3 + d_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$
$e_1 + 2e_2 + 2e_3 + e_4$	$d_2 + d_3$	$d_1 + d_4$
$e_1 + 2e_2 + 2e_3 + 2e_4$	$d_1 + 2d_2 + 2d_3 + d_4$	$d_2 + d_4$

B STRUKTURIERTE INTERVALLZERLEGUNGEN VON $\mathcal{L}(5, GF(3))$

$p_i \in H_0$	$\sigma_i \in S_{16}$	$\sigma_i \in S_{17}$
e_1	d_1	d_1
e_2	d_2	d_2
e_3	$d_1 + 2d_2 + d_3$	$d_1 + 2d_2 + 2d_3$
e_4	$d_1 + d_2 + 2d_4$	$d_1 + d_2 + d_4$
$e_1 + e_2$	$d_1 + d_2 + d_4$	$d_1 + d_2 + 2d_4$
$e_1 + 2e_2$	$d_1 + 2d_2 + 2d_3$	$d_1 + 2d_2 + d_3$
$e_1 + e_3$	$d_2 + d_3$	$d_1 + d_2 + d_3 + d_4$
$e_1 + 2e_3$	$d_1 + d_2 + 2d_3 + 2d_4$	$d_2 + 2d_3$
$e_1 + e_4$	$d_1 + 2d_2 + d_3 + d_4$	$d_2 + 2d_4$
$e_1 + 2e_4$	$d_2 + d_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$
$e_2 + e_3$	$d_1 + d_2 + d_3 + 2d_4$	$d_1 + d_3$
$e_2 + 2e_3$	$d_1 + 2d_3$	$d_1 + d_2 + 2d_3 + d_4$
$e_2 + e_4$	$d_1 + 2d_2 + d_3 + 2d_4$	$d_1 + 2d_4$
$e_2 + 2e_4$	$d_1 + d_4$	$d_1 + 2d_2 + 2d_3 + d_4$
$e_3 + e_4$	$d_3 + d_4$	$d_3 + d_4$
$e_3 + 2e_4$	$d_3 + 2d_4$	$d_3 + 2d_4$
$e_1 + e_2 + e_3$	$d_1 + d_3 + d_4$	$d_2 + d_3 + 2d_4$
$e_1 + e_2 + 2e_3$	$d_2 + 2d_3 + d_4$	$d_1 + 2d_3 + 2d_4$
$e_1 + 2e_2 + e_3$	$d_1 + 2d_2$	d_3
$e_1 + 2e_2 + 2e_3$	d_3	$d_1 + 2d_2$
$e_1 + e_2 + e_4$	d_4	$d_1 + d_2$
$e_1 + e_2 + 2e_4$	$d_1 + d_2$	d_4
$e_1 + 2e_2 + e_4$	$d_2 + d_3 + 2d_4$	$d_1 + d_3 + d_4$
$e_1 + 2e_2 + 2e_4$	$d_1 + 2d_3 + 2d_4$	$d_2 + 2d_3 + d_4$
$e_1 + e_3 + e_4$	$d_1 + 2d_2 + d_4$	$d_1 + d_2 + d_3$
$e_1 + e_3 + 2e_4$	$d_1 + 2d_3 + d_4$	$d_1 + 2d_3 + d_4$
$e_1 + 2e_3 + e_4$	$d_1 + d_3 + 2d_4$	$d_1 + d_3 + 2d_4$
$e_1 + 2e_3 + 2e_4$	$d_1 + d_2 + 2d_3$	$d_1 + 2d_2 + 2d_4$
$e_2 + e_3 + e_4$	$d_2 + 2d_3 + 2d_4$	$d_2 + 2d_3 + 2d_4$
$e_2 + e_3 + 2e_4$	$d_1 + d_2 + d_3$	$d_1 + 2d_2 + d_4$
$e_2 + 2e_3 + e_4$	$d_1 + 2d_2 + 2d_4$	$d_1 + d_2 + 2d_3$
$e_2 + 2e_3 + 2e_4$	$d_2 + d_3 + d_4$	$d_2 + d_3 + d_4$
$e_1 + e_2 + e_3 + e_4$	$d_1 + d_3$	$d_1 + d_2 + d_3 + 2d_4$
$e_1 + e_2 + e_3 + 2e_4$	$d_1 + d_2 + d_3 + d_4$	$d_2 + d_3$
$e_1 + e_2 + 2e_3 + e_4$	$d_2 + 2d_3$	$d_1 + d_2 + 2d_3 + 2d_4$
$e_1 + e_2 + 2e_3 + 2e_4$	$d_1 + d_2 + 2d_3 + d_4$	$d_1 + 2d_3$
$e_1 + 2e_2 + e_3 + e_4$	$d_1 + 2d_2 + 2d_3 + d_4$	$d_1 + d_4$
$e_1 + 2e_2 + e_3 + 2e_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$	$d_2 + d_4$
$e_1 + 2e_2 + 2e_3 + e_4$	$d_2 + 2d_4$	$d_1 + 2d_2 + d_3 + d_4$
$e_1 + 2e_2 + 2e_3 + 2e_4$	$d_1 + 2d_4$	$d_1 + 2d_2 + d_3 + 2d_4$

$p_i \in H_0$	$\sigma_i \in S_{18}$	$\sigma_i \in S_{19}$
e_1	d_1	d_1
e_2	d_2	d_2
e_3	$d_1 + 2d_2 + 2d_3$	$d_1 + d_2 + 2d_3$
e_4	$d_1 + d_2 + 2d_4$	$d_1 + 2d_2 + d_4$
$e_1 + e_2$	$d_1 + d_2 + d_4$	$d_1 + d_2 + d_3$
$e_1 + 2e_2$	$d_1 + 2d_2 + d_3$	$d_1 + 2d_2 + 2d_4$
$e_1 + e_3$	$d_1 + d_2 + d_3 + 2d_4$	$d_1 + 2d_2 + d_3 + d_4$
$e_1 + 2e_3$	$d_2 + 2d_3$	$d_2 + d_3$
$e_1 + e_4$	$d_1 + 2d_2 + 2d_3 + d_4$	$d_2 + d_4$
$e_1 + 2e_4$	$d_2 + d_4$	$d_1 + d_2 + 2d_3 + 2d_4$
$e_2 + e_3$	$d_1 + d_3$	$d_1 + 2d_2 + 2d_3 + d_4$
$e_2 + 2e_3$	$d_1 + d_2 + 2d_3 + 2d_4$	$d_1 + d_3$
$e_2 + e_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$	$d_1 + d_2 + 2d_3 + d_4$
$e_2 + 2e_4$	$d_1 + d_4$	$d_1 + 2d_4$
$e_3 + e_4$	$d_3 + d_4$	$d_3 + d_4$
$e_3 + 2e_4$	$d_3 + 2d_4$	$d_3 + 2d_4$
$e_1 + e_2 + e_3$	$d_2 + d_3 + d_4$	d_3
$e_1 + e_2 + 2e_3$	$d_1 + 2d_3 + d_4$	$d_1 + d_2$
$e_1 + 2e_2 + e_3$	d_3	$d_2 + 2d_3 + d_4$
$e_1 + 2e_2 + 2e_3$	$d_1 + 2d_2$	$d_1 + 2d_3 + 2d_4$
$e_1 + e_2 + e_4$	d_4	$d_1 + d_3 + d_4$
$e_1 + e_2 + 2e_4$	$d_1 + d_2$	$d_2 + d_3 + 2d_4$
$e_1 + 2e_2 + e_4$	$d_2 + 2d_3 + 2d_4$	$d_1 + 2d_2$
$e_1 + 2e_2 + 2e_4$	$d_1 + d_3 + 2d_4$	d_4
$e_1 + e_3 + e_4$	$d_1 + 2d_3 + 2d_4$	$d_1 + 2d_2 + d_3$
$e_1 + e_3 + 2e_4$	$d_1 + d_2 + d_3$	$d_1 + 2d_3 + d_4$
$e_1 + 2e_3 + e_4$	$d_1 + 2d_2 + d_4$	$d_1 + d_3 + 2d_4$
$e_1 + 2e_3 + 2e_4$	$d_1 + d_3 + d_4$	$d_1 + d_2 + 2d_4$
$e_2 + e_3 + e_4$	$d_1 + 2d_2 + 2d_4$	$d_2 + 2d_3 + 2d_4$
$e_2 + e_3 + 2e_4$	$d_2 + 2d_3 + d_4$	$d_1 + 2d_2 + 2d_3$
$e_2 + 2e_3 + e_4$	$d_2 + d_3 + 2d_4$	$d_1 + d_2 + d_4$
$e_2 + 2e_3 + 2e_4$	$d_1 + d_2 + 2d_3$	$d_2 + d_3 + d_4$
$e_1 + e_2 + e_3 + e_4$	$d_2 + d_3$	$d_1 + d_4$
$e_1 + e_2 + e_3 + 2e_4$	$d_1 + d_2 + d_3 + d_4$	$d_2 + 2d_4$
$e_1 + e_2 + 2e_3 + e_4$	$d_1 + 2d_3$	$d_1 + d_2 + d_3 + d_4$
$e_1 + e_2 + 2e_3 + 2e_4$	$d_1 + d_2 + 2d_3 + d_4$	$d_1 + d_2 + d_3 + 2d_4$
$e_1 + 2e_2 + e_3 + e_4$	$d_2 + 2d_4$	$d_1 + 2d_2 + d_3 + 2d_4$
$e_1 + 2e_2 + e_3 + 2e_4$	$d_1 + 2d_4$	$d_2 + 2d_3$
$e_1 + 2e_2 + 2e_3 + e_4$	$d_1 + 2d_2 + d_3 + d_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$
$e_1 + 2e_2 + 2e_3 + 2e_4$	$d_1 + 2d_2 + d_3 + 2d_4$	$d_1 + 2d_3$

B STRUKTURIERTE INTERVALLZERLEGUNGEN VON $\mathcal{L}(5, GF(3))$

$p_i \in H_0$	$\sigma_i \in S_{20}$	$\sigma_i \in S_{21}$
e_1	d_1	d_1
e_2	d_2	$d_1 + d_2$
e_3	$d_1 + d_2 + 2d_3$	$d_2 + d_3$
e_4	$d_1 + 2d_2 + 2d_4$	$d_1 + d_2 + d_3 + d_4$
$e_1 + e_2$	$d_1 + d_2 + d_3$	$d_2 + 2d_3 + d_4$
$e_1 + 2e_2$	$d_1 + 2d_2 + d_4$	$d_1 + 2d_2 + 2d_3$
$e_1 + e_3$	$d_1 + 2d_2 + d_3 + 2d_4$	$d_1 + d_2 + d_3 + 2d_4$
$e_1 + 2e_3$	$d_2 + d_3$	$d_1 + 2d_3$
$e_1 + e_4$	$d_1 + d_2 + 2d_3 + d_4$	$d_2 + d_3 + 2d_4$
$e_1 + 2e_4$	$d_2 + 2d_4$	$d_1 + d_2 + 2d_3 + 2d_4$
$e_2 + e_3$	$d_1 + 2d_2 + 2d_3 + 2d_4$	$d_1 + d_3 + d_4$
$e_2 + 2e_3$	$d_1 + d_3$	$d_1 + d_2 + 2d_3$
$e_2 + e_4$	$d_1 + d_4$	$d_3 + 2d_4$
$e_2 + 2e_4$	$d_1 + d_2 + 2d_3 + 2d_4$	$d_1 + 2d_2 + 2d_3 + d_4$
$e_3 + e_4$	$d_3 + d_4$	$d_1 + 2d_4$
$e_3 + 2e_4$	$d_3 + 2d_4$	$d_1 + d_2 + 2d_3 + d_4$
$e_1 + e_2 + e_3$	d_3	d_2
$e_1 + e_2 + 2e_3$	$d_1 + d_2$	$d_1 + 2d_2 + d_3 + d_4$
$e_1 + 2e_2 + e_3$	$d_2 + 2d_3 + 2d_4$	d_3
$e_1 + 2e_2 + 2e_3$	$d_1 + 2d_3 + d_4$	$d_1 + 2d_2 + 2d_4$
$e_1 + e_2 + e_4$	$d_2 + d_3 + d_4$	$d_1 + 2d_2 + d_3 + 2d_4$
$e_1 + e_2 + 2e_4$	$d_1 + d_3 + 2d_4$	$d_2 + 2d_3$
$e_1 + 2e_2 + e_4$	d_4	$d_1 + 2d_3 + d_4$
$e_1 + 2e_2 + 2e_4$	$d_1 + 2d_2$	$d_1 + 2d_3 + 2d_4$
$e_1 + e_3 + e_4$	$d_1 + 2d_3 + 2d_4$	$d_1 + d_2 + d_3$
$e_1 + e_3 + 2e_4$	$d_1 + 2d_2 + d_3$	d_4
$e_1 + 2e_3 + e_4$	$d_1 + d_2 + d_4$	$d_1 + d_2 + d_4$
$e_1 + 2e_3 + 2e_4$	$d_1 + d_3 + d_4$	$d_3 + d_4$
$e_2 + e_3 + e_4$	$d_1 + 2d_2 + 2d_3$	$d_2 + 2d_3 + 2d_4$
$e_2 + e_3 + 2e_4$	$d_2 + 2d_3 + d_4$	$d_1 + d_3$
$e_2 + 2e_3 + e_4$	$d_2 + d_3 + 2d_4$	$d_2 + d_4$
$e_2 + 2e_3 + 2e_4$	$d_1 + d_2 + 2d_4$	$d_2 + 2d_4$
$e_1 + e_2 + e_3 + e_4$	$d_2 + d_4$	$d_1 + d_4$
$e_1 + e_2 + e_3 + 2e_4$	$d_1 + 2d_4$	$d_2 + d_3 + d_4$
$e_1 + e_2 + 2e_3 + e_4$	$d_1 + d_2 + d_3 + d_4$	$d_1 + 2d_2 + d_3$
$e_1 + e_2 + 2e_3 + 2e_4$	$d_1 + d_2 + d_3 + 2d_4$	$d_1 + 2d_2 + d_4$
$e_1 + 2e_2 + e_3 + e_4$	$d_2 + 2d_3$	$d_1 + d_2 + 2d_4$
$e_1 + 2e_2 + e_3 + 2e_4$	$d_1 + 2d_2 + d_3 + d_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$
$e_1 + 2e_2 + 2e_3 + e_4$	$d_1 + 2d_3$	$d_1 + d_3 + 2d_4$
$e_1 + 2e_2 + 2e_3 + 2e_4$	$d_1 + 2d_2 + 2d_3 + d_4$	$d_1 + 2d_2$

$p_i \in H_0$	$\sigma_i \in S_{22}$	$\sigma_i \in S_{23}$
e_1	d_1	d_1
e_2	$d_1 + d_2$	$d_1 + d_2$
e_3	$d_2 + d_3$	$d_2 + 2d_3$
e_4	$d_1 + d_2 + d_3 + 2d_4$	$d_1 + d_2 + 2d_3 + d_4$
$e_1 + e_2$	$d_2 + 2d_3 + 2d_4$	$d_2 + d_3 + d_4$
$e_1 + 2e_2$	$d_1 + 2d_2 + 2d_3$	$d_1 + 2d_2 + d_3$
$e_1 + e_3$	$d_1 + d_2 + d_3 + d_4$	$d_1 + d_3$
$e_1 + 2e_3$	$d_1 + 2d_3$	$d_1 + d_2 + 2d_3 + 2d_4$
$e_1 + e_4$	$d_1 + d_2 + 2d_3 + d_4$	$d_2 + 2d_3 + 2d_4$
$e_1 + 2e_4$	$d_2 + d_3 + d_4$	$d_1 + d_2 + d_3 + 2d_4$
$e_2 + e_3$	$d_1 + d_3 + 2d_4$	$d_1 + d_2 + d_3$
$e_2 + 2e_3$	$d_1 + d_2 + 2d_3$	$d_1 + 2d_3 + d_4$
$e_2 + e_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$	$d_3 + d_4$
$e_2 + 2e_4$	$d_3 + d_4$	$d_1 + 2d_2 + d_3 + d_4$
$e_3 + e_4$	$d_1 + d_2 + 2d_3 + 2d_4$	$d_1 + d_2 + d_3 + d_4$
$e_3 + 2e_4$	$d_1 + d_4$	$d_1 + 2d_4$
$e_1 + e_2 + e_3$	d_2	$d_1 + 2d_2 + 2d_3 + d_4$
$e_1 + e_2 + 2e_3$	$d_1 + 2d_2 + d_3 + 2d_4$	d_2
$e_1 + 2e_2 + e_3$	d_3	$d_1 + 2d_2 + 2d_4$
$e_1 + 2e_2 + 2e_3$	$d_1 + 2d_2 + d_4$	d_3
$e_1 + e_2 + e_4$	$d_2 + 2d_3$	$d_1 + 2d_2 + 2d_3 + 2d_4$
$e_1 + e_2 + 2e_4$	$d_1 + 2d_2 + d_3 + d_4$	$d_2 + d_3$
$e_1 + 2e_2 + e_4$	$d_1 + 2d_3 + d_4$	$d_1 + d_3 + d_4$
$e_1 + 2e_2 + 2e_4$	$d_1 + 2d_3 + 2d_4$	$d_1 + d_3 + 2d_4$
$e_1 + e_3 + e_4$	d_4	$d_1 + d_2 + d_4$
$e_1 + e_3 + 2e_4$	$d_1 + d_2 + d_3$	$d_3 + 2d_4$
$e_1 + 2e_3 + e_4$	$d_3 + 2d_4$	$d_1 + d_2 + 2d_3$
$e_1 + 2e_3 + 2e_4$	$d_1 + d_2 + 2d_4$	d_4
$e_2 + e_3 + e_4$	$d_1 + d_3$	$d_2 + d_4$
$e_2 + e_3 + 2e_4$	$d_2 + 2d_3 + d_4$	$d_2 + 2d_4$
$e_2 + 2e_3 + e_4$	$d_2 + d_4$	$d_2 + d_3 + 2d_4$
$e_2 + 2e_3 + 2e_4$	$d_2 + 2d_4$	$d_1 + 2d_3$
$e_1 + e_2 + e_3 + e_4$	$d_2 + d_3 + 2d_4$	$d_1 + 2d_2 + 2d_3$
$e_1 + e_2 + e_3 + 2e_4$	$d_1 + 2d_4$	$d_1 + 2d_2 + d_4$
$e_1 + e_2 + 2e_3 + e_4$	$d_1 + 2d_2 + 2d_4$	$d_1 + d_4$
$e_1 + e_2 + 2e_3 + 2e_4$	$d_1 + 2d_2 + d_3$	$d_2 + 2d_3 + d_4$
$e_1 + 2e_2 + e_3 + e_4$	$d_1 + 2d_2 + 2d_3 + d_4$	$d_1 + 2d_3 + 2d_4$
$e_1 + 2e_2 + e_3 + 2e_4$	$d_1 + d_2 + d_4$	$d_1 + 2d_2$
$e_1 + 2e_2 + 2e_3 + e_4$	$d_1 + 2d_2$	$d_1 + d_2 + 2d_4$
$e_1 + 2e_2 + 2e_3 + 2e_4$	$d_1 + d_3 + d_4$	$d_1 + 2d_2 + d_3 + 2d_4$

B STRUKTURIERTE INTERVALLZERLEGUNGEN VON $\mathcal{L}(5, GF(3))$

$p_i \in H_0$	$\sigma_i \in S_{24}$	$\sigma_i \in S_{25}$
e_1	d_1	d_1
e_2	$d_1 + d_2$	$d_1 + d_2$
e_3	$d_2 + 2d_3$	$d_1 + d_3$
e_4	$d_1 + d_2 + 2d_3 + 2d_4$	$d_2 + 2d_3 + d_4$
$e_1 + e_2$	$d_2 + d_3 + 2d_4$	$d_2 + 2d_4$
$e_1 + 2e_2$	$d_1 + 2d_2 + d_3$	$d_1 + 2d_2 + d_3 + 2d_4$
$e_1 + e_3$	$d_1 + d_3$	$d_3 + d_4$
$e_1 + 2e_3$	$d_1 + d_2 + 2d_3 + d_4$	$d_1 + d_2 + 2d_3 + d_4$
$e_1 + e_4$	$d_1 + d_2 + d_3 + d_4$	$d_1 + d_2 + d_4$
$e_1 + 2e_4$	$d_2 + 2d_3 + d_4$	$d_1 + d_3 + 2d_4$
$e_2 + e_3$	$d_1 + d_2 + d_3$	$d_2 + d_3$
$e_2 + 2e_3$	$d_1 + 2d_3 + 2d_4$	$d_2 + 2d_3 + 2d_4$
$e_2 + e_4$	$d_1 + 2d_2 + d_3 + 2d_4$	$d_1 + d_3 + d_4$
$e_2 + 2e_4$	$d_3 + 2d_4$	$d_1 + d_2 + d_3 + 2d_4$
$e_3 + e_4$	$d_1 + d_4$	$d_1 + d_2 + d_3 + d_4$
$e_3 + 2e_4$	$d_1 + d_2 + d_3 + 2d_4$	$d_1 + d_2 + 2d_4$
$e_1 + e_2 + e_3$	$d_1 + 2d_2 + 2d_3 + 2d_4$	$d_1 + 2d_2 + 2d_3$
$e_1 + e_2 + 2e_3$	d_2	$d_1 + 2d_3$
$e_1 + 2e_2 + e_3$	$d_1 + 2d_2 + d_4$	$d_1 + 2d_2$
$e_1 + 2e_2 + 2e_3$	d_3	$d_1 + d_2 + d_3$
$e_1 + e_2 + e_4$	$d_2 + d_3$	d_2
$e_1 + e_2 + 2e_4$	$d_1 + 2d_2 + 2d_3 + d_4$	$d_1 + 2d_2 + d_3 + d_4$
$e_1 + 2e_2 + e_4$	$d_1 + d_3 + d_4$	$d_3 + 2d_4$
$e_1 + 2e_2 + 2e_4$	$d_1 + d_3 + 2d_4$	$d_1 + 2d_2 + d_3$
$e_1 + e_3 + e_4$	$d_3 + d_4$	$d_1 + d_2 + 2d_3 + 2d_4$
$e_1 + e_3 + 2e_4$	$d_1 + d_2 + 2d_4$	d_3
$e_1 + 2e_3 + e_4$	d_4	$d_1 + d_2 + 2d_3$
$e_1 + 2e_3 + 2e_4$	$d_1 + d_2 + 2d_3$	$d_2 + d_4$
$e_2 + e_3 + e_4$	$d_2 + d_4$	$d_1 + 2d_2 + 2d_4$
$e_2 + e_3 + 2e_4$	$d_2 + 2d_4$	$d_1 + 2d_3 + d_4$
$e_2 + 2e_3 + e_4$	$d_1 + 2d_3$	$d_2 + 2d_3$
$e_2 + 2e_3 + 2e_4$	$d_2 + d_3 + d_4$	d_4
$e_1 + e_2 + e_3 + e_4$	$d_1 + 2d_2 + 2d_4$	$d_2 + d_3 + 2d_4$
$e_1 + e_2 + e_3 + 2e_4$	$d_1 + 2d_2 + 2d_3$	$d_2 + d_3 + d_4$
$e_1 + e_2 + 2e_3 + e_4$	$d_2 + 2d_3 + 2d_4$	$d_1 + 2d_2 + 2d_3 + d_4$
$e_1 + e_2 + 2e_3 + 2e_4$	$d_1 + 2d_4$	$d_1 + 2d_2 + d_4$
$e_1 + 2e_2 + e_3 + e_4$	$d_1 + 2d_2$	$d_1 + 2d_3 + 2d_4$
$e_1 + 2e_2 + e_3 + 2e_4$	$d_1 + 2d_3 + d_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$
$e_1 + 2e_2 + 2e_3 + e_4$	$d_1 + 2d_2 + d_3 + d_4$	$d_1 + d_4$
$e_1 + 2e_2 + 2e_3 + 2e_4$	$d_1 + d_2 + d_4$	$d_1 + 2d_4$

$p_i \in H_0$	$\sigma_i \in S_{26}$	$\sigma_i \in S_{27}$
e_1	d_1	d_1
e_2	$d_1 + d_2$	$d_1 + d_2$
e_3	$d_1 + d_3$	$d_1 + d_2 + d_3$
e_4	$d_2 + 2d_3 + 2d_4$	$d_1 + d_3 + d_4$
$e_1 + e_2$	$d_2 + d_4$	$d_2 + d_3$
$e_1 + 2e_2$	$d_1 + 2d_2 + d_3 + d_4$	$d_1 + 2d_2 + 2d_3 + d_4$
$e_1 + e_3$	$d_3 + 2d_4$	$d_3 + d_4$
$e_1 + 2e_3$	$d_1 + d_2 + 2d_3 + 2d_4$	$d_1 + d_2 + 2d_3 + 2d_4$
$e_1 + e_4$	$d_1 + d_3 + d_4$	d_4
$e_1 + 2e_4$	$d_1 + d_2 + 2d_4$	$d_1 + d_2 + d_3 + 2d_4$
$e_2 + e_3$	$d_2 + d_3$	$d_1 + d_3 + 2d_4$
$e_2 + 2e_3$	$d_2 + 2d_3 + d_4$	$d_2 + 2d_3 + 2d_4$
$e_2 + e_4$	$d_1 + d_2 + d_3 + d_4$	$d_2 + d_3 + d_4$
$e_2 + 2e_4$	$d_1 + d_3 + 2d_4$	$d_2 + 2d_4$
$e_3 + e_4$	$d_1 + d_2 + d_4$	$d_1 + d_2 + d_4$
$e_3 + 2e_4$	$d_1 + d_2 + d_3 + 2d_4$	$d_2 + d_3 + 2d_4$
$e_1 + e_2 + e_3$	$d_1 + 2d_2 + 2d_3$	$d_2 + d_4$
$e_1 + e_2 + 2e_3$	$d_1 + 2d_3$	$d_1 + 2d_2 + d_3 + 2d_4$
$e_1 + 2e_2 + e_3$	$d_1 + 2d_2$	$d_1 + 2d_2 + 2d_4$
$e_1 + 2e_2 + 2e_3$	$d_1 + d_2 + d_3$	$d_1 + 2d_3$
$e_1 + e_2 + e_4$	$d_1 + 2d_2 + d_3 + 2d_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$
$e_1 + e_2 + 2e_4$	d_2	$d_1 + 2d_3 + 2d_4$
$e_1 + 2e_2 + e_4$	$d_1 + 2d_2 + d_3$	$d_1 + 2d_2$
$e_1 + 2e_2 + 2e_4$	$d_3 + d_4$	$d_1 + d_2 + d_3 + d_4$
$e_1 + e_3 + e_4$	d_3	$d_2 + 2d_3$
$e_1 + e_3 + 2e_4$	$d_1 + d_2 + 2d_3 + d_4$	$d_1 + 2d_3 + d_4$
$e_1 + 2e_3 + e_4$	$d_2 + 2d_4$	$d_1 + d_2 + 2d_3$
$e_1 + 2e_3 + 2e_4$	$d_1 + d_2 + 2d_3$	$d_1 + d_2 + 2d_4$
$e_2 + e_3 + e_4$	$d_1 + 2d_3 + 2d_4$	d_3
$e_2 + e_3 + 2e_4$	$d_1 + 2d_2 + d_4$	$d_1 + d_2 + 2d_3 + d_4$
$e_2 + 2e_3 + e_4$	d_4	$d_1 + d_4$
$e_2 + 2e_3 + 2e_4$	$d_2 + 2d_3$	$d_1 + 2d_2 + d_3$
$e_1 + e_2 + e_3 + e_4$	$d_2 + d_3 + 2d_4$	$d_1 + 2d_2 + 2d_3$
$e_1 + e_2 + e_3 + 2e_4$	$d_2 + d_3 + d_4$	$d_1 + 2d_2 + d_4$
$e_1 + e_2 + 2e_3 + e_4$	$d_1 + 2d_2 + 2d_4$	d_2
$e_1 + e_2 + 2e_3 + 2e_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$	$d_2 + 2d_3 + d_4$
$e_1 + 2e_2 + e_3 + e_4$	$d_1 + 2d_2 + 2d_3 + d_4$	$d_1 + d_3$
$e_1 + 2e_2 + e_3 + 2e_4$	$d_1 + 2d_3 + d_4$	$d_1 + 2d_2 + d_3 + d_4$
$e_1 + 2e_2 + 2e_3 + e_4$	$d_1 + d_4$	$d_3 + 2d_4$
$e_1 + 2e_2 + 2e_3 + 2e_4$	$d_1 + 2d_4$	$d_1 + 2d_4$

B STRUKTURIERTE INTERVALLZERLEGUNGEN VON $\mathcal{L}(5, GF(3))$

$p_i \in H_0$	$\sigma_i \in S_{28}$	$\sigma_i \in S_{29}$
e_1	d_1	d_1
e_2	$d_1 + d_2$	$d_1 + d_2$
e_3	$d_1 + d_2 + d_3$	$d_1 + d_2 + d_3$
e_4	$d_1 + d_3 + 2d_4$	$d_1 + d_2 + d_3 + d_4$
$e_1 + e_2$	$d_2 + d_3$	$d_2 + d_3 + d_4$
$e_1 + 2e_2$	$d_1 + 2d_2 + 2d_3 + 2d_4$	$d_1 + 2d_2 + 2d_4$
$e_1 + e_3$	$d_3 + 2d_4$	$d_2 + 2d_3 + 2d_4$
$e_1 + 2e_3$	$d_1 + d_2 + 2d_3 + d_4$	$d_1 + d_2 + 2d_3$
$e_1 + e_4$	$d_1 + d_2 + d_3 + d_4$	$d_3 + 2d_4$
$e_1 + 2e_4$	d_4	$d_1 + d_2 + d_3 + 2d_4$
$e_2 + e_3$	$d_1 + d_3 + d_4$	$d_3 + d_4$
$e_2 + 2e_3$	$d_2 + 2d_3 + d_4$	$d_1 + 2d_2 + d_3 + d_4$
$e_2 + e_4$	$d_2 + d_4$	$d_1 + d_4$
$e_2 + 2e_4$	$d_2 + d_3 + 2d_4$	$d_2 + d_3 + 2d_4$
$e_3 + e_4$	$d_2 + d_3 + d_4$	$d_2 + d_4$
$e_3 + 2e_4$	$d_1 + d_2 + 2d_4$	$d_1 + 2d_3 + d_4$
$e_1 + e_2 + e_3$	$d_2 + 2d_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$
$e_1 + e_2 + 2e_3$	$d_1 + 2d_2 + d_3 + d_4$	$d_2 + 2d_4$
$e_1 + 2e_2 + e_3$	$d_1 + 2d_2 + d_4$	$d_1 + d_3 + d_4$
$e_1 + 2e_2 + 2e_3$	$d_1 + 2d_3$	$d_1 + 2d_3$
$e_1 + e_2 + e_4$	$d_1 + 2d_3 + d_4$	$d_2 + d_3$
$e_1 + e_2 + 2e_4$	$d_1 + 2d_2 + 2d_3 + d_4$	$d_1 + 2d_2 + d_4$
$e_1 + 2e_2 + e_4$	$d_1 + d_2 + d_3 + 2d_4$	$d_1 + 2d_2 + 2d_3$
$e_1 + 2e_2 + 2e_4$	$d_1 + 2d_2$	$d_1 + 2d_3 + 2d_4$
$e_1 + e_3 + e_4$	$d_1 + 2d_3 + 2d_4$	$d_1 + d_2 + 2d_3 + 2d_4$
$e_1 + e_3 + 2e_4$	$d_2 + 2d_3$	d_3
$e_1 + 2e_3 + e_4$	$d_1 + d_2 + d_4$	$d_1 + d_2 + d_4$
$e_1 + 2e_3 + 2e_4$	$d_1 + d_2 + 2d_3$	$d_1 + 2d_4$
$e_2 + e_3 + e_4$	$d_1 + d_2 + 2d_3 + 2d_4$	$d_1 + d_3$
$e_2 + e_3 + 2e_4$	d_3	$d_2 + 2d_3 + d_4$
$e_2 + 2e_3 + e_4$	$d_1 + 2d_2 + d_3$	$d_2 + 2d_3$
$e_2 + 2e_3 + 2e_4$	$d_1 + 2d_4$	$d_1 + d_2 + 2d_4$
$e_1 + e_2 + e_3 + e_4$	$d_1 + 2d_2 + 2d_4$	d_2
$e_1 + e_2 + e_3 + 2e_4$	$d_1 + 2d_2 + 2d_3$	$d_1 + 2d_2 + d_3 + 2d_4$
$e_1 + e_2 + 2e_3 + e_4$	$d_2 + 2d_3 + 2d_4$	$d_1 + d_3 + 2d_4$
$e_1 + e_2 + 2e_3 + 2e_4$	d_2	$d_1 + 2d_2 + d_3$
$e_1 + 2e_2 + e_3 + e_4$	$d_1 + 2d_2 + d_3 + 2d_4$	d_4
$e_1 + 2e_2 + e_3 + 2e_4$	$d_1 + d_3$	$d_1 + 2d_2$
$e_1 + 2e_2 + 2e_3 + e_4$	$d_1 + d_4$	$d_1 + d_2 + 2d_3 + d_4$
$e_1 + 2e_2 + 2e_3 + 2e_4$	$d_3 + d_4$	$d_1 + 2d_2 + 2d_3 + d_4$

$p_i \in H_0$	$\sigma_i \in S_{30}$	$\sigma_i \in S_{31}$
e_1	d_1	d_1
e_2	$d_1 + d_2$	$d_1 + d_2$
e_3	$d_1 + d_2 + d_3$	$d_1 + 2d_3$
e_4	$d_1 + d_2 + d_3 + 2d_4$	$d_2 + d_3 + d_4$
$e_1 + e_2$	$d_2 + d_3 + 2d_4$	$d_2 + 2d_4$
$e_1 + 2e_2$	$d_1 + 2d_2 + d_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$
$e_1 + e_3$	$d_2 + 2d_3 + d_4$	$d_1 + d_2 + d_3 + d_4$
$e_1 + 2e_3$	$d_1 + d_2 + 2d_3$	$d_3 + 2d_4$
$e_1 + e_4$	$d_1 + d_2 + d_3 + d_4$	$d_1 + d_2 + d_4$
$e_1 + 2e_4$	$d_3 + d_4$	$d_1 + 2d_3 + 2d_4$
$e_2 + e_3$	$d_3 + 2d_4$	$d_2 + d_3 + 2d_4$
$e_2 + 2e_3$	$d_1 + 2d_2 + d_3 + 2d_4$	$d_2 + 2d_3$
$e_2 + e_4$	$d_2 + d_3 + d_4$	$d_1 + 2d_3 + d_4$
$e_2 + 2e_4$	$d_1 + 2d_4$	$d_1 + d_2 + 2d_3 + 2d_4$
$e_3 + e_4$	$d_1 + 2d_3 + 2d_4$	$d_1 + d_2 + 2d_4$
$e_3 + 2e_4$	$d_2 + 2d_4$	$d_1 + d_2 + 2d_3 + d_4$
$e_1 + e_2 + e_3$	$d_1 + 2d_2 + 2d_3 + d_4$	$d_1 + d_3$
$e_1 + e_2 + 2e_3$	$d_2 + d_4$	$d_1 + 2d_2 + d_3$
$e_1 + 2e_2 + e_3$	$d_1 + d_3 + 2d_4$	$d_1 + d_2 + 2d_3$
$e_1 + 2e_2 + 2e_3$	$d_1 + 2d_3$	$d_1 + 2d_2$
$e_1 + e_2 + e_4$	$d_1 + 2d_2 + 2d_4$	d_2
$e_1 + e_2 + 2e_4$	$d_2 + d_3$	$d_1 + 2d_2 + 2d_3 + d_4$
$e_1 + 2e_2 + e_4$	$d_1 + 2d_3 + d_4$	$d_3 + d_4$
$e_1 + 2e_2 + 2e_4$	$d_1 + 2d_2 + 2d_3$	$d_1 + 2d_2 + 2d_3$
$e_1 + e_3 + e_4$	d_3	$d_1 + d_2 + d_3$
$e_1 + e_3 + 2e_4$	$d_1 + d_2 + 2d_3 + d_4$	$d_2 + d_4$
$e_1 + 2e_3 + e_4$	$d_1 + d_4$	$d_1 + d_2 + d_3 + 2d_4$
$e_1 + 2e_3 + 2e_4$	$d_1 + d_2 + 2d_4$	d_3
$e_2 + e_3 + e_4$	$d_2 + 2d_3 + 2d_4$	$d_2 + d_3$
$e_2 + e_3 + 2e_4$	$d_1 + d_3$	d_4
$e_2 + 2e_3 + e_4$	$d_1 + d_2 + d_4$	$d_1 + 2d_2 + 2d_4$
$e_2 + 2e_3 + 2e_4$	$d_2 + 2d_3$	$d_1 + d_3 + d_4$
$e_1 + e_2 + e_3 + e_4$	$d_1 + 2d_2 + d_3 + d_4$	$d_1 + 2d_2 + d_3 + d_4$
$e_1 + e_2 + e_3 + 2e_4$	d_2	$d_1 + 2d_2 + d_4$
$e_1 + e_2 + 2e_3 + e_4$	$d_1 + 2d_2 + d_3$	$d_2 + 2d_3 + 2d_4$
$e_1 + e_2 + 2e_3 + 2e_4$	$d_1 + d_3 + d_4$	$d_2 + 2d_3 + d_4$
$e_1 + 2e_2 + e_3 + e_4$	$d_1 + 2d_2$	$d_1 + d_4$
$e_1 + 2e_2 + e_3 + 2e_4$	d_4	$d_1 + 2d_4$
$e_1 + 2e_2 + 2e_3 + e_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$	$d_1 + d_3 + 2d_4$
$e_1 + 2e_2 + 2e_3 + 2e_4$	$d_1 + d_2 + 2d_3 + 2d_4$	$d_1 + 2d_2 + d_3 + 2d_4$

B STRUKTURIERTE INTERVALLZERLEGUNGEN VON $\mathcal{L}(5, GF(3))$

$p_i \in H_0$	$\sigma_i \in S_{32}$	$\sigma_i \in S_{33}$
e_1	d_1	d_1
e_2	$d_1 + d_2$	$d_1 + d_2$
e_3	$d_1 + 2d_3$	$d_1 + d_2 + 2d_3$
e_4	$d_2 + d_3 + 2d_4$	$d_1 + 2d_3 + d_4$
$e_1 + e_2$	$d_2 + d_4$	$d_2 + 2d_3$
$e_1 + 2e_2$	$d_1 + 2d_2 + 2d_3 + d_4$	$d_1 + 2d_2 + d_3 + d_4$
$e_1 + e_3$	$d_1 + d_2 + d_3 + 2d_4$	$d_1 + d_2 + d_3 + 2d_4$
$e_1 + 2e_3$	$d_3 + d_4$	$d_3 + 2d_4$
$e_1 + e_4$	$d_1 + 2d_3 + d_4$	d_4
$e_1 + 2e_4$	$d_1 + d_2 + 2d_4$	$d_1 + d_2 + 2d_3 + 2d_4$
$e_2 + e_3$	$d_2 + d_3 + d_4$	$d_2 + d_3 + 2d_4$
$e_2 + 2e_3$	$d_2 + 2d_3$	$d_1 + 2d_3 + 2d_4$
$e_2 + e_4$	$d_1 + d_2 + 2d_3 + d_4$	$d_2 + 2d_3 + d_4$
$e_2 + 2e_4$	$d_1 + 2d_3 + 2d_4$	$d_2 + 2d_4$
$e_3 + e_4$	$d_1 + d_2 + 2d_3 + 2d_4$	$d_2 + 2d_3 + 2d_4$
$e_3 + 2e_4$	$d_1 + d_2 + d_4$	$d_1 + d_2 + d_4$
$e_1 + e_2 + e_3$	$d_1 + d_3$	$d_1 + 2d_2 + 2d_3 + 2d_4$
$e_1 + e_2 + 2e_3$	$d_1 + 2d_2 + d_3$	$d_2 + d_4$
$e_1 + 2e_2 + e_3$	$d_1 + d_2 + 2d_3$	$d_1 + d_3$
$e_1 + 2e_2 + 2e_3$	$d_1 + 2d_2$	$d_1 + 2d_2 + 2d_4$
$e_1 + e_2 + e_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$	$d_1 + 2d_2 + d_3 + 2d_4$
$e_1 + e_2 + 2e_4$	d_2	$d_1 + d_3 + 2d_4$
$e_1 + 2e_2 + e_4$	$d_1 + 2d_2 + 2d_3$	$d_1 + 2d_2$
$e_1 + 2e_2 + 2e_4$	$d_3 + 2d_4$	$d_1 + d_2 + 2d_3 + d_4$
$e_1 + e_3 + e_4$	$d_2 + 2d_4$	$d_1 + d_2 + d_3$
$e_1 + e_3 + 2e_4$	$d_1 + d_2 + d_3$	$d_1 + d_2 + 2d_4$
$e_1 + 2e_3 + e_4$	d_3	$d_2 + d_3$
$e_1 + 2e_3 + 2e_4$	$d_1 + d_2 + d_3 + d_4$	$d_1 + d_3 + d_4$
$e_2 + e_3 + e_4$	d_4	$d_1 + d_4$
$e_2 + e_3 + 2e_4$	$d_2 + d_3$	$d_1 + 2d_2 + 2d_3$
$e_2 + 2e_3 + e_4$	$d_1 + d_3 + 2d_4$	d_3
$e_2 + 2e_3 + 2e_4$	$d_1 + 2d_2 + d_4$	$d_1 + d_2 + d_3 + d_4$
$e_1 + e_2 + e_3 + e_4$	$d_1 + 2d_2 + 2d_4$	d_2
$e_1 + e_2 + e_3 + 2e_4$	$d_1 + 2d_2 + d_3 + 2d_4$	$d_2 + d_3 + d_4$
$e_1 + e_2 + 2e_3 + e_4$	$d_2 + 2d_3 + 2d_4$	$d_1 + 2d_2 + d_3$
$e_1 + e_2 + 2e_3 + 2e_4$	$d_2 + 2d_3 + d_4$	$d_1 + 2d_2 + d_4$
$e_1 + 2e_2 + e_3 + e_4$	$d_1 + d_4$	$d_3 + d_4$
$e_1 + 2e_2 + e_3 + 2e_4$	$d_1 + 2d_4$	$d_1 + 2d_4$
$e_1 + 2e_2 + 2e_3 + e_4$	$d_1 + 2d_2 + d_3 + d_4$	$d_1 + 2d_3$
$e_1 + 2e_2 + 2e_3 + 2e_4$	$d_1 + d_3 + d_4$	$d_1 + 2d_2 + 2d_3 + d_4$

$p_i \in H_0$	$\sigma_i \in S_{34}$	$\sigma_i \in S_{35}$
e_1	d_1	d_1
e_2	$d_1 + d_2$	$d_1 + d_2$
e_3	$d_1 + d_2 + 2d_3$	$d_1 + d_2 + 2d_3$
e_4	$d_1 + 2d_3 + 2d_4$	$d_1 + d_2 + 2d_3 + d_4$
$e_1 + e_2$	$d_2 + 2d_3$	$d_2 + 2d_3 + d_4$
$e_1 + 2e_2$	$d_1 + 2d_2 + d_3 + 2d_4$	$d_1 + 2d_2 + 2d_4$
$e_1 + e_3$	$d_1 + d_2 + d_3 + d_4$	$d_1 + d_2 + d_3$
$e_1 + 2e_3$	$d_3 + d_4$	$d_2 + d_3 + 2d_4$
$e_1 + e_4$	$d_1 + d_2 + 2d_3 + d_4$	$d_3 + d_4$
$e_1 + 2e_4$	d_4	$d_1 + d_2 + 2d_3 + 2d_4$
$e_2 + e_3$	$d_2 + d_3 + d_4$	$d_1 + 2d_2 + 2d_3 + d_4$
$e_2 + 2e_3$	$d_1 + 2d_3 + d_4$	$d_3 + 2d_4$
$e_2 + e_4$	$d_2 + d_4$	$d_1 + d_4$
$e_2 + 2e_4$	$d_2 + 2d_3 + 2d_4$	$d_2 + 2d_3 + 2d_4$
$e_3 + e_4$	$d_1 + d_2 + 2d_4$	$d_1 + d_3 + d_4$
$e_3 + 2e_4$	$d_2 + 2d_3 + d_4$	$d_2 + d_4$
$e_1 + e_2 + e_3$	$d_1 + 2d_2 + 2d_3 + d_4$	$d_2 + 2d_4$
$e_1 + e_2 + 2e_3$	$d_2 + 2d_4$	$d_1 + 2d_2 + d_3 + 2d_4$
$e_1 + 2e_2 + e_3$	$d_1 + d_3$	$d_1 + d_3$
$e_1 + 2e_2 + 2e_3$	$d_1 + 2d_2 + d_4$	$d_1 + 2d_3 + d_4$
$e_1 + e_2 + e_4$	$d_1 + d_3 + d_4$	$d_2 + 2d_3$
$e_1 + e_2 + 2e_4$	$d_1 + 2d_2 + d_3 + d_4$	$d_1 + 2d_2 + d_4$
$e_1 + 2e_2 + e_4$	$d_1 + d_2 + 2d_3 + 2d_4$	$d_1 + 2d_2 + d_3$
$e_1 + 2e_2 + 2e_4$	$d_1 + 2d_2$	$d_1 + d_3 + 2d_4$
$e_1 + e_3 + e_4$	$d_1 + d_2 + d_4$	$d_1 + d_2 + d_4$
$e_1 + e_3 + 2e_4$	$d_1 + d_2 + d_3$	$d_1 + 2d_4$
$e_1 + 2e_3 + e_4$	$d_1 + d_3 + 2d_4$	$d_1 + d_2 + d_3 + 2d_4$
$e_1 + 2e_3 + 2e_4$	$d_2 + d_3$	d_3
$e_2 + e_3 + e_4$	$d_1 + 2d_2 + 2d_3$	$d_2 + d_3$
$e_2 + e_3 + 2e_4$	$d_1 + 2d_4$	$d_1 + d_2 + 2d_4$
$e_2 + 2e_3 + e_4$	$d_1 + d_2 + d_3 + 2d_4$	$d_1 + 2d_3$
$e_2 + 2e_3 + 2e_4$	d_3	$d_2 + d_3 + d_4$
$e_1 + e_2 + e_3 + e_4$	$d_2 + d_3 + 2d_4$	$d_1 + 2d_3 + 2d_4$
$e_1 + e_2 + e_3 + 2e_4$	d_2	$d_1 + 2d_2 + 2d_3$
$e_1 + e_2 + 2e_3 + e_4$	$d_1 + 2d_2 + 2d_4$	d_2
$e_1 + e_2 + 2e_3 + 2e_4$	$d_1 + 2d_2 + d_3$	$d_1 + 2d_2 + 2d_3 + 2d_4$
$e_1 + 2e_2 + e_3 + e_4$	$d_1 + d_4$	$d_1 + d_2 + d_3 + d_4$
$e_1 + 2e_2 + e_3 + 2e_4$	$d_3 + 2d_4$	$d_1 + 2d_2 + d_3 + d_4$
$e_1 + 2e_2 + 2e_3 + e_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$	d_4
$e_1 + 2e_2 + 2e_3 + 2e_4$	$d_1 + 2d_3$	$d_1 + 2d_2$

B STRUKTURIERTE INTERVALLZERLEGUNGEN VON $\mathcal{L}(5, GF(3))$

$p_i \in H_0$	$\sigma_i \in S_{36}$	$\sigma_i \in S_{37}$
e_1	d_1	d_1
e_2	$d_1 + d_2$	$d_1 + 2d_2$
e_3	$d_1 + d_2 + 2d_3$	$d_2 + d_3$
e_4	$d_1 + d_2 + 2d_3 + 2d_4$	$d_1 + 2d_2 + 2d_3 + d_4$
$e_1 + e_2$	$d_2 + 2d_3 + 2d_4$	$d_1 + d_2 + d_3$
$e_1 + 2e_2$	$d_1 + 2d_2 + d_4$	$d_2 + 2d_3 + 2d_4$
$e_1 + e_3$	$d_1 + d_2 + d_3$	$d_1 + d_3$
$e_1 + 2e_3$	$d_2 + d_3 + d_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$
$e_1 + e_4$	$d_1 + d_2 + 2d_3 + d_4$	$d_2 + d_3 + d_4$
$e_1 + 2e_4$	$d_3 + 2d_4$	$d_1 + 2d_2 + d_3 + 2d_4$
$e_2 + e_3$	$d_1 + 2d_2 + 2d_3 + 2d_4$	$d_1 + 2d_3 + d_4$
$e_2 + 2e_3$	$d_3 + d_4$	$d_1 + 2d_2 + d_3$
$e_2 + e_4$	$d_2 + 2d_3 + d_4$	$d_1 + d_2 + d_3 + d_4$
$e_2 + 2e_4$	$d_1 + 2d_4$	$d_3 + d_4$
$e_3 + e_4$	$d_2 + 2d_4$	$d_1 + 2d_2 + d_3 + d_4$
$e_3 + 2e_4$	$d_1 + d_3 + 2d_4$	$d_1 + 2d_4$
$e_1 + e_2 + e_3$	$d_2 + d_4$	$d_1 + d_2 + 2d_4$
$e_1 + e_2 + 2e_3$	$d_1 + 2d_2 + d_3 + d_4$	d_3
$e_1 + 2e_2 + e_3$	$d_1 + d_3$	$d_1 + d_2 + 2d_3 + d_4$
$e_1 + 2e_2 + 2e_3$	$d_1 + 2d_3 + 2d_4$	d_2
$e_1 + e_2 + e_4$	$d_1 + 2d_2 + 2d_4$	$d_1 + d_3 + d_4$
$e_1 + e_2 + 2e_4$	$d_2 + 2d_3$	$d_1 + d_3 + 2d_4$
$e_1 + 2e_2 + e_4$	$d_1 + d_3 + d_4$	$d_1 + d_2 + 2d_3 + 2d_4$
$e_1 + 2e_2 + 2e_4$	$d_1 + 2d_2 + d_3$	$d_2 + 2d_3$
$e_1 + e_3 + e_4$	$d_1 + d_4$	$d_1 + 2d_2 + d_4$
$e_1 + e_3 + 2e_4$	$d_1 + d_2 + 2d_4$	$d_3 + 2d_4$
$e_1 + 2e_3 + e_4$	d_3	$d_1 + 2d_2 + 2d_3$
$e_1 + 2e_3 + 2e_4$	$d_1 + d_2 + d_3 + d_4$	d_4
$e_2 + e_3 + e_4$	$d_1 + d_2 + d_4$	$d_1 + 2d_3$
$e_2 + e_3 + 2e_4$	$d_2 + d_3$	$d_2 + 2d_3 + d_4$
$e_2 + 2e_3 + e_4$	$d_2 + d_3 + 2d_4$	$d_2 + d_4$
$e_2 + 2e_3 + 2e_4$	$d_1 + 2d_3$	$d_2 + 2d_4$
$e_1 + e_2 + e_3 + e_4$	$d_1 + 2d_2 + 2d_3$	$d_1 + 2d_3 + 2d_4$
$e_1 + e_2 + e_3 + 2e_4$	$d_1 + 2d_3 + d_4$	$d_1 + d_2$
$e_1 + e_2 + 2e_3 + e_4$	$d_1 + 2d_2 + 2d_3 + d_4$	$d_1 + 2d_2 + 2d_4$
$e_1 + e_2 + 2e_3 + 2e_4$	d_2	$d_1 + d_2 + d_3 + 2d_4$
$e_1 + 2e_2 + e_3 + e_4$	$d_1 + 2d_2 + d_3 + 2d_4$	$d_1 + d_2 + 2d_3$
$e_1 + 2e_2 + e_3 + 2e_4$	$d_1 + d_2 + d_3 + 2d_4$	$d_1 + d_2 + d_4$
$e_1 + 2e_2 + 2e_3 + e_4$	$d_1 + 2d_2$	$d_1 + d_4$
$e_1 + 2e_2 + 2e_3 + 2e_4$	d_4	$d_2 + d_3 + 2d_4$

$p_i \in H_0$	$\sigma_i \in S_{38}$	$\sigma_i \in S_{39}$
e_1	d_1	d_1
e_2	$d_1 + 2d_2$	$d_1 + 2d_2$
e_3	$d_2 + d_3$	$d_2 + 2d_3$
e_4	$d_1 + 2d_2 + 2d_3 + 2d_4$	$d_1 + 2d_2 + d_3 + d_4$
$e_1 + e_2$	$d_1 + d_2 + d_3$	$d_1 + d_2 + 2d_3$
$e_1 + 2e_2$	$d_2 + 2d_3 + d_4$	$d_2 + d_3 + 2d_4$
$e_1 + e_3$	$d_1 + d_3$	$d_1 + 2d_2 + d_3 + 2d_4$
$e_1 + 2e_3$	$d_1 + 2d_2 + 2d_3 + d_4$	$d_1 + 2d_3$
$e_1 + e_4$	$d_1 + 2d_2 + d_3 + d_4$	$d_2 + 2d_3 + d_4$
$e_1 + 2e_4$	$d_2 + d_3 + 2d_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$
$e_2 + e_3$	$d_1 + 2d_3 + 2d_4$	$d_1 + d_2 + 2d_3$
$e_2 + 2e_3$	$d_1 + 2d_2 + d_3$	$d_1 + d_3 + d_4$
$e_2 + e_4$	$d_3 + 2d_4$	$d_1 + d_2 + 2d_3 + d_4$
$e_2 + 2e_4$	$d_1 + d_2 + d_3 + 2d_4$	$d_3 + 2d_4$
$e_3 + e_4$	$d_1 + d_4$	$d_1 + 2d_4$
$e_3 + 2e_4$	$d_1 + 2d_2 + d_3 + 2d_4$	$d_1 + 2d_2 + 2d_3 + d_4$
$e_1 + e_2 + e_3$	$d_1 + d_2 + d_4$	d_3
$e_1 + e_2 + 2e_3$	d_3	$d_1 + d_2 + 2d_4$
$e_1 + 2e_2 + e_3$	$d_1 + d_2 + 2d_3 + 2d_4$	d_2
$e_1 + 2e_2 + 2e_3$	d_2	$d_1 + d_2 + d_3 + d_4$
$e_1 + e_2 + e_4$	$d_1 + d_3 + d_4$	$d_1 + 2d_3 + d_4$
$e_1 + e_2 + 2e_4$	$d_1 + d_3 + 2d_4$	$d_1 + 2d_3 + 2d_4$
$e_1 + 2e_2 + e_4$	$d_2 + 2d_3$	$d_1 + d_2 + d_3 + 2d_4$
$e_1 + 2e_2 + 2e_4$	$d_1 + d_2 + 2d_3 + d_4$	$d_2 + d_3$
$e_1 + e_3 + e_4$	$d_3 + d_4$	$d_1 + 2d_2 + d_3$
$e_1 + e_3 + 2e_4$	$d_1 + 2d_2 + 2d_4$	d_4
$e_1 + 2e_3 + e_4$	d_4	$d_1 + 2d_2 + d_4$
$e_1 + 2e_3 + 2e_4$	$d_1 + 2d_2 + 2d_3$	$d_3 + d_4$
$e_2 + e_3 + e_4$	$d_2 + 2d_3 + 2d_4$	$d_2 + d_4$
$e_2 + e_3 + 2e_4$	$d_1 + 2d_3$	$d_2 + 2d_4$
$e_2 + 2e_3 + e_4$	$d_2 + d_4$	$d_1 + d_3$
$e_2 + 2e_3 + 2e_4$	$d_2 + 2d_4$	$d_2 + d_3 + d_4$
$e_1 + e_2 + e_3 + e_4$	$d_1 + d_2$	$d_1 + 2d_2 + 2d_4$
$e_1 + e_2 + e_3 + 2e_4$	$d_1 + 2d_3 + d_4$	$d_1 + d_2 + 2d_3 + 2d_4$
$e_1 + e_2 + 2e_3 + e_4$	$d_1 + d_2 + d_3 + d_4$	$d_1 + d_3 + 2d_4$
$e_1 + e_2 + 2e_3 + 2e_4$	$d_1 + 2d_2 + d_4$	$d_1 + d_2$
$e_1 + 2e_2 + e_3 + e_4$	$d_1 + d_2 + 2d_4$	$d_1 + d_4$
$e_1 + 2e_2 + e_3 + 2e_4$	$d_1 + d_2 + 2d_3$	$d_2 + 2d_3 + 2d_4$
$e_1 + 2e_2 + 2e_3 + e_4$	$d_2 + d_3 + d_4$	$d_1 + d_2 + d_3$
$e_1 + 2e_2 + 2e_3 + 2e_4$	$d_1 + 2d_4$	$d_1 + d_2 + d_4$

B STRUKTURIERTE INTERVALLZERLEGUNGEN VON $\mathcal{L}(5, GF(3))$

$p_i \in H_0$	$\sigma_i \in S_{40}$	$\sigma_i \in S_{41}$
e_1	d_1	d_1
e_2	$d_1 + 2d_2$	$d_1 + 2d_2$
e_3	$d_2 + 2d_3$	$d_1 + d_3$
e_4	$d_1 + 2d_2 + d_3 + 2d_4$	$d_2 + d_3 + d_4$
$e_1 + e_2$	$d_1 + d_2 + 2d_3$	$d_1 + d_2 + d_3 + d_4$
$e_1 + 2e_2$	$d_2 + d_3 + d_4$	$d_2 + 2d_4$
$e_1 + e_3$	$d_1 + 2d_2 + d_3 + d_4$	$d_3 + 2d_4$
$e_1 + 2e_3$	$d_1 + 2d_3$	$d_1 + 2d_2 + 2d_3 + 2d_4$
$e_1 + e_4$	$d_1 + 2d_2 + 2d_3 + d_4$	$d_1 + d_3 + d_4$
$e_1 + 2e_4$	$d_2 + 2d_3 + 2d_4$	$d_1 + 2d_2 + 2d_4$
$e_2 + e_3$	$d_1 + 2d_2 + 2d_3$	$d_2 + d_3 + 2d_4$
$e_2 + 2e_3$	$d_1 + d_3 + 2d_4$	$d_2 + 2d_3$
$e_2 + e_4$	$d_3 + d_4$	$d_1 + d_3 + 2d_4$
$e_2 + 2e_4$	$d_1 + d_2 + 2d_3 + 2d_4$	$d_1 + 2d_2 + d_3 + d_4$
$e_3 + e_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$	$d_1 + 2d_2 + d_4$
$e_3 + 2e_4$	$d_1 + d_4$	$d_1 + 2d_2 + d_3 + 2d_4$
$e_1 + e_2 + e_3$	d_3	$d_1 + d_2$
$e_1 + e_2 + 2e_3$	$d_1 + d_2 + d_4$	$d_1 + 2d_2 + d_3$
$e_1 + 2e_2 + e_3$	d_2	$d_1 + d_2 + 2d_3$
$e_1 + 2e_2 + 2e_3$	$d_1 + d_2 + d_3 + 2d_4$	$d_1 + 2d_3$
$e_1 + e_2 + e_4$	$d_1 + 2d_3 + d_4$	$d_1 + d_2 + d_3$
$e_1 + e_2 + 2e_4$	$d_1 + 2d_3 + 2d_4$	$d_3 + d_4$
$e_1 + 2e_2 + e_4$	$d_2 + d_3$	$d_1 + d_2 + d_3 + 2d_4$
$e_1 + 2e_2 + 2e_4$	$d_1 + d_2 + d_3 + d_4$	d_2
$e_1 + e_3 + e_4$	d_4	d_3
$e_1 + e_3 + 2e_4$	$d_1 + 2d_2 + d_3$	$d_1 + 2d_2 + 2d_3 + d_4$
$e_1 + 2e_3 + e_4$	$d_3 + 2d_4$	$d_2 + d_4$
$e_1 + 2e_3 + 2e_4$	$d_1 + 2d_2 + 2d_4$	$d_1 + 2d_2 + 2d_3$
$e_2 + e_3 + e_4$	$d_2 + d_4$	$d_2 + d_3$
$e_2 + e_3 + 2e_4$	$d_2 + 2d_4$	d_4
$e_2 + 2e_3 + e_4$	$d_2 + d_3 + 2d_4$	$d_1 + d_2 + d_4$
$e_2 + 2e_3 + 2e_4$	$d_1 + d_3$	$d_1 + 2d_3 + 2d_4$
$e_1 + e_2 + e_3 + e_4$	$d_1 + d_2 + 2d_3 + d_4$	$d_1 + d_2 + 2d_3 + d_4$
$e_1 + e_2 + e_3 + 2e_4$	$d_1 + 2d_2 + d_4$	$d_1 + 2d_3 + d_4$
$e_1 + e_2 + 2e_3 + e_4$	$d_1 + d_2$	$d_1 + d_4$
$e_1 + e_2 + 2e_3 + 2e_4$	$d_1 + d_3 + d_4$	$d_1 + 2d_4$
$e_1 + 2e_2 + e_3 + e_4$	$d_2 + 2d_3 + d_4$	$d_2 + 2d_3 + d_4$
$e_1 + 2e_2 + e_3 + 2e_4$	$d_1 + 2d_4$	$d_2 + 2d_3 + 2d_4$
$e_1 + 2e_2 + 2e_3 + e_4$	$d_1 + d_2 + 2d_4$	$d_1 + d_2 + 2d_4$
$e_1 + 2e_2 + 2e_3 + 2e_4$	$d_1 + d_2 + d_3$	$d_1 + d_2 + 2d_3 + 2d_4$

$p_i \in H_0$	$\sigma_i \in S_{42}$	$\sigma_i \in S_{43}$
e_1	d_1	d_1
e_2	$d_1 + 2d_2$	$d_1 + 2d_2$
e_3	$d_1 + d_3$	$d_1 + 2d_2 + d_3$
e_4	$d_2 + d_3 + 2d_4$	$d_1 + d_3 + d_4$
$e_1 + e_2$	$d_1 + d_2 + d_3 + 2d_4$	$d_1 + d_2 + 2d_3 + d_4$
$e_1 + 2e_2$	$d_2 + d_4$	$d_2 + 2d_3$
$e_1 + e_3$	$d_3 + d_4$	$d_3 + d_4$
$e_1 + 2e_3$	$d_1 + 2d_2 + 2d_3 + d_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$
$e_1 + e_4$	$d_1 + 2d_2 + d_4$	d_4
$e_1 + 2e_4$	$d_1 + d_3 + 2d_4$	$d_1 + 2d_2 + d_3 + 2d_4$
$e_2 + e_3$	$d_2 + d_3 + d_4$	$d_2 + d_3 + d_4$
$e_2 + 2e_3$	$d_2 + 2d_3$	$d_1 + d_3 + 2d_4$
$e_2 + e_4$	$d_1 + 2d_2 + d_3 + 2d_4$	$d_2 + d_4$
$e_2 + 2e_4$	$d_1 + d_3 + d_4$	$d_2 + 2d_3 + 2d_4$
$e_3 + e_4$	$d_1 + 2d_2 + d_3 + d_4$	$d_1 + 2d_2 + d_4$
$e_3 + 2e_4$	$d_1 + 2d_2 + 2d_4$	$d_2 + 2d_3 + d_4$
$e_1 + e_2 + e_3$	$d_1 + d_2$	$d_1 + d_2 + 2d_4$
$e_1 + e_2 + 2e_3$	$d_1 + 2d_2 + d_3$	$d_1 + 2d_3$
$e_1 + 2e_2 + e_3$	$d_1 + d_2 + 2d_3$	$d_2 + 2d_4$
$e_1 + 2e_2 + 2e_3$	$d_1 + 2d_3$	$d_1 + d_2 + d_3 + 2d_4$
$e_1 + e_2 + e_4$	$d_3 + 2d_4$	$d_1 + d_2$
$e_1 + e_2 + 2e_4$	$d_1 + d_2 + d_3$	$d_1 + 2d_2 + d_3 + d_4$
$e_1 + 2e_2 + e_4$	d_2	$d_1 + d_2 + 2d_3 + 2d_4$
$e_1 + 2e_2 + 2e_4$	$d_1 + d_2 + d_3 + d_4$	$d_1 + 2d_3 + 2d_4$
$e_1 + e_3 + e_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$	$d_2 + d_3$
$e_1 + e_3 + 2e_4$	d_3	$d_1 + 2d_3 + d_4$
$e_1 + 2e_3 + e_4$	$d_1 + 2d_2 + 2d_3$	$d_1 + 2d_2 + 2d_3$
$e_1 + 2e_3 + 2e_4$	$d_2 + 2d_4$	$d_1 + 2d_2 + 2d_4$
$e_2 + e_3 + e_4$	d_4	$d_1 + d_2 + d_3$
$e_2 + e_3 + 2e_4$	$d_2 + d_3$	$d_1 + d_4$
$e_2 + 2e_3 + e_4$	$d_1 + 2d_3 + d_4$	$d_1 + 2d_2 + 2d_3 + d_4$
$e_2 + 2e_3 + 2e_4$	$d_1 + d_2 + 2d_4$	d_3
$e_1 + e_2 + e_3 + e_4$	$d_1 + 2d_3 + 2d_4$	$d_1 + d_3$
$e_1 + e_2 + e_3 + 2e_4$	$d_1 + d_2 + 2d_3 + 2d_4$	$d_1 + d_2 + d_3 + d_4$
$e_1 + e_2 + 2e_3 + e_4$	$d_1 + d_4$	$d_3 + 2d_4$
$e_1 + e_2 + 2e_3 + 2e_4$	$d_1 + 2d_4$	$d_1 + 2d_4$
$e_1 + 2e_2 + e_3 + e_4$	$d_2 + 2d_3 + d_4$	$d_1 + d_2 + 2d_3$
$e_1 + 2e_2 + e_3 + 2e_4$	$d_2 + 2d_3 + 2d_4$	$d_1 + d_2 + d_4$
$e_1 + 2e_2 + 2e_3 + e_4$	$d_1 + d_2 + 2d_3 + d_4$	d_2
$e_1 + 2e_2 + 2e_3 + 2e_4$	$d_1 + d_2 + d_4$	$d_2 + d_3 + 2d_4$

B STRUKTURIERTE INTERVALLZERLEGUNGEN VON $\mathcal{L}(5, GF(3))$

$p_i \in H_0$	$\sigma_i \in S_{44}$	$\sigma_i \in S_{45}$
e_1	d_1	d_1
e_2	$d_1 + 2d_2$	$d_1 + 2d_2$
e_3	$d_1 + 2d_2 + d_3$	$d_1 + 2d_2 + d_3$
e_4	$d_1 + d_3 + 2d_4$	$d_1 + 2d_2 + d_3 + d_4$
$e_1 + e_2$	$d_1 + d_2 + 2d_3 + 2d_4$	$d_1 + d_2 + 2d_4$
$e_1 + 2e_2$	$d_2 + 2d_3$	$d_2 + 2d_3 + 2d_4$
$e_1 + e_3$	$d_3 + 2d_4$	$d_2 + d_3 + d_4$
$e_1 + 2e_3$	$d_1 + 2d_2 + 2d_3 + d_4$	$d_1 + 2d_2 + 2d_3$
$e_1 + e_4$	$d_1 + 2d_2 + d_3 + d_4$	$d_3 + 2d_4$
$e_1 + 2e_4$	d_4	$d_1 + 2d_2 + d_3 + 2d_4$
$e_2 + e_3$	$d_2 + d_3 + 2d_4$	$d_1 + d_2 + d_3 + d_4$
$e_2 + 2e_3$	$d_1 + d_3 + d_4$	$d_3 + d_4$
$e_2 + e_4$	$d_2 + 2d_3 + d_4$	$d_2 + 2d_3 + d_4$
$e_2 + 2e_4$	$d_2 + 2d_4$	$d_1 + d_4$
$e_3 + e_4$	$d_2 + 2d_3 + 2d_4$	$d_2 + 2d_4$
$e_3 + 2e_4$	$d_1 + 2d_2 + 2d_4$	$d_1 + 2d_3 + d_4$
$e_1 + e_2 + e_3$	$d_1 + d_2 + d_4$	$d_1 + d_3 + d_4$
$e_1 + e_2 + 2e_3$	$d_1 + 2d_3$	$d_1 + 2d_3$
$e_1 + 2e_2 + e_3$	$d_2 + d_4$	$d_1 + d_2 + 2d_3 + 2d_4$
$e_1 + 2e_2 + 2e_3$	$d_1 + d_2 + d_3 + d_4$	$d_2 + d_4$
$e_1 + e_2 + e_4$	$d_1 + 2d_2 + d_3 + 2d_4$	$d_1 + d_2 + 2d_3$
$e_1 + e_2 + 2e_4$	$d_1 + d_2$	$d_1 + 2d_3 + 2d_4$
$e_1 + 2e_2 + e_4$	$d_1 + 2d_3 + d_4$	$d_2 + 2d_3$
$e_1 + 2e_2 + 2e_4$	$d_1 + d_2 + 2d_3 + d_4$	$d_1 + d_2 + d_4$
$e_1 + e_3 + e_4$	$d_1 + 2d_3 + 2d_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$
$e_1 + e_3 + 2e_4$	$d_2 + d_3$	d_3
$e_1 + 2e_3 + e_4$	$d_1 + 2d_2 + d_4$	$d_1 + 2d_2 + d_4$
$e_1 + 2e_3 + 2e_4$	$d_1 + 2d_2 + 2d_3$	$d_1 + 2d_4$
$e_2 + e_3 + e_4$	$d_1 + 2d_4$	$d_1 + 2d_2 + 2d_4$
$e_2 + e_3 + 2e_4$	$d_1 + d_2 + d_3$	$d_2 + d_3$
$e_2 + 2e_3 + e_4$	d_3	$d_2 + d_3 + 2d_4$
$e_2 + 2e_3 + 2e_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$	$d_1 + d_3$
$e_1 + e_2 + e_3 + e_4$	$d_1 + d_2 + d_3 + 2d_4$	d_4
$e_1 + e_2 + e_3 + 2e_4$	$d_1 + d_3$	$d_1 + d_2$
$e_1 + e_2 + 2e_3 + e_4$	$d_1 + d_4$	$d_1 + 2d_2 + 2d_3 + d_4$
$e_1 + e_2 + 2e_3 + 2e_4$	$d_3 + d_4$	$d_1 + d_2 + 2d_3 + d_4$
$e_1 + 2e_2 + e_3 + e_4$	$d_1 + d_2 + 2d_4$	d_2
$e_1 + 2e_2 + e_3 + 2e_4$	$d_1 + d_2 + 2d_3$	$d_1 + d_2 + d_3 + 2d_4$
$e_1 + 2e_2 + 2e_3 + e_4$	$d_2 + d_3 + d_4$	$d_1 + d_3 + 2d_4$
$e_1 + 2e_2 + 2e_3 + 2e_4$	d_2	$d_1 + d_2 + d_3$

$p_i \in H_0$	$\sigma_i \in S_{46}$	$\sigma_i \in S_{47}$
e_1	d_1	d_1
e_2	$d_1 + 2d_2$	$d_1 + 2d_2$
e_3	$d_1 + 2d_2 + d_3$	$d_1 + 2d_3$
e_4	$d_1 + 2d_2 + d_3 + 2d_4$	$d_2 + 2d_3 + d_4$
$e_1 + e_2$	$d_1 + d_2 + d_4$	$d_1 + d_2 + 2d_3 + d_4$
$e_1 + 2e_2$	$d_2 + 2d_3 + d_4$	$d_2 + 2d_4$
$e_1 + e_3$	$d_2 + d_3 + 2d_4$	$d_1 + 2d_2 + d_3 + 2d_4$
$e_1 + 2e_3$	$d_1 + 2d_2 + 2d_3$	$d_3 + d_4$
$e_1 + e_4$	$d_1 + 2d_2 + d_3 + d_4$	$d_1 + 2d_3 + d_4$
$e_1 + 2e_4$	$d_3 + d_4$	$d_1 + 2d_2 + 2d_4$
$e_2 + e_3$	$d_1 + d_2 + d_3 + 2d_4$	$d_2 + d_3$
$e_2 + 2e_3$	$d_3 + 2d_4$	$d_2 + 2d_3 + 2d_4$
$e_2 + e_4$	$d_1 + 2d_4$	$d_1 + 2d_3 + 2d_4$
$e_2 + 2e_4$	$d_2 + 2d_3 + 2d_4$	$d_1 + 2d_2 + 2d_3 + d_4$
$e_3 + e_4$	$d_1 + 2d_3 + 2d_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$
$e_3 + 2e_4$	$d_2 + d_4$	$d_1 + 2d_2 + d_4$
$e_1 + e_2 + e_3$	$d_1 + d_3 + 2d_4$	$d_1 + 2d_2 + 2d_3$
$e_1 + e_2 + 2e_3$	$d_1 + 2d_3$	$d_1 + d_2$
$e_1 + 2e_2 + e_3$	$d_1 + d_2 + 2d_3 + d_4$	$d_1 + d_3$
$e_1 + 2e_2 + 2e_3$	$d_2 + 2d_4$	$d_1 + d_2 + d_3$
$e_1 + e_2 + e_4$	$d_1 + 2d_3 + d_4$	$d_1 + d_2 + 2d_3$
$e_1 + e_2 + 2e_4$	$d_1 + d_2 + 2d_3$	$d_3 + 2d_4$
$e_1 + 2e_2 + e_4$	$d_1 + d_2 + 2d_4$	$d_1 + d_2 + 2d_3 + 2d_4$
$e_1 + 2e_2 + 2e_4$	$d_2 + 2d_3$	d_2
$e_1 + e_3 + e_4$	d_3	$d_2 + d_4$
$e_1 + e_3 + 2e_4$	$d_1 + 2d_2 + 2d_3 + d_4$	$d_1 + 2d_2 + d_3$
$e_1 + 2e_3 + e_4$	$d_1 + d_4$	d_3
$e_1 + 2e_3 + 2e_4$	$d_1 + 2d_2 + 2d_4$	$d_1 + 2d_2 + d_3 + d_4$
$e_2 + e_3 + e_4$	$d_2 + d_3$	$d_1 + d_2 + d_4$
$e_2 + e_3 + 2e_4$	$d_1 + 2d_2 + d_4$	$d_1 + d_3 + 2d_4$
$e_2 + 2e_3 + e_4$	$d_1 + d_3$	$d_2 + 2d_3$
$e_2 + 2e_3 + 2e_4$	$d_2 + d_3 + d_4$	d_4
$e_1 + e_2 + e_3 + e_4$	$d_1 + d_2$	$d_1 + d_4$
$e_1 + e_2 + e_3 + 2e_4$	d_4	$d_1 + 2d_4$
$e_1 + e_2 + 2e_3 + e_4$	$d_1 + d_2 + 2d_3 + 2d_4$	$d_1 + d_2 + d_3 + d_4$
$e_1 + e_2 + 2e_3 + 2e_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$	$d_1 + d_3 + d_4$
$e_1 + 2e_2 + e_3 + e_4$	$d_1 + d_2 + d_3 + d_4$	$d_1 + d_2 + 2d_4$
$e_1 + 2e_2 + e_3 + 2e_4$	d_2	$d_1 + d_2 + d_3 + 2d_4$
$e_1 + 2e_2 + 2e_3 + e_4$	$d_1 + d_2 + d_3$	$d_2 + d_3 + d_4$
$e_1 + 2e_2 + 2e_3 + 2e_4$	$d_1 + d_3 + d_4$	$d_2 + d_3 + 2d_4$

B STRUKTURIERTE INTERVALLZERLEGUNGEN VON $\mathcal{L}(5, GF(3))$

$p_i \in H_0$	$\sigma_i \in S_{48}$	$\sigma_i \in S_{49}$
e_1	d_1	d_1
e_2	$d_1 + 2d_2$	$d_1 + 2d_2$
e_3	$d_1 + 2d_3$	$d_1 + 2d_2 + 2d_3$
e_4	$d_2 + 2d_3 + 2d_4$	$d_1 + 2d_2 + 2d_3 + d_4$
$e_1 + e_2$	$d_1 + d_2 + 2d_3 + 2d_4$	$d_1 + d_2 + 2d_4$
$e_1 + 2e_2$	$d_2 + d_4$	$d_2 + d_3 + 2d_4$
$e_1 + e_3$	$d_1 + 2d_2 + d_3 + d_4$	$d_1 + 2d_2 + d_3$
$e_1 + 2e_3$	$d_3 + 2d_4$	$d_2 + 2d_3 + d_4$
$e_1 + e_4$	$d_1 + 2d_2 + d_4$	$d_3 + d_4$
$e_1 + 2e_4$	$d_1 + 2d_3 + 2d_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$
$e_2 + e_3$	$d_2 + d_3$	$d_3 + 2d_4$
$e_2 + 2e_3$	$d_2 + 2d_3 + d_4$	$d_1 + d_2 + 2d_3 + d_4$
$e_2 + e_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$	$d_2 + d_3 + d_4$
$e_2 + 2e_4$	$d_1 + 2d_3 + d_4$	$d_1 + d_4$
$e_3 + e_4$	$d_1 + 2d_2 + 2d_4$	$d_1 + d_3 + d_4$
$e_3 + 2e_4$	$d_1 + 2d_2 + 2d_3 + d_4$	$d_2 + 2d_4$
$e_1 + e_2 + e_3$	$d_1 + 2d_2 + 2d_3$	$d_1 + d_3$
$e_1 + e_2 + 2e_3$	$d_1 + d_2$	$d_1 + 2d_3 + d_4$
$e_1 + 2e_2 + e_3$	$d_1 + d_3$	$d_2 + d_4$
$e_1 + 2e_2 + 2e_3$	$d_1 + d_2 + d_3$	$d_1 + d_2 + d_3 + 2d_4$
$e_1 + e_2 + e_4$	$d_3 + d_4$	$d_1 + d_2 + d_3$
$e_1 + e_2 + 2e_4$	$d_1 + d_2 + 2d_3$	$d_1 + d_3 + 2d_4$
$e_1 + 2e_2 + e_4$	d_2	$d_2 + d_3$
$e_1 + 2e_2 + 2e_4$	$d_1 + d_2 + 2d_3 + d_4$	$d_1 + d_2 + d_4$
$e_1 + e_3 + e_4$	$d_1 + 2d_2 + d_3$	$d_1 + 2d_2 + d_4$
$e_1 + e_3 + 2e_4$	$d_2 + 2d_4$	$d_1 + 2d_4$
$e_1 + 2e_3 + e_4$	$d_1 + 2d_2 + d_3 + 2d_4$	$d_1 + 2d_2 + d_3 + 2d_4$
$e_1 + 2e_3 + 2e_4$	d_3	d_3
$e_2 + e_3 + e_4$	$d_1 + d_3 + d_4$	$d_2 + 2d_3 + 2d_4$
$e_2 + e_3 + 2e_4$	$d_1 + d_2 + 2d_4$	$d_1 + 2d_3$
$e_2 + 2e_3 + e_4$	d_4	$d_1 + 2d_2 + 2d_4$
$e_2 + 2e_3 + 2e_4$	$d_2 + 2d_3$	$d_2 + 2d_3$
$e_1 + e_2 + e_3 + e_4$	$d_1 + d_4$	$d_1 + 2d_2 + d_3 + d_4$
$e_1 + e_2 + e_3 + 2e_4$	$d_1 + 2d_4$	$d_1 + d_2 + d_3 + d_4$
$e_1 + e_2 + 2e_3 + e_4$	$d_1 + d_3 + 2d_4$	d_4
$e_1 + e_2 + 2e_3 + 2e_4$	$d_1 + d_2 + d_3 + 2d_4$	$d_1 + d_2$
$e_1 + 2e_2 + e_3 + e_4$	$d_1 + d_2 + d_3 + d_4$	$d_1 + 2d_3 + 2d_4$
$e_1 + 2e_2 + e_3 + 2e_4$	$d_1 + d_2 + d_4$	$d_1 + d_2 + 2d_3$
$e_1 + 2e_2 + 2e_3 + e_4$	$d_2 + d_3 + d_4$	d_2
$e_1 + 2e_2 + 2e_3 + 2e_4$	$d_2 + d_3 + 2d_4$	$d_1 + d_2 + 2d_3 + 2d_4$

$p_i \in H_0$	$\sigma_i \in S_{50}$	$\sigma_i \in S_{51}$
e_1	d_1	d_1
e_2	$d_1 + 2d_2$	$d_1 + 2d_2$
e_3	$d_1 + 2d_2 + 2d_3$	$d_1 + 2d_2 + 2d_3$
e_4	$d_1 + 2d_2 + 2d_3 + 2d_4$	$d_1 + 2d_3 + d_4$
$e_1 + e_2$	$d_1 + d_2 + d_4$	$d_1 + d_2 + d_3 + d_4$
$e_1 + 2e_2$	$d_2 + d_3 + d_4$	$d_2 + d_3$
$e_1 + e_3$	$d_1 + 2d_2 + d_3$	$d_1 + 2d_2 + d_3 + 2d_4$
$e_1 + 2e_3$	$d_2 + 2d_3 + 2d_4$	$d_3 + 2d_4$
$e_1 + e_4$	$d_1 + 2d_2 + 2d_3 + d_4$	d_4
$e_1 + 2e_4$	$d_3 + 2d_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$
$e_2 + e_3$	$d_3 + d_4$	$d_1 + 2d_3 + 2d_4$
$e_2 + 2e_3$	$d_1 + d_2 + 2d_3 + 2d_4$	$d_2 + 2d_3 + d_4$
$e_2 + e_4$	$d_1 + 2d_4$	$d_2 + d_4$
$e_2 + 2e_4$	$d_2 + d_3 + 2d_4$	$d_2 + d_3 + 2d_4$
$e_3 + e_4$	$d_2 + d_4$	$d_2 + d_3 + d_4$
$e_3 + 2e_4$	$d_1 + d_3 + 2d_4$	$d_1 + 2d_2 + d_4$
$e_1 + e_2 + e_3$	$d_1 + d_3$	$d_1 + d_3$
$e_1 + e_2 + 2e_3$	$d_1 + 2d_3 + 2d_4$	$d_1 + d_2 + 2d_4$
$e_1 + 2e_2 + e_3$	$d_2 + 2d_4$	$d_1 + d_2 + 2d_3 + 2d_4$
$e_1 + 2e_2 + 2e_3$	$d_1 + d_2 + d_3 + d_4$	$d_2 + 2d_4$
$e_1 + e_2 + e_4$	$d_1 + d_3 + d_4$	$d_1 + d_2$
$e_1 + e_2 + 2e_4$	$d_1 + d_2 + d_3$	$d_1 + 2d_2 + 2d_3 + d_4$
$e_1 + 2e_2 + e_4$	$d_1 + d_2 + 2d_4$	$d_1 + d_2 + d_3 + 2d_4$
$e_1 + 2e_2 + 2e_4$	$d_2 + d_3$	$d_1 + d_3 + 2d_4$
$e_1 + e_3 + e_4$	$d_1 + d_4$	$d_1 + 2d_2 + d_3$
$e_1 + e_3 + 2e_4$	$d_1 + 2d_2 + 2d_4$	$d_1 + 2d_2 + 2d_4$
$e_1 + 2e_3 + e_4$	d_3	$d_2 + 2d_3$
$e_1 + 2e_3 + 2e_4$	$d_1 + 2d_2 + d_3 + d_4$	$d_1 + d_3 + d_4$
$e_2 + e_3 + e_4$	$d_1 + 2d_3$	$d_1 + 2d_2 + d_3 + d_4$
$e_2 + e_3 + 2e_4$	$d_2 + 2d_3 + d_4$	d_3
$e_2 + 2e_3 + e_4$	$d_2 + 2d_3$	$d_1 + d_2 + 2d_3$
$e_2 + 2e_3 + 2e_4$	$d_1 + 2d_2 + d_4$	$d_1 + d_4$
$e_1 + e_2 + e_3 + e_4$	$d_1 + d_2 + d_3 + 2d_4$	$d_3 + d_4$
$e_1 + e_2 + e_3 + 2e_4$	$d_1 + 2d_2 + d_3 + 2d_4$	$d_1 + 2d_4$
$e_1 + e_2 + 2e_3 + e_4$	$d_1 + d_2$	$d_1 + 2d_3$
$e_1 + e_2 + 2e_3 + 2e_4$	d_4	$d_1 + d_2 + 2d_3 + d_4$
$e_1 + 2e_2 + e_3 + e_4$	$d_1 + d_2 + 2d_3$	d_2
$e_1 + 2e_2 + e_3 + 2e_4$	$d_1 + 2d_3 + d_4$	$d_2 + 2d_3 + 2d_4$
$e_1 + 2e_2 + 2e_3 + e_4$	$d_1 + d_2 + 2d_3 + d_4$	$d_1 + d_2 + d_3$
$e_1 + 2e_2 + 2e_3 + 2e_4$	d_2	$d_1 + d_2 + d_4$

B STRUKTURIERTE INTERVALLZERLEGUNGEN VON $\mathcal{L}(5, GF(3))$

$p_i \in H_0$	$\sigma_i \in S_{52}$
e_1	d_1
e_2	$d_1 + 2d_2$
e_3	$d_1 + 2d_2 + 2d_3$
e_4	$d_1 + 2d_3 + 2d_4$
$e_1 + e_2$	$d_1 + d_2 + d_3 + 2d_4$
$e_1 + 2e_2$	$d_2 + d_3$
$e_1 + e_3$	$d_1 + 2d_2 + d_3 + d_4$
$e_1 + 2e_3$	$d_3 + d_4$
$e_1 + e_4$	$d_1 + 2d_2 + 2d_3 + d_4$
$e_1 + 2e_4$	d_4
$e_2 + e_3$	$d_1 + 2d_3 + d_4$
$e_2 + 2e_3$	$d_2 + 2d_3 + 2d_4$
$e_2 + e_4$	$d_2 + d_3 + d_4$
$e_2 + 2e_4$	$d_2 + 2d_4$
$e_3 + e_4$	$d_1 + 2d_2 + 2d_4$
$e_3 + 2e_4$	$d_2 + d_3 + 2d_4$
$e_1 + e_2 + e_3$	$d_1 + d_3$
$e_1 + e_2 + 2e_3$	$d_1 + d_2 + d_4$
$e_1 + 2e_2 + e_3$	$d_1 + d_2 + 2d_3 + d_4$
$e_1 + 2e_2 + 2e_3$	$d_2 + d_4$
$e_1 + e_2 + e_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$
$e_1 + e_2 + 2e_4$	$d_1 + d_2$
$e_1 + 2e_2 + e_4$	$d_1 + d_3 + d_4$
$e_1 + 2e_2 + 2e_4$	$d_1 + d_2 + d_3 + d_4$
$e_1 + e_3 + e_4$	$d_1 + 2d_2 + d_4$
$e_1 + e_3 + 2e_4$	$d_1 + 2d_2 + d_3$
$e_1 + 2e_3 + e_4$	$d_1 + d_3 + 2d_4$
$e_1 + 2e_3 + 2e_4$	$d_2 + 2d_3$
$e_2 + e_3 + e_4$	d_3
$e_2 + e_3 + 2e_4$	$d_1 + 2d_2 + d_3 + 2d_4$
$e_2 + 2e_3 + e_4$	$d_1 + 2d_4$
$e_2 + 2e_3 + 2e_4$	$d_1 + d_2 + 2d_3$
$e_1 + e_2 + e_3 + e_4$	$d_1 + d_4$
$e_1 + e_2 + e_3 + 2e_4$	$d_3 + 2d_4$
$e_1 + e_2 + 2e_3 + e_4$	$d_1 + d_2 + 2d_3 + 2d_4$
$e_1 + e_2 + 2e_3 + 2e_4$	$d_1 + 2d_3$
$e_1 + 2e_2 + e_3 + e_4$	$d_2 + 2d_3 + d_4$
$e_1 + 2e_2 + e_3 + 2e_4$	d_2
$e_1 + 2e_2 + 2e_3 + e_4$	$d_1 + d_2 + 2d_4$
$e_1 + 2e_2 + 2e_3 + 2e_4$	$d_1 + d_2 + d_3$

Quellen

- [1] AIGNER, MARTIN: *Combinatorial Theory*. Berlin Heidelberg New York, Springer Verlag, 1. Auflage, 1979.
- [2] AIGNER, MARTIN: *Diskrete Mathematik*. Wiesbaden, Vieweg Verlag, 5. Auflage, 2004.
- [3] DIESTEL, REINHARD: *Graphentheorie*. Berlin Heidelberg New York, Springer Verlag, 3. Auflage, 2006.
- [4] FAIGLE, ULRICH: *E-Mail an Winfried Hochstättler*. Persönliche Mitteilung, 2004.
- [5] GRÄTZER, GEORGE: *General Lattice Theory*. Basel Stuttgart, Birkhäuser Verlag, 1. Auflage, 1978.
- [6] HARTLIEB, SILKE und LUISE UNGER: *Mathematische Grundlagen der Kryptografie*. FernUni Hagen, 2007. Vorlesungsskript.
- [7] HERMES, HANS: *Einführung in die Verbandstheorie*. Berlin Heidelberg New York, Springer Verlag, 2. Auflage, 1978.
- [8] HOCHSTÄTTLER, WINFRIED: *On the combinatorics of the Galois numbers*. Unveröffentlicht, 2004.
- [9] JACOBSON, NATHAN: *Basic Algebra I*. New York, W. H. Freeman and Company, 2. Auflage, 1985.
- [10] KLEINBERG, JON und ÉVA TARDOS: *Algorithm Design*. Boston, Pearson/Addison-Wesley, 1. Auflage, 2006.
- [11] KÖNIG, DÉNES: *Über Graphen und ihre Anwendung auf Determinantentheorie und Mengenlehre*. Mathematische Annalen, Band 77, Seiten 453–465, 1916.
- [12] KÖNIG, DÉNES: *Theorie der endlichen und unendlichen Graphen*. Leipzig, Teubner, 1. Auflage, 1986. Nachdruck der Ausgabe Leipzig 1936.
- [13] KRUSE, EVA: *Symmetrische Kettenzerlegungen von Verbänden und Intervallzerlegung des linearen Verbandes*. Diplomarbeit, Uni Köln, 2004.
- [14] WIKIPEDIA: *Wikipedia, Die freie Enzyklopädie*. <http://de.wikipedia.org>, 2008. [Online; Stand 2. Oktober 2008].

Index

- äquivalentes Flussproblem, 46
- adjazent, 38
- Antikette, 15
- Charakteristik, 6
- Digraph, 45
- Distanz, 41
- duale Aussage, 16
- Dualität, 16
- Einselement (Verband), 15
- Filter, 15
- Fluss, 45
 - ganzahliger, 45
 - maximaler, 46
- Galoiszahlen, 31
- Gauß'sche Koeffizienten, 27
- Grad
 - einer Körpererweiterung, 8
 - eines Knoten, 38
- Gradsatz, 9
- Graph, 38
 - bipartiter, 39
 - gerichteter, 45
 - k -regulärer, 39
 - regulärer, 39
 - schlichter, 38
 - zusammenhängender, 40
- Halbordnung, 14
- Hasse-Diagramm, 22
- Ideal (Ring), 3
- Ideal (Verband), 15
- Infimum, 15
- Integritätsbereich, 7
- Intervall (Verband), 15
- Intervallzerlegung, 33, 54
 - normierte, 58
 - projizierte, 54
 - strukturierte, 58
- inzident, 38
- Körper, 7
 - Prim-, 8
 - Unter-, 8
 - Zerfallungs-, 10
- Körpererweiterung, 8
 - endliche, 8
 - unendliche, 8
- Körperhomomorphismus, 7
- Körperisomorphismus, 7
- Kante, 38, 45
- Kantenüberdeckung, 38
- Kapazitätsfunktion, 45
 - ganzahlige, 45
- Kette, 15
- Knoten, 38, 45
- Knotenüberdeckung, 38
- Komplement (Verband), 20
- Kongruenz, 3
- Kreis, 40
- Länge eines Weges, 41
- Landau-Notation, 75
- Mächtigkeit (Verband), 19
- Matching, 40
 - in k -regulären bipartiten Graphen, 44
 - maximales, 40
 - perfektes, 40
- Matching-Intervallzerlegungs-Problem, 40
- Multimenge, 37
- Nachbarschaft, 38
- Netzwerk, 45
- Nullelement (Verband), 15
- partiell geordnete Menge, 14
- Pfad, 40
- punktweise antisymmetrisch, 52
- punktweise irreflexiv, 52
- Quaternionen, 6
- Quelle, 45
- Ring, 2
 - kommutativer, 2
 - Prim-, 5

-
- Restklassen-, 4
 - Unter-, 2
 - Ringhomomorphismus, 4
 - Bild eines, 4
 - Kern eines, 4
 - Ringisomorphismus, 4

 - Satz von König, 48
 - Satz von Wedderburn, 7
 - Schiefkörper, 6
 - Schranke
 - obere, 15
 - untere, 15
 - Senke, 45
 - Stärke eines Flusses, 46
 - Supremum, 15

 - Teilverband, 16

 - unvergleichbar, 15

 - Verband, 15, 16
 - beschränkter, 19
 - Boolescher, 21
 - distributiver, 20
 - endlicher, 19
 - komplementärer, 20
 - linearer, 25
 - modularer, 21
 - nach oben beschränkter, 19
 - nach unten beschränkter, 19
 - Teiler-, 22
 - Teilmengen-, 23
 - vollständiger, 19
 - von endlicher Länge, 19
 - Verbandsisomorphismus, 21
 - vergleichbar, 15
 - verträglich, 55

 - Weg, 40
 - alternierender, 48
 - augmentierender, 48

 - Zusammenhangskomponente, 41