DISSERTATION

Rationale Normkurven in Räumen mit positiver Charakteristik

ausgeführt zum Zwecke der Erlangung des akademischen Grades
eines Doktors der technischen Wissenschaften unter der Leitung von

Ao.Univ.Prof. Mag. Dr. Hans HAVLICEK

E 113

Institut für Geometrie

eingereicht an der Technischen Universität Wien
Technisch-Naturwissenschaftliche Fakultät

von

DI. Johannes GMAINER

Matr.: 9125153

Hauptstraße 71, 2454 Sarasdorf

Wien, im Jänner 1999

Kurzfassung

Sei K ein (kommutativer) Körper und $\mathrm{PG}(n,K)$ der n-dimensionale projektive Raum über dem $(n+1)$-dimensionalen Vektorraum K^{n+1}. Unter einer rationalen Normkurve in $\mathrm{PG}(n,K)$ verstehen wir die Punktmenge

$$\Gamma := \{K(1,t,\ldots,t^n) \mid t \in K\} \cup K(0,\ldots,0,1)$$

und jede dazu projektiv äquivalente Menge. Gilt für die Charakteristik des Grundkörpers die Einschränkung $\mathrm{char}K = 0$, dann können in Analogie zur Differentialgeometrie durch formale Differentiation Ableitungspunkte und Schmiegräume in den Normkurvenpunkten erklärt werden. Für beliebige Charakteristik ist dies nicht mehr möglich, und es wird daher auf die nicht–iterative Hasse–Differentiation von Polynomen zurückgegriffen.

Für rationale Normkurven definieren wir die k-Knoten als Durchschnitte aller k-dimensionalen Schmiegräume von Γ. Bei Charakteristik 0 erhalten wir dabei stets die leere Menge, gilt jedoch $\mathrm{char}K = p > 0$, dann führt das im allgemeinen auf die Existenz nichttrivialer Knoten. Die Untersuchung dieser Knoten bildet den ersten Hauptteil der vorliegenden Arbeit. Es zeigt sich nämlich, daß die Dimension der Knoten als Funktion von k eine Treppenfunktion bildet, deren Wertebereich durch die Verteilung der Nullen im modulo p reduzierten Pascal–Dreieck $\Delta(p)$ bestimmt wird.

In der Fraktalstruktur des modulo p reduzierten Pascal–Dreiecks liegt der Schlüssel zur Lösung vieler Probleme. In dieser Arbeit werden eine Partition der Nullen von $\Delta(p)$ vorgenommen und danach drei Funktionen auf $\Delta(p)$ definiert, mit deren Hilfe die Knotendimensionen berechnet werden können.

Da die Knoten zu jenen ausgezeichneten Unterräumen im umgebenden Raum der rationalen Normkurven zählen, die invariant unter $\mathrm{P\Gamma L}(\Gamma)$, der Gruppe der automorphen Kollineationen von Γ sind, stellt sich natürlich sofort die Frage:

„Wie sehen alle unter $\mathrm{P\Gamma L}(\Gamma)$ *invarianten Unterräume aus?“*

Die Antwort ist Inhalt des zweiten Hauptteils dieser Arbeit. Wir haben über die p-adische Darstellung der um Eins vergrößerten Raumdimension Indexmengen Λ

konstruiert, so daß bei geeignet gewähltem Koordinatensystem mit Grundpunkten P_λ die Unterräume

$$\mathcal{U} = \{P_\lambda \mid \lambda \in \Lambda\}$$

jene nichtleeren „*irreduziblen*“, unter $\mathrm{P\Gamma L}(\Gamma)$ invarianten Unterräume beschreiben, die man nur mehr in trivialer Weise als Summe von invarianten Unterräumen schreiben kann. Durch Verbinden dieser Unterräume, was dem Vereinigen der zugehörigen Indexmengen entspricht, erhält man dann alle invarianten Unterräume.

Abschließend sei noch erwähnt, daß unsere Betrachtungen den Fall eines „kleinen Körpers“ ($\#K \leq n+1$) ausgeschlossen haben. Hier müßte man nämlich in Betracht ziehen, daß die Elemente von K nichttrivialen Polynom-Identitäten genügen, wodurch unsere Ergebnisse sich noch mehr verkomplizieren würden.

Inhaltsverzeichnis

Einleitung

Zum Inhalt

Nachdem wir das Inhaltsverzeichnis durchgelesen haben, stellt sich für so manchen Leser vermutlich folgende Frage:

> *„Wie kommt es, daß in einer Arbeit in dem einen Kapitel offensichtlich das Pascal–Dreieck untersucht wird, während in den folgenden Kapiteln ausschließlich geometrische Fragestellungen im Vordergrund stehen? Wo besteht da der Zusammenhang?“*

Der Autor muß gestehen, daß diese Fragen durchaus berechtigt sind, weil deren Beantwortung ja letztlich auch geraume Zeit, eine gewisse Art von Sitzfleisch und die eine oder andere Stunde Rechenzeit eines leistungsfähigen PC's beanspruchte[1].

In welcher Weise geht nun aber die Struktur des modulo p reduzierten Pascal–Dreiecks $\Delta(p)$ in die Beantwortung der geometrischen Fragestellungen ein? Dies erläutern wir im folgenden:

Wir gehen, wie schon in der Kurzfassung beschrieben, von *rationalen Normkurven* Γ mit der Parameterdarstellung

$$\Gamma = \{K(1, t, \ldots, t^n) \mid t \in K \cup \infty\}$$

aus. Da wir die Ableitungspunkte und die Schmiegräume für beliebige Charakteristik des Grundkörpers K erklären möchten, benützen wir eine von H. Hasse, F.K. Schmidt und O. Teichmüller (vgl. [8] oder [14, 1.3]) begründete nicht–iterative Differentiation von Polynomen und folgen damit den Ausführungen von H. Havlicek in [9]. Durch diese Differentiation kommt es zum Auftreten von Binomialkoeffizienten.

[1]Bei dieser Gelegenheit möchte ich der Hochschuljubiläumsstiftung der Stadt Wien dafür danken, daß sie diese Arbeit durch die Finanzierung eines entsprechenden *Personalcomputers* unterstützt und erleichtert hat.

Wir definieren dann für rationale Normkurven den *k-Knoten* als Durchschnitt über alle k-Schmiegräume. Das bekannteste Beispiel für einen nichttrivialen Knoten ist wohl ein Kegelschnitt bei Charakteristik 2, dessen Tangenten kopunktal sind. In der Literatur wird der Begriff „Knoten“ jedoch in verschiedenster Weise benützt. Manche Autoren bezeichnen damit jenen Punkt, der eine rationale Normkurve zu einem maximalen Bogen ergänzt (K ist dabei ein endlicher Körper gerader Ordnung), andere verstehen darunter den Durchschnitt aller Schmieghyperebenen einer Veronese-Varietät.

Im Laufe dieser Arbeit stellt es sich heraus, daß sich die eben erwähnten Beispiele der von uns gegebenen Definition eines Knotens unterordnen. Eines unserer Hauptresultate ist eine Formel, mit der sämtliche Dimensionen der k-Knoten einer rationalen Normkurve in einem n-dimensionalen projektiven Raum mit Charakteristik $p > 0$ berechnet werden können. Für $k = n - 1$ hat H. Timmermann so eine Formel mit anderen Methoden bereits entwickelt (vgl. [23, 4.15], [22]). Andere Ergebnisse über Knoten verdanken wir H. Brauner [2, 10.4.10], D.G. Glynn [5, 49–50], A. Herzer [11], H. Karzel [16], J.A. Thas [20] und J.A. Thas– J.W.P. Hirschfeld [15, 25.1].

Es stellt sich heraus, daß die geometrischen Eigenschaften eines k–Knoten in engem Zusammenhang mit jenen Binomialkoeffizienten stehen, die modulo p verschwinden. Dabei spielen die p-adischen Entwicklungen der natürlichen Zahlen n, $n + 1$ und k eine entscheidende Rolle. Eine Partition der Nullen im Pascal–Dreieck modulo p drängt sich in diesem Zusammenhang förmlich auf. Wir haben im ersten Kapitel ein Tripel (T, Φ, Σ) von Funktionen auf $\Delta(p)$ definiert (diese Ergebnisse sind für sich auch ohne entsprechende Anwendungen interessant), und nach den nötigen Voraussetzungen im zweiten Kapitel dürfen diese Funktionen in Kapitel 3 entscheidend zur Bestimmung der Knotendimensionen beitragen.

Es ist auf Grund der Definition der Knoten selbstverständlich, daß es sich dabei um Unterräume handelt, die unter der Gruppe $\mathrm{P\Gamma L}(\Gamma)$ der automorphen Kollineationen von Γ invariant bleiben. Während etwa H. Timmermann in [23] für gewisse Spezialfälle (mit anderen Methoden) weitere unter $\mathrm{P\Gamma L}(\Gamma)$ invariante Unterräume angibt, haben wir es in Kapitel 4 geschafft, *alle unter* $\mathrm{P\Gamma L}(\Gamma)$ *invarianten Unterräume* zu berechnen.

Die einzige Einschränkung, die wir dabei setzen, ist, auf kleine Grundkörper zu verzichten ($\#K \geq n + 2$). In diesen Fällen wäre nämlich zusätzlich zu unseren Überlegungen zu beachten, daß die Körperelemente nichttriviale Polynom-Identitäten erfüllen. Wenn wir jedoch diese Fälle ausklammern, dann können wir zeigen, daß invariante Unterräume stets durch Grundpunkte P_λ des gewählten

Koordinatensystems aufgespannt werden, also

$$\mathcal{U} = \{P_\lambda \mid \lambda \in \Lambda\}$$

mit entsprechenden Indexmengen Λ gilt.

Den Leser wird es vielleicht ebenso überraschen, wie es den Autor anfänglich überrascht hat, daß es sich bei dem Verband aller invarianten Unterräume unter der Gruppe der automorphen Kollineationen im allgemeinen *nicht um eine Totalordnung* handelt, obwohl die Teilmenge der Knoten stets eine Kette bildet.

Nun wollen wir den Leser aber nicht weiter auf die Folter spannen. Bevor wir jedoch in medias res gehen, möchte ich noch einige Dankesworte aussprechen:

Ich erinnere mich noch gut an jenen Herbsttag im Jahre 1996, an dem mein Betreuer Univ.Prof. Dr. Hans Havlicek mich nach Beendigung meiner Diplomarbeit gebeten hatte, ich möge Ihn doch in Zukunft bei diversen Ideen und Überlegungen für diese Arbeit mehr mitleiden lassen als bisher. Hoffentlich habe ich diese Aufforderung nicht zu wörtlich genommen! Jedenfalls bin ich froh, daß dieses Leiden nun ein Ende hat und ich Ihm auf diesem Wege wirklich ein herzliches Dankeschön für die Zusammenarbeit in den letzten Jahren sagen kann.

Seine Idee war es auch, beim FWF (Fonds zur Förderung der wissenschaftlichen Forschung) die Unterstützung des Projekts *„Veronese varieties over fields with non–zero characteristic“* zu beantragen und so die nötigen Rahmenbedingungen für diese Dissertation zu schaffen. Tatsächlich stehe ich nun mittlerweile seit 1. Oktober 1997 als Projektmitarbeiter[2] unter Dienstvertrag, wofür ich dem FWF herzlich danke.

Obwohl dies zwar selbstverständlich ist, soll schließlich auch einmal angesprochen werden, wie sehr ich es zu schätzen weiß, daß meine Eltern von Kindheit an die nötigen Voraussetzungen für meinen bisherigen Lebensweg geschaffen haben. Ihnen möchte ich diese Arbeit auch widmen!

Dem Leser gebe ich schließlich noch eine Liste mit Abkürzungen und Schreibweisen auf den Weg mit.

[2]Es handelt sich hierbei um das Projekt P12353-MAT.

Bezeichnungen

allgemein

K	(kommutativer) Körper
$K^\times$	$K \setminus \{0\}$
K^+	$K \cup \{\infty\}$
$K[t]$	Polynomring in der Unbestimmten t
$\mathrm{Aut}(K)$	Gruppe der Körperautomorphismen
p	(meist feste) Primzahl
$GF(p^h)$	Galoisfeld mit p^h Elementen
$\mathrm{GL}(n, K)$	Gruppe aller regulären $(n \times n)$–Matrizen über K
$\mathrm{rg} f$	Rang der Abbildung f
$\mathrm{def} f$	Defekt von f

zu Kapitel 1

$\preceq$	$j \preceq n \Leftrightarrow \binom{n}{j} \not\equiv 0 \pmod p$ (vgl. Def. 1.1.3)
$\Delta(p)$	Pascal–Dreieck modulo p
$\Delta^i(p)$	die ersten p^i Zeilen von $\Delta(p)$ (vgl. Def. 1.2.1)
$\square(p)$	Pascal–Quadrat $\square(p) = \Delta(p)\nabla$
	mit einem „Nulldreieck“ ∇ (vgl. Def. 1.2.2)
∇^i	dreieckiges Feld mit $p^i - 1$ „Null–Einträgen“
	in der ersten Zeile (vgl. Def. 1.2.2)
$\overline{i}$	$(n, j) \in \overline{i} \Leftrightarrow (n, j) \in \nabla^i$ (vgl. Def. 1.3.1)
$\overline{i(n)}$	$(n, j) \in \overline{i(n)} \Leftrightarrow (n, j) \in \nabla^i$, wobei n fest (vgl. Def. 1.3.1)
$\Phi(i, n)$	„Anzahlfunktion“ $\Phi(i, n) = \#\overline{i(n)}$ (vgl. Satz 1.4.1)
$T(R, b)$	„top line“-Funktion $T(R, b) = \sum_{\lambda=0}^{R-1} b_\lambda p^\lambda$ (vgl. Def. 1.4.6)
$\Sigma(i, n)$	„Summenfunktion“ $\Sigma(i, n) = \sum_{\eta=i}^{\infty} \Phi(\eta, n)$ (vgl. Def. 1.4.7)

zu Kapitel 2

Γ	rationale Normkurve (vgl. Def. 2.1.1)
n	projektive Dimension
$\mathcal{P} = \mathrm{PG}(n, K)$	projektiver Raum über K^{n+1} der Dimension n
$b := n + 1$	Dimension des Vektorraums K^{n+1}
$\mathrm{P\Gamma L}(\Gamma)$	Gruppe der automorphen Kollineationen von Γ
$\mathrm{PGL}(\Gamma)$	Gruppe der projektiven Kollineationen von Γ
Kc_t	Normkurvenpunkt zum Parameterwert t
$Kc_t^{(j)}$	j-ter Ableitungspunkt (vgl. Abschnitt 2.3.2)
$\mathcal{S}_t^{(k)}\Gamma$	k-Schmiegraum von Γ in Kc_t (vgl. Def. 2.3.2)

zu Kapitel 3

$\mathcal{N}^{(k)}\Gamma$	k-Knoten: Durchschnitt aller k-Schmiegräume

zu Kapitel 4

C_t	Matrix, deren Spalten $c_t, c_t', \ldots, c_t^{(n)}$ den n-Schmiegraum $\mathcal{S}_t^{(n)}\Gamma$ beschreiben (vgl. Formel 4.4)
$\mathcal{O}_j$	der von der Bahn $\{C_t(P_j) \mid t \in K\}$ aufgespannte Unterraum (vgl. Def. 4.1.5)
$\Omega(j)$	Indexmenge mit $\mathcal{O}_j = [\{P_\omega \mid \omega \in \Omega(j)\}]$ (vgl. Def. 4.1.6)
Ψ	beliebige Indexmenge $\Psi \subset \{0, 1, \ldots, n\}$
$\square^j$	Abschnitt $\square_{p^j}$ des Pascal–Quadrats (vgl. Def. 4.1.14)
$V(i, b)$	Funktion mit $T(i, b) + V(i, b) = b$ für alle $i \in \mathbb{N}$ (vgl. Def. 4.4.1)
j^*	$n - j$ bei festem n
I_λ	Menge $\{i_\lambda, i_\lambda + 1, \ldots, i_\lambda + k_\lambda\}$ (vgl. Abschnitt 4.6.2)
$V(I_1, \ldots, I_L; i, b)$	vgl. Abschnitt 4.6.2

$\mathcal{T}(I_\lambda)$	Mengensystem $\{\{i_\lambda, i_\lambda + 1, \ldots, i_\lambda + \nu\} \mid \nu = -1, 0, \ldots, k_\lambda\}$ (vgl. Abschnitt 4.6.3)
$\mathcal{T}(I_1 \times \ldots \times I_L)$	$\mathcal{T}(I_1) \times \ldots \times \mathcal{T}(I_L)$ vgl. oben
Λ	Indexmenge, so daß $[\{P_\lambda \mid \lambda \in \Lambda\}]$ unter PΓL(Γ) invariant
$\Lambda(I_1, \ldots, I_L; i, b)$	$\bigcup \Omega(V(T_1, \ldots, T_L; i, b))$ Vereinigung über alle L-Tupel $(T_1, T_2, \ldots, T_L) \in \mathcal{T}(I_1 \times \ldots \times I_L)$ (vgl. Abschnitt 4.7)

Kapitel 1

Hilfsmittel aus der Zahlentheorie

In diesem Kapitel wird vorerst ein Lemma vorgestellt, das einerseits die Berechnung von modulo p reduzierten Binomialkoeffizienten entscheidend erleichtert, und andererseits die Fraktalstruktur des modulo p reduzierten Pascal–Dreiecks begründet. Außerdem wird eine Partition der Nullen im Pascal–Dreieck angegeben, welche schließlich zur Definition dreier Funktionen führt, die in den folgenden Kapiteln ihre Anwendungen in der Geometrie finden.

1.1 Ein Lemma von Lucas

In diesem Kapitel sei die Primzahl p stets fest gewählt. Die Darstellung einer natürlichen Zahl $n \in \mathbb{N}$ in der Basis p kann in der Form

$$n = \sum_{\lambda=0}^{\infty} n_\lambda p^\lambda =: \langle n_\lambda \rangle$$

geschrieben werden, wobei aber nur endlich viele Ziffern $n_\lambda \in \{0, 1, \ldots, p-1\}$ verschieden von 0 sind. Wir schreiben n auch in der Form

$$n = \langle \ldots, n_i, n_{i-1}, \ldots, n_0 \rangle$$

und lassen dabei auch führende Nullen zu. Beispielsweise sind für die Darstellung der Zahl 10 in der Basis 2 mehrere Schreibweisen möglich:

$$\begin{aligned} 10 &= \langle 1, 0, 1, 0 \rangle \\ &= \langle 0, 0, 1, 0, 1, 0 \rangle \end{aligned}$$

Wir wollen nun ein Lemma von Lucas vorstellen, welches die Berechnung von modulo p reduzierten Binomialkoeffizienten entscheidend erleichtert. Damit werden wir auch die Struktur des modulo p reduzierten Pascal–Dreiecks besser verstehen.

Lemma 1.1.1 (Lucas [3]) *Seien $\langle n_\lambda \rangle$ und $\langle j_\lambda \rangle$ die p-adischen Darstellungen der natürlichen Zahlen n und j, dann gilt*

$$\binom{n}{j} \equiv \prod_{\lambda=0}^{\infty} \binom{n_\lambda}{j_\lambda} \pmod{p}.$$

Beweis: Links steht der Koeffizient von x^j in $(1+x)^n$, während es sich bei dem rechten Koeffizienten um jenen von x^j in $\prod_\lambda (1+x^{p^\lambda})^{n_\lambda}$ handelt. Über Körpern mit Charakteristik p stimmen diese Polynome überein. □

Bemerkung 1.1.2 Wegen $n_\lambda \in \{0, 1, \ldots, p-1\}$ ist ein Binomialkoeffizient $\binom{n_\lambda}{j_\lambda}$ genau für $j_\lambda > n_\lambda$ kongruent 0 modulo p und $\binom{n}{j}$ verschwindet modulo p genau dann, wenn $\lambda \in \mathbb{N}$ existiert, mit $j_\lambda > n_\lambda$.

Folgende Definition trägt von nun an zur Erleichterung der Schreibweise bei.

Definition 1.1.3 *Bei gegebener Primzahl p sei auf der Menge $\mathbb{N}$ eine Halbordnung „$\preceq$“ erklärt:*

$$\langle j_\lambda \rangle \preceq \langle n_\lambda \rangle \quad :\Leftrightarrow \quad j_\lambda \leq n_\lambda \text{ für alle } \lambda \in \mathbb{N}.$$

Mit den Bezeichnungen dieser Definition folgt jetzt:

$$\binom{n}{j} \equiv 0 \pmod{p} \quad \Leftrightarrow \quad j \not\preceq n$$

1.2 Aufbau und Struktur des Pascal–Dreiecks und des Pascal–Quadrats modulo p

Mit dem Lemma von Lucas können wir jetzt die Fraktalstruktur des auch im Anhang zu Kapitel 1 abgebildeten Pascal–Dreiecks modulo p besser verstehen, und nach einigen Begriffsbildungen genauere Untersuchungen durchführen.

Definition 1.2.1 *Im folgenden bezeichne $\Delta(p)$ das modulo p reduzierte Pascal–Dreieck. Die Zeilen von $\Delta(p)$ werden bei Null beginnend gezählt. Für $i \in \mathbb{N}$ bezeichne weiters $\Delta^i(p)$ das aus den Zeilen $0, \ldots, p^i - 1$ gebildete Teildreieck von $\Delta(p)$. Für das gliedweise mit m multiplizierte und gleichzeitig modulo p reduzierte Dreieck $\Delta^i(p)$ wird $m\Delta^i(p)$ geschrieben. Wenn es klar ist, welche Primzahl p gerade gemeint ist, kürzen wir $\Delta^i(p)$ durch Δ^i ab.*

Da wir später untere Dreiecksmatrizen mit den Einträgen aus $\Delta(p)$ betrachten werden, erscheint es sinnvoll, auch ein „Pascal–Quadrat“ $\square(p)$ folgendermaßen zu definieren.

Definition 1.2.2 *Seien n und j natürliche Zahlen. An der Position (n, j) des (unendlichen) Pascal–Quadrats $\square(p)$ stehe der modulo p reduzierte Binomialkoeffizient $\binom{n}{j}$.*

Die Reihen und Spalten von $\square(p)$ werden also beginnend mit 0 durchnumeriert. Außerdem bezeichne $\square^i(p)$ ($i \in \mathbb{N}$) jene Matrix, die im Schnitt der ersten p^i Reihen und Spalten von $\square(p)$ liegt. Wie für $\Delta(p)$ führen wir auch für $\square(p)$ die Kurzschreibweise $\square$ ein.

Bei $\square^i$ handelt es sich also um eine untere Dreiecksmatrix der Form

$$\square^i = \Delta^i \nabla^i,$$

wobei ∇^i ausschließlich durch die Zahl 0 aufgebaut ist.

Man betrachte auch, daß die letzte Zeile von Δ^i aus p^i Elementen besteht, während in der ersten Zeile von ∇^i nur $p^i - 1$ Einträge stehen. Das Dreieck ∇^0 ist also leer.

Durch ein Beispiel wird die Vorstellung untermauert. Abbildung 1.1 zeigt Δ^3 für $p = 3$.

1
1 1
1 2 1
1 0 0 1
1 1 0 1 1
1 2 1 1 2 1
1 0 0 2 0 0 1
1 1 0 2 2 0 1 1
1 2 1 2 1 2 1 2 1
1 0 0 0 0 0 0 0 0 1
1 1 0 0 0 0 0 0 0 1 1
1 2 1 0 0 0 0 0 0 1 2 1
1 0 0 1 0 0 0 0 0 1 0 0 1
1 1 0 1 1 0 0 0 0 1 1 0 1 1
1 2 1 1 2 1 0 0 0 1 2 1 1 2 1
1 0 0 2 0 0 1 0 0 1 0 0 2 0 0 1
1 1 0 2 2 0 1 1 0 1 1 0 2 2 0 1 1
1 2 1 2 1 2 1 2 1 1 2 1 2 1 2 1 2 1
1 0 0 0 0 0 0 0 0 2 0 0 0 0 0 0 0 0 1
1 1 0 0 0 0 0 0 0 0 2 2 0 0 0 0 0 0 0 0 1 1
1 2 1 0 0 0 0 0 0 0 2 1 2 0 0 0 0 0 0 0 1 2 1
1 0 0 1 0 0 0 0 0 2 0 0 2 0 0 0 0 0 1 0 0 1
1 1 0 1 1 0 0 0 0 2 2 0 2 2 0 0 0 0 1 1 0 1 1
1 2 1 1 2 1 0 0 0 2 1 2 2 1 2 0 0 0 1 2 1 1 2 1
1 0 0 2 0 0 1 0 0 2 0 0 1 0 0 2 0 0 1 0 0 2 0 0 1
1 1 0 2 2 0 1 1 0 2 2 0 1 1 0 2 2 0 1 1 0 2 2 0 1 1
1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1

Abbildung 1.1: Δ^3 für $p = 3$

Wie man auch dem Lemma 1.1.1 entnehmen kann, besitzt jedes Dreieck Δ^{i+1} ($i \geq 0$) die in Abbildung 1.2 dargestellte Form.

$$\binom{0}{0}\Delta^i$$

$$\binom{1}{0}\Delta^i \quad \nabla^i \quad \binom{1}{1}\Delta^i$$

$$\binom{2}{0}\Delta^i \quad \nabla^i \quad \binom{2}{1}\Delta^i \quad \nabla^i \quad \binom{2}{2}\Delta^i$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\binom{p-1}{0}\Delta^i \quad \nabla^i \qquad\qquad \ldots \qquad\qquad \nabla^i \quad \binom{p-1}{p-1}\Delta^i$$

Abbildung 1.2: Zerlegung von Δ^{i+1}

Die Binomialkoeffizienten vor den Δ^i's entsprechen genau den Einträgen von Δ^1, und wie schon in der Bemerkung zu Lemma 1.1.1 erwähnt, ist deshalb keiner von ihnen kongruent 0 modulo p. Bei $i \geq 2$ kann jedes Teildreieck $\binom{n}{j}\Delta^i$ von oben wiederum in zu Δ^{i-1} proportionale, beziehungsweise nichtleere Dreiecke ∇^{i-1} zerlegt werden. Diesen Gedanken kann man endlich oft weiterspinnen und sich Δ^{i+1} letztlich aus Dreiecken Δ^k, mit $1 \leq k \leq i$ zusammengesetzt denken. Vergleiche dazu auch [12, 91–92] oder [17, Theorem 1].

Analog dem Schema für Δ^{i+1} drücken wir $\square^{i+1}$ in Abbildung 1.3 durch „Vielfache“ von $\square^i$ aus.

$$\begin{array}{cccccc}
\binom{0}{0}\square^i & \binom{0}{1}\square^i & \ldots & \binom{0}{p-2}\square^i & \binom{0}{p-1}\square^i \\
\binom{1}{0}\square^i & \binom{1}{1}\square^i & \ldots & \binom{1}{p-2}\square^i & \binom{1}{p-1}\square^i \\
\binom{2}{0}\square^i & \binom{2}{1}\square^i & \ldots & \binom{2}{p-2}\square^i & \binom{2}{p-1}\square^i \\
 & & \ldots & & \\
\binom{p-1}{0}\square^i & \binom{p-1}{1}\square^i & \ldots & \binom{p-1}{p-2}\square^i & \binom{p-1}{p-1}\square^i
\end{array}$$

Abbildung 1.3: Zerlegung von $\square^{i+1}$

Der Vorteil dieser Betrachtungsweise liegt darin, daß wir gewisse Ergebnisse im Kapitel über rationale Normkurven auch anschaulich recht gut verstehen werden.

1.3 Eine Klasseneinteilung der Nullen im Pascal–Quadrat

Durch die zuvor besprochene Zerlegung von Δ in Vielfache von Δ^i und ∇^i erhalten wir in natürlicher Weise eine Partition der Nullen in maximale Teildreiecke ∇^i ($i \in \mathbb{N}^+$). Wenn man noch das unendliche Dreieck ∇ hinzugibt, dann wird die Menge aller Nullen des Pascal–Quadrats modulo p partitioniert. Eine gröbere Partition von $\square$ in Klassen

$$\overline{1}, \overline{2}, \ldots, \overline{\infty}$$

erhalten wir, wenn wir alle Dreiecke ∇^i derselben Größe zu einer Klasse $\overline{i}$[1] zusammenfassen und ∇ mit $\overline{\infty}$ bezeichnen.

Diese anschaulich beschriebene Partition der Nullen in $\square(p)$ wollen wir nun durch eine formale Definition, die sich von der Anschauung löst und auf die p-adischen Zahlendarstellungen zurückgreift, auf feste Beine stellen.

Definition 1.3.1 *Sei p eine Primzahl. Ein Paar $(n, j) = (\langle n_\lambda \rangle, \langle j_\lambda \rangle)$ natürlicher Zahlen mit $j \not\leq n$ und*

$$L := \max\{\lambda \in \mathbb{N} \mid j_\lambda > n_\lambda\} \in \mathbb{N}$$

liegt in der Klasse $\overline{i}$*, falls*

$$i = \inf\{\lambda > L \mid j_\lambda < n_\lambda\} \in \mathbb{N}^+ \cup \{\infty\} \text{ gilt.}$$

Bei gegebenem $n \in \mathbb{N}$, bezeichne $\overline{i(n)}$ die Menge aller Elemente $j \in \mathbb{N}$ mit $(n, j) \in \overline{i}$.

Bemerkungen 1.3.2

1. In der obigen Definition ist wegen $j \not\leq n$ die Existenz des Maximums L gesichert. Nun gibt es zwei Fälle: Bei $j \leq n$ existiert $\lambda > L$ mit $j_\lambda < n_\lambda$ und daher auch das Minimum i all dieser Indizes λ. Im anderen Fall ($j > n$) erhält man mit einer bekannten Konvention

$$i = \inf \emptyset := \infty.$$

   Das Infimum ist daher wohldefiniert und die Definition 1.3.1 somit sinnvoll.

[1] Hinweis: Man verwechsle $\overline{i}$ nicht mit einer Restklasse von $\mathbb{Z}$ modulo p !

2. Man kann sich leicht überlegen, daß die Menge $\overline{i}$ für jedes $i \in \mathbb{N}^+ \cup \{\infty\}$ nichtleer ist und deshalb tatsächlich eine Partition vorliegt.
   In Abschnitt 1.4.2 werden wir sehen, daß die in Definition 1.3.1 formal gegebene und die durch die Anschauung gewonnene Klasseneinteilung der Nullen in $\square$ übereinstimmen.

3. Wie schon bemerkt, liegt ein Paar (n, j) in $\overline{\infty}$, wenn $j > n$ gilt. Für $j < n$ ist (n, j) in $\overline{i} \neq \overline{\infty}$, wenn die Ziffern in den p-adischen Darstellungen folgende Bedingungen erfüllen:

$$\left.\begin{array}{rcll} j_\lambda & \leq & p-1 & \text{für alle } \lambda \in \{0,1,\ldots,L-1\} \\ j_L & > & n_L & \text{für ein } L \in \{0,1,\ldots,i-1\} \\ j_\lambda & = & n_\lambda & \text{für alle } \lambda \in \{L+1, L+2,\ldots,i-1\} \\ j_i & < & n_i & \\ j_\lambda & \leq & n_\lambda & \text{für alle } \lambda \in \{i+1, i+2,\ldots\} \end{array}\right\} \qquad (1.1)$$

4. Um nachher in einem Lemma besser darauf zugreifen zu können, auf wie viele Arten bei festem n und $i \neq \infty$ der Parameter j gewählt werden kann, so daß $j \in \overline{i(n)}$ gilt, stellen wir die diversen Möglichkeiten noch detaillierter dar:

$j \in \overline{i(n)} : \quad \Leftrightarrow$

$$\begin{array}{rcll} j_0 & \in & \{0,1,\ldots,p-1\} & \text{beliebig} \\ \vdots & & \vdots & \\ j_{i-2} & \in & \{0,1,\ldots,p-1\} & \text{beliebig} \\ j_{i-1} & > & n_{i-1} & \\ j_i & < & n_i & \\ j_\lambda & \leq & n_\lambda & \lambda > i \end{array}$$

oder

$$\begin{array}{rcll} j_0 & \in & \{0,1,\ldots,p-1\} & \text{beliebig} \\ \vdots & & \vdots & \\ j_{i-3} & \in & \{0,1,\ldots,p-1\} & \text{beliebig} \\ j_{i-2} & > & n_{i-2} & \\ j_{i-1} & = & n_{i-1} & \\ j_i & < & n_i & \\ j_\lambda & \leq & n_\lambda & \lambda > i \end{array}$$

usw. bis

$$\begin{aligned} j_0 &> n_0 \\ j_1 &= n_1 \\ &\vdots \quad \vdots \\ j_{i-1} &= n_{i-1} \\ j_i &< n_i \\ j_\lambda &\leq n_\lambda \qquad \lambda > i \end{aligned}$$

Während durch die Literatur etwa die Frage nach allen Nullen von Δ innerhalb der ersten n Zeilen beantwortet wird (vgl. etwa [18]), werden wir überlegen, wie viele Nullen einer Klasse i von einer festen Zeile n des Pascal–Quadrats getroffen werden. Nach intensiver Beschäftigung mit der Literatur über das modulo p reduzierte Pascal–Dreieck hat es für uns den Anschein, als ob bis jetzt die Nullen in Δ noch nicht nach ihrem Typ unterschieden worden sind. Für die Bestimmung der Knotendimensionen rationaler Normkurven scheint dieser Schritt jedoch sehr zweckmäßig.

1.4 Drei Funktionen auf $\Delta(p)$

1.4.1 Die „Anzahlfunktion“ $\Phi(i,n)$

Im folgenden Satz bestimmt die Funktion $\Phi(i,n)$ die Anzahl der Nullen in der n–ten Zeile von Δ, die in der Klasse $\overline{i} \neq \overline{\infty}$ liegen. Es ist klar, daß jeder Zeile n von Δ stets unendlich viele Elemente von $\overline{\infty}$ angehören.

Satz 1.4.1 *Es seien $n = \langle n_\lambda \rangle \in \mathbb{N}$ und $i \in \mathbb{N}^+$ gegeben. Die Menge $\overline{i(n)}$ hat dann die Mächtigkeit*

$$\Phi(i,n) := \#\overline{i(n)} = (p^i - 1 - \sum_{\mu=0}^{i-1} n_\mu p^\mu) \cdot n_i \cdot \prod_{\lambda=i+1}^{\infty} (n_\lambda + 1). \tag{1.2}$$

Beweis: Nach den Vorbereitungen im letzten Punkt der Bemerkungen 1.3.2 müssen wir lediglich zählen, auf wie viele Arten wir die j_λ wählen können:
Wenn j dem ersten Bedingungsblock genügen soll, dann gibt es wegen

$$\begin{aligned} j_0 \text{ bis } j_{i-2} \text{ beliebig} &\Rightarrow p^{i-1} \text{ Möglichkeiten} \\ j_{i-1} > n_{i-1} &\Rightarrow p - 1 - n_{i-1} \text{ Möglichkeiten} \\ j_i < n_i &\Rightarrow n_i \text{ Möglichkeiten} \\ j_\lambda \leq n_\lambda \text{ für } \lambda \geq i+1 &\Rightarrow \prod_{\lambda=i+1}^{\infty} (n_\lambda + 1) \text{ Möglichkeiten} \end{aligned}$$

insgesamt

$$p^{i-1} \cdot (p-1-n_{i-1}) \cdot n_i \cdot \prod_{\lambda=i+1}^{\infty} (n_\lambda + 1)$$

Möglichkeiten. Mit analogen Überlegungen gibt es für den nächsten Block

$$p^{i-2} \cdot (p-1-n_{i-2}) \cdot n_i \cdot \prod_{\lambda=i+1}^{\infty} (n_\lambda + 1)$$

und schließlich für den letzten

$$p^{0} \cdot (p-1-n_{0}) \cdot n_i \cdot \prod_{\lambda=i+1}^{\infty} (n_\lambda + 1)$$

Möglichkeiten, was addiert dann

$$\begin{aligned} \Phi(i,n) &= (\sum_{\mu=0}^{i-1} p^\mu (p-1-n_\mu)) \cdot n_i \cdot \prod_{\lambda=i+1}^{\infty} (n_\lambda + 1) \\ &= (p^i - 1 - \sum_{\mu=0}^{i-1} n_\mu p^\mu) \cdot n_i \cdot \prod_{\lambda=i+1}^{\infty} (n_\lambda + 1) \end{aligned}$$

ergibt, wie behauptet worden ist. □

Man beachte, daß $\Phi(i,n)$ für $i = 0$ und $i = \infty$ nicht definiert wird, weil einerseits die Klasse $\overline{0}$ nicht existiert, und andererseits klar ist, daß in jeder Zeile von Δ unendlich viele Elemente von $\overline{\infty}$ liegen!

Wir können jetzt mühelos entscheiden, ob eine bestimmte Klasse von einer vorgegebenen Zeile getroffen wird.

Satz 1.4.2 *Aus Satz 1.4.1 folgt leicht*

$$\Phi(i,n) = 0 \quad \Longleftrightarrow \quad n_{i-1} = \ldots = n_1 = n_0 = p-1 \text{ } \textit{oder} \text{ } n_i = 0 \; . \tag{1.3}$$

Beweis: Wegen

$$\Phi(i,n) = 0 \;\Leftrightarrow\; (p^i - 1 - \sum_{\mu=0}^{i-1} n_\mu p^\mu) = 0 \text{ oder } n_i = 0 \text{ oder } \prod_{\lambda=i+1}^{\infty} (n_\lambda + 1) = 0$$

und auf Grund der Identität $p^i - 1 = \sum_{\mu=0}^{i-1}(p-1)p^\mu$ verschwindet der erste Term genau bei $n_{i-1} = n_{i-2} = \ldots = n_1 = n_0 = p-1$, der zweite trivialerweise genau bei $n_i = 0$ und der dritte nie. □

Dieses Resultat möchten wir umformulieren, indem wir auf die p–adische Entwicklung von $n+1$ zurückgreifen.

Satz 1.4.3 *Es sei $n = \langle n_\lambda \rangle \in \mathbb{N}$, $i \in \mathbb{N}^+$, und*

$$n+1 =: b = \langle b_\lambda \rangle,\ M := \min\{\lambda \mid b_\lambda \neq 0\}. \tag{1.4}$$

Dann folgt

$$\Phi(i,n) = \#\overline{i(n)} = 0 \Longleftrightarrow \begin{cases} b_{i-1} &= 0 \text{ falls } i \in \{1,2,\ldots,M\}, \\ b_i &= 0 \text{ falls } i \in \{M+1, M+2, \ldots\}. \end{cases} \tag{1.5}$$

Beweis: Aus der Definition von M folgt

$$\begin{aligned} b &= \langle \ldots, b_{M+1}, b_M, 0, \ldots, 0\rangle \qquad \text{und} \\ n &= \langle \ldots, n_{M+1}, n_M, p-1, \ldots, p-1\rangle, \end{aligned}$$

mit $b_M = n_M + 1$, $0 \leq n_M < p-1$, und

$$b_\lambda = n_\lambda \text{ für alle } \lambda \in \{M+1, M+2, \ldots\}. \tag{1.6}$$

Mit Formel (1.3) ist die Aussage aber bewiesen. □

Der große Vorteil der Formel (1.5) liegt darin, daß man lediglich die Stelle b_M und die Ziffern $b_\lambda = 0$ betrachten muß, um zu entscheiden, ob eine Menge $\overline{i(n)}$ leer ist oder nicht. Unter den Mengen $\overline{i(n)}$ kommt die leere Menge so oft vor, wie es Nullen in $\langle b_\lambda \rangle$ gibt.

1.4.2 Die „top line“–Funktion $T(R,b)$

Wir wollen jetzt zeigen, daß sich die in Definition 1.3.1 beschriebenen Klassen $\overline{i}$ ausschließlich aus Dreiecken ∇^i zusammensetzen. Wenn wir uns nun im Pascal–Quadrat $\square$ an der Stelle (n,j) befinden und es sich dabei um eine Null handelt, dann laufen wir in der j–ten Spalte so lange nach oben, bis wir das letzte Mal zu einem Eintrag gleich Null gelangen.

Die sogenannte „top line“–Funktion liefert uns dann genau die Nummer dieser letzten Zeile, in der an der Stelle j noch immer eine Null steht.

Satz 1.4.4 *Es sei $n \in \mathbb{N}$, $i \in \mathbb{N}^+$, $j \in \overline{i(n)}$, und man setze*

$$T := n - \sum_{\lambda=0}^{i-1} n_\lambda p^\lambda. \tag{1.7}$$

Dann folgt $j \preceq T-1$ und $j \in \overline{i(x)}$ für alle $x \in \{T, T+1, \ldots, n\}$.

Beweis: Wir übernehmen die Bezeichnungen von (1.1). Wenn x von n abwärts bis

$$n - \sum_{\lambda=0}^{L} n_\lambda p^\lambda = \langle \ldots, n_{i+1}, n_i, \ldots, n_{L+1}, 0, \ldots, 0 \rangle, \tag{1.8}$$

läuft[2], dann ist $j \in \overline{i(x)}$ wegen (1.1) klar.

Im Falle $n_{i-1} = \ldots = n_{L+2} = n_{L+1} = 0$ sind wir dann wegen

$$T - 1 = n - 1 - \sum_{\lambda=0}^{L} n_\lambda p^\lambda = \langle \ldots, n_{i+1}, n_i - 1, p-1, \ldots, p-1 \rangle$$

und $j \preceq T-1$ schon fertig.

Andernfalls setzen wir $L' := \min\{\lambda \in \{L+1, L+2, \ldots, i-1\} \mid n_\lambda \neq 0\}$.

Subtrahieren wir nun die Zahl 1 auf beiden Seiten von (1.8), dann ergibt das

$$n' := n - 1 - \sum_{\lambda=0}^{L} n_\lambda p^\lambda = \langle \ldots, n_{i+1}, n_i, \ldots, n_{L'} - 1, p-1, \ldots, p-1 \rangle.$$

Aus $j_{L'} = n_{L'}$ folgt $j_{L'} > n_{L'} - 1$ und somit $j \in \overline{i(n')}$. Definieren wir jetzt noch T' gemäß (1.7), indem wir n durch n' ersetzen, dann ändert das am Wert $T' = T$ nichts.

Fahren wir mit n' und j so fort wie eben, dann erhalten wir nach einer endlichen Anzahl von Schritten das gewünschte Resultat. □

Es sei also mit den Bezeichnungen des vorigen Lemmas $T =: \langle T_\lambda \rangle$. Auf Grund von $j \in \overline{i(T)}$ folgern wir $j_i < T_i = n_i$ und $j_\lambda \leq T_\lambda = n_\lambda$ für alle $\lambda \in \{i+1, i+2, \ldots\}$.

[2]Im Pascal–Quadrat läuft man dabei „aufwärts“.

Die Zahlen

$$\begin{aligned} Y &:= j - \sum_{\lambda=0}^{i-1} j_\lambda p^\lambda = \langle \ldots, j_{i+1}, j_i, 0, \ldots, 0 \rangle \\ Y + p^i &= \langle \ldots, j_{i+1}, j_i + 1, 0, \ldots, 0 \rangle \end{aligned}$$

erfüllen $Y \preceq T$ und $Y + p^i \preceq T$, während für die Zahlen dazwischen

$$\{Y + 1, Y + 2, \ldots, Y + p^i - 1\} \subset \overline{i(T)}$$

gilt. (Man beachte, daß es sich hierbei um $p^i - 1$ Zahlen handelt.)

Aus der gut bekannten Identität $\binom{r}{s} + \binom{r}{s+1} = \binom{r+1}{s+1}$ folgt, daß die Zeile T von Δ tatsächlich die erste Zeile eines Dreiecks ∇^i ist, welches durchwegs von Zahlen ungleich Null umgeben ist. Bemerkenswert ist schließlich, daß die Zahl T unabhängig von der Wahl $j \in \overline{i(n)}$ ist.

In Abbildung 1.4 wollen wir diese Überlegungen noch einmal veranschaulichen. Alle Einträge seien modulo p reduziert und die mit $*$ bezeichneten Stellen sind stets ungleich Null modulo p.

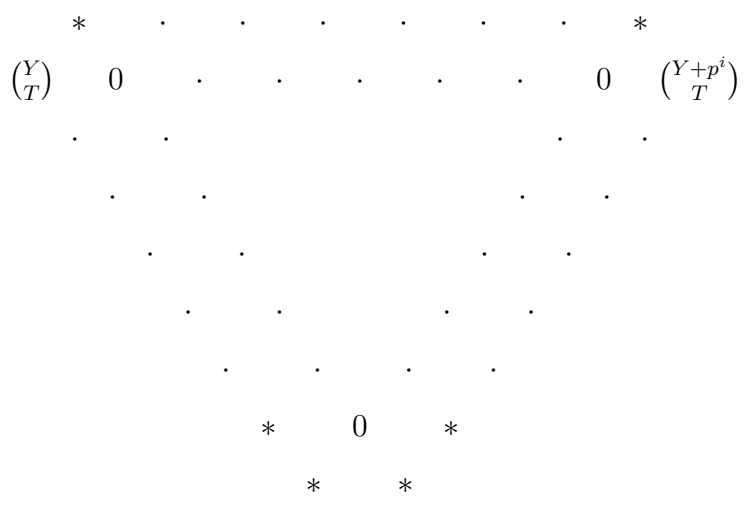


Abbildung 1.4: Konstruktion des umgebenden ∇^i für (n, j)

Zusammenfassend kann man also folgendes sagen: Bei gegebenen $i \in \mathbb{N}^+$ und $n, j \in \mathbb{N}$ gilt $(n, j) \in \overline{i}$ genau dann, wenn die Stelle (n, j) des Pascal–Dreiecks modulo p in einem maximalen Teildreieck ∇^i liegt. Die Klasse $\overline{\infty}$ entspricht dem unendlichen Dreieck ∇.

Bemerkung 1.4.5 Man könnte nun meinen, daß die in Satz 1.4.4 definierte Funktion $T = T(i, n)$ bei festem n und variablem i genau so viele verschiedene Werte annimmt, wie es verschiedene Klassen von Nullen gibt, die von der n–ten Zeile getroffen werden. An dem einfachen Beispiel einer Zahl n mit $n_0 = p - 1$ sehen wir, daß dies noch nicht der richtige Zugang sein kann, weil einerseits die Funktion $T(i, n)$ für $i = 0$ und $i = 1$ verschiedene Werte liefert, andererseits aber $\overline{1(n)} = \emptyset$ gilt.

Wir hätten gerne eine Funktion, deren Werte genau den obersten Zeilen jener ∇^i's entsprechen, die von der n–ten Zeile in Δ getroffen werden. Bis auf einen zusätzlichen Wert wird dieser Wunsch durch die sogenannte „top line"–Funktion realisiert werden.

Ähnlich wie in Satz 1.4.3 wollen wir daher im zweiten Argument der Funktion $T(i, n)$ von n zu $n + 1 =: b$ übergehen.

Definition 1.4.6 *Für $n \in \mathbb{N}$ und $b := n + 1$ sei die „top line"–Funktion $T(R, b)$ wie folgt definiert:*

$$T(R, b) := b - \sum_{\lambda=0}^{R-1} b_\lambda p^\lambda \text{ für alle } R \in \mathbb{N} \cup \{\infty\}. \tag{1.9}$$

Wegen (1.4) und (1.5) erfüllt die „top line"–Funktion $T(R, b)$ folgende Relation:

$$0 = T(\infty, b) \leq \ldots \leq T(M + 1, b) < T(M, b) = \ldots = T(0, b) = b. \tag{1.10}$$

Wenn wir $R \in \mathbb{N}$ entsprechend groß wählen, dann nimmt $T(R, b)$ also den Wert 0 an.

Worin liegt nun der wesentliche Vorteil von $T(R, b)$ gegenüber $T(R, n)$? - Für eine nichtleere Menge $\overline{i(n)} \neq \overline{\infty}$ folgt aus (1.5), daß $i > M$ ist. Die Zahl $T(i, b)$ stimmt in diesem Fall wegen (1.6) mit der entsprechenden Schranke $T = T(i, n)$ in (1.7) überein. Für $i \leq M$ bleibt $T(i, b) = b$ im Gegensatz zu $T(i, n)$ aber konstant, und somit entspricht die (wegen der Werte 0 und b) um zwei verringerte Mächtigkeit der Wertemenge von $T(R, b)$ exakt der Anzahl der verschiedenen nichtleeren Mengen $\overline{i(n)}$ $(i \neq \infty)$.

Aus (1.5) folgern wir also

$$\overline{i_1(n)} \neq \emptyset \neq \overline{i_2(n)} \text{ und } i_1 > i_2 \quad \Rightarrow \quad T(i_1, b) < T(i_2, b). \tag{1.11}$$

Während für $i \in \{1, 2, \ldots, M\}$ die Menge $\overline{i(n)}$ leer und $T(i, b) = b > n$ ist, folgt bei $\overline{i(n)} = \emptyset$ wegen Formel (1.5) die Gleichung

$$T(i, b) = T(i + 1, b) \quad \text{für} \quad i \in \{M + 1, M + 2, \ldots\}. \tag{1.12}$$

Aus (1.11) und (1.12) folgt die (nicht strenge) Anti–Monotonie

$$i_1 > i_2 \quad \Rightarrow \quad T(i_1, b) \leq T(i_2, b).$$

Außerdem erhalten wir bei $\overline{i(n)} \neq \emptyset$ die Gleichung

$$T(i,b) - 1 = \langle \ldots, n_{i+1}, n_i - 1, p-1, \ldots, p-1 \rangle = \max \overline{i(n)}, \tag{1.13}$$

weil auf Grund von $\overline{i(n)} \neq \emptyset$ mindestens eine der Ziffern $n_0, n_1, \ldots, n_{i-1}$ kleiner als $p-1$ ist und $b_i = n_i > 0$ gilt.

1.4.3 Die Summenfunktion $\Sigma(i,n)$

In diesem Abschnitt wollen wir jetzt noch abzählen, wie viele Nullen von einem Typ größer oder gleich i sich in einer festen Zeile n des Pascal–Dreiecks $\Delta(p)$ befinden.

Definition 1.4.7 *Für $n \in \mathbb{N}$ und $i \in \mathbb{N}^+$ sei die Summenfunktion Σ folgendermaßen definiert:*

$$\Sigma(i,n) := \sum_{\eta=i}^{\infty} \Phi(\eta, n)$$

Ähnlich wie für die Anzahlfunktion Φ haben wir auch für die Summenfunktion Σ einen geschlossenen Ausdruck gefunden.

Satz 1.4.8 *Für $n \in \mathbb{N}$ und $i \in \mathbb{N}^+$ folgt*

$$\Sigma(i,n) \;=\; n + 1 - (1 + \sum_{\mu=0}^{i-1} n_\mu p^\mu) \prod_{\lambda=i}^{\infty} (n_\lambda + 1) \tag{1.14}$$

Beweis: (a) Wir bestimmen vorerst alle natürlichen Zahlen $j = \langle j_\lambda \rangle$ mit $j \preceq n$. Jede einzelne Ziffer j_λ kann natürlich auf exakt $n_\lambda + 1$ Arten gewählt werden, und deshalb gibt es

$$\prod_{\lambda=0}^{\infty} (n_\lambda + 1) = n + 1 - \Sigma(1,n) \tag{1.15}$$

solche Elemente. Die Behauptung (1.14) ist also für $i = 1$ erfüllt. Tatsächlich ist (1.15) auch durchaus bekannt (vgl. etwa [12, 98]).

(b) Nehmen wir nun an, daß (1.14) bereits für $i \geq 1$ gezeigt worden sei. Aus (1.2) und (1.14) folgt dann

$$\Sigma(i+1,n) = \Sigma(i,n) - \Phi(i,n)$$

$$\begin{aligned}
&= n+1-(1+\sum_{\xi=0}^{i-1} n_\xi p^\xi)\prod_{\nu=i}^{\infty}(n_\nu+1) - (p^i - 1 - \sum_{\mu=0}^{i-1} n_\mu p^\mu) n_i \prod_{\lambda=i+1}^{\infty}(n_\lambda+1)\\
&= n+1-\{[(1+\sum_{\xi=0}^{i-1} n_\xi p^\xi)(n_i+1)] + [p^i - 1 - \sum_{\mu=0}^{i-1} n_\mu p^\mu] n_i\} \prod_{\nu=i+1}^{\infty}(n_\nu+1)\\
&= n+1-(1+\sum_{\xi=0}^{i} n_\xi p^\xi) \prod_{\nu=i+1}^{\infty}(n_\nu+1),
\end{aligned}$$

womit alles gezeigt worden ist. □

Bemerkung 1.4.9 Die Formel (1.14) hat die nette Eigenschaft, daß mit wachsendem i eine Ziffer nach der anderen vom Produkt rechts zur Summe nach links wandert, wobei man beachte, daß die Ziffern in der Summe mit, im Produkt jedoch ohne ihren Stellenwert eingehen.

Nach den vorigen Überlegungen überrascht es nicht mehr, daß sich hierbei der Wert der Funktion nicht zwingend verändert. Dies möchten wir an einem Beispiel illustrieren:

Es sei $p = 3$ und $n = 98$, also in der p–adischen Darstellung

$$n = \langle 1,0,1,2,2\rangle.$$

Aus der Darstellung $b = n+1 = \langle 1,0,2,0,0\rangle$ sehen wir, daß die Mengen $\overline{1(n)}$, $\overline{2(n)}$ und $\overline{3(n)}$ leer sind, während es sehr wohl Nullen der Klasse 4 in der n–ten Zeile gibt.

Die Funktion Σ nimmt also nur die Werte 0 und $\#\overline{4(n)}$ an. Das prüfen wir jetzt aufs Exempel:

$$\begin{aligned}
\Sigma(1,98) &= 99-(1+2)\cdot 3\cdot 2\cdot 1\cdot 2 = 63\\
\Sigma(2,98) &= 99-(1+2+2\cdot 3)\cdot 2\cdot 1\cdot 2 = 63\\
\Sigma(3,98) &= 99-(1+2+2\cdot 3+1\cdot 9)\cdot 1\cdot 2 = 63\\
\Sigma(4,98) &= 99-(1+2+2\cdot 3+1\cdot 9+0\cdot 27)\cdot 2 = 63\\
\Sigma(5,98) &= 99-(1+2+2\cdot 3+1\cdot 9+0\cdot 27+1\cdot 81) = 0
\end{aligned}$$

Wir wollen auch eine Gegenüberstellung der Werte $T(i,n)$ und $T(i,b)$ durchführen:

i	$T(i,n)$	$T(i,b)$
0	98	99
1	96	99
2	90	99
3	81	81
4	81	81
5	0	0

Man sieht hier noch einmal, daß in der Funktion T im zweiten Argument der Wert $b := n + 1$ der Zahl n vorzuziehen ist.

Nach diesem Beispiel dürfte das Hantieren mit den eingeführten Funktionen keinerlei Schwierigkeiten mehr bereiten, womit wir im nächsten Kapitel zu deren Anwendungen in der Geometrie kommen können. Davor wird im nun folgenden Anhang die Fraktalstruktur des modulo p reduzierten Pascal–Dreiecks durch einige Beispiele illustriert.

1.5 Anhang

Im folgenden haben wir für die Werte $p \in \{2, 3, 7\}$ das Pascal–Dreieck modulo p bis zu einer bestimmten Zeile berechnet und die einzelnen Restklassen durch verschiedene Farben ersetzt.

Beispiel 1

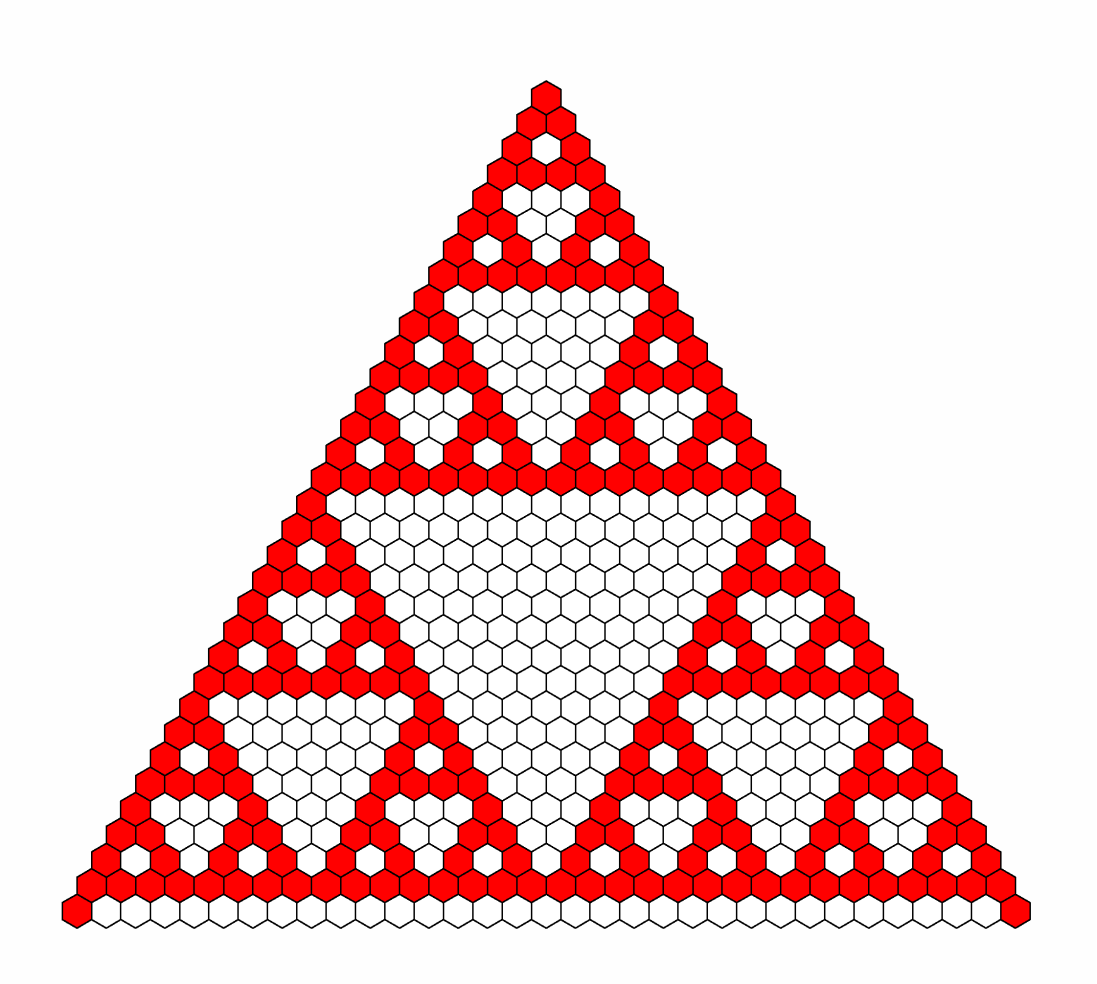


Abbildung 1.5: $\Delta(2)$ bis zur Zeile 32

Beispiel 2

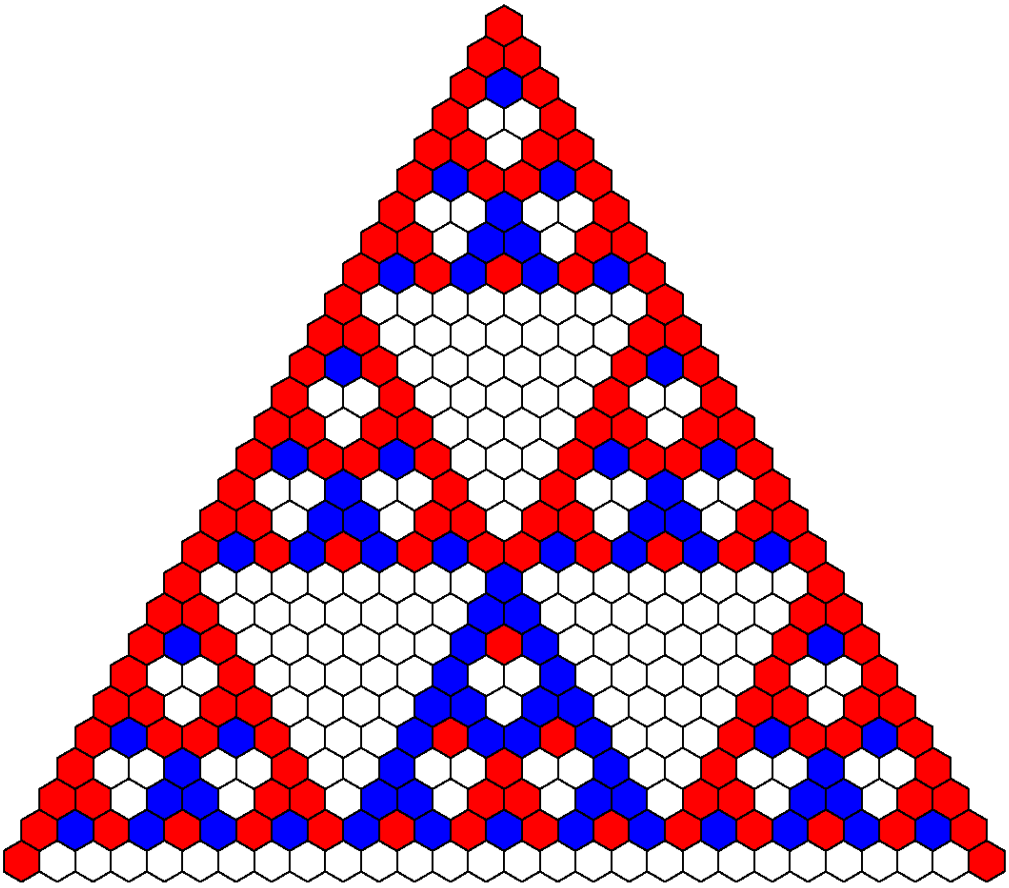


Abbildung 1.6: $\Delta(3)$ bis zur Zeile 27

Beispiel 3

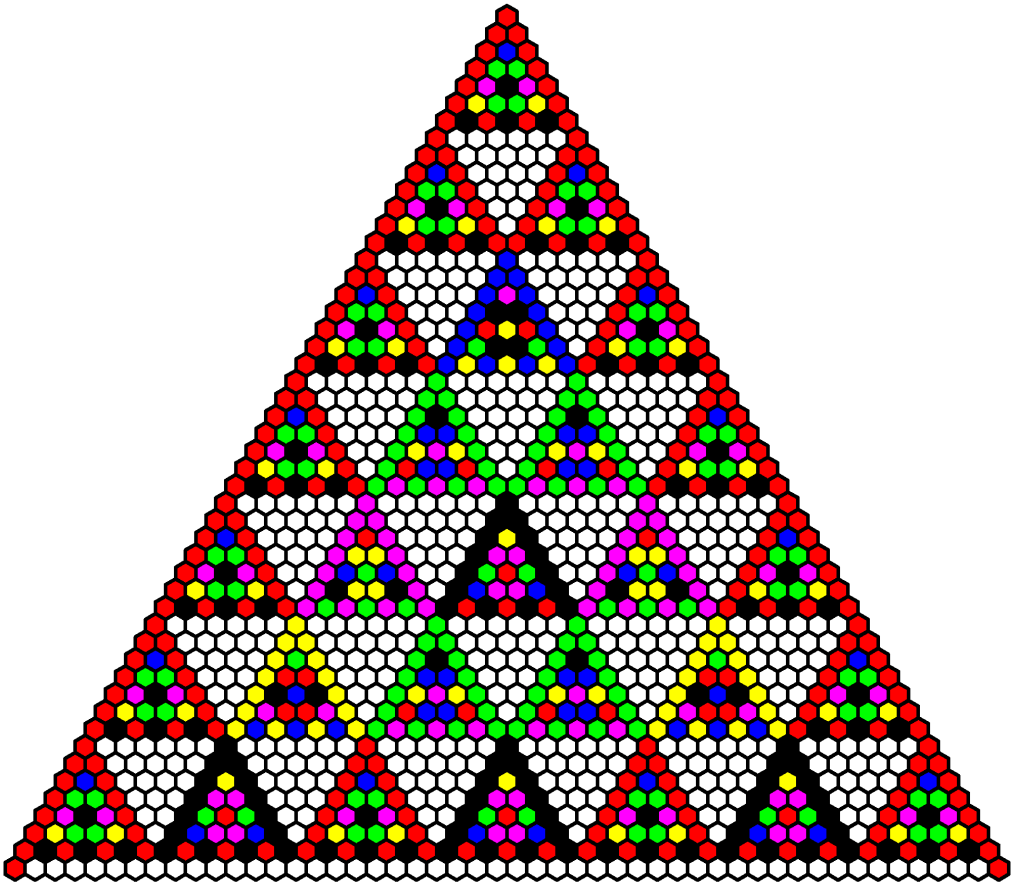


Abbildung 1.7: $\Delta(7)$ bis zur Zeile 49

Kapitel 2

Rationale Normkurven

In diesem Kapitel wird gezeigt, wie man eine rationale Normkurve Γ im n-dimensionalen projektiven Raum $\mathrm{PG}(n,K)$ als Bild einer projektiven Geraden $\mathrm{PG}(1,K)$ erhält. Projektivitäten in $\mathrm{PG}(1,K)$ induzieren in kanonischer Weise Bijektionen auf Γ, die man zu Kollineationen auf $\mathrm{PG}(n,K)$ fortsetzen kann. Wir zeigen, daß sich diese Abbildungen stets als Produkt dreier verschiedener Typen von Kollineationen schreiben lassen.

Darüber hinaus stellen wir eine nicht–iterative Differentiation vor, die es im Gegensatz zur üblichen formalen Differentiation gestattet, für beliebige Charakteristik $\mathrm{char}K = p$ die diversen Schmiegräume in den Normkurvenpunkten zu definieren. Dadurch treten letztlich jene Binomialkoeffizienten auf, die die Brücke von der Geometrie zur elementaren Zahlentheorie herstellen.

2.1 Die Veronese-Abbildung

Definition 2.1.1 *Unter einer rationalen Normkurve versteht man die Punktmenge*

$$\Gamma := \{K(1,t,\ldots,t^n) \mid t \in K \cup \{\infty\}\} \tag{2.1}$$

und jede dazu projektiv äquivalente Menge.

Man beachte, daß der formale Parameterwert $t = \infty$ den letzten Grundpunkt $K(0,\ldots,0,1)$ bezeichnet.

Definition 2.1.2 *Die Abbildung* $\sigma : \mathrm{PG}(1,K) \to \mathrm{PG}(n,K)$

$$K\begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \;\mapsto\; K\begin{pmatrix} x_0^n \\ x_0^{n-1}x_1 \\ \vdots \\ x_0x_1^{n-1} \\ x_1^n \end{pmatrix} \tag{2.2}$$

heißt Veronese-Abbildung.

Bemerkung 2.1.3 Da die Koordinatenfunktionen des Bildpunktes durchwegs homogene Polynome vom Grad n sind, ist σ wohldefiniert und tatsächlich eine Punktabbildung.

Für $x_0 = 0$ ergibt sich das Bild von $P_1 \in \mathrm{PG}(1, K)$ zu $P_n \in \mathrm{PG}(n, K)$. Im anderen Fall ($x_0 \neq 0$) setzen wir $t = x_1/x_0$, wodurch

$$K(1, t) \mapsto K(1, t, \ldots, t^n)$$

folgt. Die projektive Gerade $\mathrm{PG}(1, K)$ wird unter σ also bijektiv auf eine rationale Normkurve Γ in $\mathrm{PG}(n, K)$ abgebildet.

Sei nun μ eine Projektivität in $\mathrm{PG}(1, K)$, also

$$\mathrm{PG}(1, K) \quad \xrightarrow{\mu} \quad \mathrm{PG}(1, K),$$

dann wird dadurch eine Bijektion $\Gamma \to \Gamma$ induziert, die zu einer projektiven Kollineation $\mathrm{PG}(n, K) \longrightarrow \mathrm{PG}(n, K)$ fortgesetzt werden kann. Die Abbildung 2.1 unterstützt diese Vorstellung.

$$\begin{array}{ccc} \mathrm{PG}(1, K) & \xrightarrow{\mu} & \mathrm{PG}(1, K) \\ \sigma \big\downarrow & & \big\downarrow \sigma \\ \Gamma & \xrightarrow{\sigma \circ \mu \circ \sigma^{-1}} & \Gamma \end{array}$$

Abbildung 2.1: Induzierte Bijektion auf Γ

Bemerkungen 2.1.4

1. Für $\#K \geq n + 2$ erhalten wir mit [9, S. 214], daß die Fortsetzung der Bijektion $\sigma \circ \mu \circ \sigma^{-1}$ zu einer Kollineation auf $\mathrm{PG}(n, K)$ eindeutig ist. Im restlichen Teil der Arbeit werden wir uns häufig auf diesen Fall beschränken.

2. Gilt etwa $\#K = n + 1$, dann bildet Γ eine Fundamentalmenge. Wegen $K = GF(p^h)$ erhalten wir $\#\mathrm{Aut}(K) = h$. Jede Bijektion $\Gamma \to \Gamma$ induziert genau h Kollineationen auf $\mathrm{PG}(n, K)$, von denen genau eine projektiv ist.

3. Für $\#K < n + 1$ gilt: Je kleiner der Grundkörper ist, desto mehr Kollineationen werden von einer Bijektion $\Gamma \to \Gamma$ induziert (vgl. dazu auch [10, S. 6]).

Es stellt sich natürlich die Frage, wie man aus gegebenem μ eine induzierte Kollineation κ auf $\mathrm{PG}(n, K)$ erhält. Dies soll jetzt kurz erläutert werden:

1. Eine Kollineation μ auf $\mathrm{PG}(1,K)$ wird durch eine reguläre (also invertierbare) (2×2)–Matrix

$$A=\begin{pmatrix} a_{00} & a_{01}\\ a_{10} & a_{11}\end{pmatrix}$$

und einen Körperautomorphismus $\zeta\in\mathrm{Aut}(K)$ beschrieben:

$$\mu:\quad K\begin{pmatrix} x_0\\ x_1\end{pmatrix}\ \mapsto\ K\left(A\begin{pmatrix}\zeta(x_0)\\ \zeta(x_1)\end{pmatrix}\right)$$

2. Wir setzen vorerst $\zeta=\mathrm{id}_K$ und betrachten eine Matrix $A\in\mathrm{GL}(2,K)$. Im folgenden zeigen wir, daß es eine Matrix $B\in\mathrm{GL}(n+1,K)$ gibt, so daß κ mit

$$\begin{aligned}\kappa:\qquad \mathrm{PG}(n,K)\ &\to\ \mathrm{PG}(n,K)\\ K\begin{pmatrix} y_0\\ y_1\\ \vdots\\ y_{n-1}\\ y_n\end{pmatrix}\ &\mapsto\ K\left(B\begin{pmatrix} y_0\\ y_1\\ \vdots\\ y_{n-1}\\ y_n\end{pmatrix}\right)\end{aligned}$$

die besagte Kollineation liefert.

Dazu betrachten wir den Polynomring $K[X_0,X_1]$ in X_0,X_1 über K, der einen Vektorraum über K bildet. Bei festem n bilden die homogenen Polynome vom Grad n gemeinsam mit dem Nullpolynom einen Unterraum $U(X_0,X_1,n+1)$ der Dimension $n+1$, wobei die speziellen Polynome

$$X_0^n, X_0^{n-1}X_1,\ldots,X_0X_1^{n-1},X_1^n \tag{2.3}$$

eine Basis bestimmen.
Wir betrachten vorerst auf $U(X_0,X_1,2)$ eine lineare Abbildung

$$\begin{pmatrix} X_0\\ X_1\end{pmatrix}\ \mapsto\ A\begin{pmatrix} X_0\\ X_1\end{pmatrix}=\begin{pmatrix} a_{00}X_0+a_{01}X_1\\ a_{10}X_0+a_{11}X_1\end{pmatrix}$$

mit einer regulären Matrix A. Die Inverse A^{-1} schreibt sich dann in der Form

$$A^{-1}=\frac{1}{\det A}\begin{pmatrix} a_{11} & -a_{01}\\ -a_{10} & a_{00}\end{pmatrix}=:\begin{pmatrix} a_{00}^* & a_{01}^*\\ a_{10}^* & a_{11}^*\end{pmatrix}$$

Jetzt definieren wir eine lineare Abbildung auf $U(X_0,X_1,n+1)$, indem wir die Bilder der Basis (2.3) angeben:

$$X_0^{n-i}X_1^i\ \mapsto\ (a_{00}X_0+a_{01}X_1)^{n-i}(a_{10}X_0+a_{11}X_1)^i\quad i=0,1,\ldots,n \tag{2.4}$$

Diese Abbildung ist bijektiv, weil für jedes Element

$$\sum_{i=0}^{n} c_i X_0^{n-i} X_1^i \ \in \ U(X_0, X_1, n+1)$$

ein Urbild

$$\sum_{i=0}^{n} c_i (a_{00}^* X_0 + a_{01}^* X_1)^{n-i} (a_{10}^* X_0 + a_{11}^* X_1)^i \ \in \ U(X_0, X_1, n+1)$$

existiert und aus der Surjektivität die Injektivität folgt.

Es gibt also eine reguläre $(n+1) \times (n+1)$–Matrix B mit

$$B \begin{pmatrix} X_0^n \\ X_0^{n-1} X_1 \\ \vdots \\ X_0 X_1^{n-1} \\ X_1^n \end{pmatrix} = \begin{pmatrix} (a_{00} X_0 + a_{01} X_1)^n \\ (a_{00} X_0 + a_{01} X_1)^{n-1} (a_{10} X_0 + a_{11} X_1)^1 \\ \vdots \\ (a_{00} X_0 + a_{01} X_1)^1 (a_{10} X_0 + a_{11} X_1)^{n-1} \\ (a_{10} X_0 + a_{11} X_1)^n \end{pmatrix}.$$

Man sieht leicht, daß die so konstruierte Matrix B die gewünschte Kollineation auf $\mathrm{PG}(n, K)$ induziert, also die Einschränkung auf Γ die entsprechende Bijektion liefert, indem man für die Unbestimmten X_0 und X_1 Koordinaten x_0 und x_1 einsetzt.

3. Jetzt wählen wir einen beliebigen Körperautomorphismus ζ und für A die Einheitsmatrix E_2. Wir überlegen uns, daß die entsprechende Kollineation κ auf $\mathrm{PG}(n, K)$ durch denselben Automorphismus ζ und die Einheitsmatrix E_{n+1} gebildet wird:

   Unterwerfen wir nämlich einen Punkt $K \begin{pmatrix} x_0 \\ x_1 \end{pmatrix}$ aus $\mathrm{PG}(1, K)$ zuerst der Veronese-Abbildung (2.2) und dann der Kollineation κ, dann erhalten wir denselben Bildpunkt wie nach Hintereinanderausführung der Kollineation μ auf $\mathrm{PG}(1, K)$ und der Veronese-Abbildung σ, nämlich

$$K \begin{pmatrix} \zeta(x_0^n) \\ \zeta(x_0^{n-1} x_1) \\ \vdots \\ \zeta(x_0 x_1^{n-1}) \\ \zeta(x_1^n) \end{pmatrix}.$$

4. Abschließend erkennen wir nun leicht (indem wir die Ergebnisse der beiden letzten Punkte zusammenfassen), daß bei beliebigem Körperautomorphismus ζ und Matrix $A \in \mathrm{GL}(2, K)$ die Kollineation κ mit

$$\begin{array}{rccc} \kappa: & \mathrm{PG}(n,K) & \to & \mathrm{PG}(n,K) \\ & K\begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_{n-1} \\ y_n \end{pmatrix} & \mapsto & K\left(B\begin{pmatrix} \zeta(y_0) \\ \zeta(y_1) \\ \vdots \\ \zeta(y_{n-1}) \\ \zeta(y_n) \end{pmatrix}\right) \end{array}$$

das Gewünschte leistet.

Folgende Beispiele sollen erstens diese Überlegungen veranschaulichen, indem zu vorgegebenen Matrizen A entsprechende Matrizen B berechnet werden, und zweitens wichtige Aussagen der nächsten Kapiteln vorbereiten.

2.1.1 Beispiele

1. Wenn wir auf der projektiven Geraden $\mathrm{PG}(1, K)$ den Punkt $K\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ als Fernpunkt auffassen, wird eine Streckung mit Zentrum $K\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ um den Faktor $a \neq 0$ durch eine Projektivität mit Matrix

$$A = \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}$$

gegeben. Für $a = 1$ handelt es sich um die Identität, sonst ($a \neq 0, 1$) ist die Projektivität hyperbolisch.

Wie man sich leicht überlegt, ist die gemäß (2.4) induzierte Matrix B eine Diagonalmatrix mit den Potenzen von a in der Hauptdiagonale, also

$$B = \mathrm{diag}(1, a, a^2, \ldots, a^n).$$

2. Einer Translation um b (mit gleichem Fernpunkt wie oben) entspricht die Matrix

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

Die inverse Abbildung ist eine Schiebung zum Vektor $-b$, und daher erhält man A^{-1} durch den Übergang von b nach $-b$.

Für $b = 0$ erhalten wir die Identität, in allen anderen Fällen ist die Projektivität parabolisch.

Nach (2.4) wird die durch A induzierte automorphe Kollineation auf Γ durch die Matrix

$$B := \begin{pmatrix} \binom{0}{0} & 0 & 0 & \dots & 0 \\ \binom{1}{0}b & \binom{1}{1} & 0 & \dots & 0 \\ \binom{2}{0}b^2 & \binom{2}{1}b & \binom{2}{2} & \dots & 0 \\ \vdots & & & \ddots & \vdots \\ \binom{n}{0}b^n & \binom{n}{1}b^{n-1} & \binom{n}{2}b^{n-2} & \dots & \binom{n}{n} \end{pmatrix} \tag{2.5}$$

beschrieben. Die inverse Matrix B^{-1} erhält man ebenso wie A^{-1} durch den Übergang $b \mapsto -b$. Dieser Umstand wird in den nächsten Abschnitten entscheidend ausgenützt.

3. Eine Koordinatenvertauschung $x_0 \leftrightarrow x_1$, also

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

führt auf die Matrix

$$B = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & 1 & 0 \\ \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & 1 & \dots & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 \end{pmatrix}.$$

Die Matrix A induziert jedenfalls eine involutorische Projektivität, die für $\mathrm{char}K = 2$ parabolisch und sonst hyperbolisch ist.

Wir werden im folgenden Kapitel sehen, daß in diesen Beispielen die Antwort auf die Frage nach allen automorphen Kollineationen einer rationalen Normkurve Γ zu suchen ist.

2.2 Die projektiven automorphen Kollineationen

Da wir in diesem Abschnitt die Voraussetzung $\#K \geq n + 2$ treffen und aus den Bemerkungen 2.1.4 wissen, daß in diesem Fall die Matrizen A und B einander

bis auf einen Faktor aus K wechselseitig bedingen, werden wir im folgenden alle Matrizen A, die eine Projektivität in $\mathrm{PG}(1,K)$ induzieren, also alle regulären (2×2)–Matrizen, genauer untersuchen (vgl. [1, S. 320–321]).

Lemma 2.2.1 *Eine Matrix A, die eine Projektivität in $\mathrm{PG}(1,K)$ induziert, entspricht bis auf einen Faktor aus K einem Produkt der regulären Matrizen*

$$\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Beweis: Da die Matrix A eine Projektivität induziert, muß sie stets regulär sein. Das Körperelement a unterliegt in obigem Lemma also der Einschränkung $a \neq 0$.

Der Beweis verläuft nun in mehreren Schritten.

1. Im Fall $a_{01} = 0$, also $A = \begin{pmatrix} a_{00} & 0 \\ a_{10} & a_{11} \end{pmatrix}$, gilt $a_{00}a_{11} \neq 0$. Die Matrix A ist dann ein Vielfaches von
$$\begin{pmatrix} 1 & 0 \\ b & a \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}.$$

2. Wenn wir die obige Matrixgleichung von rechts mit $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ multiplizieren, dann ergibt das die Matrix $\begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}$. Das Lemma greift also auch für Matrizen A mit $a_{00} = 0$.

3. Setzen wir nun $a_{00} \neq 0$ voraus, dann können wir o.B.d.A. von der Matrix
$$A = \begin{pmatrix} 1 & a_{01} \\ a_{10} & a_{11} \end{pmatrix}.$$
ausgehen und außerdem noch $a_{01} \neq 0$ voraussetzen, weil der andere Fall schon positiv beantwortet worden ist. Mit dem Ansatz
$$A = \begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ d & c \end{pmatrix}$$
folgt
$$\begin{aligned} d &= 1 \\ a + bd &= a_{10} \\ c &= a_{01} \\ bc &= a_{11} \end{aligned}$$

und somit

$$\begin{aligned} a &= a_{10} - a_{11}/a_{01} \\ b &= a_{11}/a_{01} \\ c &= a_{01} \\ d &= 1. \end{aligned}$$

Man beachte, daß das Gleichungssystem für a, b, c und d wegen $a_{01} \neq 0$ lösbar ist und aus $\det A \neq 0$ auch $a \neq 0$ folgt. Wir können die Matrix A also tatsächlich als Produkt von Matrizen schreiben, wie sie in Lemma 2.2.1 vorgestellt worden sind. □

Da es sich bei den Matrizen in Lemma 2.2.1 genau um die in Abschnitt 2.1.1 vorgestellten handelt, haben wir somit folgendes Resultat gewonnen:

Satz 2.2.2 *Jede automorphe projektive Kollineation der rationalen Normkurve* Γ *erhält man als Produkt jener drei Typen von Kollineationen, welche durch die Matrizen*

$$\operatorname{diag}(1, a, \ldots, a^n), \begin{pmatrix} \binom{0}{0} & 0 & 0 & \ldots & 0 \\ \binom{1}{0}b & \binom{1}{1} & 0 & \ldots & 0 \\ \binom{2}{0}b^2 & \binom{2}{1}b & \binom{2}{2} & \ldots & 0 \\ \vdots & & & \ddots & \vdots \\ \binom{n}{0}b^n & \binom{n}{1}b^{n-1} & \binom{n}{2}b^{n-2} & \ldots & \binom{n}{n} \end{pmatrix}, \begin{pmatrix} 0 & 0 & \ldots & 0 & 1 \\ 0 & 0 & \ldots & 1 & 0 \\ \vdots & \vdots & \ldots & \vdots & \vdots \\ 0 & 1 & \ldots & 0 & 0 \\ 1 & 0 & \ldots & 0 & 0 \end{pmatrix}$$

induziert werden. Dabei ist $\#K \geq n + 2$ *vorausgesetzt.*

2.3 Die Schmiegunterräume

Wenn Kurven ganzrational parametrisiert sind und der zu Grunde liegende Skalarkörper die Charakteristik 0 hat, dann braucht man in Analogie zur Differentialgeometrie lediglich die Koordinatenfunktionen formal differenzieren, um die diversen Schmiegräume in den Kurvenpunkten zu erklären.

Bei $\operatorname{char} K = p > 0$ führt das aber zu Problemen, weil spätestens nach p Differentiationsprozessen alle Funktionen identisch verschwinden und daher für eine Kurve Γ auf diese Art und Weise höchstens $p - 1$ nichtverschwindende Ableitungsvektoren berechnet werden könnten.

Einen Ausweg aus dieser Sackgasse finden wir in der nicht–iterativen Differentiation von Polynomen nach H. Hasse, F.K. Schmidt und O. Teichmüller, deren wichtigste Eigenschaften wir hier noch besprechen möchten (vgl. etwa [8] oder [14, 1.3]).

2.3.1 Die Differentiation nach H. Hasse

Wenden wir den üblichen Differentialoperator $\frac{\mathrm{d}}{\mathrm{d}t}$ auf das Polynom $q(t) = t^n \in K[t]$ sukzessive k Mal an, dann erhalten wir bekanntlich

$$\frac{\mathrm{d}^k q(t)}{\mathrm{d}t^k} := n(n-1)\dots(n-k+1)t^{n-k}.$$

Natürlich ist diese Differentiation iterativ, im Gegensatz zur nicht–iterativen „Hasse–Differentiation“ D_t, die durch

$$(\mathrm{D}_t)^k q(t) := \binom{n}{k} t^{n-k}$$

definiert ist. Ist $\mathrm{char}K$ kein Teiler von $k!$, so gilt weiters

$$(\mathrm{D}_t)^k q(t) = \frac{1}{k!}\frac{\mathrm{d}^k q(t)}{\mathrm{d}t^k}.$$

Bemerkung 2.3.1 Wäre D_t iterativ, dann müßte für $k, l \in K$ stets

$$\binom{n}{k}\binom{n-k}{l} = \binom{n}{k+l},$$

also $k!l! = (k+l)!$ gelten, was i.a. nicht der Fall ist.

Wenn man nun einen Vektor koordinatenweise k Mal differenziert, dann unterscheiden sich die beiden Differentiationsformen bei $\mathrm{char}K = 0$ nur durch einen Faktor aus $K\setminus\{0\}$. Die Vektoren bestimmen also denselben Punkt im projektiven Raum.

Bei $\mathrm{char}K = p$ zeigt das einfache Beispiel

$$\begin{aligned}(\mathrm{D}_t)^p t^p &= \binom{p}{p} = 1\\ \frac{\mathrm{d}^p}{\mathrm{d}t^p}t^p &= p! \equiv 0 \pmod{\mathrm{char}K},\end{aligned}$$

daß dies bei Charakteristik p nicht zutrifft.

2.3.2 Berechnung der Ableitungspunkte

Da wir rationale Normkurven vorerst für beliebige Körper betrachten, benützen wir die eben besprochene Hasse–Differentiation, um in Anlehnung an [9] die Ableitungspunkte für eine rationale Normkurve Γ zu berechnen.

In den Spalten der Matrix

$$C_t := \begin{pmatrix} \binom{0}{0} & 0 & 0 & \dots & 0 \\ \binom{1}{0}t & \binom{1}{1} & 0 & \dots & 0 \\ \binom{2}{0}t^2 & \binom{2}{1}t & \binom{2}{2} & \dots & 0 \\ \vdots & & & \ddots & \vdots \\ \binom{n}{0}t^n & \binom{n}{1}t^{n-1} & \binom{n}{2}t^{n-2} & \dots & \binom{n}{n} \end{pmatrix} \tag{2.6}$$

stehen (von links nach rechts) der Vektor c_t und die mittels Hasse–Differentiation erhaltenen Ableitungsvektoren $c_t',\ c_t'',\ \dots, c_t^{(n)}$, die für alle $t \in K$ *die Ableitungspunkte* $Kc_t', Kc_t'', \dots, Kc_t^{(n)}$ zum Normkurvenpunkt Kc_t der Parameterdarstellung (2.1) *bestimmen.*

Für $t = \infty$ setzen wir außerdem $c_\infty^{(k)} := (\delta_{0,n-k}, \dots, \delta_{n,n-k})$.

Jetzt können wir wie gewohnt definieren:

Definition 2.3.2 *Der k–Schmiegraum* $\mathcal{S}_t^{(k)}\Gamma$ $(k \in \{-1, 0, \dots, n\})$ *von* Γ *im Punkt* Kc_t *ist die projektive Hülle über die Punkte* $Kc_t, Kc_t', \dots, Kc_t^{(k)}$.

Bemerkungen 2.3.3

1. Alle Schmiegräume in Kc_t bilden eine Kette mit $\dim \mathcal{S}_t^{(k)}\Gamma = k$.

2. Die Matrix C_t ist unter zweierlei Gesichtspunkten zu sehen:

   (a) In der Matrix C_t sind für alle Werte $t \in K$ zu den Punkten von Γ die zugehörigen Ableitungspunkte gespeichert.

   (b) Durch C_t wird aber nach Abschnitt 2.1.1, Beispiel 2, auch eine automorphe Kollineation von Γ definiert, die einen Punkt zum Parameterwert s stets auf jenen zum Wert $s + t$ „verschiebt“.

3. Wir müssen uns überlegen, daß die Schmiegunterräume mit Γ gegen Kollineationen invariant verknüpft sind, die „Hasse-Differentiation“ also mit semilinearen Bijektionen vertauschbar ist. Wäre das nämlich nicht der Fall, dann würden alle in dieser Arbeit erzielten Ergebnisse von der speziellen Parametrisierung (2.1) abhängen.

   Wir betrachten eine semilineare Abbildung f auf K^{n+1}

$$\begin{array}{rccc} f: & K^{n+1} & \to & K^{n+1} \\ & \begin{pmatrix} p_0 \\ p_1 \\ \vdots \\ p_n \end{pmatrix} & \mapsto & A \begin{pmatrix} \zeta(p_0) \\ \zeta(p_1) \\ \vdots \\ \zeta(p_n) \end{pmatrix}, \end{array}$$

mit einer regulären Matrix $A \in K^{(n+1)\times(n+1)}$ und einem Körperautomorphismus $\zeta \in \mathrm{Aut}(K)$. Wir setzen f zu einer Abbildung F auf $K[t]^{n+1}$ fort:

$$\begin{array}{rccc} F: & K[t]^{n+1} & \to & K[t]^{n+1} \\ & \begin{pmatrix} p_0(t) \\ p_1(t) \\ \vdots \\ p_n(t) \end{pmatrix} & \mapsto & A \begin{pmatrix} \zeta(p_0(t)) \\ \zeta(p_1(t)) \\ \vdots \\ \zeta(p_n(t)) \end{pmatrix} \end{array}$$

Dabei definieren wir für alle $i \in \{0, 1, \ldots, n\}$

$$\zeta(p_i(t)) = \zeta(\sum_{\mu=0}^{r_i} p_{i\mu} t^\mu) := \sum_{\mu=0}^{r_i} \zeta(p_{i\mu}) t^\mu.$$

Dadurch erhalten wir die für alle $x \in K$ gültige Beziehung:

$$f \begin{pmatrix} p_0(x) \\ p_1(x) \\ \vdots \\ p_n(x) \end{pmatrix} = F \begin{pmatrix} p_0(\zeta(x)) \\ p_1(\zeta(x)) \\ \vdots \\ p_n(\zeta(x)) \end{pmatrix}$$

Die „Hasse-Differentiation“ ist genau dann mit allen Kollineationen vertauschbar, wenn für jede semilineare Abbildung f mit regulärer Matrix A und alle $s \in \mathbb{N}$ die Identität

$$f \begin{pmatrix} \mathrm{D}_t^{(s)}(p_0(t))_{t=x} \\ \mathrm{D}_t^{(s)}(p_1(t))_{t=x} \\ \vdots \\ \mathrm{D}_t^{(s)}(p_n(t))_{t=x} \end{pmatrix} = \left(\mathrm{D}_t^{(s)} \circ F \begin{pmatrix} p_0(t) \\ p_1(t) \\ \vdots \\ p_n(t) \end{pmatrix} \right)_{t=\zeta(x)}$$

erfüllt ist. Das rechnen wir nach:

Die linke Seite ergibt

$$\begin{pmatrix} \sum_{\nu=0}^{n} a_{0\nu} \zeta(\sum_{\mu=0}^{r_\nu} p_{\nu\mu} \binom{\mu}{s} x^{\mu-s}) \\ \sum_{\nu=0}^{n} a_{1\nu} \zeta(\sum_{\mu=0}^{r_\nu} p_{\nu\mu} \binom{\mu}{s} x^{\mu-s}) \\ \vdots \\ \sum_{\nu=0}^{n} a_{n\nu} \zeta(\sum_{\mu=0}^{r_\nu} p_{\nu\mu} \binom{\mu}{s} x^{\mu-s}) \end{pmatrix} = \begin{pmatrix} \sum_{\nu=0}^{n} \sum_{\mu=0}^{r_\nu} a_{0\nu} \zeta(p_{\nu\mu}) \binom{\mu}{s} \zeta(x)^{\mu-s} \\ \sum_{\nu=0}^{n} \sum_{\mu=0}^{r_\nu} a_{1\nu} \zeta(p_{\nu\mu}) \binom{\mu}{s} \zeta(x)^{\mu-s} \\ \vdots \\ \sum_{\nu=0}^{n} \sum_{\mu=0}^{r_\nu} a_{n\nu} \zeta(p_{\nu\mu}) \binom{\mu}{s} \zeta(x)^{\mu-s} \end{pmatrix}.$$

Für die rechte Seite erhalten wir

$$\begin{pmatrix} \mathrm{D}_t^{(s)}(\sum_{\nu=0}^{n} a_{0\nu}\zeta(\sum_{\mu=0}^{r_\nu} p_{\nu\mu}t^\mu)) \\ \mathrm{D}_t^{(s)}(\sum_{\nu=0}^{n} a_{1\nu}\zeta(\sum_{\mu=0}^{r_\nu} p_{\nu\mu}t^\mu)) \\ \vdots \\ \mathrm{D}_t^{(s)}(\sum_{\nu=0}^{n} a_{n\nu}\zeta(\sum_{\mu=0}^{r_\nu} p_{\nu\mu}t^\mu)) \end{pmatrix}_{t=\zeta(x)} = \begin{pmatrix} \mathrm{D}_t^{(s)}(\sum_{\nu=0}^{n} a_{0\nu}\sum_{\mu=0}^{r_\nu} \zeta(p_{\nu\mu})t^\mu) \\ \mathrm{D}_t^{(s)}(\sum_{\nu=0}^{n} a_{1\nu}\sum_{\mu=0}^{r_\nu} \zeta(p_{\nu\mu})t^\mu) \\ \vdots \\ \mathrm{D}_t^{(s)}(\sum_{\nu=0}^{n} a_{n\nu}\sum_{\mu=0}^{r_\nu} \zeta(p_{\nu\mu})t^\mu) \end{pmatrix}_{t=\zeta(x)}$$

$$= \begin{pmatrix} \sum_{\nu=0}^{n}\sum_{\mu=0}^{r_\nu} a_{0\nu}\zeta(p_{\nu\mu})\binom{\mu}{s}\zeta(x)^{\mu-s} \\ \sum_{\nu=0}^{n}\sum_{\mu=0}^{r_\nu} a_{1\nu}\zeta(p_{\nu\mu})\binom{\mu}{s}\zeta(x)^{\mu-s} \\ \vdots \\ \sum_{\nu=0}^{n}\sum_{\mu=0}^{r_\nu} a_{n\nu}\zeta(p_{\nu\mu})\binom{\mu}{s}\zeta(x)^{\mu-s} \end{pmatrix}$$

Auf Grund der Gleichheit der beiden Ausdrücke können wir uns von nun an bei rationalen Normkurven tatsächlich auf die Darstellung

$$\Gamma := \{K(1, t, \ldots, t^n) \mid t \in K \cup \{\infty\}\}$$

beschränken.

Da wir aus Abschnitt 2.1.1 auch wissen, daß die Matrix C_t invertierbar ist und die Inverse ganz einfach durch den Parameterwechsel $t \mapsto -t$ zu erhalten ist (also $C_t^{-1} = C_{-t}$), macht es keine Schwierigkeiten, den k–Schmiegraum $\mathcal{S}_t^{(k)}\Gamma$ $(t \in K)$ als Nullstellenmenge eines Gleichungssystems zu schreiben. $\mathcal{S}_t^{(k)}\Gamma$ besteht aus allen Punkten $K(x_0, \ldots, x_n)$, die folgendes lineare System erfüllen:

$$\left.\begin{array}{rcl} \binom{k+1}{0}(-t)^{k+1}x_0 + \binom{k+1}{1}(-t)^k x_1 + \ldots + \binom{k+1}{k+1}x_{k+1} & = & 0 \\ \binom{k+2}{0}(-t)^{k+2}x_0 + \binom{k+2}{1}(-t)^{k+1}x_1 + \ldots + \binom{k+2}{k+2}x_{k+2} & = & 0 \\ \vdots \qquad\qquad \ddots \qquad\qquad \vdots & & \\ \binom{n}{0}(-t)^n x_0 + \binom{n}{1}(-t)^{n-1}x_1 + \ldots + \binom{n}{n}x_n & = & 0 \end{array}\right\} \quad (2.7)$$

Bemerkung 2.3.4 Die Vektoren $c_t,\ c_t', \ldots,\ c_t^{(k)}$ sind allesamt Lösungen jeder einzelnen Gleichung, da es sich hierbei um das Skalarprodukt mit der $(k+1)$-ten, $(k+2)$-ten, usw. bis n-ten Zeile von C_t^{-1} handelt.

Obwohl diese Darstellung von $\mathcal{S}_t^{(k)}\Gamma$ auf den ersten Blick nicht gerade vorteilhafter erscheinen mag, werden uns doch die folgenden Seiten zeigen, daß gerade darin die Lösung einer Frage liegt, die auf den ersten Blick recht hoffnungslos erscheint.

Wie schon bei den Ableitungspunkten bedarf es auch bei der Berechnung des k–Schmiegraumes $\mathcal{S}_\infty^{(k)}\Gamma$ in Kc_∞, dem letzten Grundpunkt, einer eigenen Vorgangsweise. Aus der Definition der Ableitungspunkte in Kc_∞ folgt für $\mathcal{S}_\infty^{(k)}\Gamma$ unmittelbar das lineare System

$$x_0 = x_1 = \ldots = x_{n-k-1} = 0. \tag{2.8}$$

Kapitel 3

Die Knoten einer rationalen Normkurve

In diesem Kapitel werden für rationale Normkurven die k-Knoten als Durchschnitte über alle k-Schmiegräume definiert. Es scheint jedoch, daß es in der Literatur in diesem Zusammenhang verschiedene Definitionen gibt. Manche Autoren benützen den Begriff „Knoten“, um jenen Punkt zu bezeichnen, der eine rationale Normkurve zu einem maximalen Bogen ergänzt (K ein endlicher Körper gerader Ordnung), andere gebrauchen diesen Begriff für den Durchschnitt aller Schmieghyperebenen einer Veronese–Varietät.

Es wird sich aber zeigen, daß diese zwei Typen von Knoten nur Beispiele unserer allgemeinen Definition sind. Wir werden mit den in Kapitel 1 vorgestellten Funktionen auf dem modulo p reduzierten Pascal–Dreieck $\Delta(p)$ sämtliche Knotendimensionen berechnen. Für $k = n - 1$ wurde so eine Formel bereits von H. Timmermann [23, 4.15] vorgestellt; vgl. auch [22]. Andere Ergebnisse über Knoten stammen von H. Brauner [2, 10.4.10], D.G. Glynn [5, 49–50], A. Herzer [11], H. Karzel [16], J.A. Thas [20] und J.A. Thas – J.W.P. Hirschfeld [15, 25.1].

3.1 Die Knotendimensionen

Da einerseits schon seit mehreren Jahrzehnten bekannt ist, daß bei $\mathrm{char}K = 2$ die Tangenten eines Kegelschnitts kopunktal sind (also eine Teilmenge des Geradenbüschels im sogenannten „Knoten“ bilden), und andererseits etwa in [23] der nichttriviale Durchschnitt aller Schmieghyperebenen einer Normkurve bei $\mathrm{char}K = p$ berechnet wird, wissen wir, daß die folgende Definition insofern interessant ist, als sie nicht ausschließlich die leere Menge beschreibt.

Definition 3.1.1 *Der k–Knoten $\mathcal{N}^{(k)}\Gamma$ ($k \in \{-1, 0, \ldots, n-1\}$) einer rationalen Normkurve Γ in $\mathrm{PG}(n, K)$ ist der Durchschnitt aller ihrer k–Schmiegräume.*

Bemerkungen 3.1.2

1. Die Knoten von Γ bilden natürlich eine aufsteigende Kette, wobei zu beachten ist, daß mit

   $$r := \lfloor \frac{n-1}{2} \rfloor \text{ und } \mathcal{S}_0^k\Gamma \cap \mathcal{S}_\infty^k\Gamma = \emptyset = \mathcal{N}^{(k)}\Gamma \text{ für alle } k \in \{-1, 0, \ldots, r\}$$

   die Inklusionskette

   $$\emptyset = \mathcal{N}^{(-1)}\Gamma = \mathcal{N}^{(0)}\Gamma = \ldots = \mathcal{N}^{(r)}\Gamma \subset \ldots \subset \mathcal{N}^{(n-1)}\Gamma \tag{3.1}$$

   folgt.

2. Wenn man einen k–Schmiegraum berechnen möchte, dann muß man die Lösung des Gleichungssystems (2.7) für einen bestimmten Parameterwert $t \in K$ finden. Die Bestimmung von $\mathcal{N}^{(k)}\Gamma$ bedeutet nun, (2.8) und (2.7) für alle Werte $t \in K$ simultan zu lösen.

   Man beachte, daß es sich hier womöglich um die Lösung eines Gleichungssystems mit unendlich vielen Gleichungen handelt!

Im folgenden Satz wird dieses Problem gelöst, indem die Knoten einer rationalen Normkurve mit jenen Binomialkoeffizienten in Zusammenhang gebracht werden, die modulo der Charakteristik von K verschwinden.

Wir werden auch sehen, daß die Definition der Knoten genau jene Partition der Nullen in $\Delta(p)$ nahelegt, die wir in der Definition 1.3.1 gegeben haben.

Satz 3.1.3 *Wenn K mindestens $k+1$ Elemente besitzt, dann entspricht der Knoten $\mathcal{N}^{(k)}\Gamma$ der rationalen Normkurve (2.1) jenem Unterraum $\mathcal{Q}$, der durch die Basispunkte P_j des Bezugssystems aufgespannt wird, deren Index $j \in \{0, 1, \ldots, n\}$ die Bedingung*

$$\binom{k+1}{j} \equiv \binom{k+2}{j} \equiv \ldots \equiv \binom{n}{j} \equiv 0 \pmod{\text{char}K} \tag{3.2}$$

erfüllt.

Beweis:

1. Es sei $K(x_0, x_1, \ldots, x_n)$ ein Punkt von $\mathcal{N}^{(k)}\Gamma$. Wegen (2.8) und $\#K \geq k+1$ ist jedes Polynom in (2.7) das Null–Polynom in t. Aus $x_j \neq 0$ folgt somit (3.2), und der Punkt liegt dann auch in $\mathcal{Q}$.

2. Angenommen, (3.2) sei für ein gewisses j erfüllt. Aus

$$\binom{r-1}{s} \equiv \binom{r}{s} \equiv 0 \pmod{\mathrm{char}K}$$

folgt

$$\binom{r-1}{s-1} \equiv 0 \pmod{\mathrm{char}K}$$

und schließlich

$$\binom{k+1}{j-l} \equiv \binom{k+2}{j-l} \equiv \ldots \equiv \binom{n-l}{j-l} \equiv 0 \pmod{\mathrm{char}K}$$

für alle $l \in \{0, 1, \ldots, n-k-1\}$. Das ist aber nur möglich, wenn $j > n-k-1$ gilt.

3. Sei nun $K(x_0, x_1, \ldots, x_n)$ ein Punkt in $\mathcal{Q}$. Aus (2) ergibt sich

$$x_0 = x_1 = \ldots = x_{n-k-1} = 0$$

in Übereinstimmung mit (2.8). Bei $x_j \neq 0$ zeigt uns (3.2), daß $(x_0, x_1, \ldots, x_n)$ ebenfalls eine Lösung von (2.7) für alle $t \in K$ ist. Der Punkt liegt also auch in $\mathcal{N}^{(k)}\Gamma$. □

Bemerkungen 3.1.4

1. Im Beweisschritt 2 wird mit den Bezeichnungen aus Kapitel 1 die j–te Spalte von $\square(p)$ untersucht. Wenn diese im Bereich von Zeile $k+1$ bis n in einem gewissen ∇^i liegt, dann konstruieren sich durch die bekannte Rekursionsformel

$$\binom{r-1}{s-1} + \binom{r-1}{s} = \binom{r}{s}$$

die Elemente, die links davon stehen, von selbst. Beispielsweise folgt aus

$$\binom{n}{j} \equiv \binom{n-1}{j} \equiv 0 \pmod{p}$$

mit der Rekursionsformel sofort

$$\binom{n-1}{j-1} \equiv 0 \pmod{p}.$$

Aus

$$\binom{n-1}{j} \equiv \binom{n-2}{j} \equiv 0 \pmod{p}$$

folgt sofort

$$\binom{n-2}{j-1} \equiv 0 \pmod{p}.$$

So zeigt man, daß letztlich die Einträge $k{+}1, k{+}2, \ldots, n{-}1$ in der $(j{-}1)$-ten Spalte von $\square$ ebenfalls der Zahl 0 entsprechen.

Wenn wir die Rekursionsformel nun für die Spalte $j-1$ anwenden, ergibt sich für die Einträge $k{+}1, k{+}2, \ldots n{-}2$ der Spalte $j{-}2$ in $\square$ die Zahl 0. Diese Vorgangsweise ist so lange durchzuführen, bis wir uns in der $(j{+}k{+}1{-}n)$-ten Spalte beim $(k+1)$-ten Eintrag befinden. Wir haben so einen Teil von ∇^i konstruiert.

2. Nach Satz 3.1.3 hat $\mathrm{char}K = 0$ stets $\mathcal{N}^{(n-1)}\Gamma = \emptyset$ zur Folge, weil hier ja sämtliche Binomialkoeffizienten von Null verschieden sind. Die Knoten einer rationalen Normkurve interessieren in diesem Fall also nicht.

Für den restlichen Teil dieses Kapitels treffen wir deshalb folgende Voraussetzungen:

$$\begin{aligned} \mathrm{char}K &=: p > 0, \\ n &=: \langle n_\lambda \rangle \quad \text{(in der Basis } p\text{)}, \\ n+1 &=: b =: \langle b_\lambda \rangle \quad \text{(in der Basis } p\text{)}. \end{aligned}$$

Durch ein Beispiel soll dem Leser der Hauptsatz zur Bestimmung der Knotendimensionen sozusagen in den Mund gelegt werden. Wir wollen für eine Normkurve in $\mathrm{PG}(14, K)$ mit $\mathrm{char}K = 2$ alle Knotendimensionen berechnen, und auch die wesentlichen Überlegungen für den *Hauptsatz* bereitstellen.

Die p–adischen Entwicklungen der Raum- bzw. Vektorraumdimension lauten:

$$\begin{aligned} n &= 14 = \langle 1, 1, 1, 0 \rangle \\ b &= 15 = \langle 1, 1, 1, 1 \rangle \end{aligned}$$

Die Abbildung 3.1 zeigt uns das Pascal–Dreieck modulo 2 bis zur 14. Zeile.
Die Werte der in (1.9) definierten „top line“–Funktion $T(i, b)$ stehen in p–adischer Darstellung links neben den entsprechenden Zeilen. Wie in Kapitel 1 dargestellt, bestimmt der Wert $T(i, b)$ zu vorgegebenem Element $(n, j) \in \overline{i}$ jene höchste Zeile $T(i, b)$ in $\Delta(p)$, so daß noch immer $(T(i, b), j) \in \overline{i}$ gilt.

Die Dimension des Durchschnitts $\mathcal{N}^{(13)}\Gamma$ aller Schmieghyperebenen hat nach Satz 3.1.3 den Wert 6, weil ja bloß die Anzahl der Nullen in der letzten Zeile zu bestimmen und danach auf Grund der projektiven Dimension die Zahl 1 zu subtrahieren ist.

		1													
		1	1												
		1	0	1											
		1	1	1	1										
		1	0	0	0	1									
		1	1	0	0	1	1								
		1	0	1	0	1	0	1							
		1	1	1	1	1	1	1	1						
$\langle 1,0,0,0\rangle$	$\rightarrow$	1	0	0	0	0	0	0	0	1					
		1	1	0	0	0	0	0	0	1	1				
		1	0	1	0	0	0	0	0	1	0	1			
		1	1	1	1	0	0	0	0	1	1	1	1		
$\langle 1,1,0,0\rangle$	$\rightarrow$	1	0	0	0	1	0	0	0	1	0	0	0	1	
		1	1	0	0	1	1	0	0	1	1	0	0	1	1
$\langle 1,1,1,0\rangle$	$\rightarrow$	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
$\langle 1,1,1,1\rangle$	$\rightarrow$														

Abbildung 3.1: Pascal–Dreieck modulo 2

Man beachte, daß zur Berechnung des 13–Knotens die Struktur der *14.* Zeile zu untersuchen ist bzw. in dieser Zeile Nullen der Klassen $1, 2$ und 3 stehen. Die „top line"–Funktion zeigt uns an, daß für die Nullen der Klasse 1 in dieser Zeile schon deren „Top–Level" erreicht ist.

Der 12– und der 11–Knoten wird dann nur mehr durch 3 Grundpunkte aufgespannt, während für die Dimensionsbestimmung der 7– bis 10–Knoten nur mehr die Anzahl der Nullen aus der Klasse 3 maßgeblich sind. Die Knoten sind also einpunktig.

Wir sehen hier sehr schön, daß es darauf ankommt, die Anzahl der Nullen einer Zeile n von $\Delta(p)$ zu bestimmen, die in einer Klasse größer oder gleich i liegen. Es handelt sich also exakt um den Wertebereich der in (1.14) definierten „Summenfunktion" $\Sigma(i, n)$.

Die Bereiche für k, die gleiche Dimensionen der k–Knoten ergeben, werden im wesentlichen durch die Schranken $T(i, b)$ festgelegt. Daher ist es auch nicht verwunderlich, daß die Größe der Wertemenge der Funktion $T(i, b)$ die Anzahl der verschiedenen Knotendimensionen bestimmt. Diese Feststellungen werden in den folgenden Sätzen konkretisiert.

Satz 3.1.5 (Hauptsatz) *Sei* Γ *eine rationale Normkurve in* $\mathrm{PG}(n, K)$*. Erfüllt eine natürliche Zahl* k *die Bedingungen* $\#K \geq k + 1$ *und*

$$T(R,b) = b - \sum_{\mu=0}^{R-1} b_\mu p^\mu \leq k+1 < b - \sum_{\lambda=0}^{Q-1} b_\lambda p^\lambda = T(Q,b) \tag{3.3}$$

mit höchstens einem $b_\lambda \neq 0$ *für* $\lambda \in \{Q, Q+1, \ldots, R-1\}$*, dann hat der* k*–Knoten von* Γ *die Dimension*

$$\dim \mathcal{N}^{(k)}\Gamma = n - (1 + \sum_{\mu=0}^{R-1} n_\mu p^\mu) \prod_{\lambda=R}^{\infty} (n_\lambda + 1) = \Sigma(R,n) - 1. \tag{3.4}$$

Beweis: Wegen der strengen Ungleichung in (3.3) gibt es genau ein

$$N \in \{Q, Q+1, \ldots, R-1\}$$

mit $b_N \neq 0$, also

$$T(R,b) = T(R-1,b) = \ldots = T(N+1,b) < T(N,b) = \ldots = T(Q,b). \tag{3.5}$$

Nach Satz 3.1.3 entspricht $\dim \mathcal{N}^{(k)}\Gamma + 1$ exakt der Anzahl von Elementen $j \in \{0, 1, \ldots, n\}$, die die Eigenschaft (3.2) besitzen. Bei gegebenem $i \geq 1$ sind die beiden Bedingungen

$$\overline{i(n)} \neq \emptyset \text{ und } T(i,b) \leq k+1 \tag{3.6}$$

gemeinsam äquivalent zur Existenz eines Elements $j \in \overline{i(n)}$, welches (3.2) erfüllt. Wenn (3.2) für mindestens ein $j \in \overline{i(n)}$ erfüllt ist, dann trifft dies nach Satz 1.4.4 für alle Elemente von $\overline{i(n)}$ zu. Es gibt jetzt drei Fälle:

1. Für $1 \leq i \leq N$ bekommt man aus (1.10), (3.5) und (3.3) die Folgerung $k+1 < T(Q,b) = T(N,b) \leq T(i,b)$, die jedoch (3.6) widerspricht.

2. Für $N+1 \leq i \leq R-1$ erhält man $\overline{i(n)} = \emptyset$ nach Satz 1.4.3. Die Bedingung (3.6) ist dann nicht erfüllt.

3. Aus $i \geq R$ erhält man schließlich nach (1.10) und (3.3) die Ungleichung $T(i,b) \leq T(R,b) \leq k+1$.

   Die Klasse $\overline{i}$ liefert dann exakt $\Phi(i,n) \geq 0$ verschiedene Lösungen von (3.2).

Die Anzahl der Elemente j, die (3.2) erfüllen, ist somit durch

$$\sum_{i=R}^{\infty} \Phi(i,n) = \Sigma(R,n)$$

gegeben, womit Satz 3.1.5 bewiesen ist. □

Nun wollen wir eine Formel vorstellen, die es gestattet, aus der p–adischen Darstellung von $n+1$ sofort die Anzahl aller verschiedenen Knoten zu bestimmen.

Satz 3.1.6 *Es sei* Γ *eine rationale Normkurve in* $\mathrm{PG}(n, K)$ *und* K *habe mindestens* n *Elemente. Dann entspricht die Anzahl* d *der von Null verschiedenen Ziffern in der Darstellung von* $b = n + 1$ *in der Basis* p *genau der Anzahl der verschiedenen Knoten von* Γ*.*

Beweis: Seien $N_1 < N_2 < \ldots < N_d$ die Positionen der von Null verschiedenen Stellen von b in der Basis p. Aus (1.10) und (1.11) folgt $0 = T(N_d{+}1, b) < T(N_d, b)$ und

$$T(N_{\alpha+1}, b) = \ldots = T(N_\alpha + 1, b) < T(N_\alpha, b) \text{ für alle } \alpha \in \{d-1, d-2, \ldots, 1\},$$

beziehungsweise $T(N_1, b) = b$.
Wir erhalten also d verschiedene „aufeinanderfolgende“ Ungleichungen

$$T(N_\alpha + 1, b) \leq k + 1 < T(N_\alpha, b) \quad (\alpha \in \{d, d-1, \ldots, 1\}). \tag{3.7}$$

Jedes $k \in \{-1, 0, \ldots, n-1\}$ ist dann Lösung von genau einer Ungleichung (3.7). Aus (1.5) und (1.14) folgt unmittelbar

$$0 = \Sigma(N_d + 1, n) < \Sigma(N_{d-1} + 1, n) < \ldots < \Sigma(N_1 + 1, n),$$

und deshalb entsprechen die verschiedenen Ungleichungen (3.7) genau den verschiedenen Dimensionen der Knoten. □

Bemerkungen 3.1.7

1. Es existiert immer mindestens eine Ungleichung (3.7). Setzt man nämlich

   $$J := N_d = \max\{\lambda \mid b_\lambda \neq 0\},$$

   dann folgt aus (3.4) und mit $\alpha := d$ aus (3.7), daß

   $$\mathcal{N}^{(k)}\Gamma = \emptyset \text{ für alle } k \in \{-1, 0, \ldots\ b_J p^J - 2\} \quad (\#K \geq k + 1) \tag{3.8}$$

   gilt und somit die Schranke aus (3.1) entscheidend verbessert wird.

2. Die Zahl $k := n - 1$ ist eine Lösung der Ungleichung (3.7) für $\alpha := 1$. Setzt man ähnlich wie oben

   $$M := N_1 = \min\{\lambda \mid b_\lambda \neq 0\},$$

   dann gilt nach (1.5) ja $\Sigma(1, n) = \Sigma(2, n) = \ldots = \Sigma(M + 1, n)$. Nach (1.15) kann man Formel (3.4) nun auch umschreiben zu

   $$\dim \mathcal{N}^{(n-1)}\Gamma = n - \prod_{\lambda=0}^{\infty}(n_\lambda + 1) \quad (\#K \geq n). \tag{3.9}$$

   Dieses Resultat kann man auch in [23, 4.15] wiederfinden.

3.2 Untersuchung der Knoten für die Raumdimensionen $n = n_J p^J$

Wir möchten hier allgemein für Raumdimensionen der Form $n = n_J p^J$ die Anzahl der verschiedenen Knoten und deren Dimensionen berechnen, um die praktische Vorgangsweise zu illustrieren. Im Anschluß daran spezifizieren wir Raumdimension und Charakteristik und erhalten bekannte Ergebnisse über Kubiken und Kegelschnitte.

Wir setzen also

$$n = n_J p^J \qquad n_J \in \{1, \ldots, p-1\}$$

und unterscheiden zwischen $J = 0$ und $J > 0$.

3.2.1 Knoten bei $n = n_0$

Wenn wir Satz 3.1.6 Revue passieren lassen, dann können wir anhand der p-adischen Darstellung von $b := n + 1$ sofort entscheiden, ob es nichtleere Knoten gibt oder nicht.

Für $n_0 < p - 1$ folgt

$$b = \langle n_0 + 1 \rangle,$$

und bei $n_0 = p - 1$ erhalten wir

$$b = \langle 1, 0 \rangle.$$

In beiden Fällen ist in der p-adischen Entwicklung von $n + 1$ nur eine Ziffer verschieden von Null, woraus wir folgern, daß es nur einen einzigen, nämlich den leeren Knoten gibt. Das wollen wir festhalten.

Folgerung 3.2.1 Wenn die Raumdimension im Vergleich zur Charakteristik des Grundkörpers hinreichend klein ist ($n < \mathrm{char}K$), ergeben sich bei der Knotenbestimmung im Vergleich zum reellen Fall keine Unterschiede.

3.2.2 Knoten bei $n = n_J p^J$ mit $J > 0$

Für $J > 0$ erhalten wir

$$b = \langle n_J, \underbrace{0, \ldots, 0}_{(J-1)-\mathrm{mal}}, 1 \rangle.$$

In dieser Darstellung haben wir einen Abschnitt von $J - 1$ Nullen, der für $J = 1$ entfällt. In jedem Fall gibt es genau zwei von Null verschiedene Ziffern, und daraus

folgern wir die Existenz von genau einem nichttrivialen Knoten, dessen Dimension wir nun berechnen.

Die Werte der sogenannten „top line“–Funktion $T(R,b)$ aus Satz 3.1.5 lauten:

$$\begin{aligned} T(0,b) &= b - \sum_{\lambda=0}^{-1} b_\lambda p^\lambda = b \\ T(1,b) &= b - \sum_{\lambda=0}^{0} b_\lambda p^\lambda = b-1 = n \\ &\vdots \\ T(J,b) &= b - \sum_{\lambda=0}^{J-1} b_\lambda p^\lambda = n \\ T(J+1,b) &= b - \sum_{\lambda=0}^{J} b_\lambda p^\lambda = 0 \end{aligned}$$

Auf Grund von

$$T(J+1,b) < T(J,b) = \ldots = T(1,b) < T(0,b)$$

erhalten wir gemäß Hauptsatz 3.1.5 die Ungleichungen

$$T(1,b) = \; n \leq k+1 < n+1 = T(0,b) \tag{3.10}$$

$$T(J+1,b) = 0 \leq k+1 < n \quad = T(J,b). \tag{3.11}$$

Aus (3.10) folgt $k = n-1$ und mit dem Hauptsatz erhalten wir

$$\begin{aligned} \underline{\dim \mathcal{N}^{(n-1)}\Gamma} &= n - (1 + \sum_{\mu=0}^{0} n_\mu p^\mu) \prod_{\lambda=1}^{\infty} (n_\lambda + 1) \\ &= \underline{n - (n_J + 1)}. \end{aligned}$$

Es ist uns bereits klar, daß für alle anderen Werte von k der k–Knoten leer sein muß. Mit Ungleichung (3.11) prüfen wir das noch nach: Für alle Werte k, die diese Ungleichung erfüllen, also $k \in \{-1, 0, \ldots, n-2\}$, erhalten wir

$$\begin{aligned} \dim \mathcal{N}^{(k)}\Gamma &= n - (1 + \sum_{\mu=0}^{J} n_\mu p^\mu) \prod_{\lambda=J+1}^{\infty} (n_\lambda + 1) \\ &= n - (n+1) = -1. \end{aligned}$$

Diese Ergebnisse spezifizieren wir nun für bekannte Beispiele.

3.2.3 Die windschiefe Kubik bei $\mathrm{char}K = 3$

Die Treffgerade der Tangenten einer windschiefen Kubik entspricht bei $\mathrm{char}K = 3$ genau dem 2–Knoten. Das sehen wir an der Matrix C_t, die die Vektoren des Kurvenpunktes Kc_t und der zugehörigen Ableitungspunkte enthält:

$$C_t = \begin{pmatrix} \binom{0}{0} & 0 & 0 & 0 \\ \binom{1}{0}t & \binom{1}{1} & 0 & 0 \\ \binom{2}{0}t^2 & \binom{2}{1}t & \binom{2}{2} & 0 \\ \binom{3}{0}t^3 & \binom{3}{1}t^2 & \binom{3}{2}t & \binom{3}{3} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ t & 1 & 0 & 0 \\ t^2 & 2t & 1 & 0 \\ t^3 & 0 & 0 & 1 \end{pmatrix}$$

Einerseits liegt der erste Ableitungspunkt stets in dem von den Basispunkten P_1 und P_2 aufgespannten Unterraum, andererseits sehen wir auf Grund der Verteilung der Nullen in der letzten Zeile von C_t, daß dieser Unterraum genau dem 2–Knoten entspricht.

Mit den Überlegungen des vorigen Abschnitts erhalten wir dieses Ergebnis unmittelbar. Für $p = 3$ und $n = 3 = n_1 p^1$ mit $n_1 = 1$ folgt

$$\begin{aligned} \dim \mathcal{N}^{(n-1)}\Gamma = \dim \mathcal{N}^{(2)}\Gamma &= n - (n_1 + 1) = 1 \\ \dim \mathcal{N}^{(1)}\Gamma &= -1. \end{aligned}$$

Die Schmiegebenen der Kubik sind also Teilmenge eines Ebenenbüschels.

3.2.4 Der Knoten eines Kegelschnitts bei $\mathrm{char}K = 2$

Während in der projektiven Ebene $\mathrm{PG}(2, K)$ im Falle $\mathrm{char}K \neq 2$ die Tangenten eines Kegelschnitts niemals kopunktal sind, bilden sie bei $\mathrm{char}K = 2$ eine Teilmenge eines Geradenbüschels im sogenannten Knoten. Aus dem letzten Punkt der Bemerkungen 3.3.2 geht hervor, daß es sich dabei genau dann um eine echte Teilmenge handelt, wenn der zu Grunde liegende Körper nicht vollkommen ist.

In diesem Fall ($n = p = 2$) gilt also $\dim \mathcal{N}^{(n-1)} = \dim \mathcal{N}^{(1)} = 0$, was man auch unmittelbar an der Matrix

$$C_t = \begin{pmatrix} \binom{0}{0} & 0 & 0 \\ \binom{1}{0}t & \binom{1}{1} & 0 \\ \binom{2}{0}t^2 & \binom{2}{1}t & \binom{2}{2} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ t & 1 & 0 \\ t^2 & 0 & 1 \end{pmatrix}$$

sieht. Der erste (vom Parameter t unabhängige) Ableitungspunkt entspricht dem Grundpunkt P_1 und bildet so den (einzigen) Knoten $\mathcal{N}^{(1)} = \mathcal{N}^{(n-1)}$ des Kegelschnitts.

All das läßt sich wieder allgemein einordnen:

- Für $p > 2$ ergibt sich $n = 2 < p$, und daher sind in Analogie zum reellen Fall alle Knoten leer.
- Für $p = 2$ erhalten wir $n = n_1 p^1$ mit $n_1 = 1$. Wie wir uns schon allgemein überlegt haben, folgt daraus

$$\dim \mathcal{N}^{(n-1)}\Gamma = \dim \mathcal{N}^{(1)}\Gamma = n - (n_1 + 1) = 0.$$

Die Tangenten an den Kegelschnitt Γ schneiden einander also genau in einem Punkt, dem „Knoten des Kegelschnitts“ (vgl. u.a. auch [9]).

Die Kegelschnittstangenten lassen sich nun folgendermaßen charakterisieren:

Korollar 3.2.2 *Eine Gerade durch den Knoten, die auch durch einen Kegelschnittspunkt Kc_t geht, ist schon die Tangente in Kc_t.*

Diese Aussage wollen wir nun für beliebige Dimension verallgemeinern.

3.3 Die k–Schmiegräume unter den k–dimensionalen Unterräumen durch den k–Knoten

Für die natürlichen Zahlen $R > Q \geq 0$ mit

$$b_R \neq 0 = b_{R-1} = \ldots = b_{Q+1} \neq b_Q$$

setze man

$$k := T(R, b) - 1 = \langle \ldots, n_{R+1}, n_R - 1, p - 1, \ldots, p - 1 \rangle. \tag{3.12}$$

Die Zahl k ist also eine *minimale* Lösung der Ungleichung (3.3) im Hauptsatz 3.1.5, welcher auch zeigt, daß $\mathcal{N}^{(k)}\Gamma$ für $\#K \geq k + 1$ ein nichtleerer Knoten ist. Wir wollen unter den k–dimensionalen Unterräumen durch $\mathcal{N}^{(k)}\Gamma$ die oskulierenden k–Schiegräume von Γ charakterisieren.

Durch Satz 3.1.3 wird eine Basis von $\mathcal{N}^{(k)}\Gamma$ beschrieben. Nach (1.13) und (1.11) lautet der größte Index j eines Basispunktes P_j dieser Basis $T(R, b) - 1 = k$, wobei also $k \in \overline{R(n)}$ gilt.

Nun definieren wir

$$U := \max\{j \in \mathbb{N} \mid j < k \text{ und } j \preceq n\} = \langle \ldots, n_{R+1}, n_R - 1, n_{R-1}, \ldots, n_0 \rangle. \tag{3.13}$$

Der U–Schmiegraum $\mathcal{S}_0^{(U)}\Gamma$ in P_0 wird durch die Punkte $P_0, P_1, \ldots, P_U$ aufgespannt, so daß

$$\mathcal{S}_0^{(U)}\Gamma \vee \mathcal{N}^{(k)}\Gamma = \mathcal{S}_0^{(k)}\Gamma$$

gilt. Die Minimalität von k ist hier wesentlich. Durch die Kollineationsgruppe $\mathrm{PGL}(\Gamma)$ wird diese Eigenschaft von $P_0 = Kc_0$ auf alle Punkte von Γ übertragen. Für unsere spezielle Wahl von k gilt daher:

Satz 3.3.1 *Mit den Bezeichnungen aus (3.12) und (3.13) ist ein k–dimensionaler Unterraum durch $\mathcal{N}^{(k)}\Gamma$ ein k–Schmiegraum von Γ, dann und nur dann, wenn er einen U–Schmiegraum von Γ enthält.*

Diese Aussage illustrieren wir an einem Beispiel:

$$\begin{aligned} p &= 2 \\ n &= 9 = \langle 1,0,0,1\rangle \\ b &= 10 = \langle 1,0,1,0\rangle \end{aligned}$$

Jene Stellen der Matrix

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

an denen in der letzten und vorletzten Zeile eine Null steht, sind für den 7–Knoten verantwortlich. Wir erhalten

$$\mathcal{N}^{(7)}\Gamma = [\{P_2, P_3, P_4, P_5, P_6, P_7\}] \neq \mathcal{N}^{(6)}\Gamma = \emptyset.$$

Die Zahl $k = 7$ erfüllt also unsere Minimalitäts-Forderung von eben. Wir können daher die 7–Schmiegräume unter den 7–dimensionalen Unterräumen durch den 7–Knoten auszeichnen (und machen das o.B.d.A. für den Normkurvenpunkt P_0).

Es ist klar, daß ein 7–dimensionaler Unterraum durch $\mathcal{N}^{(7)}\Gamma$ im Falle des Kurvenpunktes P_0 genau dann dem 7–Schmiegraum entspricht, wenn er die Tangente $P_0 \vee P_1$ (den 1–Schmiegraum) in P_0 enthält.

Die obigen Formeln liefern ebenso dieses Resultat:
Aus (3.12) folgt für $R = 3$ wegen $n = \langle 1,0,0,1\rangle$ der Wert $k = \langle 0,1,1,1\rangle = 7$, und aus (3.13) ergibt sich $U = \langle 0,0,0,1\rangle = 1$.

Bemerkungen 3.3.2

1. Am letzten Beispiel können wir deutlich die Qualität von Satz 3.3.1 erkennen: *„Ein 7-dimensionaler Unterraum durch den 7–Knoten, der eine Tangente enthält, ist schon der 7-Schmiegraum im Berührpunkt der Tangente.“*

   Die Güte des Korollars wird durch die Differenz $k-U$ bestimmt. Man kann letztlich aus den Darstellungen (3.12) und (3.13) ablesen, in welchen Fällen die Qualität der Aussage 3.3.1 maximal ist. In einem Beispiel wollen wir zeigen, daß Satz 3.3.1 auch relativ schwach sein kann:

   Es sei

   $$\begin{aligned} p &= 2 \\ n &= 6 = \langle 1,1,0\rangle \\ b &= 7 = \langle 1,1,1\rangle \end{aligned}$$

   mit

   $$\begin{aligned} k &= 5 = \langle 1,0,1\rangle \\ U &= 4 = \langle 1,0,0\rangle \end{aligned}$$

   und

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

   gegeben. Wir erhalten: *„Ein 5-dimensionaler Unterraum durch den 5-Knoten $\mathcal{N}^{(5)}\Gamma = [\{P_1, P_3, P_5\}]$, der einen 4-Schmiegraum enthält, ist schon der 5-Schmiegraum im Berührpunkt des 4-Schmiegraums.“*

2. Trivialerweise ist die Aussage aus Satz 3.3.1 auch für jedes U^* mit

   $$U \leq U^* \leq k$$

   erfüllt.

3. Die Minimalität von k geht in den Überlegungen entscheidend ein: Betrachten wir noch einmal das erste Beispiel mit $p = 2$ und $n = 9$.

   Wenn wir hier $k = 8$ nicht minimal wählten, dann erhielten wir wegen $\mathcal{N}^{(7)}\Gamma = \mathcal{N}^{(8)}\Gamma$ die triviale Aussage: *„Ein 8-dimensionaler Unterraum durch den 8-Knoten, der einen 8-Schiegraum enthält, ist der 8-Schmiegraum in einem Normkurvenpunkt.“*

4. Wir betrachten Satz 3.3.1 für

$$n = p^J$$

mit $J > 0$ und erhalten: *Eine Hyperebene durch den* $(n-1)$*– Knoten ist genau dann eine Schmieghyperebene von* Γ*, wenn sie einen Normkurvenpunkt enthält.*

Enthält nicht jede Hyperebene ε durch den $(n-1)$–Knoten einen Normkurvenpunkt und ist somit Schieghyperebene? – Dieser Frage gehen wir auf den Grund.

Wir können in der Darstellung

$$\varepsilon: \qquad a_0 x_0 + a_n x_n = 0$$

die Voraussetzung $a_0 a_n \neq 0$ treffen, weil es sich in den anderen Fällen entweder um die Schmieghyperebene in P_0 oder P_n handelt. Somit setzen wir $a_n = -1$ und schneiden dann ε mit Γ:

$$\begin{aligned} \varepsilon: &\qquad a_0 x_0 - x_n = 0 \\ \varepsilon \cap \Gamma: &\qquad a_0 \cdot 1 - t^n = 0 \end{aligned}$$

Wegen $n = p^J$ gilt es, die Gleichung

$$t^{p^J} = a_0$$

zu lösen. Nach [24, S. 139] gibt es für einen Körper der Charakteristik p genau dann zu jedem Element eine p-te Wurzel, wenn er *vollkommen*[1] ist. (Diese ist dann wegen der Injektivität von $x \mapsto x^p$ eindeutig bestimmt.)

Genau für vollkommene Körper folgt mit

$$t = (a_0)^{(\frac{1}{p})^J},$$

daß jede Hyperebene durch den $(n-1)$–Knoten automatisch Schmieghyperebene ist.

In den nächsten Abschnitten wird einerseits untersucht, für welche Raumdimension bei gegebener Charakteristik einpunktige Knoten auftreten, und andererseits diskutiert, wann der Durchschnitt der Schmiegräume fester Dimension mit dem $(n-1)$–Knoten eine Spurkurve in $\mathcal{N}^{(n-1)}\Gamma$ hinterläßt, bzw. unter welchen Voraussetzungen diese Kurven wieder Normkurven sind.

[1] Alle endlichen Körper sind vollkommen. Ein Beispiel für einen nicht vollkommenen Körper findet man etwa in [1, S. 239–240]

3.4 Spurkurven der Form $\mathcal{S}_t^{(k)}\Gamma \cap \mathcal{N}^{(n-1)}\Gamma$

Für die folgenden Untersuchungen bedarf es insofern keiner intensiven Motivation, als einerseits etwa in [13], [21] und [7] die Wechselbeziehung von MDS–Codes und k–Bögen in $\mathrm{PG}(n,q)$ bzw. das Dualitätsprinzip für MDS–Codes dargestellt worden sind und andererseits J.A. Thas darauf basierende $(q+2)$–Bögen in $\mathrm{PG}(2^h-2,2^h)$ wie folgt erzeugt hat (vgl. auch [20] und [21]):

Man betrachte eine rationale Normkurve Γ in $\mathrm{PG}(2^h-2,2^h)$ und bilde den Durchschnitt über alle Schmieghyperebenen, also $\mathcal{N}^{(n-1)}\Gamma$. Die Tangenten von Γ schneiden aus $\mathcal{N}^{(n-1)}\Gamma$ eine Spurkurve aus, die sich als rationale Normkurve in einem Unterraum $\mathrm{PG}(2^{h-1}-2,2^h)$ herausstellt[2]. Dieser Prozeß wird so lange wiederholt, bis man zum Knoten eines Kegelschnitts gelangt. Dieser Punkt ergänzt Γ dann zu einem $(q+2)$–Bogen.

In diesem Abschnitt soll allgemeiner für beliebige Charakteristik p der minimale Index k bestimmt werden, sodaß $\mathcal{S}_t^{(k)}\Gamma \cap \mathcal{N}^{(n-1)}\Gamma$, der Durchschnitt eines k–Schmiegraumes mit dem $(n-1)$– Knoten, nichtleer ist. Trivialerweise gilt dies dann für alle $t \in K^+$.

Nachdem wir aus Satz 3.1.3 bereits wissen, daß der $(n-1)$–Knoten durch jene Basispunkte P_j aufgespannt wird, für die $\binom{n}{j} \equiv 0 \pmod p$ gilt, können wir nun bei gegebener Dimension n nach dem minimalen Index j mit dieser Eigenschaft fragen. Setzen wir

$$M := \min\{\lambda | b_\lambda \neq 0\},$$
$$J := \max\{\lambda | b_\lambda \neq 0\},$$

dann folgt

$$\begin{aligned} n_\lambda &= p-1 \text{ für } \lambda < M \\ n_M &< p-1. \end{aligned}$$

Damit erhalten wir

Lemma 3.4.1 *Mit den obigen Bezeichnungen gilt: Für $J > M$ folgt*

$$\min\{j \leq n \mid j \not\preceq n\} = b_M p^M.$$

Für $J = M$ treten in der n-ten Zeile von $\Delta(p)$ keine Nullen auf.

Beweis: Die Bedingung $J > M$ ist notwendig und hinreichend dafür, daß in der n–ten Zeile von $\Delta(p)$ die Zahl 0 vorkommt. Das überlegen wir uns kurz:

[2]Bei Timmermann [23] heißen diese Kurven „Oskulanten“.

- $J = M$: Wir erhalten hier

$$\begin{aligned} b &= \langle b_J, \underbrace{0, \ldots, 0}_{J-\text{mal}} \rangle \\ n &= \langle b_J - 1, \underbrace{p-1, \ldots, p-1}_{J-\text{mal}} \rangle, \end{aligned}$$

  wobei für $J = 0$ die letzten Stellen entfallen. Mit Lemma 1.1.1 und der anschließenden Bemerkung folgt sofort, daß es in der n-ten Zeile von Δ keine verschwindenden Binomialkoeffizienten gibt.

- $J > M$: Es ergibt sich

$$\begin{aligned} b &= \langle b_J, \underbrace{\ldots\ldots\ldots\ldots}_{(J-M-1)-\text{Stellen}}, b_M, \underbrace{0, \ldots, 0}_{M-\text{mal}} \rangle \\ n &= \langle b_J, \underbrace{\ldots\ldots\ldots\ldots}_{(J-M-1)-\text{Stellen}}, b_M - 1, \underbrace{p-1, \ldots, p-1}_{M-\text{mal}} \rangle, \end{aligned}$$

  wobei manche Abschnitte nicht vorhanden sein müssen ($M = 0$ oder $J = M + 1$). Wegen $b_M - 1 < p - 1$ sehen wir sehr schön, daß

$$\begin{aligned} \min\{j \mid j \not\preceq n\} &= \langle \underbrace{0, \ldots, 0}_{(J-M)-\text{mal}}, b_M, \underbrace{0, \ldots, 0}_{M-\text{mal}} \rangle \\ &= b_M p^M \end{aligned}$$

  folgt. □

Damit kommen wir zur Kernaussage dieses Abschnitts:

Satz 3.4.2 *Für feste Charakteristik p und Raumdimension n mit $J > M$ ist $k = b_M p^M$ der minimale Index, sodaß $\mathcal{S}_t^{(k)}\Gamma \cap \mathcal{N}^{(n-1)}\Gamma$ für alle Parameterwerte t einpunktig ist, also*

$$\min\{k \geq 0 \mid \mathcal{S}_t^{(k)}\Gamma \cap \mathcal{N}^{(n-1)}\Gamma \neq \emptyset \ \forall t \in K\} = b_M p^M.$$

Beweis: Aus der Knotendefinition folgt, daß wir uns bei obiger Minimumsbildung auch auf ein fixes $t \in K$ beschränken dürfen. Mit $t = 0$ und Lemma 3.4.1 ist die Aussage aber schon bewiesen: Aus

$$\begin{aligned} \mathcal{S}_0^{(k)}\Gamma &= [\{P_0, \ldots, P_k\}], \\ \mathcal{N}^{(n-1)}\Gamma &= [\{P_{b_M p^M}, \ldots\}] \end{aligned}$$

folgt

$$\min\{k \geq 0 \mid \mathcal{S}_0^{(k)}\Gamma \cap \mathcal{N}^{(n-1)}\Gamma \neq \emptyset\} = b_M p^M. \qquad \square$$

3.4.1 Diskussion der rationalen Kurven $\bigcup_{t\in K^+}(\mathcal{S}_t^{(b_M p^M)}\Gamma \cap \mathcal{N}^{(n-1)}\Gamma)$

Wir wollen jetzt diskutieren, wann die Spur der $b_M p^M$ – Schmiegräume im $(n-1)$ – Knoten eine rationale Normkurve ist. Mit den obigen Voraussetzungen ($n+1=\sum_{\lambda=M}^{J} b_\lambda p^\lambda$) müssen wir also die $b_M p^M$-te Spalte im Pascal–Quadrat näher untersuchen.

Satz 3.4.3 *Die Kurve* $\bigcup_{t\in K^+}(\mathcal{S}_t^{(b_M p^M)}\Gamma \cap \mathcal{N}^{(n-1)}\Gamma)$ *ist eine rationale Normkurve, wenn eine der folgenden Bedingungen erfüllt ist:*

1. $J = M+1$ *und* $b_J = 1$, *also* $n+1 = p^{M+1} + b_M p^M$
2. $M = 0, b_0 = p-1$ *und der Grundkörper* K *ist vollkommen*

Beweis: Wir müssen in der $b_M p^M$-ten Spalte von $\square$ die Abfolge von Nullen und „Nicht–Nullen“ untersuchen. Wie sich gleich herausstellen wird, ist es sinnvoll, hier zwei Fälle zu unterscheiden:

1. $M = 0$: Wir durchlaufen die Spalte b_0 von der Stelle 0 bis zur Stelle n, betrachten also den Binomialkoeffizienten $\binom{\mu}{b_0}$ und lassen μ von 0 bis n laufen. Aus

$$\begin{aligned} \mu &= (\mu_J, \ldots, \mu_1, \mu_0) \\ b_0 &= (0, \ldots, 0, b_0) \end{aligned}$$

und dem Lemma 1.1.1 von Lucas folgern wir, daß einander stets Blöcke mit b_0 Nullen und solche mit $p-b_0$ Elementen ungleich Null abwechseln, je nach

$$0 \le \mu_0 \le b_0 - 1$$

oder

$$b_0 \le \mu_0 \le p-1.$$

Jetzt müssen wir zwei Möglichkeiten unterscheiden:

(a) $b_0 < p-1$: Die Länge der Abschnitte von Elementen ungleich Null ist größer als Eins. Hier handelt es sich gewiß dann um rationale Normkurven, wenn es nur einen solchen Block bis zur n–ten Zeile gibt. Es folgt $n = p + b_0 - 1$ bzw. $n+1 = p+b_0$.

(b) $b_0 = p-1$: Wie wir uns leicht überlegen, folgt in der Spalte b_0 von $\square$ einem Abschnitt von $p-1$ Nullen stets eine Eins und umgekehrt. Der Punkt $\mathcal{S}_t^{(p-1)}\Gamma \cap \mathcal{N}^{(n-1)}\Gamma$ hat dann die Gestalt

$$K(\underbrace{0,\ldots,0}_{(p-1)-\text{mal}},1,\underbrace{0,\ldots,0}_{(p-1)-\text{mal}},t^p,\underbrace{0,\ldots,0}_{(p-1)-\text{mal}},t^{2p},\ldots). \tag{3.14}$$

Laut [24, S. 139] ist ein Körper der Charakteristik p genau dann vollkommen, wenn es zu jedem Element in K eine p-te Wurzel gibt.

Ist nun der Grundkörper vollkommen, dann bilden die Punkte (3.14) eine Normkurve.

2. $M > 0$: Wir untersuchen die $b_M p^M$–te Spalte von $\square$ und fragen daher, wann der Binomialkoeffizient $\binom{\mu}{b_M p^M}$ verschwindet, während μ die natürlichen Zahlen durchläuft.

Wiederum beantworten die Darstellung

$$\begin{aligned} \mu &= (\mu_J,\ldots,\mu_M,\ldots,\mu_0) \\ b_M p^M &= (\ldots,0,b_M,0,\ldots) \end{aligned}$$

und das Lemma 1.1.1 von Lucas unsere Frage. Abhängig davon, ob

$$0 \le \mu_M \le b_M - 1$$

oder

$$b_M \le \mu_M \le p-1$$

gilt, verschwindet der entsprechende Binomialkoeffizient oder nicht. Die Blöcke der Nullen haben daher die Länge $b_M p^M$, die anderen die Länge $(p-b_M)p^M$.

Analog zum vorigen Fall wechseln diese Abschnitte einander immer wieder ab. Um rationale Normkurven handelt es sich also sicherlich, wenn wir mit μ bis zur Zeile $n = p^{M+1} + b_M p^M - 1$ laufen. $\square$

3.5 Existenz einpunktiger Knoten

Wir bestimmen für feste Charakteristik p jene Dimensionen n, für die es einpunktige Knoten gibt.

Satz 3.5.1 *Unter der Voraussetzung $\#K \ge k$ gibt es genau für*

$$n = 2p^i - 2$$

einpunktige Knoten.

Beweis: Wenn ein Knoten $\mathcal{N}^{(k)}\Gamma$ aus nur einem Punkt besteht, dann gilt notwendigerweise $\Phi(i,n) = 1$ für ein $i \in \mathbb{N}^+$. Alle Faktoren in (1.2) müssen dann den Wert 1 annehmen, also

$$\begin{aligned} n_0 &= p-2 \\ n_1 &= p-1 \\ &\vdots \\ n_{i-1} &= p-1 \\ n_i &= 1 \\ n_\lambda &= 0 \quad \text{für } \lambda \geq i+1, \end{aligned}$$

woraus

$$\begin{aligned} n &= \langle 1, p-1, \ldots, p-1, p-2 \rangle \\ &= 2p^i - 2 \end{aligned} \tag{3.15}$$

folgt. Andererseits impliziert (3.15) für alle p die Abschätzung $b = n+1 < p^{i+1}$, womit nach (1.5) die Summenfunktion $\Sigma(\mu, n)$ für $\mu \geq i+1$ stets den Wert 0 annimmt. Wie behauptet gilt also $\Phi(i,n) = \Sigma(i,n) = 1$. □

Bemerkung 3.5.2 Auf Grund der Symmetrie des Pascal-Dreiecks handelt es sich bei einpunktigen Knoten um den Basispunkt P_{p^i-1}. Man beachte, daß dieser Punkt unter allen Kollineationen der Gruppe PΓL(Γ) invariant bleibt, vgl. auch [20], [5, 49–50] und [19]. Außerdem werden wir in den nächsten Abschnitten noch sehen, daß das der einzige Punkt mit dieser Eigenschaft ist.

Kapitel 4

Die invarianten Unterräume

Aus den letzten Abschnitten geht hervor, daß die Knoten zu jenen Unterräumen in $\mathrm{PG}(n, K)$ zählen, die invariant unter der Gruppe $\mathrm{P\Gamma L}(\Gamma)$ der automorphen Kollineationen von Γ bleiben. In diesem Kapitel geben wir für $K \geq n+2$ alle invarianten Unterräume an und zeigen unter anderem, daß der zugehörige Verband im allgemeinen nicht totalgeordnet ist, was auf Grund des totalgeordneten Teilverbandes der k-Knoten a priori nicht selbstverständlich ist. Aus Satz 4.1.2 werden wir folgern, daß es genügt, jene Unterräume zu bestimmen, die unter der Gruppe $\mathrm{PGL}(\Gamma)$ aller projektiven Kollineationen invariant bleiben. Wegen der Voraussetzung $K \geq n+2$ ergibt sich dann auch die Invarianz unter $\mathrm{P\Gamma L}(\Gamma)$.

Wir machen in diesem Kapitel die Generalvoraussetzungen $\mathrm{char}K = p$ und $\#K \geq n+2$, womit auf den Sonderfall eines „kleinen“ Grundkörpers verzichtet wird. Die Sätze und Ergebnisse dieses Abschnitts können für $\#K < n+2$ nicht direkt übernommen werden, weil hier die Bedingungen für die Existenz invarianter Unterräume nicht mehr notwendig und hinreichend, sondern nur mehr hinreichend sind. Die Stellen, wo $\#K \geq n+2$ eingeht, werden wir stets herausstreichen.

4.1 Notwendige und hinreichende Bedingungen für invariante Unterräume

Wie wir aus Satz 2.2.2 bereits wissen, wird jede projektive automorphe Kollineation einer rationalen Normkurve Γ durch ein Produkt der Matrizen

$$A_a = \mathrm{diag}(1, a, \ldots, a^n), \quad B = \begin{pmatrix} 0 & 0 & \ldots & 0 & 1 \\ 0 & 0 & \ldots & 1 & 0 \\ \vdots & \vdots & \ldots & \vdots & \vdots \\ 0 & 1 & \ldots & 0 & 0 \\ 1 & 0 & \ldots & 0 & 0 \end{pmatrix}$$

$$\text{und} \quad C_t = \begin{pmatrix} \binom{0}{0} & 0 & 0 & \dots & 0 \\ \binom{1}{0}t & \binom{1}{1} & 0 & \dots & 0 \\ \binom{2}{0}t^2 & \binom{2}{1}t & \binom{2}{2} & \dots & 0 \\ \vdots & & & \ddots & \vdots \\ \binom{n}{0}t^n & \binom{n}{1}t^{n-1} & \binom{n}{2}t^{n-2} & \dots & \binom{n}{n} \end{pmatrix}$$

mit $a \in K^\times, t \in K$ induziert.

Bei der Bestimmung aller invarianten Unterräume gehen wir schrittweise vor und überlegen einmal, welche Unterräume unter allen durch Matrizen

$$A_a = \text{diag}(1, a, a^2, \dots, a^n) \tag{4.1}$$

induzierten Kollineationen invariant bleiben.

Satz 4.1.1 *Ein Unterraum $\mathcal{U}$ wird für $\#K \geq n+2$ genau dann unter allen durch Diagonalmatrizen (4.1) induzierten Kollineationen auf sich abgebildet, wenn $\mathcal{U}$ durch Grundpunkte aufgespannt wird.*

Beweis: „ $\Rightarrow$ “ : Wenn wir uns überlegen, welche Unterräume unter allen Abbildungen[1] $\text{diag}(1, a, a^2, \dots, a^n)$ invariant bleiben, müssen wir alle Fälle von $\text{char}K = p$ berücksichtigen. Wir zeigen, daß stets ein Element $\alpha \in K$ existiert, so daß die Potenzen $1, \alpha, \dots, \alpha^n$ paarweise verschieden sind.

- $K = GF(q)$: Da $K^\times$ zyklisch ist (mit erzeugendem Element α) und weiters wegen unserer Generalvoraussetzung $\#K^\times \geq n+1$ gilt, sind die Potenzen $1, \alpha, \dots, \alpha^n$ paarweise verschieden.

- Sei $\#K = \infty$ und zu jedem $n \in \mathbb{N}$ gebe es ein $q \geq n+2$ mit $GF(q) \subset K$. Aus denselben Gründen wie zuvor existiert α mit $1, \alpha, \dots, \alpha^n$ paarweise verschieden.

- Sei $\#K = \infty$ und es existiere ein maximales q mit $F = GF(q) \subset K$. Jedes Element $\alpha \in K \backslash F$ ist transzendent über F, weil sonst wäre der Zwischenkörper $F(\alpha)$ mit $F \subset F(\alpha) \subset K$ endlichdimensional über F und q nicht maximal bezüglich $GF(q) \subset K$.
  Für jedes n sind deshalb die Potenzen $1, \alpha, \dots, \alpha^n$ paarweise verschieden.

Da in der Diagonalmatrix $A := \text{diag}(1, \alpha, \alpha^2, \dots, \alpha^n)$ in der Hauptdiagonale die paarweise verschiedenen Eigenwerte stehen (mit den von der kanonischen Basis aufgespannten jeweils eindimensionalen Eigenräumen), sind die Fixpunkte unter der durch A induzierten Kollineation genau die Basispunkte.

[1] Wir unterscheiden i.f. nicht scharf zwischen einer regulären Matrix und der durch die Matrix induzierten Kollineation

Sei nun U ein invarianter Unterraum von K^{n+1} unter A, also $A(U) = U$ mit $\dim U = k \geq 1$. Wenn man im Vektorraum einen Basiswechsel so durchführt, daß man eine Basis von U durch Vektoren der kanonischen Basis zu einer Gesamtbasis ergänzt, dann entspricht der linearen Abbildung folgende Matrix:

$$\begin{pmatrix} \alpha^{j_0} & & & 0 \\ & \ddots & & \\ & & \alpha^{j_{n-k}} & \\ & & & \square \\ 0 & & & \end{pmatrix}$$

Für $s \neq t$ ist $j_s \neq j_t$, und $\square$ steht für jene quadratische Teilmatrix, die der Einschränkung $A \,|\, _U$ entspricht. Da die Eigenwerte eine Eigenschaft der Abbildung sind, ändert sich durch den Basiswechsel nichts am charakteristischen Polynom. Dieses schreibt sich auf Grund der Bauart der Matrix aber als

$$p(x) = (x - \alpha^{j_0}) \dots (x - \alpha^{j_{n-k}}) u(x),$$

wobei $u(x)$ das charakteristische Polynom von $A \,|\, _U$ ist. Da $p(x)$ in Linearfaktoren zerfällt, trifft dies auch für $u(x)$ zu, $\square$ ist diagonalisierbar, und U wird durch jene restlichen Vektoren der kanonischen Basis aufgespannt, die nicht zu einem der Eigenwerte $\alpha^{j_0}, \dots, \alpha^{j_{n-k}}$ gehören. Der zugehörige projektive Unterraum $\mathcal{U}$ wird also durch Grundpunkte aufgespannt.

„ $\Leftarrow$ “ : Wenn $\mathcal{U}$ durch Grundpunkte aufgespannt wird, dann besitzt der entsprechende Untervektorraum U eine Teilmenge der kanonischen Basis als Erzeugendensystem, und U bleibt daher unter allen Diagonalmatrizen invariant. $\square$

Wir wissen jetzt also, daß wir uns für $\#K \geq n + 2$ bei der Bestimmung aller unter $\mathrm{PGL}(\Gamma)$ invarianten Unterräume auf solche beschränken dürfen, die durch Basispunkte aufgespannt werden.

Satz 4.1.2 *Für $\#K \geq n + 2$ bleiben die unter* $\mathrm{PGL}(\Gamma)$ *invarianten Unterräume auch unter allen nicht projektiven automorphen Kollineationen von* Γ *invariant.*

Beweis: Der Beweis ist sofort erledigt: Da alle Körperautomorphismen $\zeta \in \mathrm{Aut}(K)$ die Eigenschaft

$$\begin{aligned} \zeta(0) &= 0 \\ \zeta(1) &= 1 \end{aligned}$$

besitzen und für $\#K \geq n + 2$ die unter $\mathrm{PGL}(\Gamma)$ invarianten Unterräume durch Grundpunkte aufgespannt werden, ist alles gezeigt. $\square$

Unter all diesen Unterräumen bestimmen wir nun jene, die auch unter der durch

$$B = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & 1 & 0 \\ \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & 1 & \dots & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 \end{pmatrix} \tag{4.2}$$

induzierten Kollineation invariant bleiben.

Satz 4.1.3 *Ein durch Grundpunkte P_j aufgespannter Unterraum $\mathcal{U}$ ist genau dann invariant unter der durch (4.2) induzierten Kollineation, wenn die „Symmetriebedingung“*

$$P_j \in \mathcal{U} \quad \Leftrightarrow \quad P_{n-j} \in \mathcal{U} \quad \forall j \in \{0, 1, \dots, n\} \tag{4.3}$$

erfüllt ist.

Beweis: Da $\mathcal{U}$ durch Grundpunkte aufgespannt ist, folgt der Beweis unmittelbar aus der Bauart der Matrix B. □

Bemerkung 4.1.4 Während wir in Satz 4.1.1 die Voraussetzung $\#K \geq n+2$ getroffen haben, ist Satz 4.1.3 für beliebige Grundkörper gültig.

Aus den Sätzen 4.1.1 und 4.1.3 folgern wir, daß bei $\#K \geq n+2$ ein invarianter Unterraum zwingend von Grundpunkten aufgespannt wird und die Symmetriebedingung (4.3) erfüllt. Wir müssen jetzt noch prüfen, wann ein Unterraum mit dieser Eigenschaft auch invariant unter allen Abbildungen

$$C_t := \begin{pmatrix} \binom{0}{0} & 0 & 0 & \dots & 0 \\ \binom{1}{0}t & \binom{1}{1} & 0 & \dots & 0 \\ \binom{2}{0}t^2 & \binom{2}{1}t & \binom{2}{2} & \dots & 0 \\ \vdots & & & \ddots & \vdots \\ \binom{n}{0}t^n & \binom{n}{1}t^{n-1} & \binom{n}{2}t^{n-2} & \dots & \binom{n}{n} \end{pmatrix} \tag{4.4}$$

bleibt, also $C_t(\mathcal{U}) = \mathcal{U} \ \forall \ t \in K$ gilt.

Dazu bedarf es einiger Begriffsbildungen und Überlegungen, wie etwa, daß für $P_j \in \mathcal{U}$ stets auch die Bahn $\{C_t(P_j) \mid t \in K\}$ und der von ihr aufgespannte Unterraum in $\mathcal{U}$ liegen müssen.

Definition 4.1.5 *Für alle j mit $0 \leq j \leq n$ bezeichnen wir den von der Bahn $\{C_t(P_j) \mid t \in K\}$ eines Basispunktes P_j aufgespannten Unterraum mit $\mathcal{O}_j$, also*

$$\mathcal{O}_j := [\{C_t(P_j) \mid t \in K\}]. \tag{4.5}$$

Wir entnehmen der Matrix (4.4), daß $\{P_m \mid (j \preceq m) \wedge (0 \leq m \leq n)\}$ eine Basis eines Unterraumes $\mathcal{U}_j$ mit

$$\mathcal{O}_j \subseteq \mathcal{U}_j$$

ist. Bevor wir in einem Lemma Auskunft darüber geben, wann

$$\mathcal{O}_j = \mathcal{U}_j$$

gilt, stellen wir für die Menge aller $m \leq n$ mit $m \succeq j$ eine abkürzende Schreibweise bereit.

Definition 4.1.6 *Für $j \in \mathbb{N}$ definieren wir bei festem $n \in \mathbb{N}$*

$$\Omega(j) := \{m \in \mathbb{N} \mid 0 \leq m \leq n, j \preceq m\}. \tag{4.6}$$

Damit läßt sich folgendes Lemma formulieren.

Lemma 4.1.7 *Für $\#K > n - j$ bildet $\{P_m \mid m \in \Omega(j)\}$ eine Basis von $\mathcal{O}_j$.*

Beweis: Wegen $\#K > n - j$ existieren $J := n - j + 1$ paarweise verschiedene Elemente $t_1, t_2, \ldots, t_J \in K$. Wir transponieren den j-ten Spaltenvektor $c_t^{(j)}$ der Matrix C_t, setzen für den Parameter t für $\lambda = 1, 2, \ldots, J$ die einzelnen Werte t_λ ein und fassen die so erhaltenen Zeilenvektoren zur Matrix

$$D = \begin{pmatrix} 0 & \ldots & 0 & \binom{j}{j} & \binom{j+1}{j} t_1 & \binom{j+2}{j} t_1^2 & \ldots & \binom{n}{j} t_1^{n-j} \\ 0 & \ldots & 0 & \binom{j}{j} & \binom{j+1}{j} t_2 & \binom{j+2}{j} t_2^2 & \ldots & \binom{n}{j} t_2^{n-j} \\ 0 & \ldots & 0 & \binom{j}{j} & \binom{j+1}{j} t_3 & \binom{j+2}{j} t_3^2 & \ldots & \binom{n}{j} t_3^{n-j} \\ \vdots & \ldots & \vdots & \vdots & \vdots & \vdots & \ldots & \vdots \\ 0 & \ldots & 0 & \binom{j}{j} & \binom{j+1}{j} t_J & \binom{j+2}{j} t_J^2 & \ldots & \binom{n}{j} t_J^{n-j} \end{pmatrix},$$

zusammen. Diese $J \times (n+1)$–Matrix induziert eine lineare Abbildung

$$K^{n+1} \mapsto K^J.$$

Jene Vektoren e_m der kanonischen Basis, für die $\binom{m}{j}$ modulo p verschwindet, liegen offensichtlich im Kern der Abbildung D.

Indirekt zeigen wir nun, daß diese Vektoren auch ein Erzeugendensystem des Kerns bilden: Sei also $x \in K^{n+1}$ mit $x_\mu \neq 0$, $Dx = 0$ und $\binom{\mu}{j} \not\equiv 0 \pmod{\mathrm{char}K}$ gegeben.

Es existiert also ein vom Nullpolynom verschiedenes Polynom

$$q(t) = \sum_{\lambda=0}^{n} x_\lambda \binom{\lambda}{j} t^{\lambda - j} \in K[t],$$

welches mehr Nullstellen besitzt, als der Grad angibt. Das führt jedoch zu einem Widerspruch. Mit der Rangformel

$$\mathrm{rg}D + \mathrm{def}D = \dim K^{n+1} = n+1$$

ist das Lemma dann bewiesen. □

Damit können wir jetzt in einem Satz die von Grundpunkten aufgespannten Unterräume bestimmen, die unter der Gruppe $\{C_t \mid t \in K\}$ invariant bleiben.

Satz 4.1.8 *Ein von Grundpunkten aufgespannter Unterraum* $\mathcal{U} = [\{P_\psi \mid \psi \in \Psi\}]$ *mit* $\Psi \subseteq \{0, 1, \ldots, n\}$ *ist für* $\#K > n$ *genau dann invariant unter der Gruppe* $\{C_t \mid t \in K\}$ *(vgl. (4.4)), wenn* $\mathcal{U}$ *für jeden Index* $j \in \Psi$ *auch die Menge*

$$\{P_m \mid m \in \Omega(j)\}$$

enthält.

Beweis: Der Beweis ist in zwei Richtungen zu führen:

1. „ $\Rightarrow$ “: Aus der Invarianz von $\mathcal{U}$ unter $\{C_t \mid t \in K\}$ folgt notwendigerweise für alle $j \in \Psi$ die Inklusion $\mathcal{O}_j \subseteq \mathcal{U}$. Wegen $\#K > n$ greift Lemma 4.1.7 für alle $j \leq n$. Daraus erhalten wir unmittelbar

$$\{P_m \mid m \in \Omega(j)\} \subseteq \mathcal{O}_j \subseteq \mathcal{U}.$$

2. „ $\Leftarrow$ “: Aus

$$\{P_m \mid m \in \Omega(j)\} \subseteq \mathcal{U}$$

folgt

$$\mathcal{O}_j \subseteq [\{P_m \mid m \in \Omega(j)\}] \subseteq \mathcal{U},$$

und daher sind die durch Satz 4.1.8 beschriebenen Unterräume immer (auch für $\#K \leq n$) invariant unter $\{C_t \mid t \in K\}$. Die Bedingung ist also auch hinreichend. □

Bemerkungen 4.1.9

1. Wenn bei $\#K > n$ für $P_j \in \mathcal{U}$ schon die Inklusion $\mathcal{O}_j \subseteq \mathcal{U}$ verifiziert worden ist, dann braucht dies für $m \succeq j$ nicht mehr überprüft werden, weil auf Grund der Transitivität der Halbordnung „ $\preceq$ “ unmittelbar

$$m \succeq j \;\Rightarrow\; \Omega(m) \subseteq \Omega(j) \;\Rightarrow\; \mathcal{O}_m \subseteq \mathcal{O}_j,$$

also auch $\mathcal{O}_m \subset \mathcal{U}$ folgt.

2. Für $j \not\preceq n$ gelte
$$(n, j) \in \nabla^i$$
für ein bestimmtes i. Wir überlegen uns leicht, daß für alle $m \in \Omega(j)$ dann
$$(n, m) \in \nabla^{i+\alpha},$$
für ein $\alpha \in \mathbb{N}$ gilt.

Indem wir jetzt die Sätze 4.1.1, 4.1.3 und 4.1.8 Revue passieren lassen, können wir den Hauptsatz für invariante Unterräume formulieren:

4.1.1 Der Hauptsatz

Satz 4.1.10 (Hauptsatz) *Unter der Voraussetzung $\#K \geq n + 2$ gilt mit Satz 4.1.2: Die unter* $\mathrm{PGL}(\Gamma)$ *invarianten Unterräume $\mathcal{U}$ sind auch unter* $\mathrm{P\Gamma L}(\Gamma)$ *invariant, und sie lassen sich folgendermaßen charakterisieren:*

Ein Unterraum $\mathcal{U}$ ist genau dann invariant unter $\mathrm{PGL}(\Gamma)$*, wenn er von Grundpunkten P_j aufgespannt wird und für deren Indizes j folgende Bedingungen erfüllt sind:*

1. *Für alle j wird die Symmetrieeigenschaft $P_j \in \mathcal{U} \Leftrightarrow P_{n-j} \in \mathcal{U}$ erfüllt.*
2. *Aus $P_j \in \mathcal{U}$ folgt auch $\{P_m \mid m \in \Omega(j)\} \subset \mathcal{U}$.*

Bemerkung 4.1.11 Der Hauptsatz führt eine geometrische Fragestellung in eine zahlentheoretische über. Genau dann, wenn eine Indexmenge Ψ gewisse Forderungen erfüllt, spannt die zugehörige Menge $\{P_\psi \mid \psi \in \Psi\}$ einen unter $\mathrm{PGL}(\Gamma)$ invarianten Unterraum auf. Dies halten wir jetzt in einem Korollar fest.

Korollar 4.1.12 *Ein Unterraum $\mathcal{U}$ ist genau dann invariant unter* $\mathrm{PGL}(\Gamma)$*, wenn folgende Bedingungen erfüllt sind:*

1. *Es gilt $\mathcal{U} = [\{P_\psi \mid \psi \in \Psi\}]$ und $\Psi \subset \{0, 1, \ldots, n\}$.*
2. *Für alle j wird die Symmetrieeigenschaft $j \in \Psi \Leftrightarrow n - j \in \Psi$ erfüllt.*
3. *Aus $j \in \Psi$ folgt auch $\Omega(j) \subset \Psi$.*

Wir können somit bei gegebenem n und $\mathrm{char}K$ durch Überprüfen für jede Menge Ψ von Indizes feststellen, ob $\{P_\psi \mid \psi \in \Psi\}$ einen unter $\mathrm{PGL}(\Gamma)$ invarianten Unterraum aufspannt. Durch einige Überlegungen schließen wir im folgenden gewisse Mengen Ψ aus und sparen so entscheidend Zeit.

4.1.2 Einschränkung möglicher Mengen Ψ

Satz 4.1.13 *Jeder invariante Unterraum $\mathcal{U} \neq \mathcal{P}$ liegt für $\#K \geq n+2$ im Durchschnitt aller Schmieghyperebenen, dem $(n-1)$–Knoten.*

Beweis:

1. Liegt ein Normkurvenpunkt $X \in \Gamma$ im Unterraum $\mathcal{U}$, dann folgt unmittelbar $\Gamma \subset \mathcal{U}$, indem man auf die Beziehung $X \in \mathcal{U}$ die Gruppe $\mathrm{PGL}(\Gamma)$ wirken läßt. Auf Grund der Generalvoraussetzung $\#K \geq n+2$ spannt Γ den ganzen Raum $\mathcal{P}$ auf, und daher entspricht $\mathcal{U}$ dem Gesamtraum.

2. Wenn nun $\mathcal{U}$ nicht der ganze Raum $\mathcal{P}$ ist, dann gilt jedenfalls $P_0, P_n \notin \mathcal{U}$. Der Unterraum $\mathcal{U}$ liegt somit in der Hülle der Grundpunkte $P_1, P_2, \ldots, P_{n-1}$, also
$$\mathcal{U} \subseteq (\mathcal{S}_0^{n-1}\Gamma \cap \mathcal{S}_\infty^{n-1}\Gamma).$$
Auf diese Beziehung lassen wir die Kollineationsgruppe wirken und folgern, daß $\mathcal{U}$ jeweils im Durchschnitt der Schmieghyperebenen zweier beliebiger Normkurvenpunkte enthalten ist, und daher im Durchschnitt aller (dem $(n-1)$–Knoten). □

Da wir von nun an öfters jene $(n+1) \times (n+1)$–Matrix ansprechen, die sich als Schnitt der ersten $n+1$ Zeilen und Spalten von $\square$ ergibt, möchten wir dafür eine Kurzschreibweise einführen.

Definition 4.1.14 *Die $(n+1) \times (n+1)$–Matrix, die sich als Schnitt der ersten $n+1$ Zeilen und Spalten von $\square$ ergibt, wird von nun an mit $\square_n$ abgekürzt.*

Bemerkung 4.1.15 Man beachte die Identität
$$\square^j = \square_{p^j}.$$

Nun können wir in einem Lemma eine weitere Einschränkung für Indexmengen Ψ treffen, welche zu invarianten Unterräumen führen.

Lemma 4.1.16 *Sei $\#K \geq n+2$ und $\mathcal{U} = [\{P_\psi \mid \psi \in \Psi\}]$ ein unter* $\mathrm{PGL}(\Gamma)$ *invarianter Unterraum. Wenn wir*
$$\psi_{\max} := \max \Psi$$
setzen und die $\psi_{\max}$-te Spalte von $\square_n$ betrachten, dann handelt es sich dabei stets um einen Vektor der kanonischen Basis von K^{n+1}.

Beweis: Wir führen den Beweis indirekt, und nehmen daher an, daß in der entsprechenden Spalte kein Vektor der kanonischen Basis steht. Es existiert also ein Index ν mit

$$\psi_{\max} < \nu \leq n \quad \text{und} \quad \nu \succeq \psi_{\max}.$$

Da $\mathcal{U}$ invariant ist, folgt

$$\nu \in \Omega(\psi_{max}) \subset \Psi,$$

wodurch wir sofort einen Widerspruch zu $\psi_{max} = \max \Psi$ erhalten. □

Wir fassen jetzt ausführlich zusammen, was wir aus Satz 4.1.13 und Lemma 4.1.16 folgern können.

Folgerungen 4.1.17 Bei der Auswahl der entsprechenden Indexmengen Ψ, die zur Konstruktion nichttrivialer invarianter Unterräume führen, ist das Pascal–Quadrat das wichtigste Hilfsmittel. Aus Satz 4.1.13 und Lemma 4.1.16 leiten wir folgende Vorgangsweise ab:

Wir betrachten $\square_n$, also jene $(n+1) \times (n+1)$–Matrix, die im Schnitt der ersten $n+1$ Zeilen und Spalten von $\square$ liegt. Aus der Struktur der letzten Zeile und der einzelnen Spalten können wir wertvolle Informationen für mögliche Mengen Ψ beziehen.

1. Da die Stellen der Nullen in der letzten Zeile genau jene Indizes j bestimmen, so daß die Punkte P_j den $(n-1)$–Knoten aufspannen, kommt für eine Menge Ψ, die zu einem nichttrivialen invarianten Unterraum

   $$\mathcal{U} = [\{P_\psi \mid \psi \in \Psi\}]$$

   führt, nur eine der Form

   $$\Psi = \{j \mid (0 < j < n) \wedge (j \not\preceq n)\}$$

   in Frage.

2. Der größte Index $\psi_{\max} := \max \Psi$ muß zu einer Spalte von $\square_n$ gehören, in der ein Vektor der kanonischen Basis steht.

Bevor wir eine allgemeine Theorie zur Berechnung aller invarianter Unterräume entwickeln, wollen wir im nächsten Abschnitt für einige Beispiele exemplarisch den Verband dieser Unterräume bestimmen.

4.2 Beispiele

4.2.1 Der Verband der invarianten Unterräume für $p = 2$ und $n = 4$

Dieses Beispiel wird auch in [6] angesprochen, soll aber hier mit anderen Mitteln behandelt werden.

Wir betrachten also

$$\square_4 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Da in der letzten Zeile genau an den Stellen $1, 2$ und 3 eine Null steht, haben wir für eine Basis eines nichttrivialen Unterraumes $\mathcal{U}$ genau die Grundpunkte P_1, P_2 und P_3 zur Auswahl. Da der größte Index zu einem Vektor der kanonischen Basis von K^5 gehören muß, erhalten wir zwingend $P_3 \in \mathcal{U}$.

Die Symmetriebedingung $P_j \Leftrightarrow P_{n-j}$ erzwingt dann auch $P_1 \in \mathcal{U}$. Aus der 1. Spalte ergibt sich $\Omega(1) = \{1, 3\}$ bzw. $\mathcal{O}_1 = [\{P_1, P_3\}]$. Wir sehen also nach Satz 4.1.10 bzw. Korollar 4.1.12, daß $\mathcal{U} := \mathcal{O}_1$ schon ein invarianter Unterraum ist.

Außer diesem Unterraum gibt es nur noch einen zweiten, der nichttrivial und invariant ist, nämlich den 3–Knoten mit der Basis $\{P_1, P_2, P_3\}$.

Mit

$$\begin{aligned} \mathcal{U}_1 &= \emptyset \\ \mathcal{U}_2 &= [\{P_1, P_3\}] \\ \mathcal{U}_3 &= [\{P_1, P_2, P_3\}] \\ \mathcal{U}_4 &= [\{P_0, P_1, P_2, P_3, P_4\}] = \mathcal{P} \end{aligned}$$

erhalten wir

$$\mathcal{U}_1 \subset \mathcal{U}_2 \subset \mathcal{U}_3 \subset \mathcal{U}_4.$$

Der zugehörige Unterraumverband entspricht hier einer vierelementigen Kette. Zu jedem Basispunkt P_j gibt es minimalen, P_j enthaltenden Unterraum.

Auf Grund dieses Beispiels könnte jetzt der Verdacht aufkeimen, daß die invarianten Unterräume bezüglich der mengentheoretischen Inklusion stets totalgeordnet seien, wobei es sich dabei um die in Kapitel 3 beschriebenen Knoten und gewisse Teilmengen davon handle. Durch das nächste Beispiel wird dem Leser diese Illusion geraubt.

4.2.2 Ein Verband invarianter Unterräume, der nicht totalgeordnet ist

Wir setzen $p = 2$, $n = 12$ und betrachten

$$\square_{12} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Bei der Konstruktion einer Menge Ψ beginnen wir mit dem Index 11, weil in der vorletzten Spalte von $\square_{12}$ ein Basisvektor steht. Aus Symmetriegründen folgt $1 \in \Psi$ und somit auch zwingend

$$\Omega(1) = \{1, 3, 5, 7, 9, 11\} \subset \Psi.$$

Auf Grund der Bemerkungen 4.1.9 brauchen wir für die Indizes $\mu = 3, 5, \ldots, 11$ nicht mehr die Inklusion

$$\Omega(\mu) \subset \Psi$$

zu prfen, weil aus der Transitivität von „ $\preceq$ “ sofort

$$\Omega(\mu) \subset \Omega(1) \subset \Psi$$

folgt.

Die Menge $\Omega(1)$ erfüllt auch die Symmetriebedingung, und daher ist

$$\mathcal{O}_1 = [\{P_\omega \mid \omega \in \Omega(1)\}]$$

ein invarianter Unterraum.

Gibt es nun einen weiteren Unterraum, der echt zwischen $\mathcal{O}_1$ und dem 11–Knoten $[\mathcal{O}_1 \cup \{P_2, P_6, P_{10}\}]$ liegt? Enthielte die zugehörige Menge Ψ die Zahl 10, dann aus Symmetriegründen auch 2 und wegen $\{2, 6, 10\} \subset \Omega(2)$ auch die Zahl 6.

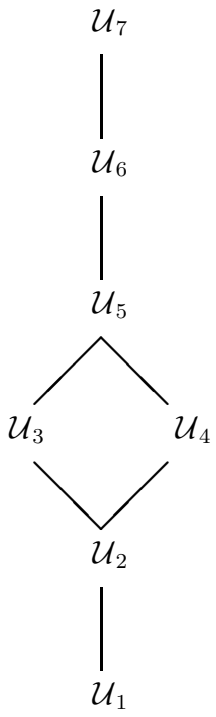
Betrachten wir hingegen $\Omega(1) \cup \{6\}$, dann erhalten wir wegen

$$\Omega(6) = \{6, 7\} \subset (\Omega(1) \cup \{6\})$$

und der „Selbstsymmetrie“ der Zahl 6 einen invarianten Unterraum, der echt zwischen $\mathcal{O}_1$ und dem 11–Knoten liegt.

Nachdem wir somit alle invarianten Unterräume zum äußersten Basisvektor von $\square_{12}$, also zum Index 11 konstruiert haben, wollen wir dies auch noch für den Index 7 machen, denn in $\square_{12}$ steht nur noch in Spalte 7 ein Vektor der kanonischen Basis. Hier sehen wir mit analogen Überlegungen, daß $\Omega(5) = \{5, 7\}$ Korollar 4.1.12 erfüllt und wir somit einen invarianten Unterraum erhalten, der echt im 10–Knoten $[\{P_5, P_6, P_7\}]$ enthalten ist.

Ein kurzer Blick auf den zugehörigem Verband der invarianten Unterräume



mit

$$
\begin{aligned}
\mathcal{U}_1 &= \emptyset \\
\mathcal{U}_2 &= [\{P_5, P_7\}] \\
\mathcal{U}_3 &= [\{P_5, P_6, P_7\}] \\
\mathcal{U}_4 &= [\{P_1, P_3, P_5, P_7, P_9, P_{11}\}] \\
\mathcal{U}_5 &= [\{P_1, P_3, P_5, P_6, P_7, P_9, P_{11}\}] \\
\mathcal{U}_6 &= [\{P_1, P_2, P_3, P_5, P_6, P_7, P_9, P_{10}, P_{11}\}] \\
\mathcal{U}_7 &= \mathcal{P}
\end{aligned}
$$

läßt uns wegen $\mathcal{U}_3 \not\subseteq \mathcal{U}_4$ und $\mathcal{U}_4 \not\subseteq \mathcal{U}_3$ erkennen, daß wir die Hypothese, es könnte sich bei dem Verband der invarianten Unterräume stets um eine Totalordnung handeln, verwerfen müssen.

4.3 Folgerungen aus den Beispielen

1. Die vorigen beiden Beispiele haben eine Gemeinsamkeit: Wir sind stets von einem Index j eines kanonischen Basisvektors ausgegangen, haben danach den symmetrischen Index $j^* := n - j$ betrachtet, die Menge $\Omega(j^*)$ bestimmt und festgestellt, daß diese Indexmenge bereits alle Punkte von Korollar 4.1.12 erfüllt. Im folgenden Abschnitt werden diese „symmetrischen Indizes“ j^* formelmäßig aus der p-adischen Darstellung der Zahl $b = n + 1$ bestimmt, und danach wird gezeigt, daß die zugehörigen Orbiträume $\mathcal{O}_{j^*}$ stets invariant unter $\mathrm{PGL}(\Gamma)$ sind.

2. Man mache sich bewußt, daß dies (Index j zu kanonischem Basisvektor von $\square_n$ bestimmen – symmetrischen Index j^* und die Menge $\Omega(j^*)$ betrachten) lediglich ein erster Schritt zur Bestimmung aller invarianten Unterräume sein kann.

3. Da dieses Vorgehen notwendig für die Invarianz eines Unterraums ist, sind die so erhaltenen Unterräume minimal in gewissem Sinne. Diese „Minimalität“ muß streng von der Aufgabe unterschieden werden, zu einem vorgegebenen Grundpunkt P_j den minimalen invarianten Unterraum zu konstruieren, der P_j enthält.

4.4 Definition der Funktion $V(i, b)$

Definition 4.4.1 *Bei fester Charakteristik p und Dimension n definieren wir die Funktion $V(i, b)$ folgendermaßen:*

$$\begin{aligned} V(i,b): \qquad \mathbb{N} \times \mathbb{N} &\to \mathbb{N} \\ (i,b) &\mapsto \sum_{\lambda=0}^{i-1} b_\lambda p^\lambda \end{aligned} \tag{4.7}$$

Wir überlegen uns jetzt, daß ein zum Index eines Basisvektors von $\square_n$ symmetrischer Index stets einem Wert $V(i, b)$ entspricht.

Bemerkung 4.4.2 Aus Satz 4.1.13 wissen wir

$$P_n \in \mathcal{U} \quad \Rightarrow \quad \mathcal{U} = \mathcal{P},$$

weshalb der letzte Basisvektor von $\square_n$ uns nicht weiter interessiert. Wenn wir

von nun an die Basisvektoren von $\square_n$ betrachten, klammern wir stets den letzten aus, weil dieser nur zu einem trivialen invarianten Unterraum führt (vgl. die Folgerungen 4.1.17).

Für nichtleere Mengen $\overline{i(n)} \neq \emptyset$ wiederholen wir Formel (1.13) aus Abschnitt 1.4.2:

$$\max \overline{i(n)} = T(i,b) - 1 = \langle \ldots, n_{i+1}, n_i - 1, p-1, \ldots, p-1 \rangle$$

Genau diese Werte $T(i,b)-1$ sind die Indizes der Basisvektoren von $\square_n$, und davon gibt es so viele (abgesehen vom letzten), wie verschiedene nichtleere Mengen $\overline{i(n)}$ existieren.

Wenn wir, wie in Abschnitt 4.3 beschrieben, zu den bezüglich n „symmetrischen“ Indizes übergehen, dann erhalten wir

$$n - (T(i,b) - 1) = b - T(i,b) = V(i,b).$$

Die für alle $i \in \mathbb{N}$ gültige Identität

$$V(i,b) = b - T(i,b) \tag{4.8}$$

geht hier entscheidend ein. Aus Symmetriegründen erhalten wir für $\overline{i(n)} \neq \emptyset$ aus

$$\max \overline{i(n)} = T(i,b) - 1$$

sofort

$$\min \overline{i(n)} = V(i,b). \tag{4.9}$$

Bemerkungen 4.4.3

1. Wenn wir wie in Abschnitt 3.4

$$M := \min\{\lambda \mid b_\lambda \neq 0\} \tag{4.10}$$
$$J := \max\{\lambda \mid b_\lambda \neq 0\} \tag{4.11}$$

setzen, erhalten wir

$$V(i,b) = 0 \quad \text{für} \quad i \leq M$$
$$V(i,b) = b = n+1 \quad \text{für} \quad i \geq J+1$$

Die zugehörigen Bereiche der Indexmenge, also

$$\{i \in \mathbb{N} \mid (i \leq M) \vee (i \geq J+1)\}$$

sind im Zusammenhang mit der Bestimmung invarianter Unterräume uninteressant.

2. Wir wollen also ab jetzt nur mehr die Menge

$$W := \{V(i,b) \mid M+1 \leq i \leq J\} \tag{4.12}$$

betrachten. Da die Abbildung

$$\{M+1, M+2, \ldots, J\} \to W : \quad i \mapsto V(i,b)$$

nicht injektiv zu sein braucht, zeichnen wir unter den Urbildern eines festen Bildes jeweils das Maximum als Repräsentant aus, um zu einer einheitlichen Bezeichnung der Elemente aus W zu gelangen.

Seien $M = N_1 < N_2 < \ldots < N_d = J$ die Positionen der von Null verschiedenen Stellen von b in der Basis p. Mit

$$V(N_\alpha + 1, b) = V(N_\alpha + 2, b) = \ldots = V(N_{\alpha+1}, b) < V(N_{\alpha+1} + 1, b)$$

für alle $\alpha \in \{1, 2, \ldots, d-1\}$ und

$$D := \{N_{\alpha+1} \mid \alpha \in \{1, 2, \ldots, d-1\}\} \tag{4.13}$$

wird die Abbildung

$$D \to W : \quad i \mapsto V(i,b)$$

bijektiv.

Jetzt überlegen wir, in welchem ∇^i die Paare $(n, V(i,b))$ mit $i \in D$ liegen:

Mit Formel (1.5) aus Abschnitt 1.4.1 erhalten wir

- im Falle $1 \leq i \leq M = N_1$: $\overline{i(n)} = \emptyset$ für alle i
- im Falle $i > M = N_1$: $\overline{i(n)} = \emptyset$ falls $b_i = 0$

Es gibt also genau $d-1$ nichtleere Mengen $\overline{i(n)} \neq \emptyset$, und zwar

$$\overline{N_2(n)}, \overline{N_3(n)}, \ldots, \overline{N_d(n)}$$

mit

$$\begin{array}{rcll} \max \overline{N_\alpha(n)} & = & T(N_\alpha, b) - 1 & \alpha \in \{2, \ldots, d\} \\ \min \overline{N_\alpha(n)} & = & V(N_\alpha, b) & \alpha \in \{2, \ldots, d\}. \end{array}$$

Wir haben die Werte $V(i,b)$ also genau so indiziert, daß

$$(n, V(i,b)) \in \nabla^i \tag{4.14}$$

gilt.

4.4.1 Praktische Berechnung der symmetrischen Indizes $V(i,b)$

An einem Beispiel soll illustriert werden, wie wir die Indizes $V(i,b)$ berechnen:

In der Basis $p = 2$ ergibt sich für die Dimension $n = 371$ etwa

$$\begin{aligned} n &= \langle 1,0,1,1,1,0,0,1,1\rangle \\ b &= \langle 1,0,1,1,1,0,1,0,0\rangle \end{aligned}$$

Mit den Bezeichnungen von vorher erhalten wir

$$N_1 = 2, N_2 = 4, N_3 = 5, N_4 = 6, N_5 = 8.$$

Die letzte Zeile in $\square_{371}$ trifft also ∇^4, ∇^5, ∇^6 und ∇^8, und es gilt:

$$\begin{aligned} V(4,b) = \min \overline{4(n)} &= \langle 0,1,0,0\rangle = 4 \\ V(5,b) = \min \overline{5(n)} &= \langle 1,0,1,0,0\rangle = 20 \\ V(6,b) = \min \overline{6(n)} &= \langle 1,1,0,1,0,0\rangle = 52 \\ V(8,b) = \min \overline{8(n)} &= \langle 0,1,1,1,0,1,0,0\rangle = 116 \end{aligned}$$

4.5 Invariante Unterräume der Form $\mathcal{O}_{V(i,b)}$

Wir zeigen in diesem Abschnitt, daß für alle $i \in D$ (vgl. (4.13)) die Menge

$$\mathcal{O}_{V(i,b)} = [\{P_\omega \mid \omega \in \Omega(V(i,b))\}]$$

den Hauptsatz 4.1.10 erfüllt.

Satz 4.5.1 *Die von Basispunkten aufgespannten Unterräume der Form*

$$\mathcal{O}_{V(i,b)} = [\{P_\omega \mid \omega \in \Omega(V(i,b))\}]$$

sind für alle $i \in D$ invariant unter der Gruppe $\mathrm{PGL}(\Gamma)$. *Der Grundkörper K unterliegt hierbei keiner Einschränkung.*

Beweis: Da es sich hier um die Bahn eines einzigen Punktes handelt (vgl. Definition 4.1.5 und Lemma 4.1.7), ist lediglich der erste Punkt des Hauptsatzes 4.1.10 zu verifizieren. Die Menge $\Omega(V(i,b))$ muß also bezüglich der „Symmetrieabbildung“

$$j \mapsto n - j =: j^*$$

abgeschlossen sein.

Wir wollen die Elemente $j \in \Omega(V(i,b))$ genauer beschreiben. Dazu wiederholen wir, was sich aus der Definition von M in Formel 4.10 unmittelbar ergibt:

$$\begin{aligned} n_0 &= n_1 = \ldots = n_{M-1} = p-1 \\ b_0 &= b_1 = \ldots = b_{M-1} = 0 \\ b_M &= n_M + 1 \\ b_\lambda &= n_\lambda \quad \text{für} \quad \lambda > M \end{aligned}$$

Daraus erhalten wir

$$j \in \Omega(V(i,b)) \quad \Leftrightarrow \quad j \leq n \text{ und } j \succeq V(i,b).$$

Letzteres bedeutet ausführlich geschrieben:

$$\begin{aligned} j_0 &\in \{0,1,\ldots,p-1\} \text{ beliebig} \\ &\vdots \\ j_{M-1} &\in \{0,1,\ldots,p-1\} \text{ beliebig} \\ j_M &> n_M \\ j_{M+1} &\geq n_{M+1} \\ &\vdots \\ j_{i-1} &\geq n_{i-1} \\ j_i &\in \{0,1,\ldots,p-1\} \text{ beliebig} \end{aligned} \tag{4.15}$$

Jetzt berechnen wir zu einem beliebigen $j \in \Omega(V(i,b))$ die symmetrische Zahl j^* und überprüfen, ob die Ziffern j^*_μ auch denselben Einschränkungen wie j_μ genügen.

Für die ersten Ziffern von j^* erhalten wir trivialerweise

$$\begin{aligned} j^*_0 &= n_0 - j_0 = p - 1 - j_0 \\ &\vdots \\ j^*_{M-1} &= n_{M-1} - j_{M-1} = p - 1 - j_{M-1} \end{aligned}$$

Die M-te Ziffer von j^* erhalten wir durch

$$j^*_M := n_M + p - j_M.$$

Um dies einzusehen, formen wir die Beziehung $n_M + 1 \leq j_M \leq p-1$ um:

$$\begin{array}{rrll} n_M + 1 \leq & j_M & \leq p-1 & \mid \cdot(-1) \\ 1-p \leq & -j_M & \leq -n_M - 1 & \mid +(n_M + p) \\ n_M + 1 \leq & \underbrace{n_M + p - j_M}_{j^*_M} & \leq p-1 & \end{array}$$

Die symmetrische Zahl j^* erfüllt also auch $j_M^* > n_M$. Bei der Addition von j und j^* bleibt wegen

$$j_M + j_M^* = n_M + p$$

in der p-adischen Darstellung „1 Rest“.

Deshalb ist zur Ermittlung von j_{M+1}^* die Gleichung

$$j_{M+1} + 1 + j_{M+1}^* \equiv n_{M+1} \qquad (\text{mod } p)$$

zu lösen. Wir setzen

$$j_{M+1}^* := n_{M+1} - j_{M+1} + p - 1.$$

Aus

$$\begin{array}{lcll} n_{M+1} \leq & j_{M+1} & \leq p-1 & \mid \cdot(-1) \\ 1-p \leq & -j_{M+1} & \leq -n_{M+1} & \mid +(n_{M+1}+p-1) \\ n_{M+1} \leq & \underbrace{n_{M+1}+p-1-j_{M+1}}_{j_{M+1}^*} & \leq p-1 & \end{array}$$

sehen wir, daß auch j_{M+1}^* die Bedingung $j_{M+1}^* \geq n_{M+1}$ erfüllt. Bei der Addition

$$j_{M+1} + 1 + j_{M+1}^* = n_{M+1} + p$$

bleibt in der p-adischen Darstellung wieder „1 Rest“.

Die restlichen Schritte $j_\mu + 1 + j_\mu^* = n_\mu + p$ $(\mu = M+2, \ldots, i-1)$ verlaufen analog dem letzten.

Wir haben damit gezeigt, daß die Menge $\Omega(V(i,b))$ bezüglich der „Symmetrieabbildung“

$$j \mapsto n - j =: j^*$$

abgeschlossen und somit der Unterraum

$$\mathcal{O}_{V(i,b)} = \{P_\omega \mid \omega \in \Omega(V(i,b))\}$$

für alle $i \in D$ invariant unter der Gruppe $\mathrm{PGL}(\Gamma)$ ist. □

Bemerkung 4.5.2 Auf Grund der Bedingungen (4.15) ergibt sich für $i_1, i_2 \in D$ stets die strenge „Anti–Monotonie“

$$\begin{array}{rcl} i_1 < i_2 & \Leftrightarrow & \Omega(V(i_1,b)) \supset \Omega(V(i_2,b)) \\ & \Leftrightarrow & \mathcal{O}_{V(i_1,b)} \supset \mathcal{O}_{V(i_2,b)} \end{array}$$

4.6 Definition der $V(I_1, \ldots, I_L; i, b)$

4.6.1 Vorbemerkung

Bevor wir ausgehend von den Werten $V(i,b)$ weitere Indizes $V(I_1, \ldots, I_L; i, b)$ durch eine formale Definition festlegen, möchten wir die entsprechende Vorgangsweise sozusagen „bildlich“ erklären:

Wir betrachten in der p-adischen Darstellung von $V(i,b)$ die Ziffern $V(i,b)_\mu$ für $\mu = 0, 1, \ldots, i-2$. Die Menge

$$\{0, 1, \ldots, i-2\}$$

der Indizes wird so in zusammenhängende Indexblöcke $I_1, I_2, \ldots, I_L$ aufgeteilt, daß die folgenden drei Postulate erfüllt sind:

1. Kein Block schließt unmittelbar an den nächsten an.
2. Die auf einen Indexblock folgende Ziffer $*$ muß man erhöhen können ($* \neq p-1$).
3. Die Ziffern $\otimes$ am Beginn eines Indexblockes müssen erniedrigt werden können ($\otimes \neq 0$).

$$V(i,b) = \langle \ldots, *, \underbrace{\otimes}_{I_L}, \ldots, *, \underbrace{\otimes}_{I_2}, \ldots, *, \underbrace{\otimes}_{I_1}, \ldots \rangle$$

Den Wert $V(I_1, \ldots, I_L; i, b)$ erhalten wir, indem wir in der Darstellung von $V(i,b)$ die zu den Indizes der Blöcke $I_1, I_2, \ldots, I_L$ gehörigen Ziffern allesamt Null setzen und die „Ziffern vor den Indexblöcken“ um Eins erhöhen:

$$V(I_1, \ldots, I_L; i, b) = \langle \ldots, *+1, \underbrace{0, \ldots, 0}_{I_L}, \ldots, *+1, \underbrace{0, \ldots, 0}_{I_2}, \ldots, *+1, \underbrace{0, \ldots, 0}_{I_1}, \ldots \rangle$$

4.6.2 Erster Teil der Definition

Es ist klar, daß wir im folgenden für die $V(I_1, \ldots, I_L; i, b)$ eine handfestere Definition benötigen. Diese wollen wir jetzt vorbereiten:

Wir betrachten eine feste Menge

$$\{0, 1, \ldots, i\}$$

und Teilmengen

$$I_\lambda := \{i_\lambda, i_\lambda + 1, \ldots, i_\lambda + k_\lambda\} \quad \text{für} \quad \lambda = 1, 2, \ldots, L.$$

Die einzelnen Indizes i_λ und k_λ erfüllen dabei folgende Bedingungen:

$$\begin{aligned} i_\lambda, k_\lambda &\in \mathbb{N} \\ i_\lambda + k_\lambda &\leq i_{\lambda+1} - 2 \quad \lambda = 1, \ldots, L-1 \\ i_L + k_L &\leq i - 2 \\ b_{i_\lambda} &> 0 \\ b_{i_\lambda + k_\lambda + 1} &< p - 1 \end{aligned}$$

Jetzt können wir die $V(I_1, \ldots, I_L; i, b)$ in entsprechender Weise definieren.

Definition 4.6.1 *Unter den Voraussetzungen*

$$\begin{aligned} i_\lambda, k_\lambda &\in \mathbb{N} \\ i_\lambda + k_\lambda &\leq i_{\lambda+1} - 2 \quad \lambda = 1, \ldots, L-1 \\ i_L + k_L &\leq i - 2 \\ b_{i_\lambda} &> 0 \\ b_{i_\lambda + k_\lambda + 1} &< p - 1 \end{aligned}$$

definieren wir

$$V(I_1, \ldots, I_L; i, b) := V(i, b) - \sum_{\lambda=1}^{L} \sum_{\mu=0}^{k_\lambda} b_{i_\lambda + \mu}\, p^{i_\lambda + \mu} + \sum_{\lambda=1}^{L} p^{i_\lambda + k_\lambda + 1}. \tag{4.16}$$

Bemerkungen 4.6.2

1. Aus der Bedingung $b_{i_\lambda} > 0$ folgt insbesondere $i_1 \geq M$.

2. Es ist klar, daß für festes J durch den allgemeinen Fall

   $$M = 0 \quad \text{und} \quad b_\lambda \in \{1, 2, \ldots, p-2\} \ \text{ für alle } \ \lambda \leq J$$

   die Anzahl der möglichen Werte $V(I_1, \ldots, I_L; i, b)$ maximiert wird. Eine obere Schranke für diese Anzahl ergibt sich durch

   $$2^0 + 2^1 + \ldots + 2^{J-1} = 2^J - 1.$$

4.6.3 Zweiter Teil der Definition

In diesem Abschnitt wollen wir die Definition 4.6.1, die nur für L-Tupel $(I_1, I_2, \ldots, I_L)$ greift, in denen niemals die leere Menge vorkommt, erweitern.

Für jede Menge I_λ definieren wir ein Mengensystem $\mathcal{T}(I_\lambda)$:

$$\mathcal{T}(I_\lambda) := \{T_{\lambda;\nu} = \{i_\lambda, i_\lambda + 1, \ldots, i_\lambda + \nu\} \mid \nu = -1, 0, \ldots, k_\lambda\} \tag{4.17}$$

Bemerkung 4.6.3 Das Teilsystem $\mathcal{T}(I_\lambda)$ der Potenzmenge $\mathcal{P}(I_\lambda)$ bildet offensichtlich eine Kette, wobei der Parameter $\nu = -1$ für die leere Menge steht.

Für das Produkt $\mathcal{T}(I_1) \times \ldots \times \mathcal{T}(I_L)$ schreiben wir

$$\mathcal{T}(I_1 \times \ldots \times I_L) := \mathcal{T}(I_1) \times \ldots \times \mathcal{T}(I_L). \tag{4.18}$$

Definition 4.6.4 *Mit den Voraussetzungen und Bezeichnungen aus Definition 4.6.1 und den Formel (4.17) und (4.18) erklären wir für alle*

$$(T_1, T_2, \ldots, T_L) \in \mathcal{T}(I_1 \times I_2 \times \ldots \times I_L)$$

Werte der Form $V(T_1, \ldots, T_L; i, b)$, indem wir im L-Tupel $(T_1, T_2, \ldots, T_L)$ nur nichtleere Mengen berücksichtigen und auf das so entstandene H-Tupel ($H \leq L$) die Definition 4.6.1 anwenden.

Bemerkungen 4.6.5

1. Für leere Blöcke T_μ ändert sich also nichts beim Übergang von $V(i, b)$ auf $V(T_1, \ldots, T_L; i, b)$. Daraus ergibt sich etwa

   $$V(i, b) = V(\emptyset, \ldots, \emptyset; i, b).$$

2. Wie wir aus (4.14) wissen, gilt stets

   $$(n, V(i, b)) \in \nabla^i.$$

   Unmittelbar ist einzusehen, daß für die Werte $V(T_1, \ldots, T_L; i, b)$ ebenfalls

   $$(n, V(T_1, \ldots, T_L; i, b)) \in \nabla^i \tag{4.19}$$

   gilt.

4.6.4 Ein Beispiel

Wir greifen jetzt das Beispiel aus Abschnitt 4.4.1 auf und berechnen für alle $V(i, b)$ die entsprechenden Werte $V(I_1, \ldots, I_L; i, b)$.

Für $p = 2$ und $n = 371$ ergab sich in Abschnitt 4.4.1:

$$\begin{aligned} V(4, b) &= \langle 0, 1, 0, 0 \rangle \\ V(5, b) &= \langle 1, 0, 1, 0, 0 \rangle \\ V(6, b) &= \langle 1, 1, 0, 1, 0, 0 \rangle \\ V(8, b) &= \langle 0, 1, 1, 1, 0, 1, 0, 0 \rangle \end{aligned}$$

- $i = 4$: Da einerseits am Beginn eines Blocks immer eine von Null verschiedene Ziffer in der Darstellung von $V(i, b)$ stehen muß, und andererseits die erste Ziffer nach dem Blockende um Eins erhöht werden muß, erhalten wir nur den einzigen Block
$$I_1 = 2.$$
Damit ergibt sich
$$V(2; 4, b) = \langle 1, 0, 0, 0\rangle.$$

- $i = 5$: Wieder gibt es auf Grund unserer Forderungen nur den Block
$$I_1 = 2,$$
woraus
$$V(2; 5, b) = \langle 1, 1, 0, 0, 0\rangle$$
folgt.

- $i = 6$: Infolge analoger Überlegungen erhalten wir
$$I_1 = 2$$
und
$$V(2; 6, b) = \langle 1, 1, 1, 0, 0, 0\rangle$$
als einzige Möglichkeit.

- $i = 8$: Wir unterscheiden zwischen der Anzahl möglicher Blöcke:
  - Wir setzen $L = 1$ und erhalten für I_1 die Möglichkeiten
$$I_1 = \begin{cases} 2 \\ 2, 3, 4, 5, 6 \\ 4, 5, 6 \\ 5, 6 \\ 6 \end{cases}$$
mit den zugehörigen Werten
$$\begin{aligned} V(2; 8, b) &= \langle 0, 1, 1, 1, 1, 0, 0, 0\rangle \\ V(2, 3, 4, 5, 6; 8, b) &= \langle 1, 0, 0, 0, 0, 0, 0, 0\rangle \\ V(4, 5, 6; 8, b) &= \langle 1, 0, 0, 0, 0, 1, 0, 0\rangle \\ V(5, 6; 8, b) &= \langle 1, 0, 0, 1, 0, 1, 0, 0\rangle \\ V(6; 8, b) &= \langle 1, 0, 1, 1, 0, 1, 0, 0\rangle. \end{aligned}$$

– Für $L = 2$ ergibt sich zwingend

$$I_1 = 2,$$

und I_2 ist wählbar

$$I_2 = \begin{cases} 4,5,6 \\ 5,6 \\ 6 \end{cases}$$

Wir erhalten also mühelos

$$\begin{aligned} V(2,4,5,6;8,b) &= \langle 1,0,0,0,1,0,0,0\rangle \\ V(2,5,6;8,b) &= \langle 1,0,0,1,1,0,0,0\rangle \\ V(2,6;8,b) &= \langle 1,0,1,1,1,0,0,0\rangle \end{aligned}$$

– $L > 2$: Da es ab der dritten Ziffer von $V(8,b)$ nur zwei Ziffern gibt, die man erhöhen kann, tritt dieser Fall nicht auf.

4.7 „Symmetrisieren“ von $\Omega(V(I_1,\ldots,I_L;i,b))$

Wir haben in Abschnitt 4.5 gesehen, daß die Mengen $\Omega(V(i,b))$ die Symmetriebedingung aus Korollar 4.1.12 erfüllen und so zu invarianten Unterräumen führen. Nun könnte man glauben, daß die Mengen $\Omega(V(I_1,\ldots,I_L;i,b))$ auch diese Eigenschaft besäßen. Der nächste Satz belehrt uns jedoch eines Besseren und zeigt, daß dies nicht so ist.

Satz 4.7.1 *Für jedes L-Tupel* $(T_1,T_2,\ldots,T_L) \in \mathcal{T}(I_1\times\ldots\times I_L)$ *existiert eine Zahl* $j \in \Omega(V(I_1,\ldots,I_L;i,b))$ *mit*

$$\begin{aligned} j^* &\in \Omega(V(T_1,\ldots,T_L;i,b)) \quad \textit{aber} \\ j^* &\notin \Omega(V(S_1,\ldots,S_L;i,b)) \quad \textit{für alle } (S_1,S_2,\ldots,S_L) \in \\ &\qquad\qquad \mathcal{T}(I_1\times I_2\times\ldots\times I_L)\setminus(T_1,T_2,\ldots,T_L) \end{aligned}$$

Dabei sei vorausgesetzt, daß $V(T_1,\ldots,T_L;i,b)$ *definiert ist.*

Bemerkung 4.7.2 Falls $V(S_1,\ldots,S_L;i,b)$ nicht definiert ist, weil in Definition 4.6.1 eine der Bedingungen nicht erfüllt ist, könnten wir

$$\Omega(V(S_1,\ldots,S_L;i,b)) = \emptyset$$

setzen.

Beweis: Wir wollen jetzt Satz 4.7.1 beweisen und setzen

$$T_\mu = T_{\mu;\, t_\mu} = \{i_\mu, i_\mu + 1, \ldots, i_\mu + t_\mu\}$$

mit

$$t_\mu \in \{-1, 0, \ldots, k_\mu\} \quad \forall\, \mu \in \{1, 2, \ldots, L\}.$$

Jetzt wählen wir j speziell aus $\Omega(V(I_1, \ldots, I_L; i, b))$, so daß sich

$$j^* = V(T_1, \ldots, T_L; i, b)$$

ergibt. Wir müssen dabei unterscheiden, ob $i_1 = M$ oder $i_1 > M$ gilt.

- In einem ersten Schritt sei $t_\mu \geq 0\ \forall\ \mu$. Die mit „ $\triangleright$ “ markierten Zeilen werden erst im nächsten Schritt angesprochen.

$$\begin{array}{lrcll}
 & j_\alpha & = & n_\alpha = p-1 & 0 \leq \alpha \leq M-1 \\
\underline{\text{nur bei } i_1 > M} & j_\beta & = & p-1 & M \leq \beta \leq i_1 - 1 \\
\underline{\text{nur bei } i_1 > M} & j_{i_1} & = & n_{i_1} - 1 & \\
\underline{\text{nur bei } i_1 = M} & j_{i_1} & = & n_{i_1} & \\
 & j_\gamma & = & n_\gamma & i_1 + 1 \leq \gamma \leq i_1 + t_1 \\
 & j_\delta & = & p-1 & i_1 + t_1 + 1 \leq \delta \leq i_2 - 1 \\
\triangleright & j_{i_2} & = & n_{i_2} - 1 & \\
\triangleright & j_\gamma & = & n_\gamma & i_2 + 1 \leq \gamma \leq i_2 + t_2 \\
 & j_\delta & = & p-1 & i_2 + t_2 + 1 \leq \delta \leq i_3 - 1 \\
 & & \vdots & & \\
 & j_{i_L} & = & n_{i_L} - 1 & \\
 & j_\gamma & = & n_\gamma & i_L + 1 \leq \gamma \leq i_L + t_L \\
 & j_\delta & = & p-1 & i_L + t_L + 1 \leq \delta \leq i - 1 \\
 & j_i & = & n_i - 1 & \\
 & j_\gamma & = & n_\gamma & i + 1 \leq \gamma \leq J
\end{array}$$

Jetzt berechnen wir j^*:

$$
\begin{array}{lrcll}
 & j^*_\alpha & = & 0 & 0 \le \alpha \le M-1 \\
\underline{\text{nur bei } i_1 > M} & j^*_M & = & n_M + 1 & \\
\underline{\text{nur bei } i_1 > M} & j^*_\beta & = & n_\beta & M+1 \le \beta \le i_1 - 1 \\
\underline{\text{unabh. von } M} & j^*_{i_1} & = & 0 & \\
 & j^*_\gamma & = & 0 & i_1 + 1 \le \gamma \le i_1 + t_1 \\
 & j^*_{i_1+t_1+1} & = & n_{i_1+t_1+1} + 1 & \\
 & j^*_\delta & = & n_\delta & i_1 + t_1 + 2 \le \delta \le i_2 - 1 \\
\triangleright & j^*_\gamma & = & 0 & i_2 \le \gamma \le i_2 + t_2 \\
\triangleright & j^*_{i_2+t_2+1} & = & n_{i_2+t_2+1} + 1 & \\
 & j^*_\delta & = & n_\delta & i_2 + t_2 + 2 \le \delta \le i_3 - 1 \\
 & & \vdots & & \\
 & j^*_\gamma & = & 0 & i_L \le \gamma \le i_L + t_L \\
 & j^*_{i_L+t_L+1} & = & n_{i_L+t_L+1} + 1 & \\
 & j^*_\delta & = & n_\delta & i_L + t_L + 2 \le \delta \le i - 1
\end{array}
$$

- Am Beispiel $t_2 = -1$ zeigen wir, wie vorzugehen ist, falls μ mit $t_\mu = -1$ existiert:

  Aus $t_2 = -1$ folgt $i_2 + t_2 + 1 = i_2$, und daher entfallen die in der Definition von j mit „$\triangleright$“ markierten Zeilen. Für den entsprechenden Abschnitt in der p-adischen Entwicklung von j erhalten wir:

  $$j_\delta = p - 1 \quad \text{für} \quad i_2 \le \delta \le i_3 - 1$$

  Welche Auswirkungen hat dies nun auf die korrespondierenden Stellen von j^*? Hier entfallen die durch „$\triangleright$“ hervorgehobenen Zeilen ebenfalls, und es gilt:

  $$j^*_\delta = n_\delta \quad \text{für} \quad i_2 \le \delta \le i_3 - 1$$

  Auf einen leeren Indexblock wird also in Analogie zur Erweiterung von Definition 4.6.1 nicht Rücksicht genommen.

Nach genauerem Hinschauen bemerken wir, daß es sich bei j^* um die Zahl

$$V(T_1, \ldots, T_L; i, b)$$

handelt. Damit haben wir also die Behauptung

$$j^* \in \Omega(V(T_1, \ldots, T_L; i, b))$$

gezeigt.

Bemerkung 4.7.3 Da wir vorausgesetzt haben, daß $V(T_1, \ldots, T_L; i, b)$ definiert ist, gilt:

$$\begin{array}{lrcll} 1. & b_{i_\mu + t_\mu + 1} & < & p-1 & \forall\, \mu \in \{1, 2, \ldots, L\} \text{ mit } T_\mu \neq \emptyset \\ 2. & b_{i_\mu} & > & 0 & \forall\, \mu \in \{1, 2, \ldots, L\} \text{ mit } T_\mu \neq \emptyset \end{array}$$

Weiters folgt aus der Definition von $V(i, b)$, daß $b_i = n_i > 0$ ist. Insgesamt sind also in der Konstruktion von j und j^* alle Schritte durchführbar.

Jetzt überlegen wir uns noch, daß

$$j^* = V(T_1, \ldots, T_L; i, b) \in \Omega(V(S_1, \ldots, S_L; i, b))$$

genau dann erfüllt ist, wenn

$$(S_1, S_2, \ldots, S_L) = (T_1, T_2, \ldots, T_L)$$

gilt. Mit

$$\begin{array}{rcl} I_\mu & = & \{i_\mu, i_\mu + 1, \ldots, i_\mu + k_\mu\} \\ T_\mu & = & \{i_\mu, i_\mu + 1, \ldots, i_\mu + t_\mu\} \\ S_\mu & = & \{i_\mu, i_\mu + 1, \ldots, i_\mu + s_\mu\} \end{array}$$

ergibt sich für $\mu \in \{1, 2, \ldots, L\}$ die Einschränkung

$$s_\mu, t_\mu \;\in\; \{-1, 0, \ldots, k_\mu\}$$

Sei $S_Y \neq T_Y$, also $s_Y \neq t_Y$ für mindestens ein Y. Wir unterscheiden:

1. $s_Y < t_Y$: Es folgt jedenfalls $t_Y \geq 0$.

   (a) $s_Y = -1$: Während für alle

   $$h \in \Omega(V(S_1, \ldots, S_L; i, b))$$

   sicherlich $h_{i_Y} \geq b_{i_Y} > 0$ gilt, wissen wir

   $$V(T_1, \ldots, T_L; i, b)_{i_Y} = 0.$$

   (b) $s_Y \geq 0$: Für

   $$h \in \Omega(V(S_1, \ldots, S_L; i, b))$$

   gilt stets $h_{i_Y + s_Y + 1} > b_{i_Y + s_Y + 1}$, aber

   $$V(T_1, \ldots, T_L; i, b)_{i_Y + s_Y + 1} = 0 \leq b_{i_Y + s_Y + 1}.$$

2. $s_Y > t_Y$: Mit $s_Y \geq 0$ unterscheiden wir:

   (a) $t_Y = -1$: Es gilt $h_{i_Y+s_Y+1} > b_{i_Y+s_Y+1}$, aber

   $$V(T_1, \ldots, T_L; i, b)_{i_Y+s_Y+1} = b_{i_Y+s_Y+1}.$$

   (b) $t_Y \geq 0$: Wir haben ebenso $h_{i_Y+s_Y+1} > b_{i_Y+s_Y+1}$, aber

   $$V(T_1, \ldots, T_L; i, b)_{i_Y+s_Y+1} = b_{i_Y+s_Y+1}.$$

Damit ist Satz 4.7.1 gänzlich bewiesen. □

Folgerung 4.7.4 Wenn wir von einer Menge $\Omega(V(I_1, \ldots, I_L; i, b))$ ausgehen und daraus eine Indexmenge Λ konstruieren wollen, die Korollar 4.1.12 genügt, dann folgt aus Satz 4.7.1 unmittelbar, daß die Inklusion

$$\bigcup \Omega(V(T_1, \ldots, T_L; i, b)) \subset \Lambda$$

erfüllt sein muß, wobei über alle L-Tupel

$$(T_1, T_2, \ldots, T_L) \in \mathcal{T}(I_1 \times \ldots \times I_L)$$

zu vereinigen ist.

Wir möchten im folgenden zeigen, daß die Menge $\bigcup \Omega(V(T_1, \ldots, T_L; i, b))$ stets symmetrisch ist. Da es sich um eine Vereinigung von Mengen der Form $\Omega(j)$ handelt, wird auch das Postulat 3 aus Korollar 4.1.12 erfüllt, und wir haben somit weitere Indexmengen konstruiert, die zu nichttrivialen invarianten Unterräumen führen.

Bevor wir soweit sind, müssen noch diverse Sätze und Lemmata bewiesen werden. Zur Erleichterung der Schreibweise definieren wir

$$\Lambda(I_1, \ldots, I_L; i, b) := \bigcup \Omega(V(T_1, \ldots, T_L; i, b)), \tag{4.20}$$

wobei über alle L-Tupel

$$(T_1, T_2, \ldots, T_L) \in \mathcal{T}(I_1 \times \ldots \times I_L)$$

zu vereinigen ist.

Hilfssatz 4.7.5 *Für ein Element $j \in \Lambda(I_1, \ldots, I_L; i, b)$ gilt genau dann*

$$j \notin \Omega(V(T_1, \ldots, T_L; i, b))$$

für alle

$$(T_1, T_2, \ldots, T_L) \in (\mathcal{T}(I_1 \times \ldots \times I_L) \setminus (I_1, I_2, \ldots, I_L)),$$

wenn für alle $\mu \in \{1, 2, \ldots, L\}$ *das Maximum*

$$\nu_\mu \;:=\; \max\{\alpha \in \{0, 1, \ldots, k_\mu\} \mid j_{i_\mu+\alpha} < b_{i_\mu+\alpha}\}$$

existiert und

$$\min\{\beta \in \{\nu_\mu + 1, \ldots, k_\mu + 1\} \mid j_{i_\mu+\beta} > b_{i_\mu+\beta}\} \;=\; k_\mu + 1 \qquad (4.21)$$

erfüllt ist.

Beweis: Der Beweis ist in zwei Richtungen zu führen:

1. „ $\Rightarrow$ “: Wegen $I_\mu \neq \emptyset$ für alle $\mu \in \{1, 2, \ldots, L\}$ und

   $$j \;\notin\; \Omega(V(T_1, \ldots, T_L; i, b))$$

   für alle

   $$(T_1, T_2, \ldots, T_L) \in (\mathcal{T}(I_1 \times \ldots \times I_L) \setminus (I_1, I_2, \ldots, I_L))$$

   ist ν_μ für alle μ definiert. Existierte nämlich $Y \in \{1, 2, \ldots, L\}$ mit

   $$j_{i_Y+\alpha} \geq b_{i_Y+\alpha} \quad \text{für} \quad \alpha = 0, 1, \ldots, k_Y,$$

   dann würde daraus entgegen den Voraussetzungen

   $$j \in \Omega(V(I_1, \ldots, I_{Y-1}, \emptyset, I_{Y+1}, \ldots, I_L; i, b))$$

   folgen.

   Völlig analog erkennen wir, daß die Existenz von $Y \in \{1, 2, \ldots, L\}$ mit

   $$\min\{\beta \in \{\nu_Y + 1, \ldots, k_Y + 1\} \mid j_{i_Y+\beta} > b_{i_Y+\beta}\} =: t_Y + 1 < k_Y + 1$$

   auf Grund von

   $$j \in \Omega(V(I_1, \ldots, I_{Y-1}, T_Y, I_{Y+1}, \ldots, I_L; i, b))$$

   ($T_Y = \{i_Y, \ldots, i_Y + t_Y\}$) den Voraussetzungen widersprechen würde.

2. „ $\Leftarrow$ “: Wir führen diese Richtung indirekt, und nehmen daher

   $$j \in \Omega(V(T_1, \ldots, T_L; i, b))$$

   mit

   $$(T_1, T_2, \ldots, T_L) \neq (I_1, I_2, \ldots, I_L)$$

   an. Es existiert also $Y \in \{1, 2, \ldots, L\}$ mit $T_Y \neq I_Y$.

   Für $h \in \Omega(V(T_1, \ldots, T_L; i, b))$ gilt dann:

   $$\begin{aligned} h_{i_Y+t_Y+1} &> b_{i_Y+t_Y+1} \\ h_{i_Y+\alpha} &\geq b_{i_Y+\alpha} \qquad t_Y + 2 \leq \alpha \leq k_Y + 1 \end{aligned}$$

- Gilt $\nu_Y \geq t_Y + 1$ dann erhalten wir aus

$$j_{i_Y+\nu_Y} < b_{i_Y+\nu_Y}$$

einen Widerspruch.

- Für $\nu_Y < t_Y + 1 < k_Y + 1$ folgt aus

$$j_{i_Y+t_Y+1} = b_{i_Y+t_Y+1}$$

ein Widerspruch. □

Bemerkung 4.7.6 Im Hilfssatz haben wir bei der Definition des Minimums und Maximums auf die p-adische Entwicklung von $b = n + 1$ zurückgegriffen. Wollen wir jedoch von der Darstellung von n ausgehen, dann müssen wir lediglich im Falle $i_1 = M$ für $\mu = 1$ die Definition des Maximums folgendermaßen modifizieren:

$$\nu_1 := \begin{cases} \max\{0, \max\{\alpha \in \{1,2,\ldots,k_1\} \mid j_{i_1+\alpha} < n_{i_1+\alpha}\}\} & \text{für } j_{i_1} \leq n_{i_1} \\ \max\{\alpha \in \{1,2,\ldots,k_1\} \mid j_{i_1+\alpha} < n_{i_1+\alpha}\} & \text{für } j_{i_1} > n_{i_1} \end{cases}$$

Im nächsten Lemma werden wir diese Überlegung verwenden.

Unter Anwendung von Hilfssatz 4.7.5 werden wir jetzt zeigen, daß für jene Elemente j von $\Lambda(I_1, \ldots, I_L; i, b)$, die nur in der Menge $\Omega(V(I_1, \ldots, I_L; i, b))$ liegen, die symmetrischen Elemente j^* die gleiche Eigenschaft besitzen.

Lemma 4.7.7 *Für $j \in \Lambda(I_1, \ldots, I_L; i, b)$ und*

$$j \notin \Omega(V(T_1, \ldots, T_L; i, b))$$

für alle

$$(T_1, T_2, \ldots, T_L) \in (\mathcal{T}(I_1 \times \ldots \times I_L) \setminus (I_1, I_2, \ldots, I_L))$$

gilt: Auch der symmetrische Index j^* erfüllt $j^* \in \Lambda(I_1, \ldots, I_L; i, b)$ und

$$j \notin \Omega(V(T_1, \ldots, T_L; i, b))$$

für alle

$$(T_1, T_2, \ldots, T_L) \in (\mathcal{T}(I_1 \times \ldots \times I_L) \setminus (I_1, I_2, \ldots, I_L)).$$

Beweis: Wir werden Hilfssatz 4.7.5 für j^* anwenden und müssen uns daher überlegen, daß

$$j^* \in \Lambda(I_1, \ldots, I_L; i, b)$$

gilt. Wenn j die Voraussetzungen des Lemmas erfüllt, wissen wir:

$$\begin{array}{lrcll}
 & j_\alpha & \in & \{0,1,\ldots,p-1\} & \text{beliebig} \quad 0 \le \alpha \le M-1 \\
\underline{\text{nur bei } i_1 > M} & j_M & > & n_M & \\
\underline{\text{nur bei } i_1 > M} & j_\beta & \ge & n_\beta & M+1 \le \beta \le i_1 - 1 \\
 & & & & \\
 & j_{i_1+k_1+1} & > & n_{i_1+k_1+1} & \\
 & j_\delta & \ge & n_\delta & i_1+k_1+2 \le \delta \le i_2-1 \\
 & & & & \\
 & j_{i_2+k_2+1} & > & n_{i_2+k_2+1} & \\
 & j_\delta & \ge & n_\delta & i_2+k_2+2 \le \delta \le i_3-1 \\
 & & \vdots & & \\
 & j_{i_L+k_L+1} & > & n_{i_L+k_L+1} & \\
 & j_\delta & \ge & n_\delta & i_L+k_L+2 \le \delta \le i-1
\end{array}$$

Die Ziffern von j^* erfüllen dann:

$$\begin{array}{lrcll}
 & j^*_\alpha & = & n_\alpha - j_\alpha = p-1-j_\alpha & 0 \le \alpha \le M-1 \\
\underline{\text{nur bei } i_1 > M} & j^*_M & > & n_M & \\
\underline{\text{nur bei } i_1 > M} & j^*_\beta & \ge & n_\beta & M+1 \le \beta \le i_1 - 1 \\
 & & & & \\
 & j^*_{i_1+k_1+1} & > & n_{i_1+k_1+1} & \\
 & j^*_\delta & \ge & n_\delta & i_1+k_1+2 \le \delta \le i_2-1 \\
 & & & & \\
 & j^*_{i_2+k_2+1} & > & n_{i_2+k_2+1} & \\
 & j^*_\delta & \ge & n_\delta & i_2+k_2+2 \le \delta \le i_3-1 \\
 & & \vdots & & \\
 & j^*_{i_L+k_L+1} & > & n_{i_L+k_L+1} & \\
 & j^*_\delta & \ge & n_\delta & i_L+k_L+2 \le \delta \le i-1
\end{array}$$

Das wollen wir uns noch kurz überlegen. Wie schon in Abschnitt 4.5 vorgezeigt, ist uns

$$\begin{array}{rcll}
j^*_\alpha & = & n_\alpha - j_\alpha & 0 \le \alpha \le M-1 \\
j^*_M & > & n_M & \\
j^*_\beta & \ge & n_\beta & M+1 \le \beta \le i_1 - 1
\end{array}$$

klar. Jetzt überlegen wir uns die Abschätzung der Ziffern j^*_δ für

$$i_\mu + k_\mu + 1 \le \delta \le i_{\mu+1} - 1 :$$

Mit den Bezeichnungen von Hilfssatz 4.7.5 folgt, daß bei der Addition

$$j_{i_\mu+\alpha} + j^*_{i_\mu+\alpha} \quad \text{für} \quad \alpha = \nu_\mu, \nu_\mu+1, \ldots, k_\mu$$

niemals „1 Rest“ bleibt. Wir lösen daher

$$j_{i_\mu+k_\mu+1} + j^*_{i_\mu+k_\mu+1} \equiv n_{i_\mu+k_\mu+1} \pmod{p}$$

Wir formen die Beziehung $n_{i_\mu+k_\mu+1} + 1 \le j_{i_\mu+k_\mu+1} \le p-1$ um:

$$\begin{array}{rcccl} n_{i_\mu+k_\mu+1}+1 & \le & j_{i_\mu+k_\mu+1} & \le & p-1 \qquad \mid \cdot(-1) \\ 1-p & \le & -j_{i_\mu+k_\mu+1} & \le & -n_{i_\mu+k_\mu+1}-1 \quad \mid +(n_{i_\mu+k_\mu+1}+p) \\ n_{i_\mu+k_\mu+1}+1 & \le & \underbrace{n_{i_\mu+k_\mu+1}+p-j_{i_\mu+k_\mu+1}}_{j^*_{i_\mu+k_\mu+1}} & \le & p-1 \end{array}$$

Daraus erhalten wir

$$j^*_{i_\mu+k_\mu+1} > n_{i_\mu+k_\mu+1}.$$

Von nun an bleibt bei der Addition der Ziffern von j und j^* stets „1 Rest“, wodurch wir für $i_\mu + k_\mu + 2 \le \delta \le i_{\mu+1} - 1$ immer

$$\begin{array}{rcl} & n_\delta \le j_\delta \le p-1 \\ \Leftrightarrow & n_\delta \le j^*_\delta \le p-1 \end{array}$$

erhalten.

Jetzt ist

$$j^* \in \Omega(V(I_1, \ldots, I_L; i, b)) \subset \Lambda(I_1, \ldots, I_L; i, b)$$

offensichtlich, und wir unterscheiden nun mit den Bezeichnungen von Hilfssatz 4.7.5 bei festem $\mu \in \{1, 2, \ldots, L\}$ zwei Fälle (wobei wir vorerst $i_1 = M$ ausklammern):

1. Wir nehmen an, daß bei der Addition

   $$j_{i_\mu+\nu_\mu-1} + j^*_{i_\mu+\nu_\mu-1} = n_{i_\mu+\nu_\mu-1}$$

   „1 Rest“ bleibt. Es gilt dann, als nächstes die Gleichung

   $$j_{i_\mu+\nu_\mu} + j^*_{i_\mu+\nu_\mu} = n_{i_\mu+\nu_\mu} - 1$$

   zu lösen. Aus $j_{i_\mu+\nu_\mu} < n_{i_\mu+\nu_\mu}$ erhalten wir sofort auch $j^*_{i_\mu+\nu_\mu} < n_{i_\mu+\nu_\mu}$. Weiters folgt

   $$j_\alpha = n_\alpha \quad \Leftrightarrow \quad j^*_\alpha = 0 \quad \text{für} \quad i_\mu + \nu_\mu \le \alpha \le i_\mu + k_\mu$$

   und

   $$\begin{array}{rcl} & j_{i_\mu+k_\mu+1} > n_{i_\mu+k_\mu+1} \\ \Leftrightarrow & j^*_{i_\mu+k_\mu+1} > n_{i_\mu+k_\mu+1} \end{array}$$

Wir sehen hier sofort, daß auch j^* mit den Parametern

$$\begin{aligned} \nu_\mu^* &= \max\{\alpha \in \{0,1,\ldots,k_\mu\} \mid j^*_{i_\mu+\alpha} < n_{i_\mu+\alpha}\} \geq \nu_\mu \\ k_\mu + 1 &= \min\{\beta \in \{\nu_\mu^* + 1, \ldots, k_\mu + 1\} \mid j^*_{i_\mu+\beta} > n_{i_\mu+\beta}\} \end{aligned}$$

die Bedingung (4.21) aus Hilfssatz 4.7.5 erfüllt.

2. Jetzt nehmen wir an, daß für festes μ bei der Addition

$$j_{i_\mu+\nu_\mu-1} + j^*_{i_\mu+\nu_\mu-1} = n_{i_\mu+\nu_\mu-1}$$

„kein Rest“ geblieben ist. Es gilt dann

$$j^*_{i_\mu+\nu_\mu} = n_{i_\mu+\nu_\mu} - j_{i_\mu+\nu_\mu}.$$

Wegen $0 \leq j_{i_\mu+\nu_\mu} \leq n_{i_\mu+\nu_\mu} - 1$ folgt $1 \leq j^*_{i_\mu+\nu_\mu} \leq n_{i_\mu+\nu_\mu}$. Für

$$j^*_{i_\mu+\nu_\mu} < n_{i_\mu+\nu_\mu}$$

sind wir in Analogie zum vorigen Fall fertig, weil wieder die Bedingung (4.21) erfüllt ist.

Bei Gleichheit müssen wir weiter untersuchen:

(a) Falls für $i_\mu + \nu_\mu \leq \alpha \leq i_\mu + k_\mu$ eine Ziffer $n_\alpha > 0$ ist, sind wir ebenfalls fertig.

(b) Sind jedoch alle diese n_α gleich Null, dann untersuchen wir in j^* die Ziffern j^*_β rückwärts, wobei wir mit der Stelle $i_\mu + \nu_\mu - 1$ beginnen:

Da wir vorausgesetzt haben, daß bei der Addition

$$j_{i_\mu+\nu_\mu-1} + j^*_{i_\mu+\nu_\mu-1}$$

kein „Rest“ geblieben ist, ergibt sich gewiß

$$j^*_{i_\mu+\nu_\mu-1} \leq n_{i_\mu+\nu_\mu-1}.$$

Nur bei Gleichheit müssen wir weitermachen. In diesem Fall gilt dann erstens

$$j_{i_\mu+\nu_\mu-1} = 0$$

und zweitens, daß bei der Addition

$$j_{i_\mu+\nu_\mu-2} + j^*_{i_\mu+\nu_\mu-2}$$

kein „Rest“ geblieben ist.

Die Annahme, daß diese Gedankenkette nicht abreißt und somit

$$j^*_\beta = n_\beta \qquad \text{für } \beta = i_\mu + \nu_\mu - 1, i_\mu + \nu_\mu - 2, \ldots, i_\mu$$

gilt, führt auf einen Widerspruch:

Bei der Addition

$$j_{i_\mu - 1} + j^*_{i_\mu - 1}$$

bleibt stets „1 Rest“, und deshalb muß unter den Voraussetzungen in diesem Fall jedenfalls

$$j^*_{i_\mu} < n_{i_\mu}$$

gelten.

Wieder ist also mit

$$\begin{aligned} \nu^*_\mu &= \max\{\alpha \in \{0, 1, \ldots, k_\mu\} \mid j^*_{i_\mu + \alpha} < n_{i_\mu + \alpha}\} \\ k_\mu + 1 &= \min\{\beta \in \{\nu^*_\mu + 1, \ldots, k_\mu + 1\} \mid j^*_{i_\mu + \beta} > n_{i_\mu + \beta}\} \end{aligned}$$

die Bedingung (4.21) erfüllt.

Jetzt überlegen wir uns noch, was sich im Sonderfall $i_1 = M$ ergibt. Nur Teil 2 des Beweises könnte prinzipiell Schwierigkeiten bereiten. Die dort angesprochene Gedankenkette reißt aber ebenso wegen

$$\begin{aligned} j_M &\leq n_M < b_M \\ j^*_M &\leq n_M < b_M \end{aligned}$$

ab.

Unter Berücksichtigung von Bemerkung 4.7.6 können wir nun Hilfssatz 4.7.5 auf j^* anwenden und erhalten die Aussage des Lemmas. □

Wir haben nun alle Vorbereitungen getroffen, um $\Lambda(I_1, \ldots, I_L; i, b)$ als symmetrische Menge identifizieren zu können, die uns zu weiteren invarianten Unterräumen führt.

Satz 4.7.8 *Die Menge*

$$\Lambda(I_1, \ldots, I_L; i, b) = \bigcup \Omega(V(T_1, \ldots, T_L; i, b))$$

(es wird über alle L-Tupel

$$(T_1, T_2, \ldots, T_L) \in \mathcal{T}(I_1 \times \ldots \times I_L)$$

vereinigt) ist symmetrisch und führt so zu einem invarianten Unterraum.

Beweis: Für $j \in \Lambda(I_1, \ldots, I_L; i, b)$ existiert ein eindeutig bestimmtes L-Tupel $(T_1, T_2, \ldots, T_L)$ mit

$$j \in \Omega(V(T_1, \ldots, T_L; i, b))$$

und

$$\sum_{\mu=1}^{L} \#T_\mu \quad \longrightarrow \quad \text{Minimum.}$$

- Falls dieses Minimum den Wert 0 annimmt, also $j \in \Omega(V(i, b))$ gilt, dann folgt mit Satz 4.5.1 auch $j^* \in \Omega(V(i, b))$.
- Jetzt setzen wir voraus, daß dieses Minimum einen Wert größer als Null besitzt. Wir schreiben nur nichtleere Mengen an, erhalten also ein H-Tupel $(T_{i_1}, \ldots, T_{i_H})$ mit $H \leq L$ und

  $$T_{i_\mu} \neq \emptyset \quad \text{für} \quad \mu = 1, 2, \ldots, H$$

  Nun können wir auf die Grundmenge

  $$(T_{i_1} \times \ldots \times T_{i_H})$$

  Lemma 4.7.7 anwenden, womit der Satz bewiesen ist. □

Wenn man den Verband aller invarianten Unterräume unter PGL(Γ) beschreiben möchte, genügt es, jene Unterräume zu kennen, die nur mehr als triviale Summe zweier invarianter Unterräume geschrieben werden können. Diese Verbandselemente verdienen eine eigene Bezeichnung.

Definition 4.7.9 *Jene Unterräume, die unter* PGL(Γ) *invariant sind und sich nur in trivialer Weise als Summe invarianter Unterräume schreiben lassen, heißen irreduzibel.*

Es ist trivial, daß der leere Unterraum irreduzibel ist. Eine auf den ersten Blick womöglich überraschende Kennzeichnung der nichtleeren irreduziblen Unterräume liefert der folgende Satz.

Satz 4.7.10 (Konstruktion aller nichtleeren irreduziblen Unterräume) *Die Unterräume der Form*

$$\mathcal{U} := [\{P_\lambda \mid \lambda \in \Lambda(I_1, \ldots, I_L; i, b)\}]$$

sind genau die nichtleeren irreduziblen invarianten Unterräume.

Beweis: Aus Satz 4.7.1 und Folgerung 4.7.4 wissen wir, daß diese Unterräume irreduzibel sind.

Wir müssen noch überlegen, ob sich tatsächlich alle irreduziblen Unterräume in dieser Form schreiben lassen. Dazu gehen wir folgendermaßen vor:

Wir konstruieren ausgehend von einem Grundpunkt P_j mit

$$\binom{n}{j} \equiv 0 \pmod{p}$$

den minimalen irreduziblen Unterraum $\mathcal{U} = [\{P_\lambda \mid \lambda \in \Lambda\}]$ mit $P_j \in \mathcal{U}$. Es stellt sich heraus, daß mit j auch die Zahl $j'^* = V(I_1, \ldots, I_L; i, b)$ in Λ enthalten sein muß, woraus sich

$$\Lambda = \Lambda(I_1, \ldots, I_L; i, b)$$

ergibt.

Im folgenden Algorithmus werden vorerst aus der p-adischen Darstellung von j und n gewisse Parameter bestimmt. Man mache sich bewußt, daß wegen $j \not\preceq n$ ein Index Y mit $j_Y > n_Y$ existieren muß.

Wegen $n_\mu = p - 1$ für $\mu < M$ starten wir mit der M-ten Ziffer:
Für $j_M \leq n_M < b_M$ setzen wir

$$i_1 := M$$

und sonst

$$i_1 := \min\{\alpha \in \{M+1, M+2, \ldots, J\} \mid j_\alpha < n_\alpha\}.$$

Nun definieren wir sukzessive

$$\begin{aligned}
i_1 + k_1 + 1 &:= \min\{\beta \in \{i_1 + 1, i_1 + 2, \ldots, J\} \mid j_\beta > n_\beta\} \\
i_2 &:= \min\{\gamma \in \{i_1 + k_1 + 2, i_1 + k_1 + 3, \ldots, J\} \mid j_\gamma < n_\gamma\} \\
i_2 + k_2 + 1 &:= \min\{\delta \in \{i_2 + 1, i_2 + 2, \ldots, J\} \mid j_\delta > n_\delta\} \qquad (4.22) \\
&\vdots \\
i := i_{L+1} &:= \min\{\omega \in \{i_L + k_L + 2, i_L + k_L + 3, \ldots, J\} \mid j_\omega < n_\omega\}
\end{aligned}$$

Es ist klar, daß der letzte Wert i genau dem Klassenindex i entspricht, mit $(n, j) \in \overline{i}$ (vgl. Definition 1.3.1).

Wir geben jetzt j' mit den Eigenschaften

$$\begin{aligned}
j' &\succeq j \\
j'^* &= V(I_1, \ldots, I_L; i, b)
\end{aligned}$$

an:

$$
\begin{array}{lrcll}
 & j'_\alpha & = & n_\alpha = p-1 & 0 \le \alpha \le M-1 \\
\underline{\text{nur bei } i_1 > M} & j'_\beta & = & p-1 & M \le \beta \le i_1 - 1 \\
\underline{\text{nur bei } i_1 > M} & j'_{i_1} & = & n_{i_1} - 1 & \\
\underline{\text{nur bei } i_1 = M} & j'_{i_1} & = & n_{i_1} & \\
 & j'_\gamma & = & n_\gamma & i_1 + 1 \le \gamma \le i_1 + k_1 \\
 & j'_\delta & = & p-1 & i_1 + k_1 + 1 \le \delta \le i_2 - 1 \\
 & j'_{i_2} & = & n_{i_2} - 1 & \\
 & j'_\gamma & = & n_\gamma & i_2 + 1 \le \gamma \le i_2 + k_2 \\
 & j'_\delta & = & p-1 & i_2 + k_2 + 1 \le \delta \le i_3 - 1 \\
 & & \vdots & & \\
 & j'_{i_L} & = & n_{i_L} - 1 & \\
 & j'_\gamma & = & n_\gamma & i_L + 1 \le \gamma \le i_L + k_L \\
 & j'_\delta & = & p-1 & i_L + k_L + 1 \le \delta \le i - 1 \\
 & j'_i & = & n_i - 1 & \\
 & j'_\gamma & = & n_\gamma & i + 1 \le \gamma \le J
\end{array}
$$

Einerseits folgt auf Grund der Definition (4.22) der Indizes i_μ und k_μ die Eigenschaft

$$j' \succeq j,$$

andererseits folgern wir aus

$$
\begin{array}{lcll}
j'_i & = & n_i - 1 & \\
j'_\gamma & = & n_\gamma & \text{für } i+1 \le \gamma \le J,
\end{array}
$$

daß $j' < n$ ist.

Völlig analog zum Beweis von Satz 4.7.1 zeigt man nun

$$j'^* = V(I_1, \ldots, I_L; i, b).$$

Daraus folgt dann zwingend

$$\Omega(V(I_1, \ldots, I_L; i, b)) \subset \Lambda,$$

und infolge der Minimalitätsforderung an Λ erhalten wir $\Lambda = \Lambda(I_1, \ldots, I_L; i, b)$. □

4.8 Exemplarische Berechnung aller irreduziblen invarianten Unterräume

Nachdem wir im vorigen Abschnitt die Theorie zur Berechnung aller irreduziblen invarianten Unterräume bei gegebener Raumdimension n und Charakteristik p

entwickelt haben, sollen dem Leser dieser Arbeit zu deren Abrundung und zum versöhnlichen Ausklang einige Beispiele präsentiert werden.

Man mache sich bewußt, daß es bei der Entwicklung der Theorie nicht leicht war, möglichst allgemeine Beispiele zu finden, und dabei verschiedene Vermutungen zu verifizieren.

- Um den in den Bemerkungen 4.6.2 angesprochenen allgemeinen Fall zu erreichen (Vermeiden der Ziffern 0 und $p-1$ in der p-adischen Darstellung der Raumdimension n), mußte die Wahl $p = 2$ vermieden werden.
- Außerdem war es klar, daß man der p-adischen Entwicklung einer kleinen Dimensionszahl kaum die Komplexität der Dinge ansehen konnte.

Erst durch den Einsatz eines leistungsfähigen PC's entstanden Beispiele, die einerseits die meisten Vermutungen des Autors bestärkten und andererseits dessen Betreuer immer mehr von deren Richtigkeit überzeugten.

Dem Leser wollen wir diese Ergebnisse nicht vorenthalten.

Beispiel 1

$$\begin{array}{rcrcl} p & = & 3 & & \\ n & = & 113 & = & \langle 1,1,0,1,2\rangle \\ b & = & 114 & = & \langle 1,1,0,2,0\rangle \end{array}$$

$$\begin{array}{rcrcl} V(3,b) & = & 6 & = & \langle 2,0\rangle \\ V(1;3,b) & = & 9 & = & \langle 1,0,0\rangle \end{array}$$

$$\begin{array}{rcrcl} V(4,b) & = & 33 & = & \langle 1,0,2,0\rangle \\ V(1;4,b) & = & 36 & = & \langle 1,1,0,0\rangle \\ V(1,2;4,b) & = & 54 & = & \langle 2,0,0,0\rangle \end{array}$$

Wir listen jetzt sämtliche nichtleeren irreduziblen invarianten Unterräume

$$\mathcal{U}_\alpha = [\{P_\lambda \mid \lambda \in \Lambda_\alpha\}]$$

auf, indem wir die zugehörigen Indexmengen Λ_α angeben:

$$\begin{array}{rcrcl} \Lambda_1 & = & \Lambda(3,b) & = & \Omega(V(3,b)) \\ \Lambda_2 & = & \Lambda(1;3,b) & = & \Omega(V(3,b)) \cup \Omega(V(1;3,b)) \end{array}$$

$$\begin{array}{rcrcl} \Lambda_3 & = & \Lambda(4,b) & = & \Omega(V(4,b)) \\ \Lambda_4 & = & \Lambda(1;4,b) & = & \Omega(V(4,b)) \cup \Omega(V(1;4,b)) \\ \Lambda_5 & = & \Lambda(1,2;4,b) & = & \Omega(V(4,b)) \cup \Omega(V(1;4,b)) \cup \Omega(V(1,2;4,b)) \end{array}$$

Obwohl wir eine (in der Basis 3) fünfstellige Raumdimension gewählt haben, besitzen die Indexmengen $\Lambda(I_1, \ldots, I_L; i, b)$ maximal einen Indexblock.

Es bedarf also eines komplexeren Beispiels, um die allgemeine Systematik zu erkennen.

Beispiel 2

$$
\begin{aligned}
p &= 2 \\
n &= 370 &&= \langle 1,0,1,1,1,0,0,1,0\rangle \\
b &= 371 &&= \langle 1,0,1,1,1,0,0,1,1\rangle \\
\\
V(1,b) &= 1 &&= \langle 1\rangle \\
\\
V(4,b) &= 3 &&= \langle 1,1\rangle \\
V(0,1;4,b) &= 4 &&= \langle 1,0,0\rangle \\
V(1;4,b) &= 5 &&= \langle 1,0,1\rangle \\
V(0,1,2;4,b) &= 8 &&= \langle 1,0,0,0\rangle \\
V(1,2;4,b) &= 9 &&= \langle 1,0,0,1\rangle \\
\\
V(5,b) &= 19 &&= \langle 1,0,0,1,1\rangle \\
V(0,1;5,b) &= 20 &&= \langle 1,0,1,0,0\rangle \\
V(1;5,b) &= 21 &&= \langle 1,0,1,0,1\rangle \\
V(0,1,2;5,b) &= 24 &&= \langle 1,1,0,0,0\rangle \\
V(1,2;5,b) &= 25 &&= \langle 1,1,0,0,0\rangle \\
\\
V(6,b) &= 51 &&= \langle 1,1,0,0,1,1\rangle \\
V(0,1;6,b) &= 52 &&= \langle 1,1,0,1,0,0\rangle \\
V(1;6,b) &= 53 &&= \langle 1,1,0,1,0,1\rangle \\
V(0,1,2;6,b) &= 56 &&= \langle 1,1,1,0,0,0\rangle \\
V(1,2;6,b) &= 57 &&= \langle 1,1,1,0,0,1\rangle \\
\\
V(8,b) &= 115 &&= \langle 1,1,1,0,0,1,1\rangle \\
V(0,1;8,b) &= 116 &&= \langle 1,1,1,0,1,0,0\rangle \\
V(1;8,b) &= 117 &&= \langle 1,1,1,0,1,0,1\rangle \\
V(0,1,2;8,b) &= 120 &&= \langle 1,1,1,1,0,0,0\rangle \\
V(1,2;8,b) &= 121 &&= \langle 1,1,1,1,0,0,1\rangle \\
V(0,1,2,3,4,5,6;8,b) &= 128 &&= \langle 1,0,0,0,0,0,0,0\rangle \\
V(1,2,3,4,5,6;8,b) &= 129 &&= \langle 1,0,0,0,0,0,0,1\rangle \\
V(4,5,6;8,b) &= 131 &&= \langle 1,0,0,0,0,0,1,1\rangle \\
V(0,1,4,5,6;8,b) &= 132 &&= \langle 1,0,0,0,0,1,0,0\rangle \\
V(1,4,5,6;8,b) &= 133 &&= \langle 1,0,0,0,0,1,0,1\rangle \\
V(0,1,2,4,5,6;8,b) &= 136 &&= \langle 1,0,0,0,1,0,0,0\rangle
\end{aligned}
$$

$$
\begin{array}{rcccl}
V(1,2,4,5,6;8,b) & = & 137 & = & \langle 1,0,0,0,1,0,0,1\rangle \\
V(5,6;8,b) & = & 147 & = & \langle 1,0,0,1,0,0,1,1\rangle \\
V(0,1,5,6;8,b) & = & 148 & = & \langle 1,0,0,1,0,1,0,0\rangle \\
V(1,5,6;8,b) & = & 149 & = & \langle 1,0,0,1,0,1,0,1\rangle \\
V(0,1,2,5,6;8,b) & = & 152 & = & \langle 1,0,0,1,1,0,0,0\rangle \\
V(1,2,5,6;8,b) & = & 153 & = & \langle 1,0,0,1,1,0,0,1\rangle \\
V(6;8,b) & = & 179 & = & \langle 1,0,1,1,0,0,1,1\rangle \\
V(0,1,6;8,b) & = & 180 & = & \langle 1,0,1,1,0,1,0,0\rangle \\
V(1,6;8,b) & = & 181 & = & \langle 1,0,1,1,0,1,0,1\rangle \\
V(0,1,2,6;8,b) & = & 184 & = & \langle 1,0,1,1,1,0,0,0\rangle \\
V(1,2,6;8,b) & = & 185 & = & \langle 1,0,1,1,1,0,0,1\rangle
\end{array}
$$

Analog dem vorigen Beispiel listen wir auch hier die entsprechenden Indexmengen auf:

$$
\begin{array}{rcl}
\Lambda(1,b) & = & \Omega(1)
\end{array}
$$

$$
\begin{array}{rcl}
\Lambda(4,b) & = & \Omega(3) \\
\Lambda(0,1;4,b) & = & \Omega(3)\cup\Omega(4) \\
\Lambda(0,1,2;4,b) & = & \Omega(3)\cup\Omega(4)\cup\Omega(8) \\
\Lambda(1;4,b) & = & \Omega(3)\cup\Omega(5) \\
\Lambda(1,2;4,b) & = & \Omega(3)\cup\Omega(5)\cup\Omega(9)
\end{array}
$$

$$
\begin{array}{rcl}
\Lambda(5,b) & = & \Omega(19) \\
\Lambda(0,1;5,b) & = & \Omega(19)\cup\Omega(20) \\
\Lambda(0,1,2;5,b) & = & \Omega(19)\cup\Omega(20)\cup\Omega(24) \\
\Lambda(1;5,b) & = & \Omega(19)\cup\Omega(21) \\
\Lambda(1,2;5,b) & = & \Omega(19)\cup\Omega(21)\cup\Omega(25)
\end{array}
$$

$$
\begin{array}{rcl}
\Lambda(6,b) & = & \Omega(51) \\
\Lambda(0,1;6,b) & = & \Omega(51)\cup\Omega(52) \\
\Lambda(0,1,2;6,b) & = & \Omega(51)\cup\Omega(52)\cup\Omega(56) \\
\Lambda(1;6,b) & = & \Omega(51)\cup\Omega(53) \\
\Lambda(1,2;6,b) & = & \Omega(51)\cup\Omega(53)\cup\Omega(57)
\end{array}
$$

$$
\begin{array}{rcl}
\Lambda(8,b) & = & \Omega(115) \\
\Lambda(0,1;8,b) & = & \Omega(115)\cup\Omega(116) \\
\Lambda(0,1,2;8,b) & = & \Omega(115)\cup\Omega(116)\cup\Omega(120)
\end{array}
$$

$$
\begin{aligned}
\Lambda(0,1,2,3,4,5,6;8,b) &= \Omega(115)\cup\Omega(116)\cup\Omega(120)\cup\Omega(128)\\
\Lambda(0,1,2,4,5,6;8,b) &= \Omega(115)\cup\Omega(116)\cup\Omega(120)\cup\Omega(131)\cup\Omega(132)\cup\Omega(136)\\
\Lambda(0,1,2,5,6;8,b) &= \Omega(115)\cup\Omega(116)\cup\Omega(120)\cup\Omega(147)\cup\Omega(148)\cup\Omega(152)\\
\Lambda(0,1,4,5,6;8,b) &= \Omega(115)\cup\Omega(116)\cup\Omega(131)\cup\Omega(132)\\
\Lambda(1;8,b) &= \Omega(115)\cup\Omega(117)\\
\Lambda(1,2;8,b) &= \Omega(115)\cup\Omega(117)\cup\Omega(121)\\
\Lambda(1,2,3,4,5,6;8,b) &= \Omega(115)\cup\Omega(117)\cup\Omega(121)\cup\Omega(129)\\
\Lambda(1,2,4,5,6;8,b) &= \Omega(115)\cup\Omega(117)\cup\Omega(121)\cup\Omega(131)\cup\Omega(133)\cup\Omega(137)\\
\Lambda(0,1,2,5,6;8,b) &= \Omega(115)\cup\Omega(117)\cup\Omega(121)\cup\Omega(147)\cup\Omega(149)\cup\Omega(153)\\
\Lambda(0,1,5,6;8,b) &= \Omega(115)\cup\Omega(116)\cup\Omega(147)\cup\Omega(148)\\
\Lambda(1,4,5,6;8,b) &= \Omega(115)\cup\Omega(117)\cup\Omega(131)\cup\Omega(133)\\
\Lambda(1,4,5,6;8,b) &= \Omega(115)\cup\Omega(117)\cup\Omega(147)\cup\Omega(149)\\
\Lambda(0,1,2,6;8,b) &= \Omega(115)\cup\Omega(116)\cup\Omega(120)\cup\Omega(179)\cup\Omega(180)\cup\Omega(184)\\
\Lambda(0,1,6;8,b) &= \Omega(115)\cup\Omega(116)\cup\Omega(179)\cup\Omega(180)\\
\Lambda(1,2,6;8,b) &= \Omega(115)\cup\Omega(117)\cup\Omega(121)\cup\Omega(179)\cup\Omega(181)\cup\Omega(185)\\
\Lambda(1,6;8,b) &= \Omega(115)\cup\Omega(117)\cup\Omega(179)\cup\Omega(181)\\
\Lambda(4,5,6;8,b) &= \Omega(115)\cup\Omega(131)\\
\Lambda(5,6;8,b) &= \Omega(115)\cup\Omega(147)\\
\Lambda(6;8,b) &= \Omega(115)\cup\Omega(179)
\end{aligned}
$$

Spätestens nach diesem Beispiel ist sich wohl jedermann der Komplexität der Aufgabe bewußt, alle irreduziblen invarianten Unterräume zu bestimmen.

Abschließende Bemerkungen

Nach der Lektüre dieser Arbeit drängen sich dem Leser gewiß mehrere Fragen auf, die wir hier nicht beantwortet haben. In gleicher Weise haben wir sicherlich Folgerungen aus dem einen oder anderen Satz nicht ausgesprochen. Einige wenige Ideen und Denkanstöße wollen wir deshalb hier noch anführen:

1. Im letzten Kapitel wurden lediglich die zu irreduziblen Unterräumen gehörigen Indexmengen angegeben. Es ist offensichtlich, daß man durch Summieren der irreduziblen Unterräume alle invarianten Unterräume

   $$\mathcal{U} = [\{P_\lambda \mid \lambda \in \Lambda\}]$$

   bekommt. Die Frage, wie sich die zugehörigen Indexmengen Λ als Vereinigung $\Lambda = \bigcup_\nu \Omega(V_\nu)$ schreiben lassen, ist gewiß nicht uninteressant, fällt jedoch in jenen Bereich, der in dieser Arbeit nicht mehr behandelt wird.

2. Die Gruppe $\mathrm{PGL}(\Gamma)$ operiert für $\#K \geq n+2$ scharf 3-fach transitiv auf den Punkten der Normkurve Γ. Wenn wir Γ aus einem der invarianten Unterräume $\mathcal{U}$ auf einen Komplementärraum $\mathcal{V}$ projizieren, dann ergibt das in diesem Raum eine rationale Kurve, die ebenfalls eine zu $\mathrm{PGL}(2, K)$ isomorphe Gruppe projektiver Kollineationen gestattet, welche gewiß auch scharf 3-fach transitiv operiert. Auch dieser Gedanke der Projektionen und deren Auswirkungen wurde nicht weiter verfolgt.

3. Rationale Normkurven sind spezielle eindimensionale Veronese Mannigfaltigkeiten. Für den höherdimensionalen Fall (vgl. [4]) kann man zum Teil analoge Fragestellungen wie in dieser Arbeit formulieren, wobei Multinomialkoeffizienten, die modulo char$K$ verschwinden, eine bedeutende Rolle spielen dürften. Näher darauf einzugehen, würde sicherlich den Rahmen dieser Arbeit sprengen.

Literaturverzeichnis

[1] Benz, W., *Vorlesungen über Geometrie der Algebren*, Springer, Berlin Heidelberg New York, 1973.

[2] Brauner, H., *Geometrie projektiver Räume II*, BI–Wissenschaftsverlag, Mannheim Wien Zürich, 1976.

[3] Brouwer, A.E., and Wilbrink, H.A., *Block Designs*, in Handbook of Incidence Geometry, Buekenhout, F., ed., Elsevier, Amsterdam, 1995, ch. 8, pp. 349–382.

[4] Burau, W., *Mehrdimensionale projektive und höhere Geometrie*, Dt. Verlag d. Wissenschaften, Berlin, 1961.

[5] Glynn, D.G., *The non-classical* 10*-arc of* $PG(4, 9)$, Discrete Math., 59 (1986), pp. 43–51.

[6] Gmainer, J. und Havlicek, H., *Nuclei of Normal Rational Curves.* J. Geometry, im Druck.

[7] Gmainer, J., *MDS–Codes und (Hyper–)Ovale*, Diplomarbeit, TU Wien, 1996.

[8] Hasse, H., *Noch eine Begründung der Theorie der höheren Differentialquotienten in einem algebraischen Funktionenkörper einer Unbestimmten*, J. reine angew. Math., 177 (1937), pp. 215–237.

[9] Havlicek, H., *Normisomorphismen und Normkurven endlichdimensionaler projektiver Desargues–Räume*, Monatsh. Math., 95 (1983), pp. 203–218.

[10] Havlicek, H., *Erzeugnisse projektiver Bündelisomorphismen*, 1984. Berichte aus der mathematisch-statistischen Sektion im Forschungszentrum Graz, No. 215.

[11] Herzer, A., *Die Schmieghyperebenen an die Veronese–Mannigfaltigkeit bei beliebiger Charakteristik*, J. Geometry, 18 (1982), pp. 140–154.

[12] Hexel, E., and Sachs, H., *Counting residues modulo a prime in Pascal's triangle*, Indian J. Math., 20 (1978), pp. 91–105.

[13] Hill, R., *A first course in coding theory*, Oxford University Press, Oxford, 1986.

[14] Hirschfeld, J.W.P., *Projective Geometry over Finite Fields*, Clarendon Press, Oxford, second ed., 1998.

[15] Hirschfeld, J.W.P., and Thas, J.A., *General Galois Geometries*, Oxford University Press, Oxford, 1991.

[16] Karzel, H., *Über einen Fundamentalsatz der synthetischen algebraischen Geometrie von W. Burau und H. Timmermann*, J. Geometry, 28 (1987), pp. 86–101.

[17] Long, C.T., *Pascal's triangle modulo p*, Fibonacci Q., 19 (1981), pp. 458–463.

[18] Roberts, J.B., *On binomial coefficient residues*, Canadian J. Math., 9 (1957), pp. 363–370.

[19] Storme, L., and Thas, J.A., *k-arcs and dual k-arcs*, Discrete Math., 125, No.1-3 (1994), pp. 357–370.

[20] Thas, J.A., *Normal rational curves and* $(q+2)$*–arcs in a Galois space* $S_{q-2,q}$ $(q = 2^h)$, Atti Accad. Naz. Lincei Rend., 47 (1969), pp. 249–252.

[21] Thas, J.A., *M.D.S. Codes and Arcs in Projective Spaces: A Survey*, Le Matematiche, 47 (1992), pp. 315–328.

[22] Timmermann, H., *Descrizioni geometriche sintetiche di geometrie proiettive con caratteristica* $p > 0$, Ann. mat. pura appl., IV. Ser. 114, (1977), pp. 121–139.

[23] Timmermann, H., *Zur Geometrie der Veronesemannigfaltigkeit bei endlicher Charakteristik*, Habilitationsschrift, Univ. Hamburg, 1978.

[24] van der Waerden, B.L., *Algebra*, Springer-Verlag, Berlin Heidelberg New York, 1966.

Lebenslauf

Ich wurde am 21. Dezember 1972 in Wien geboren. In den Jahren 1979 bis 1983 besuchte ich die Volksschule in Trautmannsdorf/Leitha. Nach weiteren 8 Jahren Bundesgymnasium Bruck/Leitha, wo ich mich für den neusprachlichen Zweig entschieden hatte, legte ich am 11. Juni 1991 die Reifeprüfung ab.

Im Oktober 1991 begann ich das Studium *Technische Mathematik* an der TU Wien, welches ich im Oktober 1996 abgeschlossen habe. Noch im Wintersemester 96/97 inskribierte ich das Doktoratsstudium.

Seit Oktober 1997 bin ich Mitarbeiter des Projekts

„Veronese varieties over fields with non–zero characteristic“,

welches vom Fonds zur Förderung der wissenschaftlichen Forschung (FWF) unterstützt wird.

Meine Dissertation „Rationale Normkurven in Räumen mit positiver Charakteristik“ habe ich am Institut für Geometrie in den Jahren 1996 - 1999 verfaßt.

Dipl.-Ing. Johannes Gmainer

Hauptstraße 71
2454 Sarasdorf