Technische Universität München

Zentrum Mathematik

Koordinatisierung miquelscher Benz-Ebenen und ihre Anwendungen in der Kryptologie

Sayed Ghahreman Taherian

Vollständiger Abdruck der von der Fakultät für Mathematik der Technischen Universität München zur Erlangung des akademischen Grades eines

Doktors der Naturwissenschaften

genehmigten Dissertation.

Vorsitzender: Univ.-Prof. Dr. K. Meyberg

Prüfer der Dissertation:

1. Univ.-Prof. Dr. H. -J. Kroll

2. Univ.-Prof. Dr. Dr.h.c. H. Karzel, em.

3. Univ.-Prof. Dr. A. Beutelspacher,
Justus-Liebig-Universität Giessen
(schriftliche Beurteilung)

Die Dissertation wurde am 14.11.2000 bei der Technischen Universität München eingereicht und durch die Fakultät für Mathematik am 20.06.2001 angenommen.

Einleitung **3**

1 Koordinatisierung miquelscher Benz-Ebenen **9**

1.1 Grundlegende Eigenschaften von Benz-Ebenen 9

1.2 Die Vierkreisrelation 19

1.3 Das Axiom von Miquel 29

1.4 Drehstreckungen 36

1.5 Koordinatisierung der miquelschen Benz-Ebenen 55

2 Anwendung der Benz-Ebenen in der Kryptologie **65**

2.1 Grundlegende Begriffe 65

2.2 Entwurf des Chiffriersystems $C(\mathbb{L}, f, \pi)$ 67

2.3 Bemerkungen zur Kryptoanalyse des Chiffriersystem $C(\mathbb{L}, f, \pi)$. 72

2.4 Das modifizierte Chiffriersystem $C(\mathbb{K})$ 81

2.5 Implementierung des Chiffriersystem $\mathcal{C}(\mathbb{K})$ als Chiffriersystem $\mathcal{C}'(\mathbb{K})$ 82

2.6 Digitale Unterschrift 84

Anhang **90**

Einleitung

Nach Erscheinen des berühmten Buches „Grundlagen der Geometrie “ von D. Hilbert im Jahre 1899 [14] setzte eine rege Forschungstätigkeit auf dem Gebiet der *Grundlagen der Geometrie* ein, die auch die Kreisgeometrie erfaßte wie man eindrucksvoll im Literaturverzeichnis von W. Benz' Monographie : „Vorlessungen über Geometrie der Algebren“ [3] feststellen kann. Aber erst 1935 bewiesen B. L. van der Waerden und L. J. Smid einen zum Darstellungssatz desarguescher affiner Ebenen analogen Satz für die Möbius- und Laguerre- Geometrie [29]. Sie erkannten die fundamentale Bedeutung des Satzes von Miquel für die Kreisgeometrie, die der der Sätze von Desargues und Pappus für die affine und projektive Geometrie entspricht. Mit ihrem Darstellungssatz für die miquelschen Möbius- und Laguerre-Ebenen gelang es ihnen diese Geometrien algebraisch darzustellen. Beim Beweis ihres Darstellungssatzes für die miquelschen Möbius-Ebenen gehen sie wie folgt vor:

1. Sie beweisen, dass jede affine Ableitung eine pappussche affine Ebene ist. Nach Auszeichnung eines Punktes ∞ können sie daher die affine Ableitung in ∞ mittels eines kommutativen Körpers K algebraisch als affine Koordinatenebene darstellen.

2. Sie zeigen, dass die Kreise, die nicht durch ∞ gehen durch quadratische Gleichungen $q(x,y) + ax + by + c = 0$, wobei $q : K \times K \to K$ eine feste nullteilige quadratische Form ist, dargestellt werden.

Aus diesem Darstellungssatz ergibt sich sofort die Darstellung miquelscher Möbius-Ebenen mittels quadratischer Körpererweiterungen:

- Als Punktmenge hat man die projektive Gerade $L \cup \{\infty\}$ über der quadratischen Erweiterung $L := K[x]/(q(x,1))$ von K und als Kreise die Bilder der projektiven Geraden $K \cup \{\infty\}$ unter den Abbildungen aus der projektiven linearen Gruppe $\mathrm{PGL}(2,L)$ (vgl. [3]).

Beim Beweis des Darstellungssatzes für die miquelschen Laguerre-Ebenen gehen van der Waerden und Smid unter Berücksichtigung von Fallunterscheidungen, die sich aus der Existenz von nicht-verbindbaren Punkten ergeben, ganz analog vor. Als quadratische Form ergibt sich hier $q(x, y) = x^2$.

Für die dritte klassische Kreisgeometrie, die Minkowski-Ebenen wurde ein entsprechendes Ergebnis dann erst 1970 erzielt. In seiner Dissertation [15] geht G. Kaerlein beim Beweis des Darstellungssatzes für die miquelschen Minkowski-Ebenen wie van der Waerden und Smid vor.

In seinen „Vorlessungen über Geometrie der Algebren"[3] stellt W. Benz 1973 die Geometrien von Möbius, Laguerre und Minkowski in einheitlicher Weise dar als Kettengeometrien $\Sigma(\mathbb{K}, \mathbb{A})$ der quadratischen Algebren $\mathbb{A}$ über einem kommutativen Körper $\mathbb{K}$. Dementsprechend stellen sich zwei Probleme:

1 Läßt sich der Darstellungssatz für die drei genannten Geometrien, die sogennanten *Benz-Ebenen*, einheitlich führen?

2 Kann die quadratische Algebra, d.h. insbesondere die Multiplikation direkt konstruiert werden?

Um diese Fragen geht es im ersten Teil der vorliegenden Arbeit. Ausgangspunkt unserer Untersuchungen ist die 1995 in den „Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg " erschienene Arbeit „Ein neuer Beweis des Darstellungssatzes für miquelsche Möbius-Ebenen" von A. Lenard [21], in der die Multiplikation des Oberkörpers direkt mittels *Drehstreckungen* konstruiert wird.

Wie wir in [20] gezeigt haben, kann der Lenardsche Beweis allerdings noch erheblich verkürzt werden, da bei konsequenter Ausnützung der Eigenschaften der Drehstreckungen der erste Beweisschritt bei Lenard, der wie bei van der Waerden und Smid im Nachweis des Satzes von Pappus für die affinen Ableitungen besteht, vermieden werden kann.

Durch Ausweitung dieser neuen Beweismethode auf alle Benz-Ebenen, also auch auf die Klasse der Laguerre und Minkowski-Ebenen, werden wir die eingangs gestellten Fragen positiv beantworten. Im einzelnen gehen wir dabei wie folgt vor.

In §1.1 stellen wir die grundlegenden Definitionen und Eigenschaften der Benz-Ebenen zusammen und beweisen darüberhinaus einen Eindeutigkeitsatz für Kreisverwandtschaften (Satz 1.1.4) und einen Isomorphiesatz für Kettengeometrien $\Sigma(\mathbb{K}, \mathbb{A})$ (Satz 1.1.5) über quadratischen Algebren.

Durch Einführung sogenannter uneigentlicher Kreise in der Laguerre- und Minkowski-Geometrie gelingt es in §1.2 die *Vierkreisrelation* auf der Menge der Punktesechstupel für alle drei Typen von Benz-Ebenen zu definieren.

Die Eigenschaften der Vierkreisrelation, insbesondere Korollar 1.2.1 ermöglichen in §1.4 die Definition der Drehstreckungen. Zuvor wird aber in §1.3 das Axiom von Miquel, dass die miquelschen Benz-Ebenen definiert, vorgestellt.

Für miquelsche Benz-Ebenen werden die eigentlichen Kreisverwandtschaften durch eine Abschwächung der definierenden Eigenschaft gekennzeichnet (Satz 1.3.2).

Nach den Vorbereitungen in §1.2 werden in §1.4 die Drehstreckungen in miquelschen Benz-Ebenen eingeführt. Im Fall einer über einer quadratischen Algebra $(\mathbb{A}, \mathbb{K})$ definierten Benz-Ebene entsprechen den Drehstreckungen mit zwei Fixpunkten die Linksmultiplikation mit Einheiten. Anderes als bei Lenard gehören jedoch bei uns die Streckungen (d.h. im Algebra-Fall die Linksmultiplikation mit von Null verschiedenen Elementen des Grundkörpers $\mathbb{K}$) nicht zu den Drehstreckungen. Es stellt sich heraus, dass die Drehstreckungen Kreisverwandtschaften sind (Satz 1.4.4). Weiter wird bewiesen, dass das Produkt von zwei Drehstreckungen mit denselben Fixpunkten entweder eine Drehstreckung ist oder eine Streckung oder eine axiale Kreisverwandtschaft, d.h eine Kreisverwandtschaft, die zwei Erzeugende punktweise festläßt (Satz 1.4.5). Auf der Grundlage dieser Ergebnisse ergibt sich, dass die von den Drehstreckungen mit zwei Fixpunkten 0 und ∞ erzeugte Gruppe $\Delta_{0,\infty}$ kommutativ ist und auf der Menge $\mathbb{A}^*$ der Punkte,

die von 0 und ∞ verschieden sind und nicht auf den Erzeugenden durch 0 und ∞ liegen, regulär operiert (Satz 1.4.6). Dadurch erhält man jetzt nebenbei, dass die affinen Ableitungen pappussch sind. Wie üblich kann man daher auf der Menge der von ∞ verschiedenen Punkte, die nicht auf den Erzeugenden durch ∞ liegen eine Addition + definieren (§1.5). Nach Auszeichnung eines Punktes $1 \in \mathbb{A}^*$ wird die Gruppenstruktur von $\Delta_{0,\infty}$ auf $\mathbb{A}^*$ übertragen. Damit hat man dann die Einheitengruppe der zu konstruierenden Algebra $\mathbb{A}$. Der Kreis E durch $0, 1, \infty$ liefert den Grundkörper $\mathbb{K} := E \setminus \{\infty\}$ (Lemma 1.5.1). Schließlich wird die Multiplikation von $\mathbb{A}^*$ auf ganz $\mathbb{A}$ so fortgesetzt, dass $(\mathbb{A}, \mathbb{K})$ eine quadratische Algebra wird (Satz 1.5.1). Mit dem Resultat, dass sich die Inversenbildung in $\mathbb{A}^*$ zu einer Kreisverwandtschaft fortsetzen lässt (vgl. Lemma 1.5.3) gelingt es endlich zu zeigen, dass jeder Kreis Bild des Kreises E unter einer Abbildung aus der projektiven linearen Gruppe $\mathrm{PGL}(\mathbb{A}, 2)$ ist (Satz 1.5.2). Damit haben wir einen einheitlichen Beweis des Darstellungssatzes für miquelsche Benz-Ebenen (Satz 1.5.3).

Im zweiten, anwendungsbezogenen Teil der Dissertation werden Fragen der Kryptologie mit Hilfe von Benz-Ebenen behandelt.

Im beginnenden Informationszeitalter mit der elektronischen Datenübertragung gewinnt die Kryptologie immer mehr an Bedeutung. Die Kryptologie hat drei Ziele. Zum ersten stellt sie Verfahren bereit, um die Vertraulichkeit von Information zu gewährleisten (Verschlüsselung). Zum zweiten werden Methoden zur Verfügung gestellt, die es ermöglichen, gezielte Veränderungen von Daten zu erkennen und zu überprüfen, ob Daten von dem angegebenen Absender stammen (Authentikation). Zum dritten werden Verfahren gesucht, durch die die Anonymität des Absenders oder Empfängers einer Nachricht (gegenüber dritten oder auch gegenseitig) gewahrt wird.

Solchen Methoden liegt in der Regel der Einsatz geheimer Schlüssel zugrunde; deshalb ist auch die sichere Verteilung und Speicherung von geheimen Schlüsseln ein zentrales Gebiet der Kryptologie.

Wie in der Codierungstheorie (vgl. z.B. [10]) lassen sich auch in der Kryptologie

endliche Geometrien mit Erfolg einsetzen(vgl. [2] Kap.VI). In [6] hat C. Capellaro als Erster endliche Benz-Ebenen zur Konstruktion von Kryptosystemen benützt. Unter Verwendung der Inzidenz-Eigenschaften konstruiert er sowohl Chiffrier- als auch Authentikationssysteme. Wir werden hier mit Hilfe der Automorphismengruppe einer miquelschen Benz-Ebene ein Chiffriersystem entwerfen (vgl. §2.2-2.5). Als Design-Kriterium verwenden wir dabei die Prinzipien der Konfusion und Diffusion (vgl. [23] Seite 145).

Im letzten Paragraphen wird schließlich mit Hilfe der Vierkreisrelation (also mit Inzidenzeigenschaften) in Möbius-Ebenen ein Verfahren zur digitalen Unterschrift vorgestellt.

Im Anhang werden die Programme zu den in §2.5, 2.6 entworfenen Verfahren angefügt.

Zum Schluß möchte ich allen meinen Dank aussprechen, die mir durch ihre Unterstützung die Promotion am Zentrum für Mathematik der Technischen Universität München ermöglicht haben.

Den Herren Professoren Dr. Dr. h. c. Helmut Karzel und Dr. Dr. h. c. Hans-Joachim Kroll danke ich für die Anregung zu dieser Arbeit.

Besonders herzlich bedanke ich mich bei Herrn Prof. Dr. Dr. h. c. Hans-Joachim Kroll für seine kompetente, intensive und nie nachlassende Betreuung der Dissertation. Ohne die durch ihn vermittelten tiefen Einsichten in die Kreisgeometrie wäre diese Arbeit nicht zustande gekommen. Darüberhinaus bin ich ihm tief verbunden für die mir entgegengebrachte Herzlichkeit und Freundschaft.

Für finanzielle Unterstützung während der Arbeit an meiner Dissertation bin ich der Diercks-von-Zweck-Stiftung (für die Gewährung eines 6-monatigen Stipendiums) und dem Zentrum Mathematik der Technischen Universität München (für die Anstellung als Wissenschaftlische Hilfskraft) zu Dank verpflichtet.

Für die angenehme, freundliche Atmosphäre gilt mein Dank auch allen Mitarbeitern des Zentrums Mathematik der Technischen Universität München.

Insbesondere danke ich für ihr Entgegenkommen und ihre Hilfsbereitschaft den

Herren Professoren Günter Kist, Kay Sörensen, Helmut Karzel, Heinrich Wefelscheid, Peter Gritzmann, Herbert Hotje, Roland Bulirsch, Kurt Meyberg, Werner Heise und den Herren Doktoren Hubert Kiechle, Thomas Honold und Sven de Vries.

Ganz herzlich danken möchte ich schließlich noch meinen Eltern, meinem Onkel Afrasiab Heidarian und meiner Tante Masoumeh für ihren Zuspruch und ihre immerwährende Unterstützung.

1 Koordinatisierung miquelscher Benz-Ebenen

1.1 Grundlegende Eigenschaften von Benz-Ebenen

Da wir die Möbius- Laguerre- und Minkowski-Ebenen einheitlich als Benz-Ebenen behandeln wollen, benötigen wir eine Definition, die das Gemeinsame dieser drei Geometrien herausstellt. Wir halten uns dabei an die in [19] gegebene Darstellung. Es seien P eine nicht-leere Menge und $\mathfrak{G}$ eine Teilmenge der Potenzmenge von P; die Elemente von P heißen *Punkte* und die von $\mathfrak{G}$ *Erzeugende*. Das Paar $(P, \mathfrak{G})$ heißt *Gitter*, wenn es eine Partition $\mathfrak{G} = \bigcup_{i \in I} \mathfrak{G}_i$ von $\mathfrak{G}$ gibt, so dass gilt:

G1 Zu jedem Punkt $p \in P$ und jedem $i \in I$ gibt es genau ein $G \in \mathfrak{G}_i$ mit $p \in G$ (Bezeichnung: $[p]_i := G$).

G2 Für alle $i, j \in I$ mit $i \neq j$ und alle $G \in \mathfrak{G}_i,\ H \in \mathfrak{G}_j$ gilt $|G \cap H| = 1$ und $|G| \geq 2$.

Falls $\mathfrak{G} = \emptyset$ ist, bedeutet **G1**, dass auch $I = \emptyset$ gilt. Für jeden Punkt $p \in P$ eines Gitters $(P, \mathfrak{G})$ sei $[p] := \bigcup_{i \in I} [p]_i \cup \{p\}$. Zwei Punkte $a, b \in P$ heißen *verbindbar*, wenn es keine Erzeugende gibt, die a und b enthält, wenn also $b \notin [a]$.

Es sei $\mathfrak{K}$ eine weitere Teilmenge der Potenzmenge von P mit $\emptyset \notin \mathfrak{K}$; die Elemente von $\mathfrak{K}$ nennen wir *Kreise*. Für $M \subseteq P$ setzen wir $\mathfrak{K}(M) := \{K \in \mathfrak{K} \mid M \subseteq K\}$.

Es sei $w \in P$. Wir setzen:

$P^w := P \setminus [w], \quad \mathfrak{K}^w := \{K \setminus \{w\} \mid K \in \mathfrak{K}(w)\},$

$\mathfrak{G}^w := \{G \setminus [w] \mid G \in \mathfrak{G},\ w \notin G\}$, sowie $\mathcal{A}(w) := (P^w, \mathfrak{K}^w \cup \mathfrak{G}^w)$.

Die Inzidenzstruktur $\mathcal{A}(w)$ heißt die *Ableitung* von $(P, \mathfrak{K}, \mathfrak{G})$ im Punkt w.

Die Inzidenzstruktur $\mathfrak{B} := (P, \mathfrak{K}, \mathfrak{G})$ heißt *Benz-Ebene*, wenn $(P, \mathfrak{G})$ ein Gitter ist mit $|I| \leq 2$ und wenn gilt [1]

[1] Für den Spezialfall $|I| = 0$ bzw. $|I| = 1$ bzw. $|I| = 2$ findet man diese Definition in [13] bzw. [18] bzw. [17].

(B) Für jeden Punkt $w \in P$ ist $\mathcal{A}(w)$ eine affine Ebene.

Für jeden Punkt $w \in P$ einer Benz-Ebene $\mathfrak{B}$ nennen wir die affine Ebene $\mathcal{A}(w)$ *die affine Ableitung von* $\mathfrak{B}$ *im Punkt* w.

Eine Benz-Ebene $\mathfrak{B}$ heißt *Möbius-* bzw. *Laguerre-* bzw. *Minkowski-Ebene*, wenn $|I| = 0$ bzw. 1 bzw. 2 ist.

Im Fall einer Laguerre-Ebene geht durch jeden Punkt $p \in P$ genau eine Erzeugende $[p]_1 = [p]$. Um Fallunterscheidungen zu vermeiden, bezeichnen wir diese Erzeugende auch mit $[p]_2$.

Für Minkowski-Ebenen $(P, \mathfrak{K}, \mathfrak{G}_1 \cup \mathfrak{G}_2)$ ist folgende Bezeichnung nützlich: Für $a, b \in P$ sei $ab := [a]_1 \cap [b]_2$ (vgl. [11]).

Wir stellen die wichtigsten Eigenschaften einer Benz-Ebene zusammen.

Satz 1.1.1 *Für jede Benz-Ebene* $\mathfrak{B} := (P, \mathfrak{K}, \mathfrak{G})$ *gilt:*

(1) *Für jeden Kreis* $K \in \mathfrak{K}$ *gilt* $|K| \geq 3$.

(2) *Jede Erzeugende schneidet jeden Kreis in genau einem Punkt.*

(3) *Zu je drei paarweise verbindbaren Punkten* $a, b, c \in P$ *gibt es genau einen Kreis* $K \in \mathfrak{K}$ *mit* $a, b, c \in K$ (Bezeichnung: $(a, b, c)^\circ := K$).

(4) *Zu jedem Kreis* K*, jedem Punkt* $a \in K$ *und jedem mit* a *verbindbaren Punkt* $b \in P \setminus K$ *gibt es genau einen Kreis* $L \in \mathfrak{K}(a, b)$ *mit* $K \cap L = \{a\}$ (Bezeichnung*:* $\beta_a(K, b) := L$*).*

(5) *Alle Kreise sind gleichmächtig. Alle Erzeugende sind gleichmächtig.*

Beweis. (1) Nach Voraussetzung gibt es einen Punkt $w \in K$. Da $K \setminus \{w\}$ eine Gerade der affinen Ebene $\mathcal{A}(w)$ ist, enthält K noch mindestens zwei (von w verschiedene) Punkte.

(2) Es seien $X \in \mathfrak{G}_1$ eine Erzeugende und $K \in \mathfrak{K}$ ein Kreis.

(a) Es sei $w \in X \cap K$. Es gilt $K \setminus \{w\} \subseteq P^w = P \setminus [w]$. Wegen $w \in X$ gilt $X \subseteq [w]$, also $(K \setminus \{w\}) \cap X = \emptyset$, d.h. $K \cap X = \{w\}$. Damit gilt $|X \cap K| = 1$.

(b) Wegen (1) und (a) gibt es zwei verschiedene Punkte $v, u \in K \setminus X$. Es sei $Y := [v]_1$ die Erzeugende aus $\mathfrak{G}_1$ durch v. In der affinen Ebene $\mathcal{A}(u)$ ist $Y \setminus [u]$ die Parallele durch v zu $X \setminus [u]$. Es gilt $Y \cap K = \{v\}$ nach (a). Daher sind in $\mathcal{A}(u)$ die Geraden $Y \setminus [u]$ und $K \setminus [u]$ und damit auch $X \setminus [u]$ und $K \setminus [u]$ nicht parallel. Daher gilt $X \cap K \neq \emptyset$, also $|X \cap K| = 1$ nach (a).

(3) Nach Voraussetzung gilt $b, c \notin [a]$, also $b, c \in P^a$. Die Verbindungsgerade von b und c in der affinen Ebene $\mathcal{A}(a)$ liegt wegen $c \notin [b]$ in $\mathfrak{K}^a$, d.h. es gibt genau einen Kreis $K \in \mathfrak{K}(a)$ mit $b, c \in K$.

(4) Es seien $K \in \mathfrak{K},\ a \in K,\ b \in P$ mit $b \notin [a],\ K$. Zu der Geraden $K \setminus \{a\}$ von $\mathcal{A}(a)$ gibt es genau eine Gerade $C \in \mathfrak{K}^a \cup \mathfrak{G}^a$ mit $C \cap (K \setminus \{a\}) = \emptyset$ und $b \in C$. Nach dem Beweis von (2) schneidet jede Gerade $Y \in \mathfrak{G}^a$ die Gerade $K \setminus \{a\}$. Deshalb gilt $C \in \mathfrak{K}$(a), d.h. es gibt genau einen Kreis $L \in \mathfrak{K}(a)$ mit $C = L \setminus \{a\}$. Damit gibt es also genau ein $L \in \mathfrak{K}(a, b)$ mit $K \cap L = \{a\}$.

(5) Es seien $K, K' \in \mathfrak{K},\ G \in \mathfrak{G},\ w \in K \setminus G,\ w' \in K' \setminus [w]$. Dann gibt es ein $L \in \mathfrak{K}(w, w')$ und es gilt $|K| = |L|$ da $K \setminus \{w\},\ L \setminus \{w\}$ Geraden der affine Ebene $\mathcal{A}(w)$ sind. Ebenso gilt $|K'| = |L|$, also $|K| = |K'|$. Weiterhin gilt $|K \setminus \{w\}| = |G \setminus [w]|$, da auch $G \setminus [w]$ eine Gerade von $\mathcal{A}(w)$ ist, also $|G| = |K|$ im Fall der Minkowski-Ebene und $|G| = |K| - 1$ im Fall der Laguerre-Ebene. □

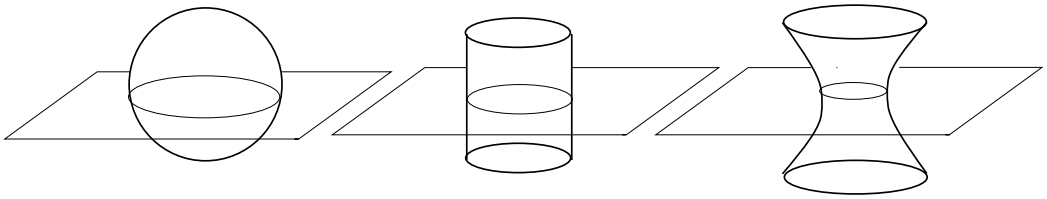
Die im Satz 1.1.1 angegebenen grundlegenden Eigenschaften einer Benz-Ebene kann man auch zur Definition einer Benz-Ebene verwenden, denn wegen Satz 1.1.1 ist $\mathfrak{B}$ auch eine Benz-Ebene im Sinne von [19].

Nach Satz 1.1.1(5) haben alle affine Ableitungen einer Benz-Ebene $\mathfrak{B}$ die gleiche Ordnung. Deshalb versteht man unter der *Ordnung* von $\mathfrak{B}$ die Ordnung einer affinen Ableitung.

Die klassischen Beispiele der Benz-Ebenen erhält man als Geometrie der ebenen Schnitte von Quadriken $\mathfrak{O}$ in einem dreidimensionalen projektiven pappusschen Raum. Dabei sind die Erzeugenden die in $\mathfrak{O}$ enthaltenen Geraden und die Kreise

die nicht-trivialen Schnitte von $\mathfrak{O}$, mit Ebenen die keine Erzeugende enthalten.

Man erhält eine Möbius- bzw. Laguerre- bzw. Minkowski-Ebene je nachdem ob $\mathfrak{O}$ eine ovale Quadrik oder ein Kegel ohne die Spitze oder eine ringartige Quadrik ist (Figur 1).



Figur 1

Es seien $(P, \mathfrak{K}, \mathfrak{G})$ und $(P', \mathfrak{K}', \mathfrak{G}')$ zwei Benz-Ebenen.

Jede Bijektion $\kappa : P \to P'$ mit $\kappa(\mathfrak{K}) = \mathfrak{K}'$ heißt *Kreisverwandtschaft*. Zwei Benz-Ebenen $(P, \mathfrak{K}, \mathfrak{G})$ und $(P', \mathfrak{K}', \mathfrak{G}')$ heißen *isomorph*, wenn es eine Kreisverwandtschaft $\kappa : P \to P'$ gibt (vgl. [3], [12]).

Satz 1.1.2 *Es seien* $\mathfrak{B} = (P, \mathfrak{K}, \mathfrak{G})$ *und* $\mathfrak{B}' = (P', \mathfrak{K}', \mathfrak{G}')$ *zwei Benz-Ebenen und* $\kappa : P \to P'$ *eine Kreisverwandtschaft. Dann gilt* $\kappa(\mathfrak{G}) = \mathfrak{G}'$, *und es gilt* $I = I'$ *sowie* $\kappa(\mathfrak{G}_i) = \mathfrak{G}'_i$ *für* $i \in I$ *oder* $\kappa(\mathfrak{G}_1) = \mathfrak{G}'_2$, $\kappa(\mathfrak{G}_2) = \mathfrak{G}'_1$.

Beweis.Es seien $G \in \mathfrak{G}_1$ und $x, y \in G,\ x \neq y$.

(1) Mit κ ist nach Voraussetzung auch κ^{-1} ein Isomorphismus.

Wäre $\kappa(y) \notin [\kappa(x)]$, so gäbe es ein $K' \in \mathfrak{K}'$ mit $\kappa(x), \kappa(y) \in K'$, und nach Voraussetzung gäbe es einen Kreis $K \in \mathfrak{K}$ mit $\kappa(K) = K'$, also $x, y \in K$ im Widerspruch zu $|G \cap K| = 1$ nach Satz 1.1.1 (2). Mit (1) gilt damit:

(2) Zwei verschiedene Punkte $x, y \in P$ sind genau dann verbindbar, wenn $\kappa(x)$ und $\kappa(y)$ verbindbar sind.

Aus (2) folgt sofort:

(3) $I \neq \emptyset$ genau dannn, wenn $I' \neq \emptyset$.

(4) Es sei $I \neq \emptyset$ und (wegen (1)) ohne Beschränkung der Allgemeinheit $|I| \leq |I'|$.

Es sei etwa $\kappa(y) \in [\kappa(x)]_1$, andernfalls vertausche man die Rolle von 1 und 2 in I'. Dann gilt $[\kappa(x)] \cap [\kappa(y)] = [\kappa(x)]_1$. Für $z \in G$ gilt also $\kappa(z) \in [\kappa(x)] \cap [\kappa(y)] = [\kappa(x)]_1$, also $\kappa(G) \subset [\kappa(x)]_1 =: G'$. Ebenso folgt $\kappa^{-1}(G') \subset [x]_1 = G$. Zusammen ergibt sich $\kappa(G) = G' \in \mathfrak{G}'_1$.

Für $F \in \mathfrak{G}_1, F \neq G$ gilt ebenso $\kappa(F) \in \mathfrak{G}$ und wegen $\kappa(G) \cap \kappa(F) = \kappa(G \cap F) = \emptyset$ gilt $\kappa(F) \in \mathfrak{G}_1$. Damit gilt $\kappa(\mathfrak{G}_1) \subset \mathfrak{G}'_1$. Ebenso folgt $\kappa^{-1}(\mathfrak{G}'_1) \subset \mathfrak{G}_1$, also $\kappa(\mathfrak{G}_1) = \mathfrak{G}'_1$.

Es sei jetzt $|I'| = 2$. Es gibt einen Kreis $A \in \mathfrak{K}$ mit $x \notin A$, also $\kappa(x) \notin \kappa(A)$. Dann gibt es also $x'_i := \kappa(A) \cap [\kappa(x)]_i$ $(i = 1, 2)$ und $x'_1 \neq x'_2$. Wegen (2) sind $x_i := \kappa^{-1}(x'_i)$ und x nicht verbindbar für $i = 1, 2$. Da andererseits x'_1 und x'_2 und damit auch x_1 und x_2 verbindbar sind, folgt $|I| = |A \cap [x]| = 2$.

Weiterhin folgt jetzt wie oben $\kappa(\mathfrak{G}_2) = \mathfrak{G}'_2$. □

Satz 1.1.3 *Es seien $(P, \mathfrak{G})$ eine affine Ebene, $A \subseteq P$ und , $\alpha, \beta : P \to P$ zwei Affinitäten mit $\alpha|_A = \beta|_A$. Wenn es durch jeden Punkt $x \in P \setminus A$ zwei verschiedene Geraden G, H gibt mit $|A \cap G| \geq 2,\ |A \cap H| \geq 2$, so gilt $\alpha = \beta$.*

Beweis. (1) Für jede Gerade $G \in \mathfrak{G}$ mit $|A \cap G| \geq 2$ gilt $\alpha(G) = \beta(G)$, denn nach Voraussetzung gibt es $g_1, g_2 \in A \cap G,\ g_1 \neq g_2$. Es gilt also $\alpha(G) = \overline{\alpha(g_1), \alpha(g_2)} = \overline{\beta(g_1), \beta(g_2)} = \beta(G)$.

(2) Zu $x \in P \setminus A$ gibt es $G, H \in \mathfrak{G}$ mit $x = G \cap H$ und $|A \cap G| \geq 2$, $|A \cap H| \geq 2$. Nach (1) gilt also $\alpha(x) = \alpha(G) \cap \alpha(H) = \beta(G) \cap \beta(H) = \beta(x)$. □

Satz 1.1.4 *Es seien $\mathfrak{B}$ eine Benz-Ebene, deren Ordnung mindestens 4 ist, α, β zwei Kreisverwandtschaften und $p, q \in \mathrm{Fix}\alpha \cap \mathrm{Fix}\beta,\ \ p \notin [q]$ und $\alpha|_{P^p \cap P^q} = \beta|_{P^p \cap P^q}$, dann gilt $\alpha = \beta$.*

Beweis. Für Möbius-Ebenen gilt die Aussage trivialerweise. Es sei also $\mathfrak{B}$ eine Laguerre- oder Minkowski-Ebene. Es sei $A := P^p \cap P^q$. Wegen $p \in \mathrm{Fix}\alpha \cap \mathrm{Fix}\beta$, sind $\alpha|_{P^p}$ und $\beta|_{P^p}$ Affinitäten von $\mathcal{A}(p)$ mit $\alpha|_A = \beta|_A$. Da die Ordnung von $\mathfrak{B}$

und damit von $\mathcal{A}(p)$ mindestens 4 ist, gibt es zu jedem $x \in P \setminus A$ zwei verschiedene Geraden G, H von $\mathcal{A}(p)$ mit $|A \cap G| \geq 2,\ |A \cap H| \geq 2$. Nach Satz 1.1.3 folgt $\alpha|_{P^p} = \beta|_{P^p}$und ebenso $\alpha|_{P^q} = \beta|_{P^q}$.

Da im Fall einer Laguerre-Ebene $[p] \cap [q] = \emptyset$, gilt in diesem Fall also $\alpha = \beta$.

Falls $\mathfrak{B}$ eine Minkowski-Ebene ist, müssen wir noch $\alpha(pq) = \beta(pq)$ und $\alpha(qp) = \beta(qp)$ zeigen. Da $\alpha|_{P^p} = \beta|_{P^p}$ gilt $\alpha([q]_i) = \beta([q]_i)$ und wegen $\alpha|_{P^q} = \beta|_{P^q}$ ebenso $\alpha([p]_i) = \beta([p]_i)$, also $\alpha(pq) = \alpha([p]_1 \cap [q]_2) = \alpha([p]_1) \cap \alpha([q]_2) = \beta([p]_1) \cap \beta([q]_2) = \beta([p]_1 \cap [q]_2) = \beta(pq)$ und ebenso $\alpha(qp) = \beta(qp)$. □

Die klassischen Modelle der Benz-Ebenen lassen sich wie folgt mit Hilfe von Algebren $(\mathbb{A}, \mathbb{K})$ von Rang 2 als Kettengeometrie $\Sigma(\mathbb{K}, \mathbb{A})$ beschreiben (vgl. [3]).

Es seien $(\mathbb{A}, \mathbb{K})$ eine kommutative und assoziative Algebra mit Einselement 1 über dem Körper $\mathbb{K}$, wobei wir uns $\mathbb{K}$ in der Form $\mathbb{K} \cdot 1 = \{k \cdot 1 \mid\ k \in \mathbb{K}\}$ in $\mathbb{A}$ eingebettet denken. Mit $\mathbb{A}^*$ bezeichnen wir die Einheitengruppe von $\mathbb{A}$.

Die Punktmenge der *Kettengeometrie* $\Sigma(\mathbb{K}, \mathbb{A})$ ist die *projektive Gerade*
$P(\mathbb{A}) := \{\mathbb{A}^*(x_1, x_2) \mid x_1, x_2 \in \mathbb{A},\ \langle x_1, x_2\rangle = \mathbb{A}\}$[2].
Die in $P(\mathbb{A})$ eingebettete projektive Gerade über $\mathbb{K}$ ist:
$P(\mathbb{K}) := \{\mathbb{A}^*(k_1, k_2) \mid k_1, k_2 \in \mathbb{K},\ (k_1, k_2) \neq (0, 0)\}$.
Die lineare Gruppe $\mathrm{GL}(2, \mathbb{A})$ besteht aus den Matrizen $\mathfrak{C} = (c_{ij})$ mit $c_{ij} \in \mathbb{A}$ und $\det\mathfrak{C} = c_{11}c_{22} - c_{12}c_{21} \in \mathbb{A}^*$. Die projektive lineare Gruppe $\mathrm{PGL}(2, \mathbb{A})$ besteht aus den Bijektionen $\gamma : P(\mathbb{A}) \to P(\mathbb{A})$, zu denen es eine 2×2-Matrix $\mathfrak{C} = (c_{ij}) \in \mathrm{GL}(2, \mathbb{A})$ gibt mit $\gamma(\mathbb{A}^*(x_1, x_2)) = \mathbb{A}^*((x_1, x_2)\mathfrak{C}) =: \widetilde{\mathfrak{C}}(\mathbb{A}^*(x_1, x_2))$. Die Menge $\mathfrak{K}$ der Ketten von $\Sigma(\mathbb{K}, \mathbb{A})$ ist $\mathfrak{K} = \{\gamma(P(\mathbb{K})) \mid \gamma \in \mathrm{PGL}(2, \mathbb{A})\}$.

Nun sei $(\mathbb{A}, \mathbb{K})$ eine Algebra von Rang 2. Dann ist $(\mathbb{A}, \mathbb{K})$ entweder eine Körpererweiterung von $\mathbb{K}$ oder eine lokale oder bilokale Algebra. Falls $(\mathbb{A}, \mathbb{K})$ lokal ist, bezeichne N_1 das maximale Ideal von $(\mathbb{A}, \mathbb{K})$; falls $(\mathbb{A}, \mathbb{K})$ bilokal ist, so seien N_1 und N_2 die beiden maximalen Ideale. Für $a = \mathbb{A}^*(a_1, a_2) \in P(\mathbb{A})$ und $i \in \{1, 2\}$

[2] $\langle x_1, x_2\rangle$ bezeichne die von $x_1,\ x_2$ erzeugte Unteralgebra von $(\mathbb{A}, \mathbb{K})$.

sei $[a]_i := \{x = \mathbb{A}^*(x_1, x_2) \in P(\mathbb{A}) \mid a_1x_2 - a_2x_1 \in N_i\}$. Mit

$$\mathfrak{G} := \begin{cases} \emptyset & falls \quad \mathbb{A}^* = \mathbb{A} \setminus \{0\} \\ \{[a]_1 \mid a \in P\} & falls \quad \mathbb{A}^* = \mathbb{A} \setminus N_1 \\ \{[a]_1 \mid a \in P\} \cup \{[a]_2 \mid a \in P\} & falls \quad \mathbb{A}^* = \mathbb{A} \setminus (N_1 \cup N_2) \end{cases}$$

ist nun $(\Sigma(\mathbb{K}, \mathbb{A}), \mathfrak{G}) = (P(\mathbb{A}), \mathfrak{K}, \mathfrak{G})$ eine Benz-Ebene, denn jede Ableitung $\mathcal{A}(w)$ ist eine zur affinen Koordinaten-Ebene $\mathcal{A}(\mathbb{A}, \mathbb{K})$ über $(\mathbb{A}, \mathbb{K})$ isomorphe affine Ebene (vgl. [3], Kp. II §3). Die Benz-Ebene $(\Sigma(\mathbb{K}, \mathbb{A}), \mathfrak{G})$ bezeichnen wir kurz auch mit $\Sigma(\mathbb{K}, \mathbb{A})$, da die Gitterstruktur $(P(\mathbb{A}), \mathfrak{G})$ schon durch $(P(\mathbb{A}), \mathfrak{K})$ bestimmt ist.

Satz 1.1.5 *Es seien* $(\mathbb{A}, \mathbb{K})$ *und* $(\mathbb{B}, \mathbb{L})$ *Algebren mit Rang*$(\mathbb{A}, \mathbb{K}) = 2$. *Dann ist* $\Sigma(\mathbb{K}, \mathbb{A})$ *genau dann isomorph zu* $\Sigma(\mathbb{L}, \mathbb{B})$, *wenn* $(\mathbb{A}, \mathbb{K})$ *isomorph zu* $(\mathbb{B}, \mathbb{L})$ *ist.*

Beweis. (1) Es sei $\varphi : \mathbb{A} \to \mathbb{B}$ ein Algebraisomorphismus.
Dann gilt für $x_1, x_2, y_1, y_2 \in \mathbb{A}$ mit $\langle x_1, x_2\rangle = \mathbb{A} = \langle y_1, y_2\rangle$:

$\mathbb{A}^*(x_1, x_2) = \mathbb{A}^*(y_1, y_2) \Leftrightarrow \mathbb{B}^*(\varphi(x_1), \varphi(x_2)) = \mathbb{B}^*(\varphi(y_1), \varphi(y_2))$.
Denn $\langle\varphi(x_1), \varphi(x_2)\rangle = \mathbb{B} = \langle\varphi(y_1), \varphi(y_2)\rangle$ und aus $(x_1, x_2) = a(y_1, y_2)$ mit $a \in \mathbb{A}^*$ folgt $(\varphi(x_1), \varphi(x_2)) = \varphi(a)(\varphi(y_1), \varphi(y_2))$ sowie $\varphi(a) \in \mathbb{B}^*$. Damit wird durch

$$\varphi' : \begin{cases} P(\mathbb{A}) \to P(\mathbb{B}) \\ \mathbb{A}^*(x_1, x_2) \mapsto \mathbb{B}^*(\varphi(x_1), \varphi(x_2)) \end{cases}$$

eine Bijektion definiert, und es gilt $\varphi'(P(\mathbb{K})) = P(\mathbb{L})$. Für $\mathfrak{C} \in \mathrm{GL}(2, \mathbb{A})$ gilt $\varphi'\widetilde{\mathfrak{C}}\varphi'^{-1}(\mathbb{B}^*(x_1, x_2)) = \varphi'\widetilde{\mathfrak{C}}(\mathbb{A}^*(\varphi^{-1}(x_1), \varphi^{-1}(x_2))) = \varphi'(\mathbb{A}^*(\varphi^{-1}(x_1), \varphi^{-1}(x_2))\mathfrak{C}) = \mathbb{B}^*((x_1, x_2)\varphi(\mathfrak{C}))^3 = \widetilde{\varphi(\mathfrak{C})}(\mathbb{B}^*(x_1, x_2))$, also $\varphi'\widetilde{\mathfrak{C}}\varphi'^{-1} = \widetilde{\varphi(\mathfrak{C})}$. Damit ergibt sich $\mathrm{PGL}(2, \mathbb{B}) = \varphi'\mathrm{PGL}(2, \mathbb{A})\varphi'^{-1}$.

Für $C \in \mathfrak{K}$, also $C = \widetilde{\mathfrak{C}}(P(\mathbb{K}))$ mit $\mathfrak{C} \in \mathrm{GL}(2, \mathbb{A})$ gilt $\varphi'(C) = \varphi'\widetilde{\mathfrak{C}}(P(\mathbb{K})) = \varphi'\widetilde{\mathfrak{C}}\varphi'^{-1}\varphi'(P(\mathbb{K})) = \widetilde{\varphi(\mathfrak{C})}(P(\mathbb{L})) \in \mathfrak{K}'$. Damit erhalten wir $\varphi'(\mathfrak{K}) = \mathfrak{K}'$.

[3] $\varphi((c_{ij})) := (\varphi(c_{ij}))$

(2) Es sei ψ ein Isomorphismus von $\Sigma(\mathbb{K},\mathbb{A})$ auf $\Sigma(\mathbb{L},\mathbb{B})$. Da $\mathrm{PGL}(\mathbb{B},\mathbb{L})$ regulär auf den Tripeln paarweise verbindbarer Punkte von $P(\mathbb{L})$ operiert (vgl. [3]), können wir $\psi(\mathbb{A}^*(1,0)) = \mathbb{B}^*(1,0)$, $\psi(\mathbb{A}^*(0,1)) = \mathbb{B}^*(0,1)$ und $\psi(\mathbb{A}^*(1,1)) = \mathbb{B}^*(1,1)$ annehmen. Mit $\infty := \mathbb{A}^*(1,0)$, $\infty' := \mathbb{B}^*(1,0)$ ist $\psi|_{P\infty}$ dann eine Affinität von $\mathcal{A}(\infty)$ auf $\mathcal{A}(\infty')$. Daher ist $\varphi : \mathbb{A} \to \mathbb{B}$, $x \mapsto \varphi(x)$ mit $\mathbb{B}^*(\varphi(x),1) := \psi(\mathbb{A}^*(x,1))$ eine Affinität. Wegen $\psi(\mathbb{A}^*(0,1)) = \mathbb{B}^*(0,1)$, $\psi(\mathbb{A}^*(1,1)) = \mathbb{B}^*(1,1)$ gilt weiter $\varphi(0) = 0$ und $\varphi(1) = 1$. Da $\mathcal{A}(\infty)$ isomorph ist zu der affinen Koordinatengeometrie $\mathcal{A}(\mathbb{A},\mathbb{K})$ und $dim(\mathbb{A},\mathbb{K}) = 2$, ist φ wegen $\varphi(0) = 0$ nach dem Fundamentalsatz der affinen Geometrie eine semilineare Bijektion (vgl. [16]) .

Damit ist $\varphi|_{\mathbb{K}} : \mathbb{K} \to \mathbb{L}$ ein Körperisomorphismus , und für $x \in \mathbb{A}$, $\lambda \in \mathbb{K}$ gilt $\varphi(\lambda x) = \varphi(\lambda)\varphi(x)$.

Für $\mathbb{K} = \mathbb{Z}_2$ rechnet man im Fall, dass $\mathbb{A}$ bilokal it sofort nach, dass φ ein Isomorphism ist. Im folgenden sei also $\mathbb{K} \neq \mathbb{Z}_2$, falls $\mathbb{A}$ bilokal ist.

Für $a \in \mathbb{A}^*$ ist $a^\bullet : \mathbb{A}^*(x,y) \mapsto \mathbb{A}^*(ax,y)$ eine Kreisverwandtschaft. Wegen $a \in \mathbb{A}^*$ sind $\mathbb{A}^*(0,1)$, $\mathbb{A}^*(a,1)$, ∞ paarweise verbindbar. Also sind auch $\mathbb{B}^*(0,1) = \psi(\mathbb{A}^*(0,1))$, $\mathbb{B}^*(\varphi(a),1) = \psi(\mathbb{A}^*(a,1))$ und ∞' paarweise verbindbar, folglich $\varphi(a) \in \mathbb{B}^*$. Dann ist $a^* : \mathbb{B}^*(x,y) \mapsto \mathbb{B}^*(\varphi(a)x,y)$ ein Automorphismus von $\Sigma(\mathbb{L},\mathbb{B})$. Da $\mathbb{L}$ kommutativ ist, ist die Affinität $: \mathbb{B} \to \mathbb{B}$, $x \mapsto \varphi(a)x$ linear. Daher gilt $a^* \in \mathrm{PGL}(\mathbb{B},\mathbb{L})$.

Da ψ ein Isomorphismus ist, ist $\psi a^\bullet \psi^{-1}$ ein Automorphismus von $\Sigma(\mathbb{L},\mathbb{B})$. Für $x \in \mathbb{B}$ gilt $\psi a^\bullet \psi^{-1}(\mathbb{B}^*(x,1)) = \psi a^\bullet(\mathbb{A}^*(\varphi^{-1}(x),1)) = \mathbb{B}^*(\varphi(a\varphi^{-1}(x)),1)$. Die Abbildung $\beta : \mathbb{B} \to \mathbb{B}$, $x \mapsto \varphi(a\varphi^{-1}(x))$ ist semilinear. Es sei $\lambda' \in \mathbb{L}$ und $x' \in \mathbb{B}$, dann gilt $\beta(\lambda' x') = \varphi(a\varphi^{-1}(\lambda' x')) = \varphi(a\varphi^{-1}(\lambda')\varphi^{-1}(x')) = \lambda'\varphi(a\varphi^{-1}(x')) = \lambda'\beta(x')$ und $\beta(x'+y') = \varphi(a\varphi^{-1}(x'+y')) = \varphi(a(\varphi^{-1}(x') + \varphi^{-1}(y'))) = \varphi(a(\varphi^{-1}(x'))) + \varphi(a(\varphi^{-1}(y'))) = \beta(x') + \beta(y')$. Daher gilt $\psi a^\bullet \psi^{-1} \in \mathrm{PGL}(\mathbb{B},\mathbb{L})$.

Wegen $\psi a^\bullet \psi^{-1}(\mathbb{B}^*(0,1)) = \mathbb{B}^*(0,1) = a^*(\mathbb{B}(0,1))$, $\psi a^\bullet \psi^{-1}(\mathbb{B}^*(1,1)) = \mathbb{B}^*(\varphi(a),1)$ $= a^*(\mathbb{B}^*(1,1))$ und $\psi a^\bullet \psi^{-1}(\infty') = \infty' = a^*(\infty')$ gilt damit $\psi a^\bullet \psi^{-1} = a^*$ (vgl. [3] Seite 88). Damit gilt also $\mathbb{B}^*(\varphi(a)\varphi(x),1) = a^*(\mathbb{B}^*(\varphi(x),1)) = \psi a^\bullet \psi^{-1}(\mathbb{B}^*(\varphi(x),1)) = \mathbb{B}^*(\varphi(ax),1)$, also $\varphi(ax) = \varphi(a)\varphi(x)$.

Es sei nun $a \in \mathbb{A} \setminus \mathbb{A}^*$. Dann gibt es $a_1, a_2 \in \mathbb{A}^*$ mit $a_1 + a_2 = a$, also $\varphi(ax) = \varphi((a_1 + a_2)x) = \varphi(a_1x + a_2x) = \varphi(a_1x) + \varphi(a_2x) = \varphi(a_1)\varphi(x) + \varphi(a_2)\varphi(x) = \varphi(a_1 + a_2)\varphi(x) = \varphi(a)\varphi(x)$. □

Es sei $\mathfrak{B} := (P, \mathfrak{K}, \mathfrak{G})$ eine Benz-Ebene. Wir betrachten zwei Punkte $p, q \in P$ mit $p \notin [q]$. Ein Automorphismus τ von $\mathfrak{B}$ heißt *q-Translation*, wenn $q \in$Fix τ und $\tau\,|_{P^q}$ eine Translation von $\mathcal{A}(q)$ ist. Ein Automorphismus σ heißt *(p,q)-Streckung*, wenn $p, q \in$Fix σ und $\sigma\,|_{P^q}$ eine Streckung von $\mathcal{A}(q)$ ist.

Die Menge $\Sigma_{p,q}$ aller (p,q)-Streckungen bzw. die Menge $T(q)$ aller q-Translationen bildet bzgl. der Komposition von Abbildungen offensichtlich eine Gruppe.

Es sei Γ eine Untergruppe von Aut$\mathfrak{B}$. Γ heißt *(p,q)-transitiv*, wenn $\Gamma \cap \Sigma_{p,q}$ *zirkular transitiv* operiert, d.h. wenn es einen Kreis $K \in \mathfrak{K}(p,q)$ gibt, so dass $\Gamma \cap \Sigma_{p,q}$ auf $K \setminus \{p,q\}$ transitiv operiert.

Satz 1.1.6 *Es sei $q \in P$ und* Aut$\mathfrak{B}$ *für jedes $p \in P \setminus [q]$ (p,q)-transitiv. Dann gilt:*

(1) *$\mathcal{A}(q)$ ist desarguessch.*

(2) *Die Gruppe $T(q)$ der q-Translationen operiert regulär auf $P \setminus [q]$.*

(3) *Jede Streckung σ von $\mathcal{A}(q)$ ist die Restriktion eine (p,q)-Streckung, d.h. jede Streckung von $\mathcal{A}(q)$ läßt sich zu einer Kreisverwandtschaft fortsetzen.*

(4) *Jede Translation τ von $\mathcal{A}(q)$ ist die Restriktion einer q-Translation, d.h. jede Translation von $\mathcal{A}(q)$ läßt sich zu einer Kreisverwandtschaft fortsetzen.*

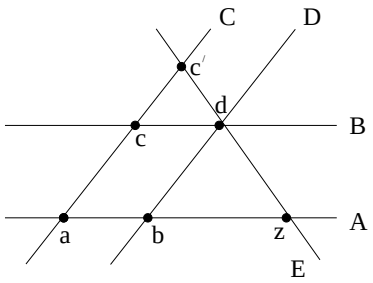
(5) *Jede q-Translation läßt sich als Produkt einer (p_1,q)-Streckung und einer (p_2,q)-Streckung mit $p_1, p_2 \in P \setminus [q]$ schreiben.*

Beweis. (1)Es seien G_1, G_2, G_3 drei verschiedene Geraden der affiner Ebene $\mathcal{A}(q)$, die sich im Punkt z schneiden und für $i \in \{1,2,3\}$ seien $a_i, b_i \in G_i \setminus \{z\}$ mit $a_i \neq b_i$, $\overline{a_1, a_2} \parallel \overline{b_1, b_2}$ und $\overline{a_2, a_3} \parallel \overline{b_2, b_3}$. Da Aut$\mathfrak{B}$ (z,q)-transitiv ist, gibt es in

$\mathcal{A}(q)$ eine Streckung σ mit $\sigma(z) = z$ und $\sigma(a_2) = b_2$. Dann gilt $\sigma(a_1) = b_1$ und $\sigma(a_3) = b_3$, folglich $\overline{a_1, a_3} \parallel \sigma(\overline{a_1, a_3}) = \overline{b_1, b_3}$. Damit ist $\mathcal{A}(q)$ desarguessch.

(2) Es seien a, b zwei verschiedene Punkte von P^q.

Wenn $b \notin [a]$, so gibt es den Kreis $A := (a, b, q)^\circ$ und einen Kreis $B \in \mathfrak{K}(q)$ mit $A \cap B = \{q\}$. Wenn $b \in [a]$, so gibt es Erzeugende $A, B \in \mathfrak{G}$ mit $a, b \in A,\ A \cap B = \emptyset,\ q \notin B$. Da die Ordnung von $\mathfrak{B}$ mindestens 3 ist, gibt es einen Punkt $c \in B$ mit $c \notin [a]$, und es existieren die Kreise $C := (a, c, q)^\circ$ und $D := \beta_q(C, b)$ (vgl. Satz 1.1.1 (4)) sowie der Punkt d mit $\{q, d\} = D \cap B$ bzw. $d = D \cap B$, wenn $B \in \mathfrak{G}$. Da die Ordnung von $\mathfrak{B}$ mindestens 3 ist, gibt es in der affinen Ableitung $\mathcal{A}(q)$ eine Gerade durch d, die von $D \setminus [q],\ B \setminus [q]$ verschieden ist, d.h. es gibt einen Kreis $E \in \mathfrak{K}(q, d)$ mit $E \neq D, B$ oder eine Erzeugende $E \in \mathfrak{G}$ mit $d \in E$ und $E \neq B$. Weiter gibt es Punkte $c', z \in E \setminus [q]$ mit $c' \in C,\ z \in A$ (Figur 2).



Figur 2

Nach Voraussetzung gibt es eine (a, q)-Streckung α mit $\alpha(c) = c'$ und eine (z, q)-Streckung β mit $\beta(c') = d$. Damit ist $\beta\alpha|_{P^q}$ eine Dilatation von $\mathcal{A}(q)$ mit $\beta\alpha(A) = A$ und $\beta\alpha(c) = d$, also $\beta\alpha(B) = B$. Wegen $A \cap B = \begin{cases} \{q\} & falls \quad b \notin [a] \\ \emptyset & falls \quad b \in [a] \end{cases}$ folgt nun, dass $\beta\alpha$ in P^q keinen Fixpunkt hat, also $\beta\alpha|_{P^q}$ eine Translation ist. Wegen $C \cap D = \{q\}$ folgt aus $\beta\alpha(c) = d$ schließlich $\beta\alpha(C) = D$ und damit $\beta\alpha(a) = b$. Damit operiert also $T(q)$ transitive auf P^q. Die Regularität folgt nun mit Satz 1.1.4 aus der Tatsache, dass es in einer affinen Ebene zu zwei Punkten x, y höchstens eine Translation τ gibt mit $\tau(x) = y$ (vgl. [1] Theorem 2.5) .

(3) Es seien σ eine Streckung von $\mathcal{A}(q)$ mit dem Fixpunkt p, $K \in \mathfrak{K}(p,q)$ und $a \in K \setminus \{p,q\}$, $a' := \sigma(a)$. Nach Voraussetzung gibt es eine (p,q)-Streckung $\sigma' : P \to P$ mit $\sigma'(a) = a'$. Da $\sigma' \mid_{P^q}$ eine Streckung von $\mathcal{A}(q)$ mit Fixpunkt p und $\sigma'(a) = a'$ ist, gilt also $\sigma = \sigma' \mid_{P^q}$ nach [1] Theorem 2.5.

(4) Der Beweis folgt aus (2) analog (3).

(5) Folgt aus dem Beweis von (2). □

Für Laguerre- und Minkowski-Ebenen definieren wir noch:

Ein Automorphismus α von $\mathfrak{B}$ heißt *axiale* Kreisverwandtschaft, wenn es zwei verschiedene Erzeugende $G, H \in \mathfrak{G}$ gibt mit $G \cup H \subseteq \mathrm{Fix}\,\alpha$; G und H heißen dann *Achsen* von α.

Offensichtlich gilt: Ist α eine axiale Kreisverwandtschaft mit den Achsen G und H, so ist für jeden Punkt $q \in (G \cup H) \setminus (G \cap H)$ die Restriktion $\alpha|_{P^q}$ eine axiale Affinität von $\mathcal{A}(q)$.

Lemma 1.1.1 *Es sei α eine axiale Kreisverwandtschaft von $\mathfrak{B}$ mit den Achsen G und H. Wenn $\alpha \neq id$, so gilt $G \cap H = \emptyset$.*

Beweis. Für Laguerre-Ebenen ist die Aussage trivial. Nun sei $\mathfrak{B}$ eine Minkowski-Ebene. Angenommen, es gibt $p \in G \cap H$. Dann gilt ohne Einschränkung $G \in \mathfrak{G}_1$ und $H \in \mathfrak{G}_2$. Da G punktweise fest bleibt, gilt $\alpha(\mathfrak{G}_1) = \mathfrak{G}_1$ und $\alpha(\mathfrak{G}_2) = \mathfrak{G}_2$ nach Satz 1.1.2 und damit $\alpha([g]_2) = [\alpha(g)]_2 = [g]_2$ für jedes $g \in G$, also $\alpha(X) = X$ für alle $X \in \mathfrak{G}_2$. Ebenso folgt $\alpha(Y) = Y$ für alle $Y \in \mathfrak{G}_1$. Für $x \in P$ erhalten wir damit $\alpha(x) = \alpha([x]_1 \cap [x]_2) = [x]_1 \cap [x]_2 = x$ im Widerspruch zu $\alpha \neq id$. □

1.2 Die Vierkreisrelation

Es sei $(P, \mathfrak{K}, \mathfrak{G})$ eine Benz-Ebene. Die klassischen Modelle der Laguerre- und Minkowski-Ebene, also die Geometrien der ebenen Schnitte eines Kegels bzw. einer ringartigen Quadrik rechtfertigen die folgende Erweiterung der Kreismenge $\mathfrak{K}$ einer Laguerre- bzw. Minkowski-Ebene (vgl. [27]).

Wir setzen dazu

$$\mathfrak{K}_u := \begin{cases} \emptyset & falls \quad |I| = 0 \\ \{G \cup H \mid G, H \in \mathfrak{G},\ G \neq H\} & falls \quad |I| = 1 \\ \{G \cup H \mid G \in \mathfrak{G}_1, H \in \mathfrak{G}_2\} & falls \quad |I| = 2 \end{cases}$$

und $\widetilde{\mathfrak{K}} := \mathfrak{K} \cup \mathfrak{K}_u$. Die Kreise in $\mathfrak{K}$ nennen wir *eigentliche* und die in $\mathfrak{K}_u$ *uneigentliche* Kreise (Figur 3).

Lemma 1.2.1 *Es seien $a, b, c \in P$ drei verschiedene Punkte mit $a \notin [b]$ oder $a \notin [c]$ oder $b \notin [c]$. Dann gibt es genau einen Kreis $K \in \widetilde{\mathfrak{K}}$ mit $a, b, c \in K$. Diesen Kreis bezeichnen wir auch mit $(a, b, c)^\circ$.*

Beweis. Da die uneigentlichen Kreise Vereinigung von zwei Erzeugenden sind, sind von drei Punkten eines uneigentlichen Kreises mindestens zwei nicht verbindbar. Wenn also a, b, c paarweise verbindbar sind, so gibt es keinen uneigentlichen Kreis der a, b, c enthält, und nach Satz 1.1.1 genau einen eigentlichen Kreis durch a, b, c.

Es sei etwa $c \in [b]_2$ und $a \notin [b]$. Dann ist $[a]_1 \cup [b]_2$ der einzige uneigentliche Kreis durch a, b, c [4] (Figur 3). □

Lemma 1.2.2 *Es sei $\mathfrak{L}$ eine Laguerre- und $\mathfrak{M}$ eine Minkowski-Ebene.*

(1) *Für je zwei uneigentliche Kreise X, Y von $\mathfrak{L}$ gilt $X \cap Y = \emptyset$ oder $X \cap Y$ ist eine Erzeugende.*

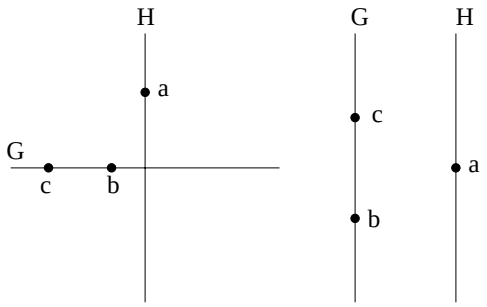
(2) *Für je zwei uneigentliche Kreise X, Y von $\mathfrak{M}$ gilt $|X \cap Y| = 2$ oder $X \cap Y$ ist eine Erzeugende.*

(3) *Für je zwei Kreise X, Y von $\mathfrak{L}$ mit $X \cap Y = \{q\}$ gilt $X, Y \in \mathfrak{K}$.*

(4) *Für je zwei Kreise X, Y von $\mathfrak{M}$ mit $X \cap Y = \{q\}$ gilt $X \in \mathfrak{K}$ oder $Y \in \mathfrak{K}$ und falls X bzw. Y uneigentlich ist, so gilt $X = [q]$ bzw. $Y = [q]$.*

[4] Man beachte die auf Seite 10 vereinbarte Bedeutung von $[b]_2$ für Laguerre-Ebenen

Beweis. Mit Satz 1.1.1 folgen (1) und (2) sofort aus der Definition von $\mathfrak{K}_u$, (3) aus (1) und (4) aus (2). □



Figur 3

Wir erweitern jetzt noch den Begriff des Berührens (vgl. [26] Seite 342).

Zwei Kreise $K, K' \in \widetilde{\mathfrak{K}}$ *berühren sich im Punkt* $p \in K \cap K'$, wenn $|K \cap K'| = \{p\}$ oder $|K \cap K'| > 2$.

Zwei uneigentliche Kreise berühren sich also genau dann, wenn sie eine Erzeugende gemeinsam haben.

Im Fall einer Laguerre-Ebene berührt kein eigentlicher Kreis einen uneigentlichen Kreis (vgl. Lemma 1.2.2).

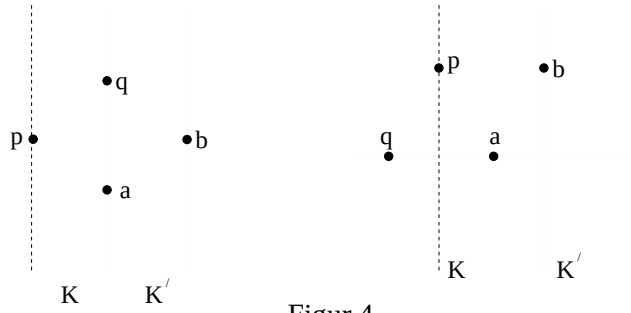
Im Fall einer Minkowski-Ebene berührt ein eigentlicher Kreis K einen uneigentlichen Kreis K' genau dann in a, wenn $K' = [a]$ gilt (vgl. Lemma 1.2.2).

Es seien $K := [p]_1 \cup [q]_2$ und $a \in K, K \neq [a]$ sowie $b \in P \setminus K$. Dann gibt es einen uneigentlichen Kreis K' durch b, der K in a berührt, nämlich

$$K' := \begin{cases} ([b]_1 \cup [a]_2) & falls \quad a \in [q]_2 \\ ([a]_1 \cup [b]_2) & falls \quad a \in [p]_1 \end{cases}$$

(Bezeichnung $K' := \beta_b(K, a)$)(Figur 4).

Zur Bezeichnung des zweiten Schnittpunktes b zweier verschiedener Kreise $X, Y \in \widetilde{\mathfrak{K}}$ durch den Punkt a mit $X \cap Y = \{a, b\}$ definieren wir $X \cap_a Y := \begin{cases} b & falls \quad a \neq b \\ a & falls \quad a = b \end{cases}$



Figur 4

Für $M \subseteq P$ setzen wir $\widetilde{\mathfrak{K}}(M) := \{K \in \widetilde{\mathfrak{K}} \mid M \subseteq K\}$.

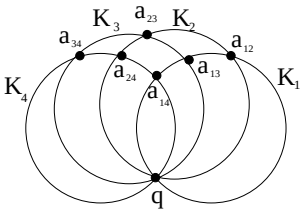
Eine Teilmenge M von Punkten heißt *konzyklisch*, wenn $\widetilde{\mathfrak{K}}(M) \neq \emptyset$ ist.

Mit den obigen Vereinbarungen definieren wir die *Vierkreisrelation* $V \subseteq P^{<6>} := \{(a_1, ..., a_6) \in P^6 \mid |\{a_1, ..., a_6\}| \geqq 5\}$ durch die Festsetzung (vgl. [21] für den Fall einer Möbius-Ebene):

Es sei $(a_{12}, a_{34}, a_{13}, a_{24}, a_{14}, a_{23}) \in V$ genau dann, wenn es vier verschiedene Kreise $K_1, K_2, K_3, K_4 \in \widetilde{\mathfrak{K}}$ und einen Punkt $q \in P$ gibt, so dass gilt (Figur 5):

(1) $| K_1 \cap K_4 | \leq 2, \ | K_2 \cap K_3 | \leq 2.$

(2) Für $1 \leq i < j \leq 4$ gilt: $K_i \cap K_j = \{a_{ij}, q\}$ oder K_i berührt K_j in q und a_{ij}.



Figur 5

Mit Hilfe der Vierkreisrelation werden wir in §1.4 die Drehstreckungen definieren. Dazu benötigen wir die in dem folgenden Lemma enthaltenen Eigenschaften der Vierkreisrelation.

Lemma 1.2.3 *Es seien* $(a, a', b, b', c, c') \in V$, *und* K_1, K_2, K_3, K_4 *die in der Definition vorkommenden vier Kreise.*

(1) *Es gilt* $(b,b',a,a',c,c') \in V$ *und wenn* $|K_1 \cap K_3| \leq 2$, $|K_4 \cap K_2| \leq 2$ *auch* $(a,a',c,c',b,b') \in V$.

(2) *Es gilt* $(a',a,b',b,c,c') \in V$, $(a',a,b,b',c',c) \in V$ *und* $(a,a',b',b,c',c) \in V$.

(3) *Für* $\kappa \in \mathrm{Aut}(P,\mathfrak{K},\mathfrak{G})$ *gilt* $(\kappa(a),\kappa(a'),\kappa(b),\kappa(b'),\kappa(c),\kappa(c')) \in V$.

Beweis. (1) , (2) ergeben sich sofort aus der Definition von V, da hier nur die Numerierung der Kreise K_i geändert wird, wobei die Bedingung über die Größe der Schnitte erhalten bleibt bzw. im zweiten Teil von (1) durch die zusätzliche Voraussetzung gesichert ist. Auch (3) ergibt sich sofort aus der Definition von V; hier sind natürlich $\kappa(K_i)$ die benötigten Kreise. □

Bemerkung. Die Voraussetzung $|K_i \cap K_j| \leq 2$ in Lemma 1.2.3(1) ist erfüllt, wenn einer der beiden Kreise K_i, K_j eigentlich ist.

Lemma 1.2.4 *Es seien* $(a,a',b,b',c,c') \in V$ *und* K_1, K_2, K_3, K_4 *die in der Definition vorkommenden vier Kreise und* q *der gemeinsamen Schnittpunkt.*

(1) *Es gilt* $a,a' \neq b,b'$. *Wenn auch* $|K_1 \cap K_3| \leq 2$, $|K_4 \cap K_2| \leq 2$ *gilt, so gilt darüberhinaus auch* $a,a',b,b' \neq c,c'$.

(2) $\bigcap_{i=1}^{4} K_i = \{q\}$.

(3) *Wenn* a,b,c *bzw.* a,b',c' *bzw.* a',b,c' *bzw.* a',b',c *nicht auf einer Erzeugenden liegen, dann gilt* $K_1 = (a,b,c)^\circ$ *bzw.* $K_2 = (a,b',c')^\circ$ *bzw.* $K_3 = (a',b,c')^\circ$ *bzw.* $K_4 = (a',b',c)^\circ$ *und* $q = K_1 \cap_c K_4$ *sowie* $c' = K_2 \cap_q K_3$.

(4) *Wenn* a',b',c *verschieden sind und paarweise verbindbar, so sind mit* a,a',b',c *konzyklisch auch* a,a',b,c' *konzyklisch.*

Beweis. (1) Angenommen, $a = b$. Dann gilt $a \neq c', c$ weil $|\{a,a',b,b',c,c'\}| \geq 5$. Aus $a,q \in K_1 \cap K_2$ und $b,q \in K_1 \cap K_3$ folgt $\{a = b, q\} \subset K_2 \cap K_3 = \{c',q\}$. Wäre $q = c'$, dann wäre $K_2 \cap K_3 = \{c'\}$ im Widerspruch zu $a = b \in K_2 \cap K_3$ und $a \neq c'$. Damit folgt $q = a = b \neq c'$, also $K_1 \cap K_2 = \{q\}$ und $K_1 \cap K_3 = \{q\}$.

Wäre K_1 uneigentlich, so wäre $K_1 = [q]$ nach Lemma 1.2.2 und damit $K_1 \cap K_4$ eine Erzeugende (weil $c, q \in K_1 \cap K_4$) im Widerspruch zu $|K_1 \cap K_4| \leq 2$. Folglich ist K_1 eigentlich. Wäre K_2 bzw. K_3 uneigentlich, so wäre $K_2 = [q]$ bzw. $K_3 = [q]$ nach Lemma 1.2.2. Da $K_2 \neq K_3$ ist, folgt daraus $\{c', q\} = K_2 \cap K_3 = \{q\}$, ein Widerspruch; also sind K_2 und K_3 eigentlich. Aus $K_1 \cap K_2 = \{q\}$, $K_1 \cap K_3 = \{q\}$ und $K_1, K_2, K_3 \in \mathfrak{K}$ folgt nun $K_2 \cap K_3 = \{q\}$, d.h. $q = c'$ ein Widerspruch zu $q \neq c'$. Damit gilt $a \neq b$

Wegen Lemma 1.2.3(2) folgt nun weiterhin $a' \neq b',\ a' \neq b,\ a \neq b'$.

Wenn auch $|K_1 \cap K_3| \leq 2,\ |K_4 \cap K_2| \leq 2$ gilt, so gilt wegen Lemma 1.2.3 auch $a, a', b, b' \neq c, c'$.

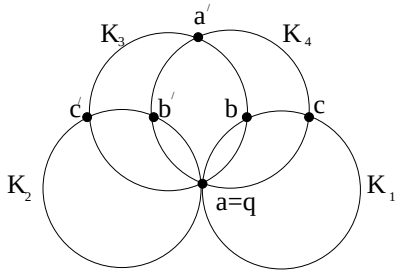
(2) Es gilt $K_1 \cap K_4 = \{c, q\}$, $K_2 \cap K_3 = \{c', q\}$.

Falls $c \neq c'$, gilt $\{q\} = \bigcap_{i=1}^{4} K_i$.

Falls $c = c'$, so gilt $\{c', a', q\} \subseteq K_3 \cap K_4$ und $c' \neq a'$ weil $|\{a, a', b, b', c, c'\}| \geq 5$. Da $K_2 \cap K_3 = \{c', q\}$, liegen c', q nicht auf einer Erzeugenden. Wären c', a', q verschieden, so wäre also $K_3 = K_4$ nach Lemma 1.2.1. Damit gilt $c' = q$ oder $a' = q$. Wäre $q = a'$, so wäre $a', b', c' \in K_2 \cap K_4$, und damit $K_2 = K_4$, da q, c' nicht auf einer Erzeugenden liegen. Damit haben wir $q = c'$ und damit $\{q\} = K_1 \cap K_4 \cap K_2 \cap K_3 = \bigcap_{i=1}^{4} K_i$.

(3) Folgt nach Definition der Vierkreisrelation und Lemma 1.2.1.

(4) Es gilt $a \in K_4 = (a', b', c)^\circ \in \mathfrak{K}$, also $a = q$ (weil $a \in K_2 \cap K_4 = \{b', q\}, a \neq b'$) und damit $a \in K_3$, d.h. a, a', b, c' sind konzyklisch (Figur 6). □



Figur 6

Satz 1.2.1 *Es seien $a, a', b, b', c \in P$ mit $a', b, b', c \notin [a],\ b', c \notin [a'],\ c \notin [b']$ und*

$b \neq a', c$. *Wenn* a, a', b, b', c *nicht konzyklisch sind, dann gibt es genau einen Punkt* $c' \in P \setminus \{b, b'\}$ *mit* $(a, a', b, b', c, c') \in V$ (Figur 5).

Beweis. Die Konstruktion von c' erfolgt nach Lemma 1.2.4(3).

Aus den Voraussetzungen folgt:

Die Kreise $K_1 := (a, b, c)^\circ$ und $K_4 := (a', b', c)^\circ$ sind nach Lemma 1.2.1 eindeutig bestimmt und nach Satz 1.1.1(3) gilt $K_4 \in \mathfrak{K}$. Da a, a', b, b', c nicht konzyklisch sind, gilt daher $|K_1 \cap K_4| \leq 2$ nach Satz 1.1.1(2),(3). Damit ist $q := K_1 \cap_c K_4$ eindeutig bestimmt.

$(*)$ Wenn $b = b'$ ist, so gilt $q = b = b' \neq c$ und $K_1 \in \mathfrak{K}$.

Denn $c \notin [b'] = [b]$, also $K_1 = (a, b, c)^\circ \in \mathfrak{K}$ und $c \neq b = b'$, folglich $q = b = b'$ wegen $b = b' \in K_1 \cap K_4 = \{c, q\}$, und es gilt $q = b \neq c$.

1. Fall: $a \notin K_4$ (also $a \neq q$) und $b = b'$.

Dann gilt $q = b = b' \neq c$ und $K_1 \in \mathfrak{K}$ nach $(*)$. Da $a, a', b = b', c$ nicht konzyklisch sind, gilt $a' \notin K_1$.

Für den zu konstruirenden Kreis K_2 muß daher $K_2 \cap K_1 = \{a, q\}$ und $K_2 \cap K_4 = \{q\}$ gelten, d.h. wegen $q = b = b' \notin [a]$ ist $K_2 = \beta_q(K_4, a)$ eindeutig bestimmt und $K_2 \in \mathfrak{K}$ sowie $K_2 \neq K_4, K_1$.

Für den zu konstruirenden Kreis K_3 muß $K_3 \cap K_1 = \{q\}$ und $K_3 \cap K_4 = \{a', q\}$ gelten, d.h. wegen $q = b = b' \notin [a']$ ist $K_3 = \beta_q(K_1, a')$ eindeutig bestimmt und $K_3 \in \mathfrak{K}$ sowie $K_3 \neq K_4, K_1$.

Wegen $K_3 \cap K_1 = \{q\}, K_2 \cap K_1 = \{a, q\}$ und $a \neq b = q$ gilt $K_2 \neq K_3$, also $|K_2 \cap K_3| \leq 2$ wegen $K_2, K_3 \in \mathfrak{K}$. Es sei $c' := K_2 \cap_q K_3$. Es gilt $c \neq c'$, denn wegen $c \neq q$ (vgl. $(*)$) wäre sonst $K_4 = (q, a', c)^\circ = (q, a', c')^\circ = K_3$. Weiter gilt $c' \neq a$, da sonst wäre $a \in K_3 \cap K_1 = \{q\}$ im Widerspruch zu $a \neq b = q$. Ebenso gilt $c' \neq a'$ wegen $K_2 \cap K_4 = \{q\}$. Schließlich gilt $c' \neq b = q = b'$, denn sonst wäre $K_3 \cap K_2 = \{q\}$, also $\{q\} = K_1 \cap K_4 = \{q, c\}$ im Widerspruch zu $q \neq c$ (vgl.

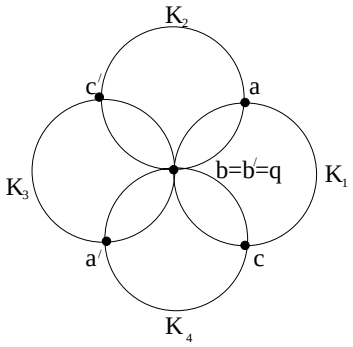
$(*)$). Damit gilt $|\{a, a', b = b', c, c'\}| = 5$. Folglich gilt $(a, a', b, b', c, c') \in V$, sowie $c' \neq b, b'$.

2. Fall: $a \notin K_4$ (also $a \neq q$) und $b \neq b'$.

Dann gilt $|\{a, a', b, b', c\}| = 5$. Es muß gelten $a, b', q \in K_2$ und $a', b, q \in K_3$. Wegen $b' \notin [a]$ und $a \neq q$ ist für $b' \neq q$ nach Lemma 1.2.1 K_2 eindeutig durch $K_2 = (q, a, b')^\circ$ bestimmt.

Für $b' = q$ folgt wegen $K_4 \in \mathfrak{K}$ und aus der Forderung $K_2 \cap K_4 = \{q\}$, dass $K_2 = \beta_q(K_4, a)$ gelten muß. Wegen $q = b' \notin [a]$ existiert $\beta_q(K_4, a) \in \mathfrak{K}$. Also ist

$$K_2 = \begin{cases} (a, b', q)^\circ & falls \quad q \neq b' \\ \beta_q(K_4, a) & falls \quad q = b' \text{ (Figur 7)} \end{cases}$$ eindeutig bestimmt.



Figur 7

Es sei zunächst $b' = q$. Dann gilt $b \neq q, a'$ und $q = b' \notin [a]$. Also ist $K_3 = (a', b, q)^\circ$ nach Lemma 1.2.1 eindeutig bestimmt. Wegen $K_2 \cap K_4 = \{q\}$, $a' \in K_3 \cap K_4$ und $a' \neq q$ gilt $K_2 \neq K_3$, wegen $K_2 \in \mathfrak{K}$ also $|K_2 \cap K_3| \leq 2$. Für $c' := K_2 \cap_q K_3$ gilt damit $(a, a', b, b', c, c') \in V$ wegen $|\{a, a', b, b', c\}| = 5$.

Jetzt sei $b' \neq q$, also $K_2 = (a, b', q)^\circ$.

Falls $b = q$ ist, gilt $b \in K_4 \in \mathfrak{K}$. Wegen $c \in K_4$, $c \neq b$ gilt also $c \notin [b]$. Da $b, c \notin [a]$ folgt also $K_1 \in \mathfrak{K}$. Daher muß für K_3 gelten $|K_3 \cap K_1| \leq 2$, also $K_3 \cap K_1 = \{b, q\} = \{q\}$, d.h. $K_3 = \beta_q(K_1, a')$ wegen $a' \in K_3$.

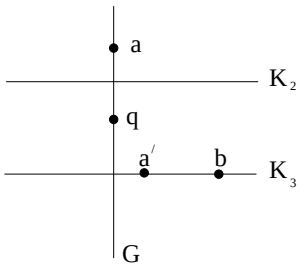
Wegen $a' \neq b = q$ und $a', q \in K_4$ ist $a' \notin [q]$. Daher existiert K_3 und $K_3 \in \mathfrak{K}$. Aus $K_3 \cap K_1 = \{q\}$ und $q \neq a \in K_1 \cap K_2$ folgt $K_2 \neq K_3$ und somit $|K_3 \cap K_2| \leq 2$,

da $K_3 \in \mathfrak{K}$. Für $c' := K_2 \cap_q K_3$ gilt (wegen $b \neq b'$) also $(a, a', b, b', c, c') \in V$ und $c' \neq b, b'$ nach Lemma 1.2.4(1).

Falls $b \neq q$ und $a' = q$ ist, gilt $K_1 = (a, c, a')^\circ$, also $K_1 \in \mathfrak{K}$, da $c, a' \notin [a]$ und $c \notin [a']$ ist. Wegen $K_4 \in \mathfrak{K}$ muß $|K_3 \cap K_4| \leq 2$ gelten, also $K_3 \cap K_4 = \{a', q\} = \{q\}$, d.h. $K_3 = \beta_q(K_4, b)$ wegen $b \in K_3$. Wegen $b, q \in K_1 \in \mathfrak{K}$ und $b \neq a' = q$ existiert K_3, und es gilt $K_3 \in \mathfrak{K}$. Wegen $b' \in K_2 \cap K_4$, $K_3 \cap K_4 = \{q\} = \{a'\}$ und $a' \neq b'$ gilt $K_2 \neq K_3$ und somit $|K_2 \cap K_3| \leq 2$ (weil $K_3 \in \mathfrak{K}$). Für $c' := K_2 \cap_q K_3$ gilt wieder $(a, a', b, b', c, c') \in V$ sowie $c' \neq b, b'$ nach Lemma 1.2.4(1).

Falls $b, a' \neq q$, ist $a' \notin [q]$ wegen $a', q \in K_4 \in \mathfrak{K}$, und wegen $b \neq a'$ ist damit K_3 nach Lemma 1.2.1 eindeutig durch $K_3 = (a', b, q)^\circ$ bestimmt. Weiterhin gilt $K_1 = (a, b, q)^\circ$ und $K_4 = (a', b', q)^\circ$. Da K_2 die Punkte b, a', q enthalten muß und $a' \notin [q]$, ist K_2 eindeutig durch $K_2 = (a', b, q)^\circ$ bestimmt. Wegen $K_1 \neq K_4$ ist auch $K_3 \neq K_2$.

Es gilt $|K_2 \cap K_3| \leq 2$. Denn aus der Annahme $|K_2 \cap K_3| \geq 3$ folgt nach Lemma 1.2.2, dass $K_2 \cap K_3$ eine Erzeugende durch q ist, etwa $K_2 \cap K_3 = [q]_1$ (Figur 8) und $K_2, K_3 \notin \mathfrak{K}$. Da $K_4 \in \mathfrak{K}$ ist, gilt $K_4 \cap [q]_1 = \{q\}$ woraus wegen $q \neq a', b'$ und $a', b' \in K_4$ sofort $K_2 = [q]_1 \cup [b']_2$ und $K_3 = [q]_1 \cup [a']_2$ folgt (im Fall der Laguerre-Ebene sei $[x]_2 := [x]_1 = [x]$) mit $[a']_2 \neq [b']_2$. Wegen $a \in K_2$ und $b' \notin [a]$ gilt $a \in [q]_1$; wegen $b \in K_3$ und $b \notin [a]$ gilt $b \notin [q]_1$, also $b \in [a']$ und somit $K_1 = [q]_1 \cup [a']_2$ also $\{c, q\} = K_1 \cap K_4 = \{a', q\}$ im Widerspruch zu $c \neq a'$.



Figur 8

Damit ist $c' := K_2 \cap_q K_3$ eindeutig bestimmt, und es gilt $(a, a', b, b', c, c') \in V$.

Wenn K_1 uneigentlich ist, so gilt $c \in [b]$ und wegen $K_4 \in \mathfrak{K}$, also $q \notin [c]$, folgt $q \in [a] \setminus [b]$, folglich $K_3 \cap K_1 = \{q, b\}$. Damit gilt also stets $|K_3 \cap K_1| \leq 2$. Es gilt $K_4 \neq K_2$ da $a \in K_2$ und $a \notin K_4$. Da $K_4 \in \mathfrak{K}$ ist, gilt $|K_4 \cap K_2| \leq 2$ folglich $c' \neq b, b'$ nach Lemma 1.2.4(1).

4. Fall: $a \in K_4$.

Da $a \in K_1 \cap K_4 = \{c, q\}$ und $c \neq a$ ist, gilt $a = q$.

Es gilt $K_1 \neq [q]$. Denn sonst wäre $b \in K_1 = [q] = [a]$. Weiter gilt $b' \notin K_1$, denn sonst wäre $b' \in K_1 \cap K_4 = \{c, a\}$ im Widerspruch zu $c \notin [b'], b' \neq c$. Da der Kreis K_2 den Kreis K_1 in $a = q$ berühren muß, ist der Kreis K_2 also wegen $b' \in K_2$ durch $K_2 = \beta_q(K_1, b')$ eindeutig festgelegt.

Durch die Forderungen $b \in K_3$ und $K_3 \cap K_4 = \{a', q\} = \{a', a\}$, ist der Kreis K_3 wegen $a', b \notin [a]$ und $b \neq a'$ nach Lemma 1.2.1 durch $K_3 = (a', a, b)^\circ$ eindeutig bestimmt (Figur9). Aus $K_1 \cap K_2 = \{a\}$, $b \in K_1 \cap K_3$ und $a \neq b$ folgt $K_2 \neq K_3$.

Aus $b' \notin K_1$ folgt $K_2 \neq K_1$. Wegen $c \notin [a]$ gilt $|K_1 \cap K_4| = 2$, also $K_2 \neq K_4$. Weiter gilt $K_3 \neq K_1$, denn sonst wäre $a' \in K_1 \cap K_4 = \{c, a\}$, also $a' = c$ oder $a' = a$ im Widerspruch zu $c \notin [a']$ bzw. $a' \notin [a]$. Da a, a', b, b', c nicht konzyklisch sind, gilt $K_3 \neq K_4$.

Wenn $b \notin [c]$, so gilt $K_1 \in \mathfrak{K}$, folglich $K_2 \in \mathfrak{K}$, also $\mid K_2 \cap K_3 \mid \leq 2$.

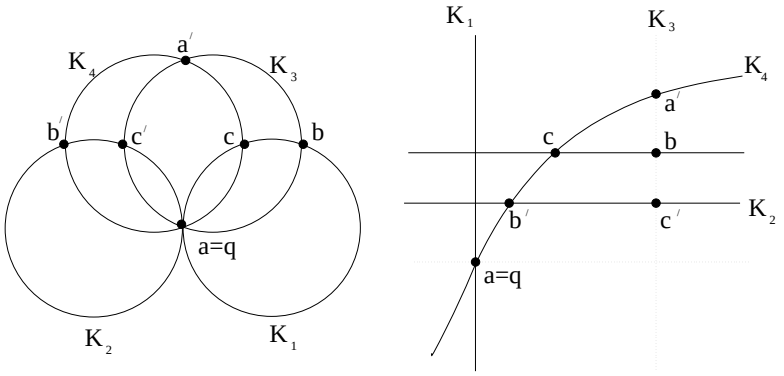
Wenn $b \in [c]$, etwa $b \in [c]_2$, so gilt $K_1 = (a, b, c)^\circ = [a]_1 \cup [b]_2$, $K_2 = [a]_1 \cup [b']_2 \in \mathfrak{K}_u$.

Wenn auch $K_3 \in \mathfrak{K}_u$[5], also $b \in [a']$, so gilt $a' \in [b]_1$, denn sonst wäre $c, a' \in [b]_2$ im Widerspruch zu $c \notin [a']$, und damit gilt $K_3 = [a']_1 \cup [a]_2$, also $\mid K_2 \cap K_3 \mid \leq 2$, da $b' \notin [a]_2$ (Figur 9).

Für $c' := K_2 \cap_a K_3$ gilt also wieder $(a, a', b, b', c, c') \in V$.

Wäre $c' = b'$, so wäre $K_4 = (a', b', q)^\circ = (a', b', a)^\circ = (a', c', q)^\circ = K_3$, wegen $a \in K_4 \setminus ([a'] \cup [b'])$. Wäre $c' = b$, so wäre $a = q, b = c' \in K_1 \cap K_2$ im Widerspruch zu $a \neq b$ und $K_1 \cap K_2 = \{a\}$. □

[5]Das kann nur im Fall einer Minkowski-Ebene auftreten.



Figur 9

Korollar 1.2.1 *Es seien $E \in \mathfrak{K}$ und $0, \infty, u \in E$ verschieden sowie $u^* \in P$ mit $u^* \notin E \cup [0] \cup [\infty] \cup [u]$.*

(1) *Zu jedem $x \in P^\infty = P \setminus [\infty]$ mit $x \neq 0, u$ gibt es genau ein $x^* \in P \setminus \{x, u^*\}$ mit $(\infty, 0, x, u^*, u, x^*) \in V$.*

(2) *Zu jedem $x \in P^0 = P \setminus [0]$ mit $x \neq \infty, u$ gibt es genau ein ${}^*x \in P \setminus \{x, u^*\}$ mit $(0, \infty, x, u^*, u, {}^*x) \in V$.*

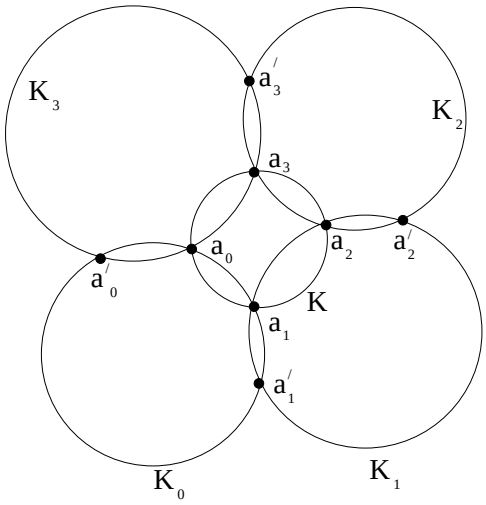
Beweis. $(a, a', b, b', c) := (\infty, 0, x, u^*, u)$ bzw. $(a, a', b, b', c) := (0, \infty, x, u^*, u)$ erfüllt die Voraussetzung von Satz 1.2.1, somit existiert genau ein $c' = x^*$ bzw. $c' = {}^*x$ mit $(\infty, 0, x, u^*, u, x^*) \in V$ bzw. $(0, \infty, x, u^*, u, {}^*x) \in V$. □

1.3 Das Axiom von Miquel

Wie beim Studium von affinen und projektiven Ebenen spielen auch bei der Untersuchung von Benz-Ebenen Schließungssätze als Axiome eine wichtige Rolle. Die Rolle des Satzes von Pappus übernimmt hier der Satz von Miquel. Um den Satz von Miquel, den wir als Axiom benützen werden, zu formulieren, führen wir den Begriff der Miquel-Konfiguration ein.

Es sei $M = \{a_0, a_1, a_2, a_3, a_0', a_1', a_2', a_3'\} \subseteq P$ mit $\mid M \mid \geq 6$.

Wir nennen $(a_0, a_1, a_2, a_3, a_0', a_1', a_2', a_3')$ eine *Miquel-Konfiguration*, wenn es Kreise $K_0, K_1, K_2, K_3, K \in \mathfrak{K}$ gibt mit $K_i \cap K = \{a_i, a_{i+1}\}$, $K_i \cap K_{i+1} = \{a_{i+1}, a_{i+1}'\}$, wobei die Indizes modulo 4 genommen werden (Figur 10).



Figur 10

Lemma 1.3.1 *Es sei $(a_0, a_1, a_2, a_3, a'_0, a'_1, a'_2, a'_3)$ eine Miquel-Konfiguration und K_0, K_1, K_2, K_3, K die in der Definition vorkommenden Kreise.*

(1) *Die Kreise K_0, K_1, K_2, K_3, K sind verschieden.*

(2) *Es gilt stets $a_i \neq a_{i+2}$ und $a'_i \neq a'_{i+2}$ sowie $a_i \neq a'_{i+1}$, $a_i \neq a'_{i+2}$ und $a_i \neq a'_{i+3}$.*

(3) *Die Kreise K_0, K_1, K_2, K_3, K sind eindeutig bestimmt.*

(4) *Falls $a_{i+1} = a'_{i+1}$, so ist $K_i = \beta_{a_{i+1}}(K_{i+1}, a_i)$ der Kreis durch a_i der K_{i+1} in a_{i+1} berührt.*

(5) *Falls $a_i = a_{i+1}$, so berührt K_i den Kreis K in a_i.*

Beweis. Es sei $M := \{a_0, a_1, a_2, a_3, a'_0, a'_1, a'_2, a'_3\}$.

(1),(2) Wegen $|K \cap K_i| \leq 2$ gilt $K \neq K_i$ für $i = 0, 1, 2, 3$. Wegen $|K_i \cap K_{i+1}| \leq 2$ gilt ebenfalls $K_i \neq K_{i+1}$ für $i = 0, 1, 2, 3$.

(a) Es gilt $a_i \neq a_{i+2}$ und $a'_i \neq a'_{i+2}$.

Annahme $a_i = a_{i+2}$. Dann gilt $a_i = a_{i+2}, a_{i+1}, a'_{i+1} \in K_i \cap K_{i+1}$ und $a_i = a_{i+2}, a_{i+3}, a'_{i+3} \in K_i \cap K_{i+3}$. Wegen $|M| \geq 6$ sind $a_i = a_{i+2}, a_{i+1}, a'_{i+1}$ oder $a_i = a_{i+2}, a_{i+3}, a'_{i+3}$ drei verschiedene Punkte, also gilt $K_i = K_{i+1}$ oder $K_i = K_{i+3}$ im Widerspruch zu $K_i \neq K_j$ für $i \neq j$.

Ebenso führt die Annahme $a_i' = a_{i+2}'$ zum Widerspruch $K_i = K_{i+1}$ oder $K_i = K_{i+3}$.

(b) Wäre $a_i = a_{i+1}'$, so wäre $a_i = a_{i+1}' \in K_{i+1} \cap K = \{a_{i+1}, a_{i+2}\}$, also $a_{i+1}' = a_i = a_{i+1}$ wegen $a_i \neq a_{i+2}$ (vgl. (a)), also $K_i \cap K = \{a_{i+1} = a_i = a_{i+1}'\} = K_{i+1} \cap K_i$, folglich $K = \beta_{a_i}(K_i, a_{i+2}) = K_{i+1}$ nach Satz 1.1.1(4) im Widerspruch zu $K \neq K_{i+1}$.

(c) Wäre $a_i = a_{i+2}'$, so wäre $a_{i+2}' = a_i \in K_{i+2} \cap K = \{a_{i+2}, a_{i+3}\}$, also $a_{i+2}' = a_i = a_{i+3}$ wegen (a), damit wäre $a_{i+1} \neq a_{i+2}$ wegen $|M| \geq 6$. Weiter gilt $a_{i+1} \neq a_{i+2}' = a_i$ wegen (b) und $a_i \neq a_{i+2}$ wegen (a), also $K = (a_{i+2}' = a_i, a_{i+1}, a_{i+2})^\circ = K_{i+1}$ im Widerspruch zu $K \neq K_{i+1}$.

(d) Wäre $a_i = a_{i+3}'$, so wäre $a_i = a_{i+3}' \in K_{i+2} \cap K = \{a_{i+2}, a_{i+3}\}$, also $a_{i+3}' = a_i = a_{i+3}$ wegen (a), folglich wäre $K_{i+3} \cap K = \{a_{i+3} = a_i = a_{i+3}'\} = K_{i+2} \cap K_{i+3} = \{a_{i+3}'\}$ und $a_{i+2} \neq a_{i+3}'$ wegen $|M| \geq 6$, folglich $K = \beta_{a_{i+3}'}(K_{i+3}, a_{i+2}) = K_{i+2}$ nach Satz 1.1.1(4) im Widerspruch zu $K_{i+2} \neq K$.

Mit (a), (b), (c), (d) ist (2) bewiesen.

Es ist noch $K_i \neq K_{i+2}$ zu zeigen. Wäre $K_i = K_{i+2}$, so wäre $\{a_i, a_{i+1}\} = K \cap K_i = K \cap K_{i+2} = \{a_{i+2}, a_{i+3}\}$ und damit $a_i = a_{i+2}$ und $a_{i+1} = a_{i+3}$ oder $a_i = a_{i+3}$ und $a_{i+1} = a_{i+2}$, also $a_i = a_{i+3}$ und $a_{i+1} = a_{i+2}$ wegen (a).

Wegen $\{a_{i+1}, a_{i+1}'\} = K_i \cap K_{i+1} = K_{i+1} \cap K_{i+2} = \{a_{i+2}, a_{i+2}'\}$, wäre damit $a_{i+1}' = a_{i+2}'$ im Widerspruch zu $|M| \geq 6$.

(3) Es gilt nach Definition $A := \{a_0, a_1, a_2, a_3\} \subseteq K$ und $A_i := \{a_i, a_i', a_{i+1}, a_{i+1}'\} \subseteq K_i$. Wenn $|A| \geq 3$ bzw. $|A_i| \geq 3$, so gilt $\mathfrak{K}(A) = \{K\}$ bzw. $\mathfrak{K}(A_i) = \{K_i\}$. Wegen $|M| \geq 6$ gilt $|A|,\ |A_i| \geq 2$.

1. Fall $|A_i| = 2$. Ohne Beschränkung der Allgemeinheit können wir $i = 0$ annehmen. Nach (2) gilt $a_0 \neq a_1'$ und $a_0' \neq a_1$.

Wir haben daher nur die zwei Fälle zu unterscheiden:

a) Falls $a_0 = a_1,\ a_0' = a_1'$, so sind $a_0, a_2, a_3, a_0', a_2', a_3'$ verschieden und damit $|A|,\ |A_1|,\ |A_2|,\ |A_3| \geq 3$, also K_1, K_2, K_3, K eindeutig bestimmt. Wegen $K \cap K_0 =$

$\{a_0\}$, ist $K_0 = \beta_{a_0}(K, a_1')$ als Berührkreis eindeutig bestimmt.

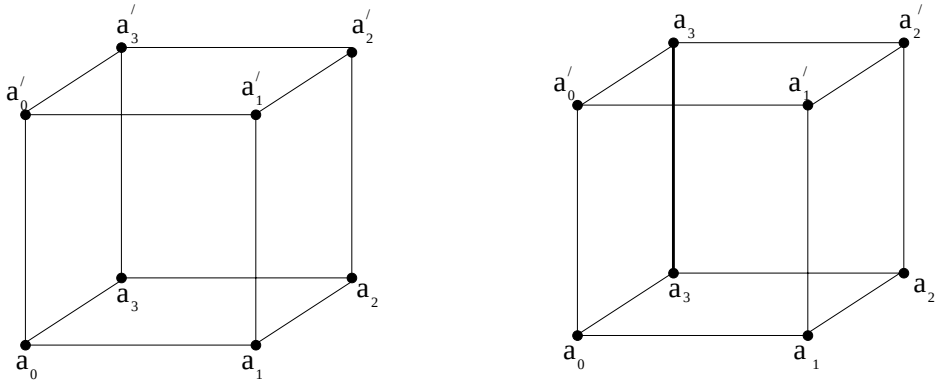
b) Falls $a_0 = a_0'$, $a_1 = a_1'$, so sind $a_0, a_1, a_2, a_3, a_2', a_3'$ verschieden und damit $|A| = 4$, $|A_1| = 3$, $|A_2| = 4$, $|A_3| = 3$, also K_1, K_2, K_3, K eindeutig bestimmt. Wegen $K_0 \cap K_3 = \{a_0\}$ ist $K_0 = \beta_{a_0}(K_3, a_1)$ als Berührkreis eindeutig bestimmt.

2. Fall $|A| = 2$. Nach (2) gilt $a_0 \neq a_2$ und $a_1 \neq a_3$.

Wir haben jetzt wieder zwei Fälle zu unterscheiden, nämlich $a_0 = a_1$, $a_2 = a_3$ sowie $a_0 = a_3$, $a_1 = a_2$. In beiden Fällen sind $a_0, a_2, a_0', a_1', a_2', a_3'$ verschieden, und es gilt $|A_i| \geq 3$, d.h die vier Kreise K_i $(i = 0, 1, 2, 3)$ sind eindeutig bestimmt. Wegen $K \cap K_0 = \{a_0\}$ bzw. $K \cap K_1 = \{a_1\}$ ist K als Berührkreis $K = \beta_{a_0}(K_0, a_2)$ bzw. $K = \beta_{a_1}(K_1, a_0)$ eindeutig bestimmt.

(4), (5) folgen sofort aus dem Beweis von (3). □

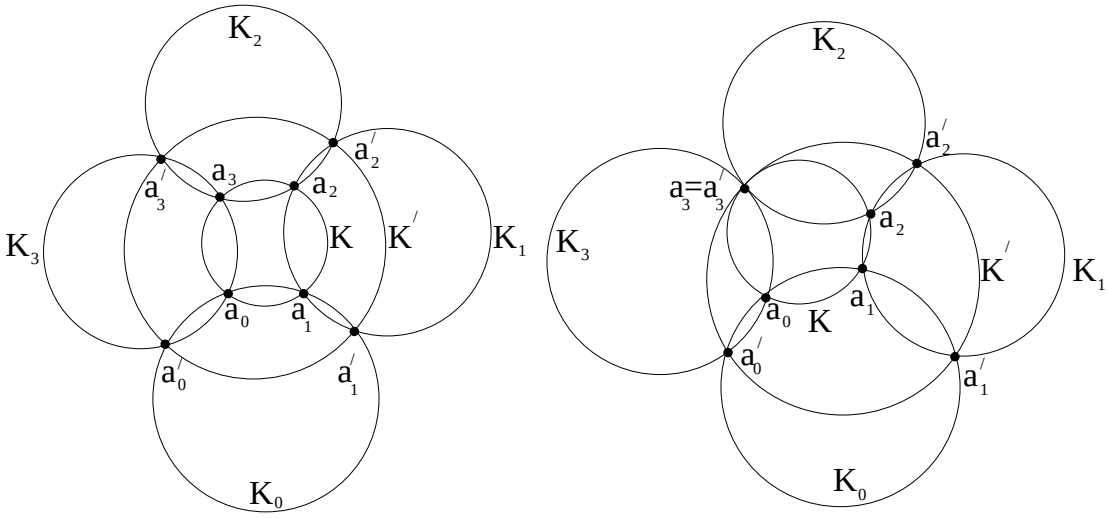
Eine Miquel-Konfiguration können wir uns an einem Würfel veranschaulichen: die Punkte $a_0, a_1, a_2, a_3, a_0', a_1', a_2', a_3'$ lassen sich so den acht Ecken eines Würfels zuordnen, dass es fünfmal vorkommt, dass den vier Eckpunkten einer Seitenfläche vier konzyklische Punkte und den vier Eckpunkten der sechsten Seitenfläche die Punkte a_0', a_1', a_2', a_3' entsprechen. Jedem der fünf Kreis K_0, K_1, K_2, K_3, K entspricht also jeweils eine Seitenfläche des Würfels. Wegen Lemma 1.3.1(2) können dabei höchstens durch eine Kante verbundene Punkte gleich sein. Solche Kanten werden dann fett gezeichnet (Figur 11).



Figur 11

Eine Benz-Ebene $\mathfrak{B}$ heißt *miquelsch*, wenn das folgende Axiom von Miquel gilt.

Axiom von Miquel (**M**). Es seien $(a_0, a_1, a_2, a_3, a_0', a_1', a_2', a_3')$ eine Miquel-Konfiguration und K_0, K_1, K_2, K_3, K die zugehörigen fünf verschiedenen Kreise und $a_0' \notin [a_2']$. Dann gibt es einen eigentlichen Kreis $K' \in \mathfrak{K}$ mit $K_i \cap K' = \{a_i', a_{i+1}'\}$ (Figur 12).



Figur 12

Nach H.-J. Samaga [25] Theorem 3B gilt:

Satz 1.3.1 *Jede Benz-Ebene* $\mathfrak{B} = \Sigma(\mathbb{K}, \mathbb{A})$ *über einer quadratischen Algebra* $(\mathbb{A}, \mathbb{K})$ *ist miquelsch.* □

Bemerkung. Mit Theorem 3B wird in [25] die allgemeinste und umfassenste Form des Satzes von Miquel für Benz-Ebenen über quadratischen Algebren bewiesen. Da in dieser Arbeit der Satz von Miquel als Axiom vorausgesetzt wird, haben wir die schwächere Aussage (**M**) gewählt.

Auch diese Fassung kann für Möbius-Ebenen noch durch die Zusatzvoraussetzung in (**M**), dass $M = \{a_0, a_1, a_2, a_3, a_0', a_1', a_2', a_3'\}$ aus acht Punkten besteht, abgeschwächt werden, denn Y. Chen hat in [7] bewiesen, dass dann der sogenannte volle Satz von Miquel gilt, mit dem B. L. Van der Waerden und J. Smid die Begründung der klassischen Möbius-Ebenen in [29] durchführten.

Im folgenden sei $\mathfrak{B} = (P, \mathfrak{K}, \mathfrak{G})$ eine miquelsche Benz-Ebene.

Lemma 1.3.2 *Wenn* $(a_0, a_1, a_2, a_3, a_0', a_1', a_2', a_3')$ *eine Miquel- Konfiguration ist, dann gilt* $a_2' \in [a_0']$ *genau dann wenn* $a_3' \in [a_1']$.

Beweis. Nach Lemma 1.3.1(2) gilt $a_0' \neq a_2'$, $a_1' \neq a_3'$

(1) Wenn $a_2' \notin [a_0']$, so liegen a_0', a_1', a_2', a_3' nach (M) auf einem eigentlichen Kreis, also gilt auch $a_3' \notin [a_1']$.

(2) Da mit $(a_0, a_1, a_2, a_3, a_0', a_1', a_2', a_3')$ auch $(a_1, a_2, a_3, a_0, a_1', a_2', a_3', a_0')$ eine Miquel-Konfiguration ist, folgt aus $a_3' \notin [a_1']$ ebenso $a_2' \notin [a_0']$. □

Satz 1.3.2 *Es seien* $(P, \mathfrak{K}, \mathfrak{G})$ *und* $(\bar{P}, \bar{\mathfrak{K}}, \bar{\mathfrak{G}})$ *zwei miquelsche Benz-Ebenen vom gleichen Typ (d.h.* $I = \bar{I}$*) mit einer Ordnung* $n \geq 6+2|I|$. *Weiter seien* $\alpha : P \to \bar{P}$ *eine Bijektion und* $p, q \in P$ *mit* $p \notin [q]$ *und* $\alpha([p]_i) = [\alpha(p)]_i$, $\alpha([q]_i) = [\alpha(q)]_i$ *für* $i \in I$. *Wenn für alle* $X \in \mathfrak{K}(p) \cup \mathfrak{K}(q)$ *gilt* $\alpha(X) \in \bar{\mathfrak{K}}$, *dann ist* α *eine Kreisverwandschaft.*

Beweis. Es sei $K \in \mathfrak{K}$ mit $p, q \notin K$. Wegen $n \geq 6 + 2|I|$ gibt es drei verschiedene Punkte $u, v, w \in K \setminus ([p] \cup [q])$. Dann gilt $(q, u, v)^\circ \in \mathfrak{K}$ und damit $\alpha((q, u, v)^\circ) \in \bar{\mathfrak{K}}$, folglich $\alpha(v) \notin [\alpha(u)]$, und wegen $(q, u, w)^\circ, (q, w, v)^\circ \in \mathfrak{K}$ ebenso $\alpha(w) \notin [\alpha(u)]$, $\alpha(w) \notin [\alpha(v)]$. Daher gilt $\bar{A} := (\alpha(u), \alpha(v), \alpha(w))^\circ \in \bar{\mathfrak{K}}$.

Wir zeigen nun zunächst

(1) $\alpha(K \setminus [q]) = \bar{A} \setminus [\alpha(q)]$.

Wegen $|K| > 6+2|I|$ gibt es $a, b \in K \setminus ([p] \cup [q])$ mit $a \neq b$ und $b \neq (p, q, a)^\circ \cap_a K =: a'$.

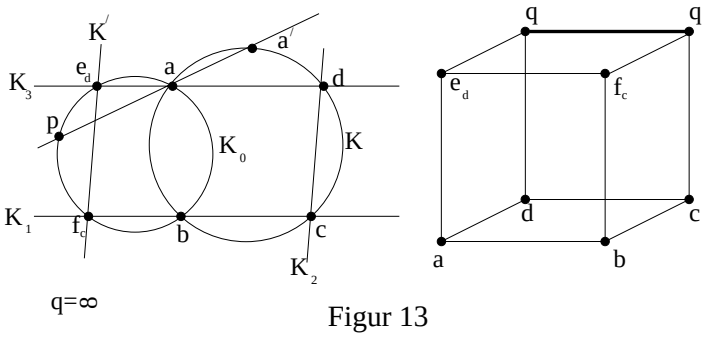
Weiter gibt es ein $c \in K \setminus ([q] \cup \beta_b(K, q))$ mit $c \neq a, a', b$. Wir setzen $\bar{K} := (\alpha(a), \alpha(b), \alpha(c))^\circ$.

Wegen $|K| > 6 + 2|I|$ gilt $K \setminus ([q] \cup \{a, b, c, a'\}) \neq \emptyset$.

Für $d \in K \setminus \{a, b, c\}$, $d \notin [q]$ setzen wir $K_3 := (q, a, d)^\circ$, $K_0 := (p, a, b)^\circ$, $K_1 := (q, b, c)^\circ$, $K_2 := (q, c, d)^\circ$, $e_d := K_3 \cap_a K_0$, $f_c := K_0 \cap_b K_1$. Wegen $c \notin \beta_b(K, q)$ gilt $K_1 \neq \beta_b(K, q)$ und damit $f_c \neq b$.

Damit ist $(a, b, c, d, e_d, f_c, q, q)$ eine Miquel-Konfiguration mit $e_d \notin [q]$ und nach $(\mathbf{M})$ gibt es einen Kreis K' mit $e_d, f_c \in K'$ und $K_3 \cap K' = \{q\}$ (Figur 13).

Nach Voraussetzung gilt $\alpha(K'), \alpha(K_i) \in \bar{\mathfrak{K}}(\alpha(p)) \cup \bar{\mathfrak{K}}(\alpha(q))$ für $0 \leq i \leq 3$. Damit ist $(\alpha(e_d), \alpha(f_c), \alpha(q), \alpha(q), \alpha(a), \alpha(b), \alpha(c), \alpha(d))$ eine Miquel-Konfiguration mit $\alpha(a) \notin [\alpha(c)]$. Nach $(\mathbf{M})$ gilt damit $\alpha(d) \in \bar{K}$.



Figur 13

Damit gilt also $\alpha(K \setminus [q]) \subset \bar{K}$.

Wegen $\alpha(u), \alpha(v), \alpha(w) \in \alpha(K \setminus [q])$ folgt $\bar{A} = \bar{K}$ und damit $\alpha(K \setminus [q]) \subseteq \bar{A} \setminus [\alpha(q)]$. Für α^{-1} gilt ebenso $\alpha^{-1}(\bar{A} \setminus [\alpha(q)]) \subseteq K \setminus [q]$, folglich $\bar{A} \setminus [\alpha(q)] \subseteq \alpha(K \setminus [q]) \subseteq \bar{A} \setminus [\alpha(q)]$, also $\alpha(K \setminus [q]) = \bar{A} \setminus [\alpha(q)]$.

Durch Vertauschen der Rollen von p und q ergibt sich ebenso

(2) $\alpha(K \setminus [p]) = \bar{A} \setminus [\alpha(p)]$.

Für $i \in I$ seien $p_i := K \cap [p]_i$, $q_i := K \cap [q]_i$, und $p'_i := \bar{A} \cap [\alpha(p)]_i$; sowie $q'_i := \bar{A} \cap [\alpha(q)]_i$. Es gilt $p_1 \neq q_1$, $p_2 \neq q_2$.

(3) Falls $p_1 \neq q_2$, so gilt $p_1 \notin [q]$ und damit $\alpha(p_1) \in \bar{A}$ nach (1), also $\alpha(p_1) = \bar{A} \cap [\alpha(p)]_1 = p'_1$, und ebenso $q'_2 = \alpha(q_2) \in \bar{A}$ nach (2). Genauso gilt bei $p_2 \neq q_1$: $p'_2 = \alpha(p_2),\ q'_1 = \alpha(q_1) \in \bar{A}$.

(4) Falls $p'_1 \neq q'_2$, so gilt nach (3) für α^{-1}: $\alpha^{-1}(p'_1) = p_1,\ \alpha^{-1}(q'_2) = q_2$.

(5) Falls $p_1 = q_2$ [6], so gilt $p'_1 = q'_2$ wegen (4), also $\alpha(q_2) = \alpha(p_1) = \alpha([p]_1 \cap [q]_2) = [\alpha(p)]_1 \cap [\alpha(q)]_2 = [p'_1] \cap [q'_2] = p'_1 = q'_2 \in \bar{A}$. Falls $p_2 = q_1$, so gilt ebenso $\alpha(p_2) = \alpha(q_1) \in \bar{A}$.

[6] Das kann nur im Fall einer Minkowski-Ebene auftreten.

Aus (1), (2), (3) und (5) folgt $\alpha(K) = \bar{A} \in \bar{\mathfrak{K}}$. $\square$

1.4 Drehstreckungen

In diesem Paragraphen sei $\mathfrak{B} = (P, \mathfrak{K}, \mathfrak{G})$ eine miquelsche Benz-Ebene der Ordnung $n \geq 6 + 2|I|$. Korollar 1.2.1 legt es nahe folgende Klasse von Abbildungen zu betrachten.

Es seien $E \in \mathfrak{K}$ und $\infty, 0, u \in E$ verschieden sowie $u^* \in P$ mit $u^* \notin E \cup [\infty] \cup [0] \cup [u]$. Nach Korollar 1.2.1 gibt es zu jedem $x \in P^\infty$ mit $x \neq u, 0$ genau ein $x^* \in P \setminus \{x, u^*\}$ mit $(\infty, 0, x, u^*, u, x^*) \in V$ und zu jedem $x \in P^0$ mit $x \neq u, \infty$ genau ein ${}^*x \in P \setminus \{x, u^*\}$ mit $(0, \infty, x, u^*, u, {}^*x) \in V$. Wir setzen nun $0^* = 0, {}^*\infty = \infty$. Die damit definierte Abbildung $\delta_{u,u^*} : P \to P$;

$$x \longmapsto \begin{cases} x^* & \text{für} \quad x \in (P^\infty \setminus [u]) \cup \{u\} \text{ oder } |I| = 1, 0 \text{ und } x \in [u] \\ x & \text{für} \quad x \in [0] \cap [\infty] \\ {}^*x & \text{für} \quad x \in [\infty] \setminus [0] \\ [x_0^*] \cap [u^*] & \text{für} \quad i \in \{1, 2\}\ ,\ x \in [u]_i \setminus ([\infty] \cup \{u\}) \text{ mit } x_0 := [x] \cap [0]_i \end{cases}$$

nennen wir eine $(\infty, 0)$-*Drehstreckung*. Da wir für diesen Paragraphen die Punkte $\infty, 0$ fest gewählt haben, sprechen wir hier auch kurz von Drehstreckungen. Nach Definition gilt $\delta_{u,u^*}(0) = 0$, $\delta_{u,u^*}(\infty) = \infty$ und $\delta_{u,u^*}(u) = u^*$.

Lemma 1.4.1 **(1)** *Für $i \in I$ und $p \in \{\infty, 0\}$ gilt $\delta_{u,u^*}([p]_i) \subseteq [p]_i$.*

(2) $\mathrm{Fix}\delta_{u,u^*} = \{\infty, 0\} \cup ([\infty] \cap [0])$.

(3) *Für $i \in I$ gilt $\delta_{u,u^*}([u]_i) \subseteq [u^*]_i$.*

(4) $\delta_{u,u^*}(P^\infty) \subseteq P^\infty$.

(5) *Für $x \in P, x \neq 0, u$ gilt $\delta_{u,u^*}(x) \notin \{0, u^*\}$.*

Beweis. Für $x \in P,\ x \notin [\infty],\ x \neq 0$ und im Fall $|I| = 2$ [7], $x \notin [u] \setminus ([\infty] \cup [0])$, erfolgt die Konstruktion von $\delta_{u,u^*}(x) = x^*$ nach der Konstruktion aus dem Beweis

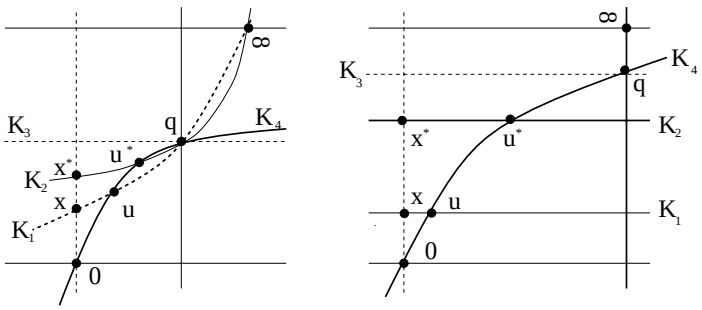
[7] d.h. im Fall einer Minkowski-Ebene.

vom Satz 1.2.1, wobei $(\infty, 0, x, u^*, u, x^*)$ die Rolle von (a, a', b, b', c, c') spielt und alle benötigten Hilfskreise und -punkte wie im Beweis vom Satz 1.2.1 bezeichnet seien, also $K_4 = (0, u, u^*)^\circ \in \mathfrak{K}$ und $\infty \notin K_4$.

(1) Es sei etwa $i = 1$ und $p = 0$. Es gilt $\delta_{u,u^*}(0), \delta_{u,u^*}([0]_1 \cap [\infty]) \in [0]_1$. Für $x \in [0]_1 \setminus [\infty],\ x \neq 0$ liegt der zur Konstruktion vom x^* benötigte Hilfspunkt $q = (0, u, u^*)^\circ \cap_u (\infty, x, u)^\circ$ nicht auf $[0]_1$, weil $K_4 \cap [0]_1 = 0 \neq x = K_1 \cap [0]_1$ und $q = K_4 \cap_u K_1$. Der Punkt x^* liegt auf dem uneigentlichen Kreis $K_3 = (0, x, q)^\circ = [0]_1 \cup [q]_2$. Es gilt $\{q, x^*\} = K_2 \cap K_3$.

Angenommen $x^* = q$. Wegen $K_3 \in \mathfrak{K}_u$ und $|K_2 \cap K_3| = 1$ ist dann $\mathfrak{B}$ eine Minkowski-Ebene und $K_2 \in \mathfrak{K}$ nach Lemma 1.2.2(4). Wegen $|K_2 \cap K_3| = 1$ und $K_3 = [0]_1 \cup [q]_2$ gilt somit $\{q\} = K_2 \cap K_3 = [0]_1 \cap [q]_2$, d.h. $q \in [0]_1$ im Widerspruch zu $q \notin [0]_1$. Damit gilt $x^* \neq q$.

Wegen $q \notin [0]_1$ und $|K_2 \cap K_3| = \{x^*, q\}$ folgt also $x^* \in [0]_1$, also gilt $\delta_{u,u^*}([0]_1) \subseteq [0]_1$ (Figur 14).



Figur 14

Für $x \in [\infty]_1$ zeigt man analog: $\delta_{u,u^*}(x) = {}^*x \in [\infty]_1$.

(2) Nach Definition gilt $\{\infty, 0\} \cup ([\infty] \cap [0]) \subseteq \mathrm{Fix}\delta_{u,u^*}$. Für $x \in P^\infty \setminus \{0\}$ gilt $x^* \neq x$ nach Korollar 1.2.1 und für $x \in [\infty] \setminus [0]$ ebenso ${}^*x \neq x$. Daher gilt $\delta_{u,u^*}(x) \neq x$ für alle $x \in P$ mit $x \notin \{0, \infty\}$ für $|I| = 0, 1$ und $x \notin \{0, \infty\} \cup ([0] \cap [\infty]) \cup ([u] \setminus ([\infty] \cup [0]))$ für $|I| = 2$. Im Fall $|I| = 2$ gilt für $x \in [u] \setminus [\infty]$ etwa $x \in [u]_1, x_0 = [x]_2 \cap [0]_1 \neq 0,\ x_0 \notin [\infty]$, also $x_0^* \neq x$, folglich $[x_0^*]_2 \neq [x]_2$ und damit $\delta_{u,u^*}(x) = [x_0^*]_2 \cap [u^*]_1 \neq x$. Damit folgt $\mathrm{Fix}\delta_{u,u^*} = \{\infty, 0\} \cup ([\infty] \cap [0])$.

(3) Im Fall $|I| = 0$, ist die Behauptung trivial.

Es sei $i = 1$. Für $x \in [u]_1$, $x \neq u$ ist der zur Konstruktion von q benötigte Kreis K_1 uneigentlich, $K_1 = (\infty, x, u)^\circ = [u]_1 \cup [\infty]_2$. Es gilt $q = K_1 \cap_u K_4 = [\infty]_2 \cap K_4$, also $q \in [\infty]_2$, und damit ist $K_2 = (q, \infty, u^*)^\circ = [u^*]_1 \cup [\infty]_2$ uneigentlich.

Im Fall $|I| = 1$ ist $K_3 = (q, x, 0)^\circ$ eigentlich, und $x^* = K_3 \cap_q K_2 = K_3 \cap [u^*]_1 \in [u^*]_1$.

Im Fall $|I| = 2$ gilt nach Definition $\delta_{u,u^*}([u]_1 \setminus ([0] \cup [\infty])) \subseteq [u^*]_1$. Für $x = [u]_1 \cap [0]_2$ ist $K_3 = (0, x, q)^\circ = [0]_2 \cup [q]_1$ uneigentlich, und es gilt wie oben $x^* = K_3 \cap_q K_2 = K_3 \cap [u^*]_1 \in [u^*]_1$. Für $x \in [u]_1 \cap [\infty]_2$ gilt analog ${}^*x \in [u^*]_1$.

Für $[u]_2$ gilt ebenso $\delta_{u,u^*}([u]_2) \subseteq [u^*]_2$.

(4),(5) Es gilt $\delta_{u,u^*}([\infty]) \subseteq [\infty]$ Nach (1) und $0, u^* \notin [\infty]$, also $\delta_{u,u^*}(x) \neq 0, u^*$ für $x \in [\infty]$. Es sei $x \in P^\infty$ mit $x \neq 0, u$, also $(\infty, 0, x, u^*, u, x^*) \in V$. Wegen $K_4 = (0, u, u^*)^\circ \in \mathfrak{K}$ gilt $|K_4 \cap K_2| \leq 2$, und wegen $\infty \notin K_4$ gilt $q = K_1 \cap_u K_4 \neq \infty$.

Für $x \notin [u]$ gilt $K_1 = (\infty, x, u)^\circ \in \mathfrak{K}$, also $q \notin [\infty]$ wegen $q \neq \infty$. Damit ist auch $K_2 = \begin{cases} (\infty, u^*, q)^\circ & falls \quad q \neq u^* \\ \beta_{u^*}(K_4, \infty) & falls \quad q = u^* \end{cases}$ ein eigentlicher Kreis. Wegen $K_1 \in \mathfrak{K}$ gilt weiter $|K_1 \cap K_3| \leq 2$. Damit folgt also $\infty, 0, u^* \neq x^*$ nach Lemma 1.2.4(1), folglich $x^* \notin [\infty]$ wegen $x^*, \infty \in K_2$ und $K_2 \in \mathfrak{K}$.

Damit gilt $\delta_{u,u^*}(x) \in P^\infty$ falls $x \notin [u]$, und $x^* \notin \{0, u^*\}$.

Im Fall $|I| = 0$ und $|I| = 1$ gilt $[u^*] \subseteq P^\infty$, also $\delta_{u,u^*}([u]) \subseteq [u^*] \subseteq P^\infty$ nach (3) und für $x \in [u], x \neq u$ gilt $x^* \neq u^*$ nach Korollar 1.2.1(1). Weiter gilt $x^* \neq 0$ weil $0 \notin [u^*]$.

Es sei jetzt $|I| = 2$. Für $x \in [u] \cap [0]$, etwa $x = [u]_1 \cap [0]_2$ gilt nach (1), (3) $x^* = [u^*]_1 \cap [0]_2 \neq u^*, 0$, weil $u^* \notin [0]$, und weiter $x^* \notin [\infty]$, da $[u^*] \cap [\infty] \cap [0] = \emptyset$.

Für $x \in [u] \setminus [\infty], x \neq u$, etwa $x \in [u]_1$ gilt mit $x_0 = [x]_2 \cap [0]_1$: $x_0^* \notin [\infty]$ und damit $\delta_{u,u^*}(x) = [x_0^*]_2 \cap [u^*]_1 \notin [\infty]$. Da $x_0 \notin [u]$, ist der zur Konstruktion von x_0^* benötigte Kreis K_2 wie oben eigentlich. Damit gilt $x_0^* \notin [u^*]$, da $x_0^* \neq u^*$ (wegen $x_0^* \in [0]$) und $x_0^*, u^* \in K_2$, folglich gilt $x^* = \delta_{u,u^*}(x) = [x_0^*]_2 \cap [u^*]_1 \neq u^*$. Wegen $x^* \in [u^*]$ gilt $x^* \neq 0$. □

Satz 1.4.1 *Die Drehstreckung δ_{u,u^*} ist eine Bijektion, und es gilt $\delta_{u,u^*}^{-1} = \delta_{u^*,u}$.*

Beweis. Für $x \in P$ schreiben wir zur Abkürzung $x^* := \delta_{u,u^*}(x)$. Für $x, v \notin [\infty] \cup \{0, u\}$ und im Fall $|I| = 2$ zusätzlich $x, v \notin P^0 \cap [u]$ gilt damit $(\infty, 0, x, u^*, u, x^*) \in V$. Für $x \in P^\infty$ mit $x \neq 0, u$ und im Fall $|I| = 2$ zusätzlich $x, v \notin [u] \setminus [0]$ gilt $x^* \in P^\infty \setminus \{u^*, 0\}$ nach Lemma 1.4.1. Nach Definition gilt $(\infty, 0, x, u^*, u, x^*) \in V$. Es sei q der gemeinsame Schnittpunkt der vier zugehörigen Kreise $K_1 = (\infty, u, x)^\circ$, $K_2 = (\infty, u^*, x^*)^\circ$, $K_4 = (0, u, u^*)^\circ$ und K_3 mit $0, x, x^* \in K_3$. Es gilt $\mid K_1 \cap K_3 \mid \leq 2$, denn wenn K_1 und K_3 uneigentlich sind und $K_1 \cap K_3 = G$ eine Erzeugende wäre mit $x, q \in G$, so wäre $u \in G$ wegen $u, x \notin [\infty]$, im Widerspruch zu $K_4 \in \mathfrak{K}$, da $u, q \in K_4$ und $q \in [\infty]$ wegen $K_1 \in \widetilde{\mathfrak{K}} \setminus \mathfrak{K}$. Es gilt damit $(\infty, 0, x^*, u, u^*, x) \in V$ nach Lemma 1.2.3(1), also $\delta_{u^*,u}(x^*) = x$.

Für $x \in [\infty]$ gilt ${}^*x = \delta_{u^*,u}(x) \in [\infty]$ nach Lemma 1.4.1(1). Durch Vertauschen der Rollen von 0 und ∞ in den obigen Ausführungen erhalten wir auch hier $\delta_{u^*,u}(x^*) = x$.

Für $|I| = 2$ und $x \in [u]$, etwa $x \in [u]_1$ gilt mit $x_0 = [x]_2 \cap [0]_1$ für $\delta_{u,u^*}(x) = [x_0^*]_2 \cap [u^*]_1$, also $x_0^* = [\delta_{u,u^*}(x)]_2 \cap [0]_1$ und damit $\delta_{u^*,u}(\delta_{u,u^*}(x)) = [\delta_{u^*,u}(x_0^*)] \cap [u]_1 = [x_0]_2 \cap [u]_1 = x$.

Damit gilt also $\delta_{u^*,u} \circ \delta_{u,u^*} = id$. Ebenso haben wir $\delta_{u,u^*} \circ \delta_{u^*,u} = id$. □

Aus Satz 1.4.1 und Lemma 1.4.1(1),(3) folgt.

Lemma 1.4.2 *Für die Drehstreckung δ_{u,u^*} gilt $\delta_{u,u^*}([u]_i) = [u^*]_i$, $\delta_{u,u^*}([\infty]_i) = [\infty]_i$ und $\delta_{u,u^*}([0]_i) = [0]_i$ für $i \in \{1, 2\}$.*

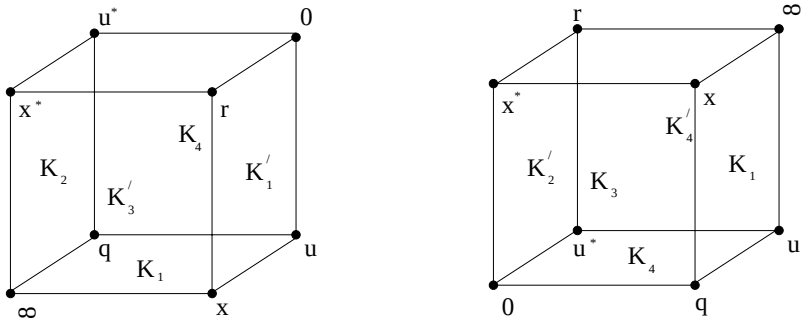
Satz 1.4.2 *Für $x, x^* \in P \setminus ([0] \cup [u] \cup [\infty])$ gilt*

$$(\infty, 0, x, u^*, u, x^*) \in V \Leftrightarrow (0, \infty, x, u^*, u, x^*) \in V$$

Beweis. „⇒“: Es gilt $x^* = \delta_{u,u^*}(x) \neq x$ nach Lemma 1.4.1(2). Nach Satz 1.4.1 und Lemma 1.4.2 gilt $x^* \notin [0] \cup [\infty]$.

Nach Lemma 1.2.4(3) sind die eigentlichen Kreise $K_1 = (\infty, u, x)^\circ$, $K_2 = (\infty, u^*, x^*)^\circ$, $K_3 = (0, x, x^*)^\circ, K_4 = (0, u, u^*)^\circ$ verschieden und es existiert ein Punkt $q = \bigcap_{i=1}^{4} K_i$. Weiterhin sind keine fünf der sechs Punkte $\infty, 0, x, u^*, u, x^*$ konzyklich.

Nach Voraussetzung sind die Kreise $K_1' = (0, u, x)^\circ, K_4' = (\infty, u, u^*)^\circ$ eigentlich. Es sei $r := K_1' \cap_u K_4'$. Es gilt $r \in K_1', K_4'$, also sind r, x, ∞ paarweise verbindbar. Ebenso sind $r, u^*, 0$ paarweise verbindbar. Damit sind die Kreise $K_2' = (r, u^*, 0)^\circ$, $K_3' = (r, x, \infty)^\circ$ eigentlich. Da K_1, K_2, K_3, K_4 verschieden sind, sind auch K_1', K_2', K_3', K_4' verschieden, denn wäre $K_i' = K_j'$ für $i \neq j$, so wären fünf der sechs Punkte $\infty, 0, x, u^*, u, x^*$ konzyklisch. Weiterhin gilt $K_1', K_3' \notin \{K_1, K_2, K_3\}$ und $K_2', K_4' \notin \{K_1, K_4, K_3\}$, da sonst wegen $q \in K_i$ zwei der vier Kreise K_1, K_2, K_3, K_4 gleich wären. Damit ist $(\infty, x, u, q, x^*, r, 0, u^*)$ eine Miquel-Konfiguration mit $x^* \notin [0]$ (Figur 15). Nach **(M)** gilt also $x^* \in K_2'$. Folglich ist auch $(0, q, u, u^*, x^*, x, \infty, r)$ eine Miquel-Konfiguration mit $x^* \notin [\infty]$ (Figur 15) und nach **(M)** gilt $x^* \in (\infty, r, x)^\circ = K_0'$.



Figur 15

Damit gilt $(0, \infty, x, u^*, u, x^*) \in V$.

„$\Leftarrow$“ ergibt sich durch Vertauschen der Rolle von 0 und ∞ im Beweisschritt „$\Rightarrow$“.

□

Indem man die Rollen von 0, ∞ in der Definition von δ_{u,u^*} vertauscht, so erhält man mit ${}^*u := u^*$ eine Abbildung $\tilde{\delta}_{u,u^*} : P \to P$;

$$x \longmapsto \begin{cases} {}^*x & f\ddot{u}r \quad (x \in P^0 \setminus [u]) \cup \{u\} \; oder \; |I| = 1,0 \; und \; x \in [u] \\ x & f\ddot{u}r \quad x \in [0] \cap [\infty] \\ x^* & f\ddot{u}r \quad x \in [0] \setminus [\infty] \\ [{}^*x_0] \cap [u^*] & f\ddot{u}r \quad i \in \{1,2\} \; , \; x \in [u]_i \setminus ([0] \cup \{u\}) \; mit \; x_0 := [x] \cap [\infty]_i \end{cases}$$

Für diese Abbildung gelten auch Lemma 1.4.1, Lemma 1.4.2 und Satz 1.4.1.

Lemma 1.4.3 *Für $x \in P$ mit $x \notin [u] \setminus ([\infty] \cup [0] \cup \{u\})$ gilt $\delta_{u,u^*}(x) = \tilde{\delta}_{u,u^*}(x)$.*

Beweis. Für $x, x^* \in P \setminus ([0] \cup [u] \cup [\infty])$ gilt nach Satz 1.4.2:

$(\infty, 0, x, u^*, u, x^*) \in V \Leftrightarrow (0, \infty, x, u^*, u, x^*) \in V$, d.h. $\delta_{u,u^*}(x) = \tilde{\delta}_{u,u^*}(x)$.

Weiter gilt $\delta_{u,u^*}(x) = x = \tilde{\delta}_{u,u^*}(x)$ für $x \in \{\infty, 0\} \cup ([0] \cap [\infty])$ und $\delta_{u,u^*}(u) = u^* = \tilde{\delta}_{u,u^*}(u)$.

Für $x \in [\infty] \setminus [0]$ gilt nach Definition:

$(0, \infty, x, u^*, u, \delta_{u,u^*}(x)) \in V$ sowie $(0, \infty, x, u^*, u, \tilde{\delta}_{u,u^*}(x)) \in V$, also $\delta_{u,u^*}(x) = \tilde{\delta}_{u,u^*}(x)$ nach Korollar 1.2.1.

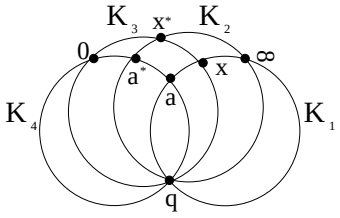
Ebenso gilt für $x \in [0] \setminus [\infty]$: $\delta_{u,u^*}(x) = \tilde{\delta}_{u,u^*}(x)$. □

Lemma 1.4.4 *Für $X \in \mathfrak{K}(\infty, u) \cup \mathfrak{K}(0, u)$ gilt $\delta_{u,u^*}(X) \in \mathfrak{K}(\infty, u^*) \cup \mathfrak{K}(0, u^*)$.*

Beweis. (i) Es sei $X \in \mathfrak{K}(\infty, u)$. Es gilt $K_4 = (u, u^*, 0)^\circ \in \mathfrak{K}$. Für jedes $x \in X$mit $x \neq \infty, u$ ist der zur Konstruktion von $x^* = \delta_{u,u^*}(x)$ benötigte Kreis $K_1 = (\infty, x, u)^\circ = X \in \mathfrak{K}$ (vgl. Beweis von Satz 1.2.1) und damit der Hilfspunkt $q = K_1 \cap_u K_4$ konstant, folglich ist der Hilfskreis $K_2 = \begin{cases} (\infty, u^*, q)^\circ & falls \quad q \neq u^* \\ \beta_{u^*}(K_4, \infty) & falls \quad q = u^* \end{cases}$ konstant und daher $x^* \in K_2$ für alle $x \in X$, d.h. $\delta_{u,u^*}(X) \subseteq K_2$. Mit Satz 1.4.1 ist $\delta^{-1}_{u,u^*}(K_2) = \delta_{u^*,u}(K_2)$ ebenso konzyklich, also $\delta^{-1}_{u,u^*}(K_2) \subseteq X$. Zusammen ergibt sich $\delta_{u,u^*}(X) = K_2$ (Figur 16).

(ii) Für $X \in \mathfrak{K}(0, u)$ gilt analog (i) $\tilde{\delta}_{u,u^*}(X) \in \mathfrak{K}(0, u^*)$. Da $[u] \cap X = \{u\}$ folgt

wegen Lemma 1.4.3 also $\delta_{u,u^*}(X) \in \mathfrak{K}(0,u^*)$. □



Figur 16

Lemma 1.4.5 *Die Drehstreckung δ_{u,u^*} hat die folgenden Eigenschaften.*

(1) *Für $v \in P \setminus ([\infty] \cup [0] \cup [u])$ sind $\infty, 0, v, \delta_{u,u^*}(v)$ nicht konzyklisch, und es gilt $\delta_{u,u^*}(v) \notin [v]$.*

(2) *Für $i \in I$ und $G \in \mathfrak{G}_i$ gilt $\delta_{u,u^*}(G) \in \mathfrak{G}_i$.*

(3) *Es sei $K_4 := (0,u,u^*)^\circ$. Für $v \in P \setminus ([\infty] \cup [0] \cup [u])$, $v \notin E \cup K_4 \cup \beta_u(K_4, \infty)$ und $v^* := \delta_{u,u^*}(v)$ gilt: $\delta_{u,u^*} = \delta_{v,v^*}$.*

Beweis. Für $x \in P$ schreiben wir zur Abkürzung $x^* := \delta_{u,u^*}(x)$. Für $x, v \notin [\infty] \cup \{0,u\}$ und zusätzlich $x, v \notin [u] \setminus [0]$ im Fall $|I| = 2$ gilt damit $(\infty, 0, x, u^*, u, x^*) \in V$ und $(\infty, 0, v, u^*, u, v^*) \in V$. Es sei q bzw. q' der gemeinsame Schnittpunkt der vier zugehörigen Kreise $K_1 = (\infty, u, x)^\circ$, $K_2 = (\infty, u^*, x^*)^\circ$, K_3 mit $0, x, x^* \in K_3$, $K_4 = (0, u, u^*)^\circ$ bzw. $K_1' = (\infty, u, v)^\circ$, $K_2' = (\infty, u^*, v^*)^\circ$, K_3' mit $0, v, v^* \in K_3'$, $K_4' = (0, u, u^*)^\circ$. Es gilt $q, q' \neq \infty$, da $\infty \notin K_4 = K_4'$. Weiter gilt $K_4 \in \mathfrak{K}$.

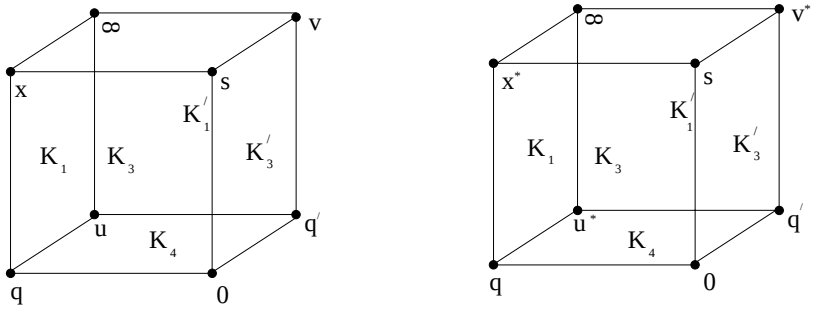
(1) Wegen $v \notin [0]$ gilt $K_3' = (0, v, v^*)^\circ$. Wären $\infty, 0, v, v^*$ konzyklisch, so wäre $\infty = q' = K_2' \cap_{v^*} K_3'$ der zur Kostruktion von v^* benötigte Hilfspunkt, und damit wäre $\infty = q' \in K_4' = K_4$ im Widerspruch zu $\infty \notin K_4$.

Der zur Konstruktion von $v^* \neq v$ benötigte Kreis $K_4' = K_4$ ist eigentlich, also sind 0 und q' verbindbar. Wegen $v \notin E$ gilt $q' \neq 0$. Da $v \notin [0] \cup [u]$, ist auch K_1' eigentlich und damit sind auch v und q' verbindbar, folglich sind $0, q', v$ paarweise verbindbar, also $K_3' = (0, v^*, v)^\circ = (0, q', v)^\circ \in \mathfrak{K}$ und damit $v^* \notin [v]$.

(2) Falls $v \in G$ für $v \in \{\infty, 0, u\}$ gilt die Behauptung nach Lemma 1.4.2. Es sei jetzt $\infty, 0, u \notin G$ und etwa $G \in \mathfrak{G}_1$. Da $|G| \geq n \geq 6 + 2|I|$ gibt es ein

$v \in P$ mit $v \notin [\infty] \cup [0] \cup [u] \cup E \cup K_4 \cup \beta_u(K_4, \infty)$. Wir zeigen für $i \in I$ gilt $\delta_{u,u^*}([v]_i \setminus [u]) = [v^*]_i \setminus [u^*]$.

Wegen $v \notin E \cup K_4 \cup \beta_u(K_4, \infty)$ gilt $q' \neq 0, v, u$. Wegen $q' \neq \infty$ und $v \notin [\infty] \cup [0] \cup [u]$ sind also $q', \infty, 0, u, v$ fünf verschiedene Punkte. Es sei $x \in [v], x \neq v$, $x \notin [\infty] \cup [0] \cup [u]$. Wegen $q', v \in K_3'$, $q' \neq v$ und $x \in [v]$ gilt $q' \neq x$, also $|\{0, q', u, x, v, \infty\}| = 6$. Wegen (1) sind $K_3 = (0, x^*, x)^\circ, K_3' = (0, v^*, v)^\circ$ eigentlich. Weiter gilt $K_1, K_1', K_4 \in \mathfrak{K}$. Mit $s := K_3 \cap_0 K_3'$ ist daher $(q, 0, q', u, x, s, v, \infty)$ eine Miquel-Konfiguration (Figur 17). Wegen $x \in [v]$ gilt $s \in [\infty]$ nach Lemma 1.3.2. Insbesondere gilt also $s \neq 0$, da $0 \notin [\infty]$. Wegen $|\{\infty, 0, u, v, x\}| = 5$ gilt $|\{\infty, 0, u^*, v^*, x^*\}| = 5$ nach Satz 1.4.1 und Lemma 1.4.1(2). Da $u^*, x^*, v^* \in P^\infty$ nach Lemma 1.4.1(4) und $s \in [\infty]$, gilt $s \neq u^*, x^*, v^*$. Weiter gilt $s \neq 0$ und wegen (1) auch $s \neq \infty$. Damit gilt $|\{\infty, 0, u^*, v^*, x^*, s\}| = 6$, folglich ist auch $(q, 0, q', u^*, x^*, s, v^*, \infty)$ eine Miquel-Konfiguration. Wegen $s \in [\infty]$ folgt also $x^* \in [v^*]$ nach Lemma 1.3.2 (Figur 17).



Figur 17

Mit Lemma 1.4.2 und Satz 1.4.1 folgt also

(i) $\delta_{u,u^*}([v] \setminus ([\infty] \cup [0] \cup [u])) = [v^*] \setminus ([\infty] \cup [0] \cup [u^*])$.

Im Fall einer Laguerre-Ebene gilt also $\delta_{u,u^*}([v]) = [v^*]$, da hier $[v] \cap [p] = \emptyset$ für $p \in \{\infty, 0, u\}$.

Für den Beweis von (3) halten wir noch fest:

($*$) Wenn $\mathfrak{L}$ eine Laguerre-Ebene ist, so gilt für $v \in P \setminus ([\infty] \cup [0] \cup [u])$ mit $v \notin E \cup K_4 \cup \beta_u(K_4, \infty)$:

(a) $(\infty, 0, x, v^*, v, x^*) \in V$ für $x \in [v]$, $x \neq v$, da hier $s \in [v] \cup [\infty] = (x, v, \infty)^\circ$

und $s \in [v^*] \cup [\infty] = (x^*, v^*, \infty)^\circ$.

Ebenso gilt:

(b) $(\infty, 0, x, v^*, v, x^*) \in V$ für $x \in [\infty] \cup [0] \cup [u]$.

Um den Beweis von (2) abzuschließen, haben wir nur noch den Fall einer Minkowski-Ebene zu betrachten.

Es sei etwa $i = 1$. Da $|[v]_1| = n + 1 \geq 7 + 2|I| = 11$ gibt es ein $w \in [v]_1$, $w \neq v$ mit $w \notin [\infty] \cup [0] \cup [u]$ und $w \notin K_4 \cup \beta_u(K_4, \infty) \cup E$.

Mit w anstelle von v gilt nach (i) $\delta_{u,u^*}([w] \setminus ([\infty] \cup [0] \cup [u])) = [w^*] \setminus ([\infty] \cup [0] \cup [u^*])$. Weiter gilt $w^* \in [v^*]$ nach (i). Daher ist $[w^*] \cap [v^*]$ eine Erzeugende. Wir zeigen:

(ii) $G' := [w^*] \cap [v^*] \in \mathfrak{G}_1$.

Denn andersfalls gilt für $z' := G' \cap [v]_1$ wegen $v^*, w^* \notin [\infty] \cup [0] \cup [u^*]$ und $[v] \cap [w] = [v]_1$, dass $z := \delta_{u,u^*}^{-1}(z') \in [v]_1 \setminus ([\infty] \cup [0] \cup [u])$ nach (i), also $z^* = z' \in [v]_1 = [z]_1$ im Widerspruch zu $z^* \notin [z]$ nach (1).

Aus (i) und (ii) folgt:

(iii) $\delta_{u,u^*}([v]_1 \setminus ([\infty]_2 \cup [0]_2 \cup [u]_2)) = [v^*]_1 \setminus ([\infty]_2 \cup [0]_2 \cup [u^*]_2)$.

Es sei $x := [v]_1 \cap [0]_2$ und $K := (\infty, u, x)^\circ = K_1$. Wegen Lemma 1.4.4 gilt $\delta_{u,u^*}(K) = K_2$. Es sei nun $\tilde{z} := [v^*]_1 \cap K_2$. Wegen $u^* \in K_2$ und $u^* \notin [v^*]$ nach Lemma 1.4.2 und Satz 1.4.1 gilt $\tilde{z} \notin [u^*]$. Ebenso gilt $\tilde{z} \notin [\infty]$. Deshalb gilt $z := \delta_{u,u^*}^{-1}(\tilde{z}) \in K$ und $z \notin [\infty] \cup [u]$ wegen Lemma 1.4.2 und Satz 1.4.1. Es gilt $z \in [0]$, denn wäre $z \notin [0]$, so wäre $z^* = \tilde{z} \notin [0]$ nach Satz 1.4.1 und Lemma 1.4.2 und damit $z \in [v]_1$ nach (iii), also $z = [v]_1 \cap K = x \in [0]_2$.

Wegen $z \in [0]$ gilt $z^* = \tilde{z} \in [0]$, also $z^* \in [0]_2$, da $[0]_1 \cap [v^*]_1 = \emptyset$, folglich gilt $x^* = [0]_2 \cap K_2 = z^* = \tilde{z} \in [v^*]_1$.

Wegen Lemma 1.4.3 gilt für $x := [v]_1 \cap [\infty]_2$ analog: $\delta_{u,u^*}(x) \in [v^*]_1$.

Es sei schließlich $x \in [v]_1 \cap [u]$. Für $x_0 := [x]_1 \cap [0]_2 = [v]_1 \cap [0]_2$ gilt $x_0^* \in [v^*]_1$ und $\delta_{u,u^*}(x) = [x_0^*]_1 \cap [u^*]_2 = [v^*]_1 \cap [u^*]_2 \in [v^*]_1$.

Damit gilt also $\delta_{u,u^*}([v]_1) = [v^*]_1$

(3) Nach (1) sind $\infty, 0, v, v^*$ nicht konzyklich und $v^* \notin [v]$. Damit ist die Drehstreckung δ_{v,v^*} definiert.

Aus der Definition der $(\infty, 0)$-Drehstreckungen folgt:

(i) Für $x \in \{0, \infty, v\} \cup ([0] \cap [\infty])$ gilt $\delta_{u,u^*}(x) = \delta_{v,v^*}(x)$.

Aus $(\infty, 0, v, u^*, u, v^*) \in V$ und $K_3', K_4' \in \mathfrak{K}$, also $|K_1' \cap K_3'| \leq 2,\ |K_2' \cap K_4'| \leq 2$ folgt $(\infty, 0, u, v^*, v, u^*) \in V$ nach Lemma 1.2.3(1), also

(ii) $\delta_{v,v^*}(u) = u^* = \delta_{u,u^*}(u)$.

Wir setzen $A := [u] \cup [v] \cup [0] \cup [\infty]$, $A^c := P \setminus A$ und zeigen:

(iii) Für $x \in A^c$ gilt $\delta_{u,u^*}(x) = \delta_{v,v^*}(x)$.

Wegen $v^* \notin [v],\ x^* \notin [x]$ (vgl. (1)) sind die Kreise $K_3 = (0, x, x^*)^\circ$ und $K_3' = (0, v, v^*)^\circ$ eigentlich. Es sei $s := K_3 \cap_0 K_3'$.

Nach Voraussetzung sind $\infty, 0, u, v$ verschieden, wegen $x \notin A$ sind also $\infty, 0, u, v, x$ verschieden. Nach Satz 1.4.1 sind also auch $\infty = \infty^*, 0 = 0^*, u^*, v^*, x^*$ verschieden. Es gilt $q' \neq \infty$ und $q' \neq 0, v, u$ wegen $v \notin E \cup K_4 \cup \beta_u(K_4, \infty)$.

(a) Es gilt $|\{q, q', s\}| = 3$ oder $q = q' = s$.

Denn falls $q = q'$, so gilt $q = q' \in K_3 \cap K_3'$ und wegen $q' \neq 0$ folgt $s = q' = q$. Falls $q' = s$, so gilt $s = q' \in K_3 \cap K_4$. Wegen $q' \neq 0, K_3 \neq K_4$ folgt $q = q' = s$. Falls $q = s$, so gilt $q = s \in K_3' \cap K_4$. Wäre $q = 0 = s$, so wäre $K_3' \cap K_3 = \{0\}$ und $K_3 \cap K_4 = \{0\}$, also $\{q', 0\} = K_3' \cap K_4 = \{0\}$ im Widerspruch zu $q' \neq 0$. Damit gilt $s = q \neq 0$, folglich $s = q = q'$ wegen $q, q' \in K_3' \cap K_4$.

(b) Es sei $q = q'$. Dann gilt $\delta_{u,u^*}(x) = \delta_{v,v^*}(x)$.

Denn aus $q = q'$ folgt $q = q' = s$ nach (a). Weiter gilt $q = q' \in (\infty, u, v)^\circ =: \bar{K_1}$, also $x \in \bar{K_1}$ und $q' = q \in (\infty, u^*, x^*)^\circ =: \bar{K_2}$, also $v^* \in \bar{K_2}$ sowie $q' = q = s \in K_3 \cap K_3'$. Wegen $K_3 \neq K_3'$ sind die Kreise $\bar{K_1} = K_1' = K_1$, $\bar{K_2} = K_2 = K_2'$, $\bar{K_3} := K_3, \bar{K_4} := K_3'$ verschieden, und es gilt $\bar{K_1} \cap \bar{K_2} = \{\infty, q\}$, , $\bar{K_1} \cap \bar{K_3} = \{x, q\}$, $\bar{K_1} \cap \bar{K_4} = \{v, q\}$, $\bar{K_2} \cap \bar{K_3} = \{x^*, q\}$, $\bar{K_2} \cap \bar{K_4} = \{v^*, q\}$, $\bar{K_3} \cap \bar{K_4} = \{0, q\}$. Damit gilt $(\infty, 0, x, v^*, v, x^*) \in V$, folglich $\delta_{v,v^*}(x) = x^* = \delta_{u,u^*}(x)$.

(c) Es sei $q' = x$. Dann gilt $\delta_{u,u^*}(x) = \delta_{v,v^*}(x)$.

Denn dann gilt $x = q' \in K_4$, also $q = x = q'$, folglich $\delta_{v,v^*}(x) = x^*$ nach (b)

Analog (c) gilt:

(d) Es sei $q' = x^*$. Dann gilt $\delta_{u,u^*}(x) = \delta_{v,v^*}(x)$.

(e) Es sei $q' \neq u^*, v^*$. Dann gilt $\delta_{u,u^*}(x) = \delta_{v,v^*}(x)$.

Wegen (c) und (d) können wir zum Beweis von (e) $q \neq x, x^*$ annehmen. Da sowohl $\infty, 0, u, v, x$ als auch $\infty, 0, u^*, v^*, x^*$ verschieden sind und $q' \neq \infty, 0, u, v, x$, gilt also $|\{\infty, 0, u, v, x, q'\}| = 6 = |\{\infty, 0, u^*, v^*, x^*, q'\}|$, folglich sind $(q, 0, q', u, x, s, v, \infty)$ und $(q, 0, q', u^*, x^*, s, v^*, \infty)$ Miquel-Konfigurationen mit $x \notin [v]$ und $x^* \notin [v^*]$ (Figur 17), also $s \in (\infty, v, x)^\circ =: \bar{K}_1$ und $s \in (\infty, v^*, x^*)^\circ =: \bar{K}_2$ nach **(M)**, folglich gilt $(\infty, 0, x, v^*, v, x^*) \in V$. Damit haben wir $\delta_{u,u^*}(x) = \delta_{v,v^*}(x)$.

(f) Es sei $q' = u^*$. Dann gilt $\delta_{u,u^*}(x) = \delta_{v,v^*}(x)$.

Wegen (a) und (b) dürfen wir zum Beweis $|\{q, q', s\}| = 3$ annehmen. Damit gilt $q \neq u^*$ und wegen (c) auch $q' \neq x$. Damit ist $(q, 0, q', u, x, s, v, \infty)$ wieder eine Miquel-Konfiguration, und es gilt $s \in (\infty, v, x)^\circ =: \bar{K}_1$.

Wegen $q' = u^*$ gilt $K_2' \cap K_4 = \{u^*\}$, folglich $u^* \neq v^* \notin K_4$, also $q \neq v^*$.

(f_1) Wenn $q \neq 0, x^*$ oder $s \neq 0, v^*, x^*$ ist, so ist auch wieder $(q, 0, q', u^*, x^*, s, v^*, \infty)$ eine Miquel-Konfiguration und wie in (e) folgt $\delta_{u,u^*}(x) = \delta_{v,v^*}(x)$.

(f_2) Es sei $q = 0$. Dann gilt $K_3 \cap K_4 = \{0\}$. Wegen $s \neq q = 0$ und $x^* \neq 0, u^*$ sowie $x^* \in K_2$ gilt $s \neq x^*$, da $K_2 \cap K_3' = \{u^*, 0\}$. Wegen (f_1) haben wir noch den Fall $s = v^*$ zu betrachten. Da $n \geq 6 + 2|I|$ gibt es ein $w \in K_1'$ mit $w \neq \infty, u, v, u^*$, $w \notin [0] \cup [x]$ und $K_2' \cap_{v^*} K_3 \notin K_3'' = (0, u^*, w)^\circ$. Es gilt $w \notin [\infty] \cup [0] \cup [u] \cup [v]$ und $w \notin E \cup K_4 \cup \beta_u(K_4, \infty)$. Die Hilfselemente zur Konstruktion von $\delta_{u,u^*}(w) = w^*$ seien durch $''$ gekenzeichnet. Es gilt $q'' = u^*$. Nach Konstruktion gilt $s'' \neq w^*$. Wegen $\infty \notin K_3''$ gilt $x^* \notin K_3''$, also $s'' \neq x^*$. Wegen $K_4 \neq K_3''$, $K_3 \cap K_4 = \{0\}$ und $|K_3'' \cap K_4| = 2$ gilt $s'' \neq 0$

Damit gilt nach (f_1) $\delta_{u,u^*}(x) = \delta_{w,w^*}(x)$.

Mit $\bar{K}_1 = K_1'$, $\bar{K}_2 = K_2'$, $\bar{K}_3 = K_3'' = (0, w, w^*)^\circ$ und $\bar{K}_4 = K_3'$, $\bar{q} = q' = u^*$ erkennt man $(\infty, 0, w, v^*, v, w^*) \in V$, also $\delta_{v,v^*}(w) = w^*$. Wegen $\bar{q} = u^* \neq v^*, w^*$

(weil $x \notin [\infty] \cup [0] \cup [v] \cup [w]$) gilt nun nach (e) $\delta_{v,v^*}(x) = \delta_{w,w^*}(x) = \delta_{u,u^*}(x)$.

(f_3) Es sei $q = x^*$. Wenn $s \neq 0, v^*$, so gilt wegen $s \neq q$ nach (f_1): $\delta_{u,u^*}(x) = \delta_{v,v^*}(x)$.

Wir haben also noch die Fälle $s = v^*$ und $s = 0$ zu betrachten.

1. Fall: $s = v^*$. Da $n \geq 6+2|I|$, gibt es ein $w \in K_1'$ mit $w \neq \infty, u, v, u^*$, $w \notin [0] \cup [x]$ und $w^* \notin K_3, w^* \notin \beta_0(K_3, u^*)$. Dann folgt wie in (f_2) $\delta_{w,w^*}(x) = \delta_{u,u^*}(x)$ und $\delta_{w,w^*}(x) = \delta_{v,v^*}(x)$.

2. Fall: $s = 0$. Dann gibt es ein $w \in K_1'$ mit $w \neq \infty, u, v, u^*$, $w \notin [0] \cup [x]$ und $w^* \notin K_3$. Wie in (f_2) folgt dann wieder die Behauptung.

(g) Es sei $q' = v^*$. Dann gilt $\delta_{u,u^*}(x) = \delta_{v,v^*}(x)$.

Wegen (a) und (b) dürfen wir zum Beweis $|\{q, q', s\}| = 3$ annehmen, also $q \neq v^*$, und wegen (c) auch $q' \neq x$.

Dann gilt wieder $s \in (\infty, v, x)^\circ =: \bar{K}_1$, $s \neq \infty$. Wegen $q' = v^*$ gilt $K_2' \cap K_3' = \{v^*\}$.

(g_1) Wenn $q \neq 0, u^*, x^*$ oder $s \neq 0, u^*, x^*$ so gilt wieder $\delta_{u,u^*}(x) = \delta_{v,v^*}(x)$.

(g_2) Es sei $q = 0$. Dann gilt $s \neq 0, v^*$. Wegen $q = 0$ gilt $K_3 \cap K_4 = \{0\}$, also $s \neq u^*$. Wenn $s \neq x^*$, so folgt wieder, dass $(q, 0, q', u^*, x^*, s, v^*, \infty)$ eine Miquel-Konfiguration ist und damit wie in (e) $\delta_{u,u^*}(x) = \delta_{v,v^*}(x)$.

Es sei also $s = x^*$. Dann gibt es ein $w \in K_1'$ mit $w \neq v, v^*, u, \infty$, $w \notin [0] \cup [x]$. Die zur Konstruktion von $w^* = \delta_{u,u^*}(w)$ nötigen Hilfselemente werden wieder mit $''$ gekenzeichnet. Für $K_3'' = (w^*, v^*, 0)^\circ$ gilt $s'' = K_3'' \cap_0 K_3 \neq s, 0$, also $s'' \neq x^*, u^*, q'' = q' \neq w^*, u^*$. Es folgt also $\delta_{w,w^*}(x) = \delta_{u,u^*}(x)$ nach (e). Wie im Beweis von (f_2) gilt $\delta_{v,v^*}(w) = w^*$. Der dazu nötige Hilfspunkt ist $\bar{q} = v^*$. Wegen $K_3'' \cap_0 K_3 \neq x^*$ folgt nach (f_2) $\delta_{v,v^*}(x) = \delta_{w,w^*}(x) = \delta_{u,u^*}(x)$.

(g_3) Es sei $q = u^*$. Dann gilt $\delta_{u,u^*}(x) = \delta_{v,v^*}(x)$.

Falls $s \neq 0, x^*$ folgt die Behauptung wieder wie in (e). In den beiden Fällen $s = 0$ und $s = x^*$ erhält man mit einem Hilfspunkt $w \in K_1'$ mit $w \neq v, v^*, u, \infty$ und $w \notin [0] \cup [x]$ und $x^* \notin (w, v^*, 0)^\circ$, falls $s = 0$ bzw.$(w, v^*, 0)^\circ \cap K_3 \neq \{0\}$ falls $s = x^*$ wieder mit (f_2):

$\delta_{v,v^*}(x) = \delta_{w,w^*}(x) = \delta_{u,u^*}(x)$.

Mit (i), (ii), (iii) gilt für Möbius-Ebene die Aussage (3).

Im Fall einer Laguerre-Ebene gilt mit $(*)$ aus dem Beweis von (2) für $x \in A$: $\delta_{v,v^*}(x) = x^* = \delta_{u,u^*}(x)$ und wegen (iii) damit $\delta_{v,v^*} = \delta_{u,u^*}$.

Im Fall einer Minkowski-Ebene gibt es zu $x \in [u]_1, x \neq u, u0, u\infty$ ein $y \in [x]_2 \cap A^c$, also $x = uy$. Unter Berücksichtigung von (2) $\delta_{u,u^*}(x) = \delta_{u,u^*}([u]_1 \cap [y]_2) = [u^*]_1 \cap [\delta_{u,u^*}(y)]_2 = [\delta_{v,v^*}(u)]_1 \cap [\delta_{v,v^*}(y)]_2 = \delta_{v,v^*}([u]_1 \cap [y]_2) = \delta_{v,v^*}(x)$.

Ebenso gilt für $x \in [u]_2 \cup [v]_1 \cup [v]_2 \cup [0]_1 \cup [0]_2 \cup [\infty]_1 \cup [\infty]_2 : \delta_{u,u^*}(x) = \delta_{v,v^*}(x)$.

Weiter gilt nach (2)

$\delta_{u,u^*}(v\infty) = \delta_{u,u^*}([v]_1 \cap [\infty]_2) = [v^*]_1 \cap [\infty]_2 = v^*\infty = \delta_{v,v^*}(v\infty)$ und ebenso

$\delta_{u,u^*}(\infty v) = \infty v^* = \delta_{v,v^*}(\infty v)$, $\delta_{u,u^*}(v0) = v^*0 = \delta_{v,v^*}(v0)$, $\delta_{u,u^*}(0v) = 0v^* = \delta_{v,v^*}(0v)$, $\delta_{u,u^*}(0\infty) = 0\infty = \delta_{v,v^*}(0\infty)$, $\delta_{u,u^*}(\infty 0) = \infty 0 = \delta_{v,v^*}(\infty 0)$.

Damit gilt also die Aussage (3). □

Korollar 1.4.1 *Für $v \in P^\infty \setminus [0]$ und $v^* := \delta_{u,u^*}(v)$ sind $\infty, 0, v, v^*$ nicht konzyklisch, und es gilt $v^* \notin [v]$ sowie $\delta_{v,v^*} = \delta_{u,u^*}$.*

Beweis. Es seien $K := (0, u, u^*)^\circ, B := \beta_u(K, \infty)$. Für $v \in P^\infty \setminus [0]$ setzen wir $K' := (0, v, v^*)^\circ$, $B' := \beta_v(K', \infty)$ und $E' := (0, v, \infty)^\circ$ sowie $A := E \cup K \cup B \cup E' \cup K' \cup B' \cup [\infty] \cup [0] \cup [u] \cup [v]$[8]. Falls $\mathfrak{B}$ nicht endlich ist, so gibt es einen Kreis $C \in \mathfrak{K}(0, u)$ mit $C \neq E, E', K, K'$ und es gilt $C \setminus A \neq \emptyset$, da $|C \cap X| \leq 2$ für $X \in \{E, K, B, E', K', B'\}$ und $|C \cap [x]| \leq 2$ für $x \in \{\infty, 0, u, v\}$. Für $w \in C \setminus A$ gilt nun $\delta_{u,u^*} = \delta_{w,w^*} = \delta_{v,v^*}$ nach Lemma 1.4.5(3).

Die Ordnung n von $\mathfrak{B}$ sei nun endlich. Nach Voraussetzung gilt $n \geq 6 + 2|I|$.

(1) Wenn $E' = E = (0, u, \infty)^\circ$, d.h. $v \in E$, so gilt $\delta_{u,u^*} = \delta_{v,v^*}$.

Zum Beweis dürfen wir $v \neq u$ annehmen.

Es gilt $|E \cup K \cup B \cup K' \cup B'| \leq 5n - 3$ und wegen $0 \in E \cap K \cap K'$ gilt :

[8] $E = (0, u, u^*)^\circ$ vgl. Seite 35.

$|[0] \setminus (\{0\} \cup B \cup B')| \leq |I|(n-2)$. Ebenso gilt $|[u] \setminus (\{u\} \cup K' \cup B')| \leq |I|(n-2)$, $|[v] \setminus (\{v\} \cup K \cup B)| \leq |I|(n-2)$, $|[\infty] \setminus (\{\infty\} \cup K \cup K')| \leq |I|(n-2)$. Damit ergibt sich $|A| \leq 5n - 3 + 4|I|(n-2) = (5+4|I|)n - 8|I| - 3$. Für $n \geq 6 + 2|I|$ ergibt sich $|P| \geq |A|$. Denn für $|I| = 0$ ergibt sich aus $n \geq 5$ sofort $n^2 > 5n - 4$, also $|P| = n^2 + 1 > 5n - 3 \geq |A|$, für $|I| = 1$ ergibt sich aus $n \geq 8$ sofort $n^2 > 8n - 11$, folglich $|P| = n^2 + n > 9n - 11 \geq |A|$, und schließlich ergibt sich für $|I| = 2$ aus $n \geq 10$ sofort $n^2 > 11n - 20$, also $|P| = n^2 + 2n + 1 > 13n - 19 \geq |A|$ [9]. Damit existiert ein $w \in P \setminus A$. Nach Lemma 1.4.5(3) gilt $\delta_{u,u^*} = \delta_{w,w^*} = \delta_{v,v^*}$.

(2) Für $v \notin E$ sei $A' := E' \cup B' \cup K' \cup [\infty] \cup [0] \cup [v]$. Es gilt $|E \cap A'| \leq 4 + |I| < 6 + 2|I|$. Wegen $|E| = n + 1 > 6 + 2|I|$ gibt es also ein $w \in E \setminus A'$. Nach Lemma 1.4.5(3) gilt also $\delta_{v,v^*} = \delta_{w,w^*}$ und nach (1) auch $\delta_{w,w^*} = \delta_{u,u^*}$. □

Satz 1.4.3 *Es gilt* $\delta_{u,u^*} = \tilde{\delta}_{u,u^*}$.

Beweis. Für $x \in P \setminus [u]$ gilt nach Lemma 1.4.3 $\delta_{u,u^*}(x) = \tilde{\delta}_{u,u^*}(x)$.

Es sei $x \in [u]$. Wir wählen $v \in P$ mit $v \notin ([0] \cup [u] \cup [\infty])$. Nach Korollar 1.4.1 gilt $\delta_{u,u^*} = \delta_{v,v^*}$ und analog $\tilde{\delta}_{u,u^*} = \tilde{\delta}_{v,v^*}$. Mit v anstelle von u gilt nach Lemma 1.4.3 $\delta_{v,v^*}(x) = \tilde{\delta}_{v,v^*}(x)$, also $\delta_{u,u^*}(x) = \delta_{v,v^*}(x) = \tilde{\delta}_{v,v^*}(x) = \tilde{\delta}_{u,u^*}(x)$. Damit ist die Behauptung auch für Laguerre- und Minkowski-Ebenen gezeigt. □

Korollar 1.4.2 *Es seien* $a, a', b', c \in P$ *verschieden und paarweise verbindbar und* $b, c' \in P$ *dann gilt:*

$(a, a', b, b', c, c') \in V \iff (a', a, b, b', c, c') \in V \iff (a, a', b', b, c, c') \in V \iff (a, a', b, b', c', c) \in V$.

Beweis. Die erste Äquivlenz folgt aus Satz 1.4.3 mit a, a', b', c anstelle von $\infty, 0, u, u^*$. Die zweite und dritte Äquivlenz gilt nach Lemma 1.2.3(2). □

Lemma 1.4.6 *Für alle* $X \in \mathfrak{K}(0) \cup \mathfrak{K}(\infty)$ *gilt* $\delta_{u,u^*}(X) \in \mathfrak{K}(0) \cup \mathfrak{K}(\infty)$.

[9] Wenn man im Fall $|I| = 2$ genauer abzählt, erhält man eine bessere Abschätzung für $|A|$ als $13n - 19$.

Beweis. Es sei $a \in X$ mit $a \notin [0] \cup [\infty]$. Mit $a^* = \delta_{u,u^*}(a)$ gilt nach Korrolar 1.4.1 $\delta_{a,a^*} = \delta_{u,u^*}$. Nach Lemma 1.4.4 gilt also $\delta_{u,u^*}(X) = \delta_{a,a^*}(X) \in \mathfrak{K}(\infty, a^*) \cup \mathfrak{K}(0, a^*)$. □

Aus Lemma 1.4.6 folgt mit Lemma 1.4.5(2) nach Satz 1.3.2.

Satz 1.4.4 *Die Drehstreckungen δ_{u,u^*} sind Kreisverwandtschaften.* □

Satz 1.4.5 *Für je zwei $(\infty, 0)$-Drehstreckungen δ_1, δ_2 gilt eine der Aussagen:*

(1) *$\delta_1\delta_2$ ist eine $(\infty, 0)$-Drehstreckung.*

(2) *$\delta_1\delta_2$ ist eine $(\infty, 0)$-Streckung.*

(3) *$\delta_1\delta_2$ ist axial mit den Achsen $[0]_1, [\infty]_1$ bzw. $[0]_2, [\infty]_2$.*

Beweis. Für $x \in P$ seien $x' := \delta_1(x),\ x^* := \delta_2(x)$. Für jedes $u \in P \setminus ([0] \cup [\infty])$ gilt $\delta_1 = \delta_{u,u'},\ \delta_2 = \delta_{u',u'^*}$ nach Korollar 1.4.1. Wegen Satz 1.4.4 ist $\delta_1\delta_2$ eine Kreisverwandtschaft.

Falls es ein $u \in P \setminus ([0] \cup [\infty])$ mit $u'^* = u$ gibt, so ist $\delta_2 = \delta_{u',u} = \delta_1^{-1}$ nach Satz 1.4.1 und damit $x'^* = x$ für alle $x \in P$.

Im folgenden können wir also $\delta_2 \neq \delta_1^{-1}$ und damit $x'^* \neq x$ für alle $x \in P \setminus ([0] \cup [\infty])$ annehmen. Es sei $u \in P \setminus ([0] \cup [\infty])$. Für $A := [\infty] \cup [0] \cup [u]$ gilt $A' = \delta_1(A) = [\infty] \cup [0] \cup [u']$ und $A'^* = \delta_2(A') = [\infty] \cup [0] \cup [u'^*]$ nach Lemma 1.4.2.

(a) Für $x \in P \setminus A$ gilt $(\infty, 0, x, u'^*, u, \delta_2\delta_1(x)) \in V$.

Denn wegen $(\infty, 0, x', u'^*, u', x'^*) \in V$ gilt $(\infty, 0, x', u'^*, x'^*, u') \in V$ nach Korollar 1.4.2, also $(\infty, 0, x'^*, u', x', u'^*) \in V$ nach Lemma 1.2.3(1), d.h. $\delta_{x',u'}(x'^*) = u'^*$ und damit nach Korollar 1.4.1

$(*)$ $\delta_{x',u'} = \delta_{x'^*,u'^*}$.

Weiter gilt $(\infty, 0, x, u', u, x') \in V$, also $(\infty, 0, x, u', x', u) \in V$ nach Korollar 1.4.2, d.h. $\delta_{x',u'}(x) = u$. Mit $(*)$ ergibt sich also $\delta_{x'^*,u'^*}(x) = u$, d.h. $(\infty, 0, x, u'^*, x'^*, u) \in$

V. Da $\delta_2\delta_1$ eine Kreisverwandtschaft ist, sind mit $\infty, 0, x, u$ auch $\infty, 0, x^{'*}, u^{'*}$ paarweise verbindbar. Nach Korollar 1.4.2 folgt nun $(\infty, 0, x, u^{'*}, u, x^{'*}) \in V$.

(b) Es sei $u^{'*} \notin (\infty, 0, u)^\circ \cup [u]$. Wegen (a) gilt dann für die Drehstreckung δ_{u,u'^*}:

$(**)$ $\delta_{u,u'^*}(x) = \delta_2\delta_1(x)$ für alle $x \in P \setminus A$.

Weiter gilt $\delta_{u,u'^*}(u) = \delta_2\delta_1(u)$, $\delta_{u,u'^*}(\infty) = \infty = \delta_2\delta_1(\infty)$, $\delta_{u,u'^*}(0) = 0 = \delta_2\delta_1(0)$.

Damit gilt für jede Erzeugende $[v]_i \in \mathfrak{G}$ mit $v \in \{\infty, 0, u\}$ nach Lemma 1.4.5(2) $\delta_{u,u'^*}([v]_i) = [\delta_{u,u'^*}(v)]_i = [\delta_2\delta_1(v)]_i = \delta_2\delta_1([v]_i)$. Es sei $x \in [v]_i$. Es gibt einen Kreis X mit $x = X \cap [v]_i$ und $|X \cap (P \setminus A)| \geq 3$. Also $\delta_2\delta_1(X) = \delta_{u,u'^*}(X)$ nach $(**)$ und Satz 1.4.4. Mit Lemma 1.4.5 folgt also $\delta_2\delta_1(x) = \delta_2\delta_1(X) \cap [\delta_2\delta_1(v)]_i = \delta_{u,u'^*}(X) \cap [\delta_{u,u'^*}(v)]_i = \delta_{u,u'^*}(x)$.

Damit ist also $\delta_2\delta_1 = \delta_{u,u'^*}$ eine $(\infty, 0)$-Drehstreckung.

(c) Wenn $\infty, 0, u, u^{'*}$ konzyklisch sind, d.h. $u^{'*} \in (\infty, 0, u)^\circ$, dann sind nach Lemma 1.2.4(4) wegen (a) für $x \in P \setminus A$ auch $\infty, 0, x, \delta_2\delta_1(x)$ konzyklisch. Wegen $n \geq 6 + 2|I|$ gibt es zu jedem Kreis $X \in \mathfrak{K}(\infty, 0)$ ein $x \in X \setminus A$, also $\delta_2\delta_1(x) \in X$, folglich $\delta_2\delta_1(X) = X$ wegen $0, \infty \in \mathrm{Fix}\delta_2\delta_1$. Damit ist $\delta_2\delta_1$ eine $(\infty, 0)$-Streckung.

(d) Falls $u^{'*} \in [u]_1$, so ist $\delta_2\delta_1$ eine axiale Kreisverwandtschaft.

(d_1) Wäre für ein $X \in \mathfrak{G}_1$ das Bild $\delta_2\delta_1(X) \neq X$, so wäre $X \cap \delta_2\delta_1(X) = \emptyset$ nach Lemma 1.4.5 und damit wäre für $v \in X$ das Bild $v^{'*} \notin X = [v]_1$. Wäre nun $v^{'*} \in [v]$ für alle $v \in X$, d.h $v^{'*} \in [v]_2$ (was ja nur noch in einer Minkowski-Ebene sein könnte), so wäre $\delta_2\delta_1(Y) = Y$ für alle $Y \in \mathfrak{G}_2$ insbesondere $\delta_2\delta_1([u]_2) = [u]_2$ und damit $u^{'*} \in [u]_2$, also $u^{'*} = u$ wegen $u^{'*} \in [u]_1$, im Widerspruch zu $u^{'*} \neq u$. Damit gibt es also ein $v \in X$ mit $v^{'*} \notin [v]$. Folglich wäre $\delta_2\delta_1$ eine $(\infty, 0)$-Drehstreckung oder $(\infty, 0)$-Streckung nach (b), (c). Dann wäre $u^{'*} \notin [u]_1$ im Widerspruch zu $u^{'*} \in [u]_1$. Für alle $X \in \mathfrak{G}_1$ gilt damit $\delta_2\delta_1(X) = X$.

(d_2) Aus $\delta_2\delta_1(X) = X$ für alle $X \in \mathfrak{G}_1$ folgt in Fall einer Minkowski-Ebene wegen $\delta_2\delta_1([\infty]_2) = [\infty]_2$ und $\delta_2\delta_1([0]_2) = [0]_2$, dass $[\infty]_2$ und $[0]_2$ punktweise fest bleiben.

(d_3) Es sei nun $(P, \mathfrak{K}, \mathfrak{G})$ eine Laguerre-Ebene. Die Restriktion $\delta_2\delta_1 \mid_{P\infty}$ ist wegen

(d_1) eine Affinität, die das Parallelbüschel $\mathfrak{G} \setminus \{\infty\}$ geradeweise fest lässt. Da auch $\delta_2\delta_1(0) = 0$ ist, ist $\delta_2\delta_1 \mid_{P^\infty}$ keine Translation. Folglich muß eine Gerade F durch 0 punktweise festbleiben. Da $\operatorname{Fix}\delta_2\delta_1 = ([\infty] \cap [0]) \cup \{\infty, 0\}$ nach Lemma 1.4.1, gilt also $F = [0] = [0]_1$. Ebenso bleibt auch $[\infty] = [\infty]_1$ punktweise fest. □

Der Beweis von Satz 1.4.5 enthält noch die folgenden Kennzeichnungen der Produkte von zwei Drehstreckungen.

Korollar 1.4.3 *Es seien $\delta_1,\ \delta_2$ zwei $(\infty, 0)$-Drehstreckungen. Dann gelten:*

1. *$\delta_2\delta_1$ ist eine $(\infty, 0)$-Drehstreckung genau dann, wenn es einen Punkt $x \in P \setminus ([\infty] \cup [0])$ gibt mit $\delta_2\delta_1(x) \notin [x] \cup (\infty, 0, x)^\circ$.*

2. *$\delta_2\delta_1$ ist eine $(\infty, 0)$-Streckung genau dann, wenn es ein $x \in P \setminus ([\infty] \cup [0])$ gibt mit $\delta_2\delta_1(x) \in (\infty, 0, x)^\circ$.*

3. *$\delta_2\delta_1$ ist eine axiale Kreisverwandtschaft genau dann, wenn es einen Punkt $x \in P \setminus ([\infty] \cup [0])$ gibt mit $\delta_2\delta_1(x) \in [x]$.* □

Lemma 1.4.7 *Je zwei $(\infty, 0)$-Drehstreckungen δ_1, δ_2 sind vertauschbar: $\delta_2\delta_1 = \delta_1\delta_2$.*

Beweis. Für $x \in P$ sei wieder $x' := \delta_1(x),\ x^* := \delta_2(x)$. Es sei $v \in P \setminus ([\infty] \cup [0])$.

(a) Zunächst sei $\delta_2\delta_1$ eine Drehstreckung. Wegen $n \geq 6 + 2|I|$ gibt es ein $x \in P$ mit $x \notin ([\infty] \cup [0] \cup [v] \cup [\delta_1(v)] \cup [\delta_2^{-1}(v)] \cup [\delta_2^{-1}\delta_1^{-1}\delta_2\delta_1(v)])$. Nach Lemma 1.4.5 gilt damit $x^* \notin ([\infty] \cup [0] \cup [v] \cup [x] \cup [v'^*])$ und $x^{*\prime} \notin [v'^*]$ wegen $x \notin [\delta_2^{-1}\delta_1^{-1}\delta_2\delta_1(v)]$. Damit sind die Kreise $(\infty, x, x^*)^\circ,\ (0, x, v')^\circ,\ (\infty, v', x^{*\prime})^\circ,\ (\infty, x^*, v'^*)^\circ,\ (0, x, v)^\circ$ und $(0, x^{*\prime}, v'^*)^\circ$ eigentlich. Weiter ist $(\infty, x^*, x^{*\prime})^\circ$ nach Korollar 1.4.1 eigentlich.

Da $\infty, 0, v', v$ verschieden und paarweise verbindbar sind (vgl. Korollar 1.4.1), folgt aus $(\infty, 0, x^*, v', v, x^{*\prime}) \in V$ nach Korollar 1.4.2 $(\infty, 0, x^*, v', x^{*\prime}, v) \in V$ und damit $(\infty, 0, x^{*\prime}, v, x^*, v') \in V$ nach Lemma 1.2.3(1) wegen $(\infty, x^*, x^{*\prime})^\circ, (\infty, v, v')^\circ \in \mathfrak{K}$. Also gilt:

(i) $\delta_{x^*,v}(x^{*\prime}) = v'$

Für $m := \delta_{v,x}(x^*)$, gilt $m \notin ([\infty] \cup [0])$ nach Lemma 1.4.5 und $(\infty, 0, x^*, x, v, m) \in V$. Da $\infty, 0, x, v$ paarweise verbindbar sind, folgt aus $(\infty, 0, x^*, x, v, m) \in V$ nach Korollar 1.4.2 $(\infty, 0, x^*, x, m, v) \in V$ und damit $(\infty, 0, m, v, x^*, x) \in V$ nach Lemma 1.2.3(1) wegen $(\infty, x, v)^\circ, (0, v, x^*)^\circ \in \mathfrak{K}$, d.h. $\delta_{x^*,v}(m) = x$, folglich $\delta_{x^*,v} = \delta_{m,x}$ nach Korollar 1.4.1. Mit (i) haben wir also $\delta_{m,x}(x^{*\prime}) = v'$, d.h. $(\infty, 0, x^{*\prime}, x, m, v') \in V$ und damit $(\infty, 0, x, x^{*\prime}, v', m) \in V$ nach Lemma 1.2.3(2). Wegen $x^{*\prime} \notin [v']$ folgt nun $(\infty, 0, x, x^{*\prime}, m, v') \in V$ nach Korollar 1.4.2, also $(\infty, 0, m, v', x, x^{*\prime}) \in V$ nach Lemma 1.2.3(1) wegen $(0, x, v')^\circ, (\infty, x^{*\prime}, v')^\circ \in \mathfrak{K}$, d.h. $\delta_{x,v'}(m) = x^{*\prime}$. Nach Korollar 1.4.1 gilt daher:

(ii) $\delta_{x,v'} = \delta_{m,x^{*\prime}}$.

Wegen $(0, v', v^{'*})^\circ, (\infty, x, v')^\circ \in \mathfrak{K}$ folgt aus $(\infty, 0, x, v^{'*}, v', x^*) \in V$ nach Lemma 1.2.3(1) $(\infty, 0, v', x^*, x, v^{'*}) \in V$, also $(\infty, 0, x^*, v', v^{'*}, x) \in V$ nach Lemma 1.2.3(2), folglich $(\infty, 0, x^*, v', x, v^{'*}) \in V$ nach Korollar 1.4.2, d.h. $\delta_{x,v'}(x^*) = v^{'*}$. Mit (ii) folgt daher $\delta_{m,x^{*\prime}}(x^*) = v^{'*}$, d.h. $(\infty, 0, x^*, x^{*\prime}, m, v^{'*}) \in V$, also $(\infty, 0, x^{*\prime}, x^*, v^{'*}, m) \in V$ nach Lemma 1.2.3(2). Wegen $x \notin [\delta_2^{-1}\delta_1^{-1}\delta_2\delta_1(v)]$ gilt $x^* \notin [v^{'*}]$ nach Lemma 1.4.5. Damit erhalten wir $(\infty, 0, x^{*\prime}, x^*, m, v^{'*}) \in V$ nach Korollar 1.4.2.

Wegen $(\infty, x^*, v^{'*})^\circ$, $(0, v^{'*}, x^{*\prime})^\circ \in \mathfrak{K}$ folgt nun $(\infty, 0, m, v^{'*}, x^{*\prime}, x^*) \in V$ nach Lemma 1.2.3(1), also $(\infty, 0, v^{'*}, m, x^*, x^{*\prime}) \in V$ nach Lemma 1.2.3(2), d.h. $\delta_{x^*,m}(v^{'*}) = x^{*\prime}$. Nach Korollar 1.4.1 gilt damit

(iii) $\delta_{x^*,m} = \delta_{v^{'*},x^{*\prime}}$

Aus $m = \delta_{v,x}(x^*)$ folgt $\delta_{x^*,m}(v) = x$ nach Korollar 1.4.1. Mit (iii) folgt $\delta_{v^{'*},x^{*\prime}}(v) = x$, d.h. $(\infty, 0, v, x^{*\prime}, v^{'*}, x) \in V$, also $(\infty, 0, v^{'*}, x, v, x^{*\prime}) \in V$ nach Lemma 1.2.3(1), da $\infty, 0, x, v$ paarweise verbindbar sind, folglich $(\infty, 0, x, v^{'*}, v, x^{*\prime}) \in V$ nach Korollar 1.4.2, also

(iv) $\delta_{v,v^{'*}}(x) = x^{*\prime} = \delta_1\delta_2(x)$.

Da $\delta_2\delta_1$ eine Drehstreckung mit $\delta_2\delta_1(v) = v^{'*}$ und $\delta_2\delta_1(x) = x^{'*}$ ist, gilt $x^{'*} \notin [x] \cup (\infty, 0, x)^\circ$ und $\delta_2\delta_1 = \delta_{x,x^{'*}} = \delta_{v,v^{'*}}$ nach Korollar 1.4.1. Mit (iv) folgt also

$\delta_1\delta_2(x) = x^{*\prime} = \delta_{v,v'^*}(x) = \delta_2\delta_1(x) = x^{'*}$. Damit ist nach Korollar 1.4.3 auch $\delta_1\delta_2$ eine Drehstreckung, und es gilt $\delta_1\delta_2 = \delta_{x,x'^*} = \delta_2\delta_1$ nach Korollar 1.4.1.

(b) Es sei $\delta_2\delta_1$ keine Drehstreckung.

Es gilt also $v^{'*} \in (\infty, 0, v)^\circ =: A$ oder $v^{'*} \in [v]$ nach Korollar 1.4.3. Wenn $\delta_2^{-1}\delta_1$ eine Drehstreckung ist, so gilt $\delta_2^{-1}\delta_1 = \delta_1\delta_2^{-1}$ nach (a) und damit $\delta_2\delta_1 = \delta_1\delta_2$.

Es sei jetzt also auch $\delta_2^{-1}\delta_1$ keine Drehstreckung. Da $n \geq 6 + 2|I|$ gilt, gibt es einen Punkt $w \in P$ mit $w \notin [\infty] \cup [0] \cup A \cup \delta_2^{-1}\delta_1(A) \cup \delta_2^{-1}(A) \cup [v] \cup [\delta_1(v)] \cup [\delta_2^{-1}\delta_1(v)] \cup [\delta_2^{-1}(v)]$.

Wir betrachten die Drehstreckung $\delta_3 := \delta_{v',w}$. Es gilt $\delta_3\delta_1(v) = w \notin A \cup [v] \cup [v']$ nach Voraussetzung. Damit ist $\delta_3\delta_1$ nach Korollar 1.4.3 eine Drehstreckung. Weiter gilt $w \notin \delta_2^{-1}\delta_1(A) \cup [\delta_2^{-1}\delta_1(v)] = \delta_2^{-1}\delta_1(A) \cup \delta_2^{-1}\delta_1[v] = \delta_2^{-1}\delta_1(A \cup [v])$, d.h. $\delta_2(w) \notin \delta_1(A \cup [v])$, also $\delta_2\delta_3(v') = \delta_2(w) \notin \delta_1(A \cup [v]) = (\infty, 0, v')^\circ \cup [v']$. Damit ist auch $\delta_2\delta_3$ nach Korollar 1.4.3 eine Drehstreckung, also $\delta_2\delta_3 = \delta_3\delta_2$ nach (a) .

Schließlich haben wir $\delta_2\delta_3\delta_1(v) = \delta_2(w) \notin A \cup [v]$. Damit ist $\delta_2(\delta_3\delta_1)$ nach Korollar 1.4.3 auch eine Drehstreckung und damit $\delta_2(\delta_3\delta_1) = (\delta_3\delta_1)\delta_2$. Mit $\delta_2\delta_3 = \delta_3\delta_2$ haben wir also $\delta_3\delta_2\delta_1 = \delta_3\delta_1\delta_2$, folglich $\delta_2\delta_1 = \delta_1\delta_2$. □

Es sei $\Delta_{\infty,0}$ die von den $(\infty, 0)$-Drehstreckungen erzeugte Gruppe und $\Sigma_{\infty,0}$ die Gruppe der $(\infty, 0)$-Streckungen.

Satz 1.4.6 *Die Gruppe $\Delta_{\infty,0}$ ist kommutativ und operiert regulär auf $P \setminus ([\infty] \cup [0])$. Jedes Element von $\Delta_{\infty,0}$, das keine Drehstreckung ist, ist Produkt von zwei Drehstreckungen.*

Beweis. Die Kommutativität folgt mit Lemma 1.4.7. Es sei $a, b \notin ([\infty] \cup [0])$.

Falls $b \notin (\infty, 0, a)^\circ \cup [a]$, so ist $\delta = \delta_{a,b}$ eine Drehstreckung mit $\delta(a) = b$.

Falls $b \in (\infty, 0, a)^\circ \cup [a]$, so gibt es wegen $n \geq 6 + 2|I|$ ein $c \in P$ mit $c \notin [\infty] \cup [0] \cup [a] \cup [b]$ und $c \notin (\infty, 0, a)^\circ \cup (\infty, 0, b)^\circ$. Dann ist $\delta = \delta_{c,b} \circ \delta_{a,c}$ eine Streckung bzw. axiale Kreisverwandtschaft je nachdem ob $b \in (\infty, 0, a)^\circ$ oder

$b \in [a]$ (vgl. Beweis von Satz 1.4.5), und es gilt $\delta(a) = b$. Damit operiert $\Delta_{\infty,0}$ also transitiv und wegen der Kommutativität damit regulär auf $P \setminus ([\infty] \cup [0])$. □

Aus dem Beweis von Satz 1.4.6 ersehen wir noch, dass die Streckungsgruppe $\Sigma_{\infty,0}$ für jedes $X \in \mathfrak{K}(\infty, 0)$ transitiv auf $X \setminus \{\infty, 0\}$ operiert und dass $\Sigma_{\infty,0} \leq \Delta_{\infty,0}$ ist, d.h. es gilt:

Satz 1.4.7 *Die Gruppe $\Sigma_{\infty,0}$ ist $(\infty, 0)$-transitiv.* □

Da wegen Satz 1.4.7 für jedes $q \in P$ mit $q \notin [\infty]$ die Gruppe $\Sigma_{\infty,q}$ der (∞, q)-Streckungen, (∞, q)-transitiv ist, gilt nach Satz 1.1.6(1).

Satz 1.4.8 *Die affine Ableitung $\mathcal{A}(\infty)$ ist desarguessch.* □

Bemerkung. Wegen der Kommutativität von $\Sigma_{\infty,0}$ ist $\mathcal{A}(\infty)$ sogar pappussch (vgl.[16] Aufgabe 5.11 Seite 35).

1.5 Koordinatisierung der miquelschen Benz-Ebenen

Es sei $(P, \mathfrak{K}, \mathfrak{G})$ eine miquelsche Benz-Ebene der Ordnung $n \geq 6 + 2|I|$. Wir zeichnen zwei Punkte $\infty, 0 \in P$ mit $0 \notin [\infty]$ aus und setzen $\mathbb{A} := P \setminus [\infty]$. Nach Satz 1.4.7 und Satz 1.1.6(3) ist jede Translation τ von $\mathcal{A}(\infty)$ die Restriktion einer ∞-Translation, oder anders ausgedrückt, jede Translation τ von $\mathcal{A}(\infty)$ lässt sich zu einer Kreisverwandtschaft fortsetzen. Diese Fortsetzung ist wegen Satz 1.1.4 eindeutig. Wir fassen deshalb die Translationen von $\mathcal{A}(\infty)$ als Kreisverwandtschaften auf. Wegen Satz 1.4.7 operiert nach Satz 1.1.6 die Gruppe T der Translationen von $\mathcal{A}(\infty)$ regulär auf $\mathbb{A}$. Daher gibt es zu jedem $a \in \mathbb{A}$ genau ein $a^+ \in T$ mit $a^+(0) = a$, und wie üblich wird damit auf $\mathbb{A}$ durch $a + b := a^+(b)$ eine Addition definiert, so dass $(\mathbb{A}, +)$ eine kommutative Gruppe ist (vgl. [16]).

Es sei nun $1 \in \mathbb{A} \setminus [0]$ ein weiterer fest gewählter Punkt. Da $\Delta_{\infty,0}$ nach Satz 1.4.6 regulär auf $\mathbb{A}^* := \mathbb{A} \setminus [0]$ operiert, gibt es zu jedem $a \in \mathbb{A}^*$ genau ein $a^\bullet \in \Delta_{\infty,0}$

mit $a^\bullet(1) = a$, und durch $a \cdot b = a^\bullet(b)$ wird eine Multiplikation $\cdot : \mathbb{A}^* \times \mathbb{A} \to \mathbb{A}$ definiert. Weiterhin setzen wir für jedes $a \in A$ noch $0 \cdot a := 0$.

Es sei $\mathbb{K} := (\infty, 0, 1)^\circ \setminus \{\infty\}$ und $\mathbb{K}^* := \mathbb{K} \setminus \{0\}$. Für jedes $\lambda \in \mathbb{K}^*$ ist $\lambda^\bullet$ nach Korollar 1.4.3 eine $(\infty, 0)$-Streckung.

Lemma 1.5.1 *Für die Multiplikation* $\cdot : \mathbb{A}^* \times \mathbb{A} \to \mathbb{A},\ (a, b) \mapsto a \cdot b = a^\bullet(b)$ *gilt:*

(1) $(\mathbb{A}^*, \cdot)$ *ist eine kommutative Gruppe mit dem Einselement* 1.

(2) *Für* $a \in \mathbb{A}^*,\ b, c \in \mathbb{A}$ *gilt* $a \cdot (b + c) = a \cdot b + a \cdot c$.

(3) $(\mathbb{K}, +, \cdot)$ *ist ein kommutativer Körper.*

(4) $(\mathbb{A}, \mathbb{K})$ *ist ein zweidimensionaler Vektorraum.*

(5) $\mathcal{A}(\infty) = \mathcal{A}(\mathbb{A}, \mathbb{K})$ *ist die affine Koordinationebene über* $\mathbb{K}$.

Beweis. (1) Nach Satz 1.4.6 ist die Abbildung $\bullet : \mathbb{A}^* \to \Delta_{\infty,0} \quad a \mapsto a^\bullet$ eine Bijektion. Für $a, b \in \mathbb{A}^*$ gilt $(a \cdot b)^\bullet(1) = a \cdot b = a^\bullet(b) = a^\bullet b^\bullet(1)$, also $(a \cdot b)^\bullet = a^\bullet b^\bullet$ nach Satz 1.4.6. Damit ergibt sich, dass $\bullet$ ein Isomorphismus ist, folglich die Behauptung nach Satz 1.4.6.

(2) Nach Satz 1.4.4 ist $a^\bullet$ eine Kreisverwandtschaft, und es gilt $a^\bullet(\infty) = \infty$, $a^\bullet(0) = 0$, d.h. $a^\bullet \mid_{\mathbb{A}} : \mathbb{A} \to \mathbb{A}$ ist eine Affinität, die 0 fest läßt, folglich ein Endomorphismus der kommutativen Gruppe $(\mathbb{A}, +)$ (vgl. [16]), also $a \cdot (b + c) = a^\bullet(b + c) = a \cdot b + a \cdot c$.

(3) Da das Produkt von zwei $(\infty, 0)$-Streckungen eine $(\infty, 0)$-Streckung ist, gilt $\mathbb{K}^* \cdot \mathbb{K}^* \subseteq \mathbb{K}^*$. Mit α ist auch α^{-1} eine Streckung, und es gilt $\alpha^{-1} = (\alpha(1)^\bullet)^{-1} = (\alpha(1)^{-1})^\bullet$, folglich haben wir $\mathbb{K}^{*-1} \subseteq \mathbb{K}^*$. Damit ist $(\mathbb{K}^*, \cdot)$ eine Untergruppe von $(\mathbb{A}^*, \cdot)$. Da $\mathbb{K}$ eine Gerade durch 0 von $\mathcal{A}(\infty)$ ist, ist $(\mathbb{K}, +)$ eine Untergruppe von $(\mathbb{A}, +)$. Mit $0 \cdot a = 0$ für alle $a \in \mathbb{A}$, ist nun $(\mathbb{K}, +, \cdot)$ ein kommutativer Körper.

(4) Mit der äußeren Operation $\mathbb{K} \times \mathbb{A} \to \mathbb{A}$, $(\lambda, a) \mapsto \lambda^\bullet(a) = \lambda \cdot a$, ist $(\mathbb{A}, \mathbb{K})$ wegen (2),(3) ein Vektorraum. Es sei nun $i \in \mathbb{A} \setminus \mathbb{K}$. Da $\mathcal{A}(\infty)$ eine affine Ebene ist, ist $(\mathbb{A}, +)$ die direkte Summe von $\mathbb{K}$ und $\mathbb{K}i$, also $\mathbb{A} = \mathbb{K} \oplus \mathbb{K}i$.

(5) Es sei $\widehat{0}$ das Büschel der Geraden von $\mathcal{A}(\infty)$ durch 0. Für $X \in \widehat{0},\ x \in X$ mit $x \neq 0$, ist $(X,+)$ eine Untergruppe von $(\mathbb{A},+)$, und $X = \mathbb{K}x$, da $\Sigma_{\infty,0}$ transitiv auf $X \setminus \{0\}$ operiert. Damit erhalten wir, dass $\{a + \mathbb{K}b \mid a,b \in \mathbb{A}, b \neq 0\}$ die Geradenmennge von $\mathcal{A}(\infty)$ ist. Also gilt die Behauptung. □

Bemerkung. (3),(4),(5) von Lemma 1.5.1 erhält man auch aus dem Darstellungssatz für desarguessche affine Ebenen (vgl. [16]).

Satz 1.5.1 *Die Multiplikation* $\cdot : \mathbb{A}^* \times \mathbb{A} \to \mathbb{A}$ *lässt sich, so zu einer Multiplikation* $\bullet$ *fortsetzen, dass* $(\mathbb{A},\mathbb{K},+,\bullet)$ *eine kommutative quadratische Algebra über* $\mathbb{K}$ *ist. Dabei ist* $(\mathbb{A},\mathbb{K},+,\bullet)$ *ein Körper, die Algebra der Dualzahlen über* $\mathbb{K}$ *oder die Algebra der anormal-komplexen Zahlen je nachdem ob* $(P,\mathfrak{K},\mathfrak{G})$ *eine Möbius- Laguerre- oder Minkowski-Ebene ist.*

Beweis. Die in Lemma 1.5.1 zusammengestellten Eigenschaften von $(\mathbb{A},\mathbb{K},+,\bullet)$ werden im folgenden stillschweigend benützt.

(a) Falls $(P,\mathfrak{K},\mathfrak{G})$ eine Möbius-Ebene ist, so gilt $\mathbb{A}^* = \mathbb{A} \setminus \{0\}$. Damit ist $(\mathbb{A},+,\cdot)$ ein kommutativer Körper. Folglich ist $(\mathbb{A},\mathbb{K})$ eine quadratische Körpererweiterung.

(b) Es sei nun $(P,\mathfrak{K},\mathfrak{G})$ eine Laguerre-Ebene. Hier ist noch die Multiplikation mit Elementen $n \in N{:=}[0]$ zu erklären. Für jedes $n \in N$ gilt $n+1 \notin [0]$, d.h. $n+1 \in \mathbb{A}^*$. Für $x \in \mathbb{A}$ können wir daher $n \cdot x := (n+1) \cdot x - x$ definieren.

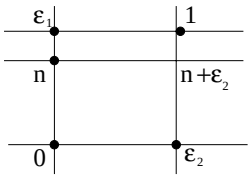
Falls $x \in \mathbb{A}^*$ ist, so gilt $(n+1) \cdot x = x \cdot (n+1) = x \cdot n + x$, also $n \cdot x = x \cdot n$.

$(n+1)^\bullet(1) = n+1 \in 1+N = [1]$, da $[0]$ und $[1]$ in $\mathcal{A}(\infty)$ parallele Geraden sind. Da $(n+1)^\bullet$ keine $(\infty,0)$-Drehstreckung ist, ist $(n+1)^\bullet$ nach Satz 1.4.6 Produkt von zwei $(\infty,0)$-Drehstreckungen. Wegen $n+1 \in [1]$ ist $(n+1)^\bullet$ also nach Korollar 1.4.3(3) eine axiale Kreisverwandtschaft mit der Achse $[0] = N$, folglich gilt $(n+1)^\bullet(m) = m$ für alle $m \in N$, also $n \cdot m = (n+1)^\bullet(m) - m = m - m = 0 = n - n = (m+1)^\bullet(n) - n = m \cdot n$.

Da $(N,+)$ eine Untergruppe von $(\mathbb{A},+)$ und $(\mathbb{A},\cdot)$ kommutativ ist, folgen die

Distributivgesetze für ganz $(\mathbb{A}, +, \cdot)$. Damit erhalten wir, dass $(\mathbb{A}, \mathbb{K})$ eine $\mathbb{K}$-Algebra ist. Weiterhin gilt für jedes $n \in N = [0]$ und $x \in \mathbb{A}^*$ nach Lemma 1.4.1(1) $n \cdot x = x^\bullet(n) \in [0] = N$. Mit $N \cdot N = \{0\}$ folgt also, dass N ein Ideal ist. Wegen $N = [0] = \mathbb{A} \setminus \mathbb{A}^*$ ist $(\mathbb{A}, \mathbb{K})$ also eine quadratische Algebra mit genau einem maximalen Ideal.

(c) Schließlich sei $(P, \mathfrak{K}, \mathfrak{G})$ eine Minkowski-Ebene. Es seien $\varepsilon_1 = [1]_2 \cap [0]_1$, $\varepsilon_2 = [1]_1 \cap [0]_2$ (Figur 18).



Figur 18

Es gilt $\varepsilon_1 + \varepsilon_2 = 1$. Für $n \in [0]_1, n \neq 0$ gilt $n + \varepsilon_2 \in [\varepsilon_2]_1 = [1]_1$ und $n + \varepsilon_2 \notin [0]$. Nach Korollar 1.4.3(3) ist $(n + \varepsilon_2)^\bullet$ daher eine axiale Kreisverwandtschaft mit Achse $[0]_2$. Damit gilt:

(1) $(n + \varepsilon_2) \cdot x = (n + \varepsilon_2)^\bullet(x) = x$ für $n \in [0]_1,\ n \neq 0,\ x \in [0]_2$.

Ebenso haben wir:

(2) $(m + \varepsilon_1) \cdot x = x$ für $m \in [0]_2,\ m \neq 0,\ x \in [0]_1$.

Da $\{\varepsilon_1, \varepsilon_2\}$ eine Basis von $(\mathbb{A}, \mathbb{K})$ ist, gilt weiter:

(3) $\mathbb{A} = \mathbb{K}\varepsilon_1 \oplus \mathbb{K}\varepsilon_2$.

Durch bilineare Fortsetzung von $\varepsilon_1 \bullet \varepsilon_1 = \varepsilon_1,\ \varepsilon_2 \bullet \varepsilon_2 = \varepsilon_2,\ \varepsilon_1 \bullet \varepsilon_2 = 0 = \varepsilon_2 \bullet \varepsilon_1$ definieren wir eine Multiplikation $\bullet : \mathbb{A} \times \mathbb{A} \to \mathbb{A}$ auf $\mathbb{A}$. Dann ist $(\mathbb{A}, \mathbb{K}, +, \bullet)$ die Algebra der anormal-komplexen Zahlen.

Die Einheitengruppe von $(\mathbb{A}, \bullet)$ ist $U := \mathbb{A} \setminus (\mathbb{K}\varepsilon_1 \cup \mathbb{K}\varepsilon_2) = \mathbb{A}^*$.

Für $a, b, c, d \in \mathbb{K}$ und $x = a\varepsilon_1 + b\varepsilon_2 \in \mathbb{A}^*$, d.h. $ab \neq 0$ und $y = c\varepsilon_1 + d\varepsilon_2 \in \mathbb{A}$ gilt

$$x \bullet y = (a\varepsilon_1 + b\varepsilon_2) \bullet (c\varepsilon_1 + d\varepsilon_2) = ac\varepsilon_1 + bd\varepsilon_2$$

und wegen $a^{-1}b\varepsilon_2 \in [0]_2 \setminus \{0\}$ und $b^{-1}a\varepsilon_1 \in [0]_1 \setminus \{0\}$ (vgl. Lemma 1.4.1).

$x \cdot y = (a\varepsilon_1 + b\varepsilon_2) \cdot (c\varepsilon_1 + d\varepsilon_2) = (a\varepsilon_1 + b\varepsilon_2) \cdot (c\varepsilon_1) + (a\varepsilon_1 + b\varepsilon_2) \cdot (d\varepsilon_2)$
$= a(\varepsilon_1 + a^{-1}b\varepsilon_2) \cdot (c\varepsilon_1) + b(b^{-1}a\varepsilon_1 + \varepsilon_2) \cdot (d\varepsilon_2) = ac\varepsilon_1 + bd\varepsilon_2$
nach (1) und (2). Damit gilt also $x \cdot y = x \bullet y$, d.h. $\bullet$ ist eine Fortsetzung von $\cdot : \mathbb{A}^* \times \mathbb{A} \to \mathbb{A}$. □

Um die Benz-Ebene $\mathfrak{B} = (P, \mathfrak{K}, \mathfrak{G})$ mittels $\mathbb{A}$ zu koordinatisieren, betrachten wir die injektive Abbildung $\varphi : \begin{cases} \mathbb{A} \to P(\mathbb{A}) \\ x \mapsto \mathbb{A}^*(x, 1) \end{cases}$ von $\mathbb{A}$ in die projektive Gerade über $\mathbb{A}$.

Lemma 1.5.2 *Für jede Erzeugende $G \in \mathfrak{G}$ mit $\infty \notin G$ ist $\varphi(G \cap \mathbb{A})$ in einer Erzeugenden von $\Sigma(\mathbb{K}, \mathbb{A})$ enthalten.*

Beweis. Für $G = g + [0]_i$ mit $g \in \mathbb{A}$, gilt
$\varphi(G \cap \mathbb{A}) = \{\mathbb{A}^*(g+n, 1) \mid n \in [0]_i \setminus [\infty]\}$ und $\begin{vmatrix} g + n_1 & 1 \\ g + n_2 & 1 \end{vmatrix} = n_1 - n_2 \in [0]_i \setminus [\infty]$
für $n_1, n_2 \in [0]_i \setminus [\infty]$ (vgl. Seite 15). □

Die Injektion φ wollen wir im Folgenden zu einer Koordinatisierung von $\mathfrak{B}$ fortsetzen, d.h. zu einer kreistreuen Bijektion $\varphi : P \to P(\mathbb{A})$. Als erstes setzen wir dazu $\varphi(\infty) := \mathbb{A}^*(1, 0)$. Für den Fall einer Möbius-Ebene haben wir damit schon eine Bijektion der Punktmenge P auf die projektive Gerade $P(\mathbb{A})$.

Wegen der Gitterstruktur kann man auch im Fall der Minkowski-Ebenen die Injektion φ in natürlicher Weise zu einer gittertreuen Bijektion fortsetzen.

Dagegen läßt sich im Fall der Laguerre-Ebenen die Fortsetzung an dieser Stelle noch nicht angeben (jede Fortsetzung ist hier gittertreu).

Die folgenden Betrachtungen dienen der Vorbereitung der Fortsetzung von φ. Wegen Satz 1.4.6 gibt es zu $c \in \mathbb{A}^*, c \notin [1], c \notin (\infty, 0, 1)^\circ$ genau eine $(c, 1)$-Drehstreckung δ mit $\delta(\infty) = 0$. Im folgenden werden wir mit solchen Drehstreckungen zeigen, dass die gebrochen affinen Abbildungen von $\mathbb{A}$ Kreisverwandtschaften von $\mathfrak{B}$ sind.

Lemma 1.5.3 *Es seien* $c \in \mathbb{A}^*, c \notin [1], c \notin (\infty, 0, 1)^\circ$ *und* δ *die* $(c,1)$*-Drehstreckung mit* $\delta(\infty) = 0$ *sowie* $\gamma := (-c)^\bullet \circ \delta \circ (1+c)^+$. *Dann ist* γ *eine involotorische Kreisverwandtschaft, und für alle* $x \in \mathbb{A}^*$ *gilt* $\gamma(x) = \frac{1}{x}$. *Weiter gilt für* $i \in I : \gamma([0]_i) = [\infty]_i$.

Beweis.Wir zeigen zunächst:

(1) Für $x \in \mathbb{A}$ mit $x \notin [c] \cup [\delta^{-1}(\infty)] \cup [1] \setminus \mathrm{Fix}\delta$ gilt

$(*)$ $(x-1-c)\delta(x) = -c$

Nach Lemma 1.4.1 gilt $\mathrm{Fix}\delta = \{c, 1\} \cup ([c] \cap [1])$. Damit gilt $(*)$ für $x = 1$ und $x = c$. Für $x \in [c] \cap [1]$[10] folgt die Gleichung $(*)$ mit der im Beweis von Satz 1.5.1 angegebenen Darstellung der Algebra $\mathbb{A}$: Ist $c = c_1\varepsilon_1 + c_2\varepsilon_2$ mit $c_i \in \mathbb{K}^*$ und etwa $x = [1]_1 \cap [c]_2 = c_1\varepsilon_1 + \varepsilon_2$, so gilt $(x-1-c)\delta(x) = -(\varepsilon_1 + c_2\varepsilon_2)(c_1\varepsilon_1 + \varepsilon_2) = -(c_1\varepsilon_1 + c_2\varepsilon_2) = -c$.

Es sei jetzt $x \in \mathbb{A},\ x \notin [c] \cup [\delta^{-1}(\infty)] \cup [1]$. Wegen $x \notin [\delta^{-1}(\infty)]$ gilt $\delta(x) \notin [\infty]$, also $\delta(x) \in \mathbb{A}$. Weiter gilt $(c, 1, x, 0, \infty, \delta(x)) \in V$ und $(\infty, 0, 1)^\circ, (\infty, x, c)^\circ \in \mathfrak{K}$, folglich $(\infty, \delta(x), c, 1, x, 0) \in V$ nach Lemma 1.2.3(1). Da die Translationen Kreisverwandtschaften sind, ist also insbesondere $(-\delta(x))^+$ eine Kreisverwandtschaft. Wegen $x \notin [c] \cup [1]$ gilt $\delta(x) \notin [x]$ nach Korollar 1.4.1, folglich $x - \delta(x) \notin [0]$, d.h. $x - \delta(x) \in \mathbb{A}^*$, also $((x-\delta(x))^{-1})^\bullet \in \Delta_{\infty,0} \subseteq \mathrm{Aut}(P, \mathfrak{K}, \mathfrak{G})$. Aus $(\infty, \delta(x), c, 1, x, 0) \in V$ folgt damit nach Lemma 1.2.3(3) $(\infty, 0, c - \delta(x), 1 - \delta(x), x - \delta(x), -\delta(x)) \in V$ und weiter:
$(\infty, 0, (x-\delta(x))^{-1}(c-\delta(x)), (x-\delta(x))^{-1}(1-\delta(x)), 1, -(x-\delta(x))^{-1}\delta(x)) \in V$.

Wegen $x \notin [c]$ gilt $\delta(x) \notin [\delta(c)] = [c]$ und $c \notin [x]$, also $c - \delta(x) \notin [0]$ und $c - \delta(x) \notin [x - \delta(x)]$, folglich $y := (x-\delta(x))^{-1}(c-\delta(x)) \notin [0] \cup [1]$. Wegen $x \notin [1]$ gilt $\delta(x) \notin [\delta(1)] = [1]$, also $1 - \delta(x) \notin [0]$, folglich $a := (x-\delta(x))^{-1}(1-\delta(x)) \in \mathbb{A}^*$.

Nach Satz 1.4.6 und dem Beweisschritt (a) von Satz 1.4.5 folgt nun:

$(\infty, 0, y, a, 1, ay) \in V$. Wegen $(\infty, 0, y, a, 1, -(x-\delta(x))^{-1}\delta(x)) \in V$ folgt damit $-(x-\delta(x))^{-1}\delta(x) = ay = (x-\delta(x))^{-1}(1-\delta(x))(x-\delta(x))^{-1}(c-\delta(x))$ nach Korollar

[10] Dieser Fall tritt nur bei Minkowski-Ebenen auf.

1.2.1(1), folglich $(x-\delta(x))\delta(x) = -(1-\delta(x))(c-\delta(x))$, also $(x-1-c)\delta(x) = -c$.

(2) Für $x \in \mathbb{A}$ gilt: $x - 1 - c \in [0] \setminus [\infty] = \mathbb{A} \setminus \mathbb{A}^* \Leftrightarrow x \in [1+c]$.

Da $-c$ eine Einheit ist, sind auch die Faktoren $x-1-c$ und $\delta(x)$ der linken Seite der Gleichung $(*)$ Einheiten.

Aus (1) und (2) folgt damit $[1+c] \subseteq ([\delta^{-1}(\infty)] \cup [1] \cup [c] \setminus \mathrm{Fix}\delta)$. Wegen $\mathrm{Fix}\delta \subseteq [1] \cup [c]$ folgt damit

(3) $[1+c] = [\delta^{-1}(\infty)]$, also $\delta([1+c]) = [\infty]$.

(4) Es sei $\tilde{\mathfrak{C}}$ die durch die Matrix $\mathfrak{C} := \begin{pmatrix} 0 & 1 \\ -c & -1-c \end{pmatrix}$ induzierte Kreisverwandtschaft der Kettenebene $\Sigma(\mathbb{K}, \mathbb{A})$ (vgl. Seite 14). Es gilt:

$\tilde{\mathfrak{C}}\varphi(x) = \mathbb{A}^*(-c, x-1-c)$ für $x \in \mathbb{A}$.

Wegen (2) und (1) folgt aus (4):

(5) Für $x \in \mathbb{A} \setminus [1+c]$, $x \notin ([1] \cup [c]) \setminus \mathrm{Fix}\delta$ gilt: $\tilde{\mathfrak{C}}\varphi(x) = \mathbb{A}^*(\frac{-c}{x-1-c}, 1) = \varphi\delta(x)$.

(6) Im Fall einer Möbius- oder Minkowski-Ebene gilt $\tilde{\mathfrak{C}}\varphi(x) = \varphi\delta(x)$ für alle $x \in \mathbb{A} \setminus [1+c]$. Für Möbius-Ebenen folgt die Behauptung sofort aus (1).

Es sei nun $(P, \mathfrak{K}, \mathfrak{G})$ eine Minkowski-Ebene. Wegen (5) ist die Behauptung nur noch für $x \in \mathbb{A} \setminus [1+c]$ mit $x \notin ([1] \cup [c]) \setminus ([1] \cap [c])$ zu zeigen. Es sei etwa $x \in [1]_1 \setminus [c]$. Da $|[x]_2| \geq 6 + 2|I|$ gibt es ein $y \in \mathbb{A} \cap [x]_2$ mit $y \notin [1] \cup [c] \cup [1+c]$. Nach (5) gilt $\tilde{\mathfrak{C}}\varphi(y) = \varphi\delta(y)$. Weiter gilt $x = [1]_1 \cap [y]_2$, mit Lemma 1.5.2 also: $\tilde{\mathfrak{C}}\varphi(x) = \tilde{\mathfrak{C}}\varphi([1]_1 \cap [y]_2) = [\tilde{\mathfrak{C}}\varphi(1)]_1 \cap [\tilde{\mathfrak{C}}\varphi(y)]_2 = [\varphi\delta(1)]_1 \cap [\varphi\delta(y)]_2 = \varphi\delta([1]_1 \cap [y]_2) = \varphi\delta(x)$.

(7) Es gilt $\gamma(\infty) = (-c^{-1})^\bullet \circ \delta \circ (1+c)^+(\infty) = (-c^{-1})^\bullet \circ \delta(\infty) = 0$.

(8) Es gilt $\gamma^2(x) = x$ und $\gamma(x) = \frac{1}{x}$ für alle $x \in \mathbb{A}^*$.

Zum Beweis von (8) betrachten wir zunächst den Fall einer Möbius- oder Minkowski-Ebene. Für $x \in \mathbb{A}^*$ gilt $1+c+x \notin [1+c]$, nach (6) also $\gamma(x) = (-c^{-1})^\bullet \circ \delta \circ (1+c)^+(x) = (-c^{-1})^\bullet \delta(1+c+x) = (-c^{-1})^\bullet \varphi^{-1}(\mathbb{A}^*(-c, x)) = (-c^{-1})^\bullet \varphi^{-1}(\mathbb{A}^*(-\frac{c}{x}, 1)) = \frac{1}{x}$. Damit gilt $\gamma^2(x) = x$ für alle $x \in \mathbb{A}^*$. Da γ^2 eine Kreisverwandtschaft von $\mathfrak{B}$ ist, folgt $\gamma^2 = id$ nach Satz 1.1.4.

Es sei jetzt $\mathfrak{B}$ eine Laguerre-Ebene.

(i) Für $x \in \mathbb{A}$ gilt $x \in [-1] \cup [-c] \Leftrightarrow 1 + c + x \in [1] \cup [c]$.

Mit (5) folgt aus (i) wie oben:

(ii) Für $x \in \mathbb{A}^*$, $x \notin [-1] \cup [-c]$ gilt $\gamma(x) = \frac{1}{x}$.

Weiter gilt:

(iii) Für $x \in \mathbb{A}^*$ gilt: $x \in [-c] \Leftrightarrow \frac{1}{x} \in [-\frac{1}{c}]$ und $x \in [-1] \Leftrightarrow \frac{1}{x} \in [-1]$.

Wir setzen $B := \mathbb{A}^* \setminus ([-1] \cup [-c] \cup [-\frac{1}{c}])$. Wegen (iii) gilt $B = B^{-1}$. Nach (ii) gilt für alle $x \in B$: $\gamma(x) = \frac{1}{x}$, also $\gamma^2(x) = x$, wegen $B = B^{-1}$.

Es sei $p \in B$ und $A := B \setminus [p] \subseteq P^p$. Die Abbildung $\gamma^2|_{P^p}$ ist eine Affinität mit $\gamma^2|_A = id_A$.

Für jeden Kreis $X \in \mathfrak{K}(p)$ gilt $|(X \setminus \{p\}) \cap A| = n - 5 \geq 2$. Für jeden Punkt $x \in P^p$ gibt es $X_1, X_2 \in \mathfrak{K}(p)$ mit $X_1 \cap X_2 = \{x, p\}$. Damit folgt nun $\gamma^2|_{P^p} = id$ nach Satz 1.1.3. Wegen $[p] \cap [q] = \emptyset$ für $p \neq q$ gilt $[p] \subseteq B$. Damit folgt also $\gamma^2 = id$.

Nach (7) gilt $\gamma(\infty) = 0$, also $\infty = \gamma(0) = (-c^{-1})^\bullet \delta(1+c)$ und damit $\delta(1+c) = \infty$. Wir zeigen jetzt:

(iv) Für $x \in \mathbb{A} \setminus [1 + c]$ gilt $\tilde{\mathfrak{C}}\varphi(x) = \varphi(\delta(x))$.

Wegen (5) ist die Behauptung nur noch für $x \in \mathbb{A}$ mit $x \in ([1] \cup [c])$ etwa $x \in [1]$ zu zeigen. Es sei $G := (x, 1 + c, \infty)^\circ$. Nach (5) gilt:

(**) Für alle $g \in G \setminus \{\infty, 1 + c, x\}$: $\tilde{\mathfrak{C}}\varphi(g) = \varphi\delta(g)$.

Es gilt $\infty \in G$ und wegen $1 + c \in G$ auch $\infty = \delta(1 + c) \in \delta(G)$. Damit sind $\varphi(G \setminus \{\infty\})$ und $\varphi\delta(G) \setminus \{\varphi(\infty)\}$ Geraden der affinen Ableitung $\mathcal{A}(\varphi(\infty))$ von $\Sigma(\mathbb{K}, \mathbb{A})$. Da $|G| \geq 7$ folgt mit (iv)

$\tilde{\mathfrak{C}}\varphi(G)\setminus\{\varphi(\infty)\} = \tilde{\mathfrak{C}}\varphi(G\setminus\{\infty\}) = \varphi\delta(G\setminus\{\infty\}) = \varphi\delta(G)\setminus\{\varphi(\infty)\}$, also $\tilde{\mathfrak{C}}\varphi(G) = \varphi\delta(G)$. Damit folgt wieder mit Lemma 1.5.2 $\tilde{\mathfrak{C}}\varphi(x) = \tilde{\mathfrak{C}}\varphi([1] \cap G) = [\tilde{\mathfrak{C}}\varphi(1)] \cap \tilde{\mathfrak{C}}\varphi(G) = [\varphi\delta(1)] \cap \varphi\delta(G) = \varphi\delta(x)$. Aus (iv) folgt jetzt wie im Möbius- und Minkowski- Fall: $\gamma(x) = \frac{1}{x}$ für $x \in \mathbb{A}^*$. Da $\gamma^2 = id$ folgt $\gamma(0) = \infty$ nach (7) und damit ergibt sich unter Berücksichtigung von Lemma 1.4.5(2) und (3) sofort $\gamma([0]_i) = (-c^{-1})^\bullet \delta([1 + c]_i) = (-c^{-1})^\bullet([\infty]_i) = [\infty]_i$. □

Mit Hilfe der Kreisverwandschaft γ aus Lemma 1.5.3 setzen wir jetzt die Injektion φ von $\mathbb{A}$ auf P fort:

Für $w \in [\infty] \setminus [0]$ gilt $\gamma(w) \in [0] \setminus [\infty] \subseteq \mathbb{A}$ nach Lemma 1.5.3 und wir setzen $\varphi(w) = \mathbb{A}^*(1, \gamma(w))$

Für $w_{ij} := [0]_i \cap [\infty]_j$ mit $i \neq j$ sei $\varphi(w_{ij}) := \mathbb{A}^*(\varepsilon_i, \varepsilon_j)$.

Lemma 1.5.4 *Mit* $I^* = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in GL(2, \mathbb{A})$ *gilt* $\gamma = \varphi^{-1}\widetilde{I}^*\varphi$.

Beweis. Für alle $x \in \mathbb{A}^*$ gilt $\varphi^{-1}\widetilde{I}^*\varphi(x) = \varphi^{-1}(\mathbb{A}^*(1, x)) = \frac{1}{x} = \gamma(x)$ nach Lemma 1.5.3 .

Für $w \in [\infty] \setminus [0]$ gilt $\varphi^{-1}\widetilde{I}^*\varphi(w) = \varphi^{-1}(\mathbb{A}^*(\gamma(w), 1)) = \gamma(w)$.

Für $n \in [0] \setminus [\infty]$ gilt $w = \gamma(n) \in [\infty] \setminus [0]$ nach Lemma 1.5.3, und es gilt $\varphi^{-1}\widetilde{I}^*\varphi(n) = \varphi^{-1}(\mathbb{A}^*(1, n)) = \varphi^{-1}(\mathbb{A}^*(1, \gamma(w))) = w = \gamma(n)$.

Für $i, j \in I,\ i \neq j$ und $w_{ij} = [0]_i \cap [\infty]_j$ gilt $\varphi^{-1}\widetilde{I}^*\varphi(w_{ij}) = \varphi^{-1}\widetilde{I}^*(\mathbb{A}^*(\varepsilon_i, \varepsilon_j)) = \varphi^{-1}(\mathbb{A}^*(\varepsilon_j, \varepsilon_i)) = [\infty]_i \cap [0]_j = \gamma([0]_i \cap [\infty]_j) = \gamma(w_{ij})$. □

Satz 1.5.2 *Die Bijektion* $\varphi : P \to P(\mathbb{A})$ *ist eine Kreisverwandtschaft.*

Beweis. Nach Lemma 1.5.1(5) gilt $\mathcal{A}(\infty) = \mathcal{A}(\mathbb{A}, \mathbb{K})$.

(1) Zu jedem Kreis $C \in \mathfrak{K}(\infty)$ gibt es also $a, b \in \mathbb{A}, b \neq 0$ mit $C = (a + \mathbb{K}\, b) \cup \{\infty\}$. Für $a, a + b \in C$ gilt $a + b \notin [a] = a + [0]$, folglich $b \notin [0]$, d.h. $b \in \mathbb{A}^*$. Damit ist $\varphi(C) = \{\mathbb{A}^*(a + \lambda b, 1) \mid \lambda \in \mathbb{K}\} \cup \{\mathbb{A}^*(1, 0)\}$ nach [3] (Satz 3.1 Seite 104) ein Kreis vom $\Sigma(\mathbb{K}, \mathbb{A})$.

(2) Nun sei $C \in \mathfrak{K}(0)$. Dann gilt $\gamma(C) \in \mathfrak{K}(\infty)$ nach Lemma 1.5.3. Nach Lemma 1.5.4 gilt $\varphi\gamma = \widetilde{I}^*\varphi$, also $\widetilde{I}^*\varphi(C) = \varphi\gamma(C)$. Nach (1) ist $\varphi\gamma(C)$ gleich $\widetilde{I}^*\varphi(C)$ ein Kreis vom $\Sigma(\mathbb{K}, \mathbb{A})$ durch $\mathbb{A}^*(1, 0)$. Da $\widetilde{I}^*$ eine involutorische Kreisverwandtschaft von $\Sigma(\mathbb{K}, \mathbb{A})$ ist, ist $\varphi(C)$ also ein Kreis von $\Sigma(\mathbb{K}, \mathbb{A})$ durch $\widetilde{I}(\mathbb{A}^*(1, 0)) = \mathbb{A}^*(0, 1) = \varphi(0)$.

(3) Im Fall einer Laguerre-Ebene haben wir $\varphi([0]_1) = \{A^*(n,1) \mid n \in [0]_1\}$ und $\varphi([\infty]_1) = \{A^*(1,n) \mid n \in [0]_1\}$. Damit sind also $\varphi([0]_1)$ und $\varphi([\infty]_1)$ Erzeugende von $\Sigma(\mathbb{K}, \mathbb{A})$.

Im Fall einer Minkowski-Ebene gilt $\varphi([0]_i) = \{A^*(n,1) \mid n \in [0]_i\} \cup \{A^*(\varepsilon_i, \varepsilon_j)\}$ für i, j mit $I = \{i, j\}$ und $\varphi[\infty]_i = \{A^*(1,n) \mid n \in [0]_i\} \cup \{A^*(\varepsilon_j, \varepsilon_i)\}$. Damit sind $\varphi([0]_i)$ und $\varphi([\infty]_i)$ Erzeugende von $\Sigma(\mathbb{K}, \mathbb{A})$.

(4) Aus (1),(2),(3) folgt nach Satz 1.3.2 , dass φ ein Isomorphismus ist. □

Zussamenfassend haben wir mit Satz 1.1.5 den Darstellungsatz für miquelsche Benz-Ebenen:

Satz 1.5.3 *Zu jeder miquelschen Benz-Ebene $\mathfrak{B}$, deren Ordnung mindestens $6 + 2|I|$ ist, gibt es bis auf Isomorphie genau eine quadratische Algebra $(\mathbb{A}, \mathbb{K})$, so dass $\mathfrak{B}$ isomorph ist zu $\Sigma(\mathbb{K}, \mathbb{A})$.* □

2 Anwendung der Benz-Ebenen in der Kryptologie

2.1 Grundlegende Begriffe

Die Kryptologie hat im wesentlichen drei Ziele, woraus sich folgende Aufgaben ergeben:

1 Entwicklung von Verschlüsselungsmethoden und ihre Sicherheit.

2 Bereitstellung von Verfahren, die es ermöglichen, gezielte Veränderungen von Daten zu erkennen und zu überprufen, ob Daten von einem autorisierten Absender stammen (Authentikation).

3 Methoden zu finden, durch die die Anonymität des Senders oder Empfängers einer Nachricht (gegenüber dritten oder auch gegenseitig) gewahrt wird.

Es seien M, C, K nicht-leere Mengen. Die Elemente von M bzw. C heißen *Klar-* bzw. *Geheimtexte*, die von K *Schlüssel*. Weiter sei $E : M \times K \to C$ und $D : C \times K \to M$ Abbildungen. (E, D) heißt *Krypto-* oder auch *Chiffriersystem*, wenn für jedes $k \in K$ und jedes $m \in M$ gilt $D(E(m, k), k) = m$.

Für $k \in K$ nennen wir die Abbildung $E_k : M \to C,\ m \mapsto E(m, k)$ *Verschlüsselungsfunktion* zum Schlüssel k und die Abbildung $D_k : C \to M,\ c \mapsto D(c, k)$ *Entschlüsselungsfunktion* zum Schlüssel k. Damit ist (E, D) genau dann ein Chiffriersystem, wenn für all $k \in K$ gilt $D_k \circ E_k = id_M$, d.h. in einem Chiffriersystem (E, D) sind die Abbildungen $E_k : M \to C$ alle injekiv und die Abbildungen $D_k : C \to M$ surjektiv.

Unter diese allgemeine Definition eines Chiffriersystems fällt eine Fülle von Beispielen. Wir erwähnen hier nur einige der bekanntesten Beispiele wie das Vernam-Chiffriersystem [30], den RSA-Algoritmus von Rivest, Schamir und Aldeman [24], das (DES) Chiffriersystem „Data Encryption Standard“ [2] und das ElGamal Chiffriersystem [8].

Eine spezielle Klasse sind die perfekten Chiffriersysteme (vgl. [4]). Ein Chiffriersystem (E, D) heißt *perfekt*, wenn für alle $m \in M$ und alle $c \in C$ gilt

$$\frac{|\{E_k \mid k \in K, E_k(m) = c\}|}{\Sigma_{x \in M}|\{E_k \mid k \in K, E_k(x) = c\}|} = \frac{1}{|M|}$$

Perfekte Chiffriersysteme erhält man z.B. mit Hilfe von transitiven Permutationsgruppen. Es sei (P, Γ) eine Permutationsgruppe, d.h. P ist eine nicht-leere Menge und Γ eine Untergruppe der symmetrischen Gruppe von P. Wir wählen $n \in \mathbb{N}$ und setzen $M := P^n =: C$. Es seien $K := \Gamma^n$,

$E : M \times K \to C;\ ((a_1, ..., a_n), (\sigma_1, ..., \sigma_n)) \mapsto (\sigma_1(a_1), ..., \sigma_n(a_n))$ und

$D : C \times K \to C; ((a_1, ..., a_n), (\sigma_1, ..., \sigma_n)) \mapsto (\sigma_1^{-1}(a_1), ..., \sigma_n^{-1}(a_n))$.

Dann ist $\mathcal{C}(P, \Gamma, n) := (E, D)$ ein Chiffriersystem, da die Abbildungen

$\sigma_i : P \to P; x \mapsto \sigma_i(x)$ bijektiv sind.

Lemma 2.1.1 *Für jede transitive Permutationsgruppe (P, Γ) ist $\mathcal{C}(P, \Gamma, n)$ ein perfektes Chiffriersystem.*

Beweis. Es genügt den Fall $n = 1$ zu betrachten. Es seien $a, b \in M$ sowie $\gamma \in \Gamma$ mit $\gamma(a) = b$. Für die Standuntergruppen Γ_a und Γ_b gilt dann $\Gamma_b = \gamma\Gamma_a\gamma^{-1}$ (vgl. etwa [22], Aufgabe 2.12 a). Weiter gilt $\gamma\Gamma_a = \{\sigma \in \Gamma \mid \sigma(a) = b\} = \{E_k \mid\ k \in K,\ E_k(a) = b\}$.

Für jedes $x \in P$ gilt damit $N(x, b) := |\{E_k \mid k \in K, E_k(x) = b\}| = |\Gamma_x| = |\Gamma_b|$ und $\Sigma_{x \in M}|\{E_k \mid k \in K, E_k(x) = b\}| = |M||\Gamma_b|$, folglich gilt

$$\frac{N(a, b)}{\Sigma_{x \in M} N(x, b)} = \frac{1}{|M|}$$

□

Transitive Permutationsgruppen findet man vor allem in der Geometrie.

Z.B. operiert die von den Drehstreckungen einer miquelschen Benz-Ebene erzeugte Gruppe Δ transitiv auf der Punktmenge. Für zwei feste Punkte $0, \infty$ ist das

Komplement $P^\infty \cap P^0$ der Erzeugenden durch $0, \infty$ eine Bahn der Standuntergruppe $\Delta_{0,\infty}$. Nach Satz 1.5.1 entspricht dieser Gruppe die der Linksmultiplikationen mit Einheiten der zugehörigen quadratischen Algebra. Nach Satz 1.4.8 operiert $\Delta_{0,\infty}$ transitiv auf $P^\infty \cap P^0$. Damit erhalten wir nach Lemma 2.1.1 als unser erstes Chiffriersystem $\mathcal{C}(P^\infty \cap P^0, \Delta_{0,\infty}, n)$ ein perfektes Chiffriersystem.

An ein Chiffriersystem stellt man heutzutage hohe Anforderungen (vgl [5], [9])

Auch wenn der verwendete Algorithmus bekannt ist, darf der Schlüssel nicht bestimmbar sein, wenn

1 eine gewisse Anzahl von Geheimtexten (known ciphertext attack) oder

2 eine Anzahl von Klartexten und korrespondierenden Geheimtexten (known plaintext attack) oder

3 zu einer Anzahl von freiwählbaren Klartexten die korrespondierenden Geheimtexte (chosen plaintext attack)

bekannt sind.

Hier ist zu bemerken, dass perfekte Chiffriersysteme dem „known ciphertext attack“ nicht Stand zu halten brauchen, z.B kann man bei der Vernam-Chiffre aus einem Klartext und korrespondierenden Geheimtext sofort den Schlüssel berechnen.

Da für scharf n-fach transitive Permutationgruppen (P, Γ) die Schlüsselmenge Γ^n regulär auf der Menge $P^{(n)}$ [11] operiert, ist auch das perfekte Chiffriersystem $\mathcal{C}(P, \Gamma, n)$ einem „known plaintext attack“ - Angriff nicht gewachsen.

2.2 Entwurf des Chiffriersystems $C(\mathbb{L}, f, \pi)$

Es sei $\mathfrak{B} = \Sigma(\mathbb{K}, \mathbb{L})$ eine Benz-Ebene über der quadratischen Algebra $(\mathbb{L}, \mathbb{K})$. Die von den Drehstreckungen von $\mathfrak{B}$ erzeugte Gruppe von Automorphismen ist die

[11] Für eine Menge M und $n \in \mathbb{N}$ sei $M^{(n)} := \{(x_1, ..., x_n) \in M^n \mid |\{x_1, ..., x_n\}| = n\}$.

projektive lineare Gruppe $\mathrm{PGL}(2,\mathbb{L})$.

Da $\mathrm{PGL}(2,\mathbb{L})$ transitiv auf der Punktmenge $P(\mathbb{L})$ von $\mathfrak{B}$ operiert, erhält man nach Lemma 2.1.1 ein perfektes Chiffriersystem mit $P(\mathbb{L})$ als Klar- und Geheimtextmenge sowie $\mathrm{PGL}(2,\mathbb{L})$ als Schlüsselmenge. Allerdings hält dieses System einem Angriff der Art „known plaintext attack“ nicht stand, denn da $\mathrm{PGL}(2,\mathbb{L})$ regulär auf den Tripeln (a,b,c) paarweise verbindbarer Punkte a,b,c operiert, ist der Schlüssel γ aus der Kenntnis eines Klartexttripels (a,b,c) und zugehörigen Geheimtexttripels $(\gamma(a),\gamma(b),\gamma(c))$ zu berechnen.

Im folgenden modifizieren wir das oben erwähnte Chiffriersystem. Zur Konstruktion wenden wir zwei allgemeine Prinzipien an (vgl. [23] Seite 145).

1. **Konfusion:** Der Zusammenhang zwischen Geheimtext und Schlüssel wird verkompliziert.
2. **Diffusion:** Die im Klartext enthaltene Information wird über die ganze Länge des Textes verschmiert.

Es seien $\lambda \in \mathbb{L}^*$ eine Einheit und $a,b \in \mathbb{L}$ mit $a-b \in \mathbb{L}^*$. Dann gilt

$$(b-\lambda a)(\lambda b-a)-(1-\lambda)(\lambda-1)ab = \lambda(a-b)^2 \in \mathbb{L}^*$$

Daher wird durch die Matrix

$$\mathfrak{B} := \begin{pmatrix} b-\lambda a & 1-\lambda \\ (\lambda-1)ab & \lambda b-a \end{pmatrix}$$

eine Abbildung $\delta_{\lambda,a,b} := \widetilde{\mathfrak{B}} \in \mathrm{PGL}(2,\mathbb{L})$ induziert (vgl. Seite 14). Es gilt dann:

1. $\delta_{\lambda,a,b}^{-1} = \delta_{\lambda,b,a}$

2. Für $\lambda \neq 1$ hat $\delta_{\lambda,a,b}$ genau die beiden Fixpunkte $\mathbb{L}^*(a,1)$ und $\mathbb{L}^*(b,1)$.

3. $\delta_{1,a,b} = id$

Bemerkung. Mit der Einbettung $\iota : \mathbb{L} \to P(\mathbb{L}),\ a \mapsto \mathbb{L}^*(a,1)$ gilt für $x \in P(\mathbb{A}) \setminus ([a] \cup [b]) : \lambda = Dv(a,b,x,\delta_{\lambda,a,b}(x))$, wobei Dv das *Dopelverhältnis* von $P(\mathbb{L})$ bezeichnet (vgl.[3]).

Wir setzen $\mathbb{L}^{[2]} := \{(a,b) \in \mathbb{L}^2 \mid a - b \in \mathbb{L}^*\}$.

Für unser Chiffriersystem benötigen wir eine Abbildung $f : P(\mathbb{L}) \to \mathbb{N}$ und eine Abbildung $\pi : P(\mathbb{L}) \to \mathbb{L}$. Beide Abbildungen können ganz beliebig sein.

Als Klartext- und auch als Geheimtextmenge nehmen wir $M := \bigcup_{2 \le n} P(\mathbb{L})^n =: C$, und vorläufig sei die Schlüsselmenge

$$K_v := (\mathrm{PGL}(2,\mathbb{L}))^2 \times (\mathbb{L}^* \setminus \{1\})^2 \times \mathbb{L}^{[2]} \times \mathbb{L}^{[2]} \times \{1, ..., |\mathbb{L}^*|\}$$

Für $k = (\gamma, \sigma, \lambda, \mu, a, b, c, d, q) \in K_v$ wird die Verschlüsselungsfunktion E_k definiert durch folgenden **Verschlüsselungsalgorithmus**:

Für $x \in P(\mathbb{L})$ sei $f_q(x) \in \{1, ..., q\}$ mit $f_q(x) - 1 \equiv f(x)\ mod\ q$.

Es sei $m = (m_0, ...m_n) \in M$ ein Klartext. Wir setzen

$$m_0' := \gamma \circ \delta_{\lambda,a,b}(m_0)$$

Für $i = 1, 2, ...$ sei

$$m_{2i-1}' := \begin{cases} \gamma^{2i}\delta_{\lambda,a,\pi(m_{2i-2}')}(m_{2i-1}) & falls \quad a - \pi(m_{2i-2}') \in \mathbb{L}^* \\ \gamma^{2i}\delta_{\lambda,a,b}(m_{2i-1}) & falls \quad a - \pi(m_{2i-2}') \notin \mathbb{L}^* \end{cases}$$

und

$$m_{2i}' := \begin{cases} \gamma^{2i+1}\delta_{\lambda,b,\pi(m_{2i-1}')}(m_{2i}) & falls \quad b - \pi(m_{2i-1}') \in \mathbb{L}^* \\ \gamma^{2i+1}\delta_{\lambda,b,a}(m_{2i}) & falls \quad b - \pi(m_{2i-1}') \notin \mathbb{L}^* \end{cases}$$

Weiter sei

$$m_0'' := \begin{cases} \sigma^{f_q(m_n')}\delta_{\mu,d,\pi(m_n')}(m_0') & falls \quad d - \pi(m_n') \in \mathbb{L}^* \\ \sigma^{f_q(m_n')}\delta_{\mu,d,c}(m_0') & falls \quad d - \pi(m_n') \notin \mathbb{L}^* \end{cases}$$

und für $i = 1, 2, ...$ sei

$$m''_{2i-1} := \begin{cases} \sigma^{f_q(m''_{2i-2})}\delta_{\mu,c,\pi(m''_{2i-2})}(m'_{2i-1}) & falls \quad c - \pi(m''_{2i-2}) \in \mathbb{L}^* \\ \sigma^{f_q(m''_{2i-2})}\delta_{\mu,c,d}(m'_{2i-1}) & falls \quad c - \pi(m''_{2i-2}) \notin \mathbb{L}^* \end{cases}$$

und

$$m''_{2i} := \begin{cases} \sigma^{f_q(m'_{2i-1})}\delta_{\mu,d,\pi(m'_{2i-1})}(m'_{2i}) & falls \quad d - \pi(m'_{2i-1}) \in \mathbb{L}^* \\ \sigma^{f_q(m'_{2i-2})}\delta_{\mu,d,c}(m'_{2i}) & falls \quad d - \pi(m'_{2i-1}) \notin \mathbb{L}^* \end{cases}$$

Dann ist $E_k(m_0, ..., m_n) := (m''_0, ..., m''_n)$ die Verschlüsselung von $(m_0, ..., m_n)$.

Die Entschlüsselungsfunktion D_k wird ebenfalls in zwei Schritten definiert durch den **Entschlüsselungsalgorithmus** :

Es sei $(c_0, ..., c_n) \in C$. Für $i = 1, 2, ...$ setzen wir

$$c'_{2i-1} := \begin{cases} \delta_{\mu,\pi(c_{2i-2}),c}\ \sigma^{-f_q(c_{2i-2})}(c_{2i-1}) & falls \quad c - \pi(c_{2i-2}) \in \mathbb{L}^* \\ \delta_{\mu,d,c}\ \sigma^{-f_q(c_{2i-2})}(c_{2i-1}) & falls \quad c - \pi(c_{2i-2}) \notin \mathbb{L}^* \end{cases}$$

und

$$c'_{2i} := \begin{cases} \delta_{\mu,\pi(c'_{2i-1}),d}\ \sigma^{-f_q(c'_{2i-1})}(c_{2i}) & falls \quad d - \pi(c'_{2i-1}) \in \mathbb{L}^* \\ \delta_{\mu,c,d}\ \sigma^{-f_q(c'_{2i-1})}(c_{2i}) & falls \quad d - \pi(c'_{2i-1}) \notin \mathbb{L}^* \end{cases}$$

Weiter sei

$$c'_0 := \begin{cases} \delta_{\mu,\pi(c'_n),d}\ \sigma^{-f_q(c'_n)}(c_0) & falls \quad d - \pi(c'_n) \in \mathbb{L}^* \\ \delta_{\mu,c,d}\ \sigma^{-f_q(c'_n)}(c_0) & falls \quad d - \pi(c'_n) \notin \mathbb{L}^* \end{cases}$$

$$c''_0 := \delta_{\lambda,b,a}\ \gamma^{-1}(c'_0)$$

und für $i = 1, 2, ...$ sei

$$c''_{2i-1} := \begin{cases} \delta_{\lambda,\pi(c'_{2i-2}),a}\ \gamma^{-2i}(c'_{2i-1}) & falls \quad a - \pi(c'_{2i-2}) \in \mathbb{L}^* \\ \delta_{\lambda,b,a}\ \gamma^{-2i}(c'_{2i-1}) & falls \quad a - \pi(c'_{2i-2}) \notin \mathbb{L}^* \end{cases}$$

und

$$c''_{2i} := \begin{cases} \delta_{\lambda,\pi(c'_{2i-1}),b}\ \gamma^{-2i-1}(c'_{2i}) & falls \quad b - \pi(c'_{2i-1}) \in \mathbb{L}^* \\ \delta_{\lambda,a,b}\ \gamma^{-2i-1}(c'_{2i}) & falls \quad b - \pi(c'_{2i-1}) \notin \mathbb{L}^* \end{cases}$$

Dann ist $D_k(c_0, ..., c_n) := (c''_0, ..., c''_n)$ die Entschlüsselung von $(c_0, ..., c_n)$.

Nach Konstruktion gilt $D_k \circ E_k = id_M = E_k \circ D_k$, d.h. D_k und E_k sind zueinander inverse Bijektionen. Damit ist $\mathcal{C}(\mathbb{L}, f, \pi) := (E, D)$ ein Chiffriersystem.

Durch die Abbildungen $\delta_{\nu,v,u}$ aus $\mathrm{PGL}(2, \mathbb{L})$ und die Abbildung f_q zur Berechnung der Exponenten wird das am Anfang erwähnte mit der $\mathrm{PGL}(2, \mathbb{L})$ erklärte Chiffriersystem sowohl verkompliziert als auch über den gesamten Klartext verschmiert.

Bemerkungen. Die Parameter a, b in $\delta_{\lambda,a,b}$ sind im Grunde genommen die Punkte $\mathbb{L}^*(a, 1), \mathbb{L}^*(b, 1)$. Die ursprüngliche Idee für unseren Algorithmus war $\mathbb{L}^*(a, 1)$ und $\mathbb{L}^*(b, 1)$ abwechselned durch die m'_i zu ersetzen. Da wir $\delta_{\lambda,a,b}$ aber nur für *„eigentliche“* Punkte $\mathbb{L}^*(a, 1)$ und $\mathbb{L}^*(b, 1)$ definiert haben, benötigen wir die Abbildung π, die den *„uneigentlichen“* Punkten $\mathbb{L}^*(1, 0)$ usw. Elemente aus $\mathbb{L}$ zuordnet.

Für unsere Programme haben wir im Hinblick auf eine möglichst einfache Implementierung als Grudkörper $\mathbb{K}$ nur Primkörper einer Charakteristik $p \neq 2$ benutzt und dabei $\mathbb{K} = \mathbb{Z}_p$ mit $\{0, 1, ..., p-1\} \subseteq \mathbb{N}$ identifiziert. Weiterhin haben wir die Algebra $\mathbb{L}$ mit $\mathbb{K} \times \mathbb{K}$ identifiziert [12], so dass gegebenfalls das Ideal $N_1 = \{0\} \times \mathbb{K}$ und das Ideal $N_2 = \mathbb{K} \times \{0\}$ ist.

In den Programmen werden folgende Abbildungen π und f benutzt:

[12] Die zur Identifikation benötigte Basis spielt an dieser Stelle keine Rolle. Die genaue Darstellung von $\mathbb{L}$ ist auf Seite 82 angegeben.

$$\pi : P(\mathbb{L}) \to \mathbb{L},\ \mathbb{L}^*(u,v) \mapsto \begin{cases} v^{-1}u & falls \quad v \in \mathbb{L}^* \\ (2,0) + u^{-1}v & falls \quad v \in N_1, u \in \mathbb{L}^* \\ (1,0) + u^{-1}v & falls \quad v \in N_2 \setminus \{0\}, u \in \mathbb{L}^* \\ (0,1) & falls \quad u \in N_2, v \in N_1 \\ (0,2) & falls \quad u \in N_1, v \in N_2 \end{cases}$$

Mit den Projektionen $\pi_i : \mathbb{K} \times \mathbb{K} \to \mathbb{K}, (x_1, x_2) \mapsto x_i, i \in \{1,2\}$ definieren wir:

$$f : P(\mathbb{L}) \to \mathbb{N},\ \mathbb{L}^*(u,v) \mapsto \begin{cases} \pi_1(uv^{-1}) + \pi_2(uv^{-1}) \cdot p & falls \quad v \in \mathbb{L}^* \\ p^2 + \pi_2(vu^{-1}) & falls \quad v \in N_1, u \in \mathbb{L}^* \\ p^2 + p + \pi_2(vu^{-1}) & falls \quad v \in N_2 \setminus \{0\}, u \in \mathbb{L}^* \\ p^2 + 2 \cdot p & falls \quad u \in N_2, v \in N_1 \\ p^2 + p & falls \quad u \in N_1, v \in N_2 \end{cases}$$

2.3 Bemerkungen zur Kryptoanalyse des Chiffriersystem $C(\mathbb{L}, f, \pi)$

Zunächst einmal wollen wir die Klar- und Geheimtextmenge $M = C$ sowie die Schlüsselmenge K_v abzählen.

Für die projektive Gerade $P(\mathbb{L})$ über der quadratischen Algebra $(\mathbb{L}, \mathbb{K})$ gilt:

$$|P(\mathbb{L})| = \begin{cases} |\mathbb{K}|^2 + 1 & falls\ \mathbb{L}\ ein\ Körper\ ist \\ (|\mathbb{K}| + 1)|\mathbb{K}| & falls\ \mathbb{L}\ die\ Algebra\ der\ Dualzahlen\ ist \\ (|\mathbb{K}| + 1)^2 & falls\ \mathbb{L}\ die\ Algebra\ der\ anormal-komplexen\ Zahlen\ ist \end{cases}$$

Damit können wir also die Klartextmengen $M_n := P(\mathbb{L})^n$ mit Texten der Länge $n \geq 2$ abzählen.

Um die Schlüsselmenge K_v abzuzählen, müssen wir zunächst die Ordnung der projektiven linearen $\mathrm{PGL}(2, \mathbb{L})$ bestimmen. Nach Definition sind die Elemente von $\mathrm{PGL}(2, \mathbb{L})$ Klassen von 2×2-Matrizen über $\mathbb{L}$ (vgl. §1.1). Für die Implementierung des oben entworfenen Chiffriersystems $C(\mathbb{L}, f, \pi)$ ist ebenso wie für das Abzählen die Angabe eines Repräsentantensystem zweckmäßig.

Für $\mathfrak{C} = \binom{a\ b}{c\ d} \in M_{2,2}(\mathbb{L})$ mit $ad - bc \in \mathbb{L}^*$ gilt $a \in \mathbb{L}^*$ oder $c \in \mathbb{L}^*$. Daher lassen sich die Abbildungen aus $\mathrm{PGL}(2, \mathbb{L})$ umkehrbar eineindeutig durch Matrizen der Form $\binom{1\ b}{c\ d}$ mit $(b, c) \in \mathbb{L}^2$ und $d \in \mathbb{L}^* + bc$ und $\binom{a\ b}{1\ d}$ mit $a \in \mathbb{L} \setminus \mathbb{L}^*, d \in \mathbb{L}$ und $b \in \mathbb{L}^* + ad$ repräsntieren. Damit ergibt sich:

$$|\mathrm{PGL}(2, \mathbb{L})| = |\mathbb{L}|^2 |\mathbb{L}^*| + (|\mathbb{L}| - |\mathbb{L}^*|)|\mathbb{L}||\mathbb{L}^*| = (2|\mathbb{L}| - |\mathbb{L}^*|)|\mathbb{L}||\mathbb{L}^*|.$$

Bemerkung. Falls $\mathbb{L}$ ein Körper ist, so gilt $|\mathrm{PGL}(2, \mathbb{L})| = (|\mathbb{L}| - 1)|\mathbb{L}||\mathbb{L} + 1|$ (vgl. z.B. [10] Seite 206).

Damit ergibt sich für die vorläufige Schlüsselmenge K_v:

$(*)$ $|K_v| = (2|\mathbb{L}| - |\mathbb{L}^*|)^2 |\mathbb{L}|^4 |\mathbb{L}^*|^5 (|\mathbb{L}^*| - 1)^2$

Für einen Klartext $\mathfrak{m} \in P(\mathbb{L})^n$ und einen Geheimtext $\mathfrak{c} \in P(\mathbb{L})^n$ bezeichne $\#(\mathfrak{m}, \mathfrak{c}) := |\{k \in K_v |\ E_k(\mathfrak{m}) = \mathfrak{c}\}|$ die Anzahl der Schlüssel, die bei der Verschlüsselung von $\mathfrak{m}$ den Geheimtext $\mathfrak{c}$ liefern und

$$d_{\mathfrak{m}}(n) = \frac{1}{|P(\mathbb{L})|^n} \sum_{\mathfrak{c} \in P(\mathbb{L})^n} \#(\mathfrak{m}, \mathfrak{c}) = \frac{K_v}{|P(\mathbb{L})|^n}$$

den Durchschnitt dieser Anzahlen.

Mit $(*)$ ergibt sich:

$(**)$ $\qquad d_{\mathfrak{m}}(n) \geq \frac{(|\mathbb{L}^*|-1)^{13}}{|P(\mathbb{L})|^n} \geq \frac{(|\mathbb{K}^*|^2-1)^{13}}{(|\mathbb{K}|+1)^{2n}}$

Bei einem Angriff von der Art „known plaintext attack“ stehen dem Angreifer Klar-Geheimtext-Paare zur Verfügung. Für einen Klartext $\mathfrak{m} = (m_0, ..., m_n) \in P(\mathbb{L})^{n+1}$ sei also der Geheimtext $\mathfrak{m}'' = (m_0'', ..., m_n'')$ bekannt. Will man aus der Kenntnis von $(\mathfrak{m}, \mathfrak{m}'')$ den Schlüssel $k = (\gamma, \sigma, \lambda, \mu, a, b, c, d, q) \in K_v$ berechnen, so erhält man, indem man wie bei der Entschlüsselung vorgeht, folgendes Gleichungssystem:

Für $i = 1, 2, ...$ haben wir die Gleichungen:

$$m'_{2i-1} := \begin{cases} \delta_{\mu,\pi(m''_{2i-2}),c}\ \sigma^{-f_q(m''_{2i-2})}(m_{2i-1}) & falls \quad c - \pi(m''_{2i-2}) \in \mathbb{L}^* \\ \delta_{\mu,d,c}\ \sigma^{-f_q(m''_{2i-2})}(m''_{2i-1}) & falls \quad c - \pi(m''_{2i-2}) \notin \mathbb{L}^* \end{cases}$$

$$m'_{2i} := \begin{cases} \delta_{\mu,\pi(m'_{2i-1}),d}\ \sigma^{-f_q(m'_{2i-1})}(m''_{2i}) & falls \quad d-\pi(m'_{2i-1}) \in \mathbb{L}^* \\ \delta_{\mu,c,d}\ \sigma^{-f_q(m'_{2i-1})}(m''_{2i}) & falls \quad d-\pi(m'_{2i-1}) \notin \mathbb{L}^* \end{cases}$$

$$m'_0 := \begin{cases} \delta_{\mu,\pi(m'_n),d}\ \sigma^{-f_q(m'_n)}(m''_0) & falls \quad d-\pi(m'_n) \in \mathbb{L}^* \\ \delta_{\mu,c,d}\ \sigma^{-f_q(m'_n)}(m''_0) & falls \quad d-\pi(m'_n) \notin \mathbb{L}^* \end{cases}$$

$$m_0 := \delta_{\lambda,b,a}\ \gamma^{-1}(m'_0)$$

$$m_{2i-1} := \begin{cases} \delta_{\lambda,\pi(m'_{2i-2}),a}\ \gamma^{-2i}(m'_{2i-1}) & falls \quad a-\pi(m'_{2i-2}) \in \mathbb{L}^* \\ \delta_{\lambda,b,a}\ \gamma^{-2i}(m'_{2i-1}) & falls \quad a-\pi(m'_{2i-2}) \notin \mathbb{L}^* \end{cases}$$

und

$$m_{2i} := \begin{cases} \delta_{\lambda,\pi(m'_{2i-1}),b}\ \gamma^{-2i-1}(m'_{2i}) & falls \quad b-\pi(m'_{2i-1}) \in \mathbb{L}^* \\ \delta_{\lambda,a,b}\ \gamma^{-2i-1}(m'_{2i}) & falls \quad b-\pi(m'_{2i-1}) \notin \mathbb{L}^* \end{cases}$$

Schon die beiden Fälle für m'_i bzw. m_i, die ja von den Unbekannten a, b, c, d abhängen, führen auf eine Fülle von Fallunterscheidungen.

Da es verhältnismäßig sehr viel weniger Nichteinheiten als Einheiten gibt, ist natürlich bei den beiden Fällen für m'_i, m_i der obere jeweils der wahrscheinlichere (die Wahrscheinlichkeit für den oberen Fall ist $\frac{|\mathbb{L}^*|}{|\mathbb{L}|}$, die für den unteren $\frac{|\mathbb{L}\setminus\mathbb{L}^*|}{|\mathbb{L}|}$).

Aber selbst wenn man sich deshalb zunächst bei der Aufstellung des Gleichungssystems nur auf diesen Hauptfall (d.h. jeweils nur den oberen Fall) beschränkt, so ergeben sich aus der Tatsache, dass die Exponenten $-f_q(m''_{2i-2}),\ -f_q(m'_{2i-1}),\ -f_q(m'_n)$ nicht bekannt sind, weitere Fallunterscheidungen. Erschwerend kommt hier noch hinzu, dass nicht einmal die Berechnung von $f(m'_{2i-1}),\ f(m'_n)$ möglich ist, da in $m'_{2i-1},\ m'_n$ schon die Unbekanten eingehen. Für jede Wahl der Exponenten $-f_q(m''_{2i-2}),\ -f_q(m'_{2i-1}),\ -f_q(m'_n)$ ergibt sich ein nicht-lineares System algebraischer Gleichungen, wobei noch zu beachten ist, dass sowohl die Koeffizienten als auch die Lösungen in einer quadratischen Algebra, also nicht notwendig in einem Körper liegen.

Wegen der Kompliziertheit dieses Ansatzes und der wachsenden Ordnung wird ein Angreifer bei einem Angriff der Art „chosen plaintext attack “ wohl zunächst Klartexte der Länge 2, d.h. mit $n = 1$ wählen. Nach $(**)$ gibt es dann aber zu $(\mathfrak{m}, \mathfrak{m}'')$ mit $|\mathbb{K}| = p$ im Durchschnitt mindestens $d_{\mathfrak{m}}(2) \geq \frac{(p^2-2p)^{13}}{(p^2+2p+1)^2}$ Schlüssel k mit $D_k(\mathfrak{m}'') = \mathfrak{m}$.

Für $p \geq 5$ gilt $d_{\mathfrak{m}}(2) \geq p^{10}(p-2)^{10}$. Auch wenn man eine ganze Folge von Paaren $(\mathfrak{m}_i, \mathfrak{m}_i'') \in P(\mathbb{L})^2 \times P(\mathbb{L})^2$ zur Verfügung hat, dürfte es wegen der oben geschilderten Schwierigkeiten für einen Ansatz unmöglich sein, den Schlüssel k zu bestimmen. Eine Berechnung des Schlüssels k scheint damit aussichtslos zu sein.

Es erhebt sich nun die Frage, ob statistische Betrachtungen bei der Suche nach dem Schlüssel eingesetzt werden können. Will man dazu die „Bahnen “$B(\mathfrak{m}) := \{E_k(\mathfrak{m})|\ k \in K_v\}$[13]einzelner Klartexte $\mathfrak{m}$ bestimmen, so muß man sich wegen der Größe der Schlüsselmenge auf Algebren $\mathbb{L}$ mit kleiner Elementzahl beschränken. Selbst für $\mathbb{K} = \mathbb{Z}_3$, also $\mathbb{L} = 9$ ergibt sich noch eine Schlüsselmenge K_v mit

$$|K_v| = \begin{cases} (720)^2 \cdot 49 \cdot 81 \cdot 64 \cdot 8 & \textit{falls } \mathbb{L} \textit{ ein Körper ist} \\ (648)^2 \cdot 25 \cdot 81 \cdot 36 \cdot 6 & \textit{falls } \mathbb{L} \textit{ die Algebra der Dualzahlen ist} \\ (504)^2 \cdot 9 \cdot 81 \cdot 16 \cdot 4 & \textit{falls } \mathbb{L} \textit{ die Algebra der anormal-komplexen Zahlen ist} \end{cases}$$

d.h. $|K_v| \geq 11\ 851\ 370\ 496$. Da $\mathbb{K}$ in $\mathbb{L}$ eingebettet ist, gilt für $q \in \{1, ..., |\mathbb{L}^*|\}$

$K_0 := (\mathrm{PGL}(2, \mathbb{K}))^2 \times (\mathbb{K}^* \setminus \{1\})^2 \times \mathbb{K}^{[2]} \times \mathbb{K}^{[2]} \times \{q\} \subseteq K_v$ und $P(\mathbb{K}) \subseteq P(\mathbb{L})$ (vgl. §1.5). Falls $\mathbb{L}$ ein Körper ist so gilt $\pi(P(\mathbb{K})) \subseteq \mathbb{K}$. Daher betrachten wir hier in folgenden nur den Fall, dass $\mathbb{L}$ ein Körper ist. Für die beiden anderen Algebren, müßte π abgeändert werden, damit $\pi(P(\mathbb{K})) \subseteq \mathbb{K}$ gilt.

Für $k \in K_0$ und $n \in \mathbb{N}, n \geq 2$ gilt dann $E_k(P(\mathbb{K})^n) = P(\mathbb{K})^n$. Mit $p = |\mathbb{K}|$ gilt $|K_0| = (p+1)^2 p^4 (p-1)^4 (p-2)^2$, also $|K_0| = \begin{cases} 20736 & \textit{für } p = 3 \\ 51\ 840\ 000 & \textit{für } p = 5 \end{cases}$

Für die Fälle $\mathbb{K} = \mathbb{Z}_3$ und $\mathbb{K} = \mathbb{Z}_5$ wurden für den Klartext $\mathfrak{m} = (\mathbb{K}^*(0,1), \mathbb{K}^*(0,1))$ die Anzahlen $\#(\mathfrak{c}) = |\{k \in K_0|\ E_k(\mathfrak{m}) = \mathfrak{c}\}|,\ \mathfrak{c} \in P(\mathbb{K})^2 =: T$ berechnet. In den folgenden Tabellen wird für $x \in \mathbb{K}$ der Punkt $\mathbb{K}^*(x, 1)$ mit x 1 und der Punkt $\mathbb{K}^*(1, 0)$ mit 2 0 bezeichnet. Für den Klartext $\mathfrak{m} = 0\ 1\ \ 0\ 1$ steht neben dem Geheimtext $\mathfrak{c} = x_1 i_1\ x_2 i_2$ die Anzahl $\#(\mathfrak{c})$.

[13]Die Menge $\{E_k|\ k \in K_v\}$ ist aber keine Gruppe.

Text	#	Text	#	Text	#	Text	#
01 01	1843	11 01	1471	21 01	1429	20 01	1361
01 11	1056	11 11	895	21 11	1390	20 11	1237
01 21	1108	11 21	1371	21 21	960	20 21	1240
01 20	1105	11 20	1447	21 20	1405	20 20	1418

Tabelle 1: $p = 3,\ q = 5,\ \bar{x} = 1296,\ S = 234.59.$

Text	#	Text	#	Text	#	Text	#
01 01	1873269	11 01	1478996	21 01	1466303	31 01	1473131
41 01	1443029	20 01	1448446	01 11	1364784	11 11	1205914
21 11	1500849	31 11	1492643	41 11	1484968	20 11	1479657
01 21	1370842	11 21	1486014	21 21	1215458	31 21	1476039
41 21	1499495	20 21	1432314	01 31	1365330	11 31	1495261
21 31	1493562	31 31	1056959	41 31	1495722	20 31	1471634
01 41	1375845	11 41	1464562	21 41	1504104	31 41	1479244
41 41	1214986	20 41	1474690	01 20	1360370	11 20	1490653
21 20	1494044	31 20	1473584	41 20	1483200	20 20	1454099

Tabelle 2: $p = 5,\ q = 5,\ \bar{x} = 1439999.875,\ S = 126874.48.$

Die Tabellen 1 und 2 zeigen, dass $\#(\mathfrak{c})$ nicht konstant ist, d.h. das Chiffriersystem $C(\mathbb{L}, f, \pi)$ ist nicht perfekt.

Es seien $\bar{x} := \frac{1}{|T|} \sum_{\mathfrak{c} \in T} \#(\mathfrak{c}) = d_{\mathfrak{m}}(2)$ der Durchschnitt und $S := \sqrt{\frac{1}{|T|-1} \sum_{\mathfrak{c} \in T} (\#(\mathfrak{c}) - \bar{x})^2}$ die Standardabweichung.

Bezeichnen wir die Texte $\mathfrak{c} \in T$, für die $\#(\mathfrak{c})$ nicht zwischen $\bar{x} - 2s$ und $\bar{x} + 2s$ liegt als *Ausreißer*, so ersehen wir aus den Tabellen, dass es jeweils genau einen Ausreißer $\mathfrak{c}_0$ gibt.

Um eine günstigere, d.h. gleichmäßigere Verteilung der Anzahlen $\#(\mathfrak{c})$ zu erreichen, kann man nun versuchen, die vorläufige Schlüsselmenge K_v zu modifizieren.

Als erstes lassen wir alle Schlüssel $k = (\gamma, \sigma, \lambda, \mu, a, b, c, d, q)$ mit $\gamma = id = \sigma$ weg. Wir nehmen also als neue Schüsselmenge $K' = \{k = (\gamma, \sigma, \lambda, \mu, a, b, c, d, q) \in K_v |\ \gamma \neq id$ oder $\sigma \neq id\}$. Für die entsprechend modifizierte Schlüsselmenge K'_0 gilt: $|K'_0| = ((p+1)^2 p^2 (p-1)^2 - 1) p^2 (p-1)^2 (p-2)^2$ also

$$|K'_0| = \begin{cases} 20\ 700 & für\ p = 3 \\ 51\ 836\ 400 & für\ p = 5 \end{cases}$$

Text	#	Text	#	Text	#	Text	#
01 01	1819	11 01	1469	21 01	1429	20 01	1361
01 11	1054	11 11	895	21 11	1390	20 11	1237
01 21	1104	11 21	1367	21 21	960	20 21	1240
01 20	1105	11 20	1447	21 20	1405	20 20	1418

Tabelle 3: $p = 3,\ q = 5,\ \bar{x} = 1293.75,\ S = 231.08.$

Text	#	Text	#	Text	#	Text	#
01 01	1871829	11 01	1478916	21 01	1466239	31 01	1473077
41 01	1442947	20 01	1448404	01 11	1364711	11 11	1205914
21 11	1500774	31 11	1492550	41 11	1484881	20 11	1479595
01 21	1370763	11 21	1485939	21 21	1215458	31 21	1475970
41 21	1499430	20 21	1432254	01 31	1365235	11 31	1495170
21 31	1493491	31 31	1056959	41 31	1495649	20 31	1471567
01 41	1375750	11 41	1464501	21 41	1504027	31 41	1479153
41 41	1214986	20 41	1474633	01 20	1360312	11 20	1490600
21 20	1493981	31 20	1473531	41 20	1483147	20 20	1454057

Tabelle 4: $p = 5,\ q = 5,\ \bar{x} = 1439899.875,\ S = 126724.80.$

Wie die Tabellen 3 und 4 für $\mathbb{K} = \mathbb{Z}_3$ und $\mathbb{K} = \mathbb{Z}_5$ zeigen, bewirkt die Modifikation schon eine Verbesserung. Zwar ist $\mathfrak{c}_0$ hier auch wieder ein Ausreißer, aber der Vergleich der Anzahl $|\mathbb{K}_0| - |\mathbb{K}'_0|$ der weggelassenen Schlüssel mit der Diffe-

renz $\#(\mathfrak{c}_0) - \#'(\mathfrak{c}_0)$ macht deutlich, dass die Ausreißersituation für $\#(\mathfrak{c}_0)$ bei der Schlüsselmenge K_v zu einem wesentlichen Teil von den Schlüsseln mit $\gamma = id = \sigma$ verursacht wird.

Als zweite Modifikation wurden jetzt noch alle Schlüssel mit $\gamma = id$ oder $\sigma = id$ weggelassen, also als neue Schlüsselmenge $K'' = \{k = (\gamma, \sigma, \lambda, \mu, a, b, c, d, q) \in K_v | \ \gamma \neq id \ , \sigma \neq id\}$ genommen. Für die entsprechend modifizierte Schlüsselmenge K_0'' gilt: $|K_0''| = ((p+1)p(p-1)-1)^2 p^2 (p-1)^2 (p-2)^2$, also

$$|K_0''| = \begin{cases} 19\ 044 & für\ p = 3 \\ 50\ 979\ 600 & für\ p = 5 \end{cases} .$$

Text	#	Text	#	Text	#	Text	#
01 01	1537	11 01	1343	21 01	1318	20 01	1251
01 11	1011	11 11	849	21 11	1270	20 11	1161
01 21	1049	11 21	1255	21 21	892	20 21	1172
01 20	1053	11 20	1326	21 20	1290	20 20	1267

Tabelle 5: $p = 3,\ q = 5,\ \bar{x} = 1190.25,\ S = 179.98.$

Text	#	Text	#	Text	#	Text	#
01 01	1801253	11 01	1454615	21 01	1442745	31 01	1449223
41 01	1420760	20 01	1424976	01 11	1345985	11 11	1191228
21 11	1475393	31 11	1467153	41 11	1459858	20 11	1454757
01 21	1351719	11 21	1461054	21 21	1200442	31 21	1451245
41 21	1474549	20 21	1409675	01 31	1346409	11 31	1469999
21 31	1468432	31 31	1044779	41 31	1470197	20 31	1446756
01 41	1356880	11 41	1440576	21 41	1478381	31 41	1454092
41 41	1199886	20 41	1450244	01 20	1341374	11 20	1466213
21 20	1469357	31 20	1449313	41 20	1458555	20 20	1431527

Tabelle 6: $p = 5,\ q = 5,\ \bar{x} = 1416099.875,\ S = 119257.15$

Wie die Tabellen 5 und 6 für $\mathbb{K} = \mathbb{Z}_3$ und $\mathbb{K} = \mathbb{Z}_5$ zeigen, bewirkt diese Modifikation eine wesentliche Verbesserung, auch wenn $\mathfrak{c}_0$ weiterhin ein Ausreißer bleibt. Als weitere Modifikation wurden jetzt noch alle Schlüssel $k = (\gamma, \sigma, \lambda, \mu, a, b, c, d, q)$ weggelassen, bei denen $\mathbb{L}^*(a, 1)$ oder $\mathbb{L}^*(b, 1)$ ein Fixpunkt von γ bzw. $\mathbb{L}^*(c, 1)$ oder $\mathbb{L}^*(d, 1)$ ein Fixpunkt von σ ist, also

$K_0''' = \{(\gamma, \sigma, \lambda, \mu, a, b, c, d, q) \in K_v |\, \mathbb{L}^*(c, 1), \mathbb{L}^*(d, 1) \notin \mathrm{Fix}\gamma\,, \mathbb{L}^*(c, 1), \mathbb{L}^*(d, 1) \notin \mathrm{Fix}\sigma\}$

als Schlüsselmenge genommen. Für die entsprechend reduzierte Schlüsselmenge K_0''' gilt: $|K_0''| = (p^2(p-1)^4(p-2)^2(p^2-p+1)^2$ also $|K_0''| = \begin{cases} 7056 & für\ p = 3 \\ 25\ 401\ 600 & für\ p = 5 \end{cases}$.

Text	#	Text	#	Text	#	Text	#
01 01	478	11 01	439	21 01	483	20 01	460
01 11	463	11 11	343	21 11	405	20 11	443
01 21	514	11 21	438	21 21	325	20 21	452
01 20	485	11 20	444	21 20	428	20 20	456

Tabelle 7: $p = 3,\ q = 5,\ \bar{x} = 441,\ S = 49.08$.

Text	#	Text	#	Text	#	Text	#
01 01	685361	11 01	720329	21 01	724071	31 01	714452
41 01	727540	20 01	707527	01 11	731469	11 11	608247
21 11	727481	31 11	727543	41 11	716350	20 11	725854
01 21	729490	11 21	721673	21 21	579055	31 21	710889
41 21	723632	20 21	710736	01 31	727808	11 31	730683
21 31	721972	31 31	560841	41 31	722226	20 31	719496
01 41	734326	11 41	707242	21 41	723984	31 41	717254
41 41	605315	20 41	724885	01 20	725928	11 20	719394
21 20	716997	31 20	714733	41 20	715659	20 20	721158

Tabelle 8: $p = 5,\ q = 5,\ \bar{x} = 705599.9375,\ \S = 43455.078$.

Die Tabellen 7 und 8 machen deutlich, dass die Verteilung bei der Schlüsselmenge K_0''' wirklich nochmals verbessert wird. Auch wenn für $K = \mathbb{Z}_3$ die Schlüsselmenge K_0''' nur ein gutes Drittel die Schlüsselmenge K_0 ausmacht, so zeigt der Quotient $\frac{|K_0'''|}{|K_0|} = (\frac{p^2-p+1}{p^2+p})^2$, der ja für wachsende p schnell gegen 1 geht, dass für große Primzahlen p die Schlüsselmenge K_0''' fast die ganze vorläufige Schlüsselmenge K_0 ausmacht.

Für $n \in \mathbb{N},\ n \geq 2$ und festgewählten Modul q ergibt sich für $\mathbb{K} = \mathbb{Z}_p$ und die Schlüsselmenge K_0 als Durchschnitt der Anzahlen wie oft ein fester $n-$elementiger Klartext auf einen Geheimtext abgebildet wird $d(p,n) = \frac{p^2(p-1)^4(p-2)^2}{(p+1)^{n-2}}$.

Für $n \geq 12$ ergibt sich, dass $d(p,n) \leq 1$. Für kleine p wird $d(p,n) \leq 1$ schon für kleinere n erreicht, wie die Tabelle 9 zeigt:

p	3	5	7
n mit $d(p,n) \leq 1$	8	10	11

Tabelle 9

Bei $d(p,n) \leq 1$ wäre die beste Verteilung, diejenige bei der als Anzahlen $\#(\mathfrak{c})$ nur 1 und 0 auftreten. Wie die Tabellen 10 und 11 zeigen, kommen für $n \geq 8$ bei $p = 3$ auch tatsächlich für $\mathfrak{m} = (\mathbb{K}^*(0,1), ..., \mathbb{K}^*(0,1))$ als Anzahlen $\#(\mathfrak{c})$ fast nur die Werte 1 und 0 vor. Mit $T_0 = \{\mathfrak{c} \in T \mid \#(\mathfrak{c}) \neq 0\}$ ist die Anzahl der Texte in Tabelle 10 bzw. 11 $|T_0| = 3628$ bzw. $= 1628$, d.h $6561 - 3628 = 2933$ bzw. $6561 - 1628 = 4933$ Texte sind nicht als Bild vorgekommen.

Um solche Tabellen für $p = 32027$ [14] mit dem fünft schnellsten Rechner der Welt (LRZ Rechner im Jahre 2000) zu generieren, braucht man mehr als 10^{120} Jahre.

[14] 32027 wird in unsern Programmen genommen.

Text	#	Text	#
01 01 01 01 01 01 01 01	1134	01 01 21 01 01 01 01 01	5
11 01 01 01 11 01 01 01	23	21 11 01 21 11 01 01 01	2
01 01 11 21 11 01 01 01	1	21 11 20 21 11 01 01 01	1
20 01 01 20 11 01 01 01	1	20 20 01 20 11 01 01 01	2
.	.	.	.
.	.	.	.
20 20 01 20 20 20 20 20	1	20 20 20 20 20 20 20 20	804

Tabelle 10: $p = 3,\ q = 5$ für nicht modifizierte Schlüsselmenge K_0.

Text	#	Text	#
01 01 01 01 01 01 01 01	100	01 01 21 01 01 01 01 01	1
11 01 01 01 11 01 01 01	9	21 11 01 21 11 01 01 01	2
01 01 11 21 11 01 01 01	1	21 11 20 21 11 01 01 01	1
20 01 01 20 11 01 01 01	1	20 20 01 20 11 01 01 01	2
.	.	.	.
.	.	.	.
20 20 01 20 20 20 20 20	1	20 20 20 20 20 20 20 20	156

Tabelle 11: $p = 3,\ q = 5$ für modifizierte Schlüsselmenge K_0'''.

2.4 Das modifizierte Chiffriersystem $C(\mathbb{K})$

Die oben geschilderten Experimente mit dem Chiffriersystem $\mathcal{C}(\mathbb{L}, f, \pi)$ legen es nahe als Schlüsselmenge K''' zu nehmen.

Als *Typ* der Algebra $\mathbb{L}$ definieren wir die Zahl 0 bzw. 1 bzw. 2 je nachdem ob $\mathbb{L}$ eine quadratische Körpererweiterung, die Algebra der Dualzahlen oder die Algebra der anormal-komplexen Zahlen über $\mathbb{K}$ ist. Über jedem endlichen Körper $\mathbb{K}$ gibt es von jedem der drei Typen bis auf Isomorphie genau eine Algebra. Wenn

wir noch geheimhalten welche Algebra wir benützen, so können wir die Schlüssel noch um den Typ der benützten Algebra erweitern. Bezeichnen wir mit mit $\mathbb{T} := \{0, 1, 2\}$ die Menge der Typen, so erhalten wir als Schlüsselmenge $K := \mathbb{T} \times K'''$. Jedem endlichen Körper $\mathbb{K}$ wird mit den oben angegebenen Abbildungn f und π damit ein Chiffriersystem $\mathcal{C}(\mathbb{K})$ mit der Schlüsselmenge $K := \mathbb{T} \times K'''$ zugeordnet.

2.5 Implementierung des Chiffriersystem $\mathcal{C}(\mathbb{K})$ als Chiffriersystem $\mathcal{C}'(\mathbb{K})$

Die meisten zu verschlüsselnden Daten liegen in Textformat vor. Um das Chiffriersystem $\mathcal{C}(\mathbb{K})$ praktisch anwenden zu können, d.h. Daten in einem üblichen Textformat verschlüsseln zu können, müssen wir also noch eine Einbettung der Menge der Texte im üblichen Textformat in die Klartextmenge $D = \bigcup_{n \geq 2} P(\mathbb{L})^n$ vornehmen. Dazu verwenden wir eine Binärdarstellung der Tastatur-Zeichen. Ein geeigneter standardisierter Zeichensatz ist der 7-Bit-ASCII-Code. Dieser Code erlaubt die Darstellung von 128 verschiedenen Zeichen, wobei neben Zahlen, Groß- und Kleinbuchstaben auch viele Sonderzeichen erfasst werden.

Wir beschreiben nun den Übergang von Texten in ASCII-Zeichen zu einer Folge von Punkten einer miquelschen Benz-Ebene über dem Primkörper $\mathbb{K} = \mathbb{Z}_p$.

Es seien k eine natürliche Zahl mit $2^{7k} - 1 \leq p^2 + 1$, A die Menge der ASCII Zeichen und $m = m_0 m_1 ... m_{k-1} \in A^k$ eine Folge von k ASCII-Zeichen. Der Folge m soll ein Punkt der Benz-Ebene $\Sigma(\mathbb{L}, \mathbb{K})$ zugeordenet werden. Jedes ASCII Zeichen m_j wird durch 7 Binärzeichen dargestellt:

$$m_j = d_{7j} d_{7j+1} ... \ d_{7j+6}$$

Durch die Voraussetzung $2^{7k} - 1 \leq p^2 + 1$ ist sichergestellt, dass die Folge $\widetilde{m} := (d_i)_{0 \leq i \leq 7k-1}$ aus $7k$ Binärzeichen eineindeutig auf einen Punkt der Benz-Ebene abgebildet werden kann.

Der Binärfolge $\widetilde{m}$ entspricht umkehrbar eineindeutig die natürliche Zahl $\widetilde{\widetilde{m}} := \sum_{i=0}^{7k-1} d_i 2^i < p^2 + 1$.

Für unsere Programme haben wir konkret $p = 32027$ gewählt. Dann kann man mit $k = 4$ arbeiten.

Für $r \in \mathbb{N}$ mit $r \geq 1$ bezeichnen wir mit $\mathbb{N}_r = \{0, ..., r-1\}$ den Abschnitt der ersten r natürlichen Zahlen.

Zu $c \in \mathbb{N}_{p^2+1}$ mit $c \neq p^2$ gibt es eindeutig bestimmte Zahlen $x, y \in \mathbb{N}_p$ mit $c = x + yp$ (Bezeichnung $\kappa(c) := (x, y)$).

Mittels der Abbildung

$$\alpha : \mathbb{N}_{p^2+1} \to P(\mathbb{L}),\ c \mapsto \begin{cases} \mathbb{L}^*(\kappa(c), \mathbf{1}) & für \quad c < p^2 \\ \mathbb{L}^*(\mathbf{1}, \mathbf{0}) & für \quad c = p^2 \end{cases}$$

wird damit die Menge der Folgen aus k ASCII-Zeichen durch die Injektion

$$\beta : \begin{cases} A^k \to P(\mathbb{L}) \\ m \mapsto \alpha(\widetilde{\widetilde{m}}) \end{cases}$$

in die Benz-Ebene eingebettet. Ein beliebiger Text aus ASCII-Zeichen wird gegebenfalls durch „padding“ mit einem Zeichen, z.B. „.“ so aufgefüllt, dass ein Text der Länge $n'+1$ mit $n'+1 \equiv 0\ mod\ k$ entsteht. Dem Text $t = m_0 m_1 ... m_n \in A^{n+1}$ mit $n + 1 = mk$ wird nun das m-Tupel $(\beta(m_{kj} m_{kj+1} ... m_{kj+k-1}))_{0 \leq j \leq m-1}$ von Punkten der Benz-Ebene zugeordenet.

Mit der Abbildung $\beta : \mathcal{T} := \bigcup_{i \in \mathbb{N}} A^i \to \bigcup_{j \in \mathbb{N}} P(\mathbb{L})^j$ haben wir eine Injektion der Menge $\mathcal{T}$ der Texte im üblichen Textformat in die Klartextmenge von $\mathcal{C}(\mathbb{K})$. Mit der von uns benützten injektiven Abbildung f definieren wir die Injektion $\mathfrak{f} : \bigcup_{j \geq 2} P(\mathbb{L})^j \to \bigcup_{i \geq 2} \mathbb{N}^i =: \mathcal{G}$ durch komponentenweise Anwendung von f. Als Verschlüsselungsfunktion nehmen wir nun $E'_k := \mathfrak{f} \circ E_k \circ \beta : \mathcal{T} \to \mathcal{G}$ und als Entschlüsselungsfunktion $D'_k := \beta^{-1} \circ D_k \circ \mathfrak{f}^{-1}$. Das so definierte Chiffriersystem (E', D') bezeichnen wir mit $\mathcal{C}'(\mathbb{K})$. Die Klartextmenge $\mathcal{T}$ besteht hier also aus allen Texten im üblichen Textformat mit mindestens 4 Zeichen. Die Geheimtextmenge $\mathcal{G}$ besteht aus endlichen Folgen von natürlichen Zahlen.

Implementiert haben wir das Chiffriersystem $\mathcal{C}'(\mathbb{K})$ nur für Primzahlen $p \equiv 3\ mod\ 4$. In diesem Fall ist ja -1 kein Quadrat in $\mathbb{K} = \mathbb{Z}_p$ und wir können

die quadratische Körpererweiterung $\mathbb{L}$ für jedes p als $\mathbb{L} = \mathbb{K}(\sqrt{-1})$ darstellen. Um die Arithmetik der Algebren $(\mathbb{L}, \mathbb{K})$ mit $Dim_{\mathbb{K}}\mathbb{L} = 2$ zu implementieren, haben wir im Fall der Körpererweiterung und der Dualzahlen eine Basis $\{\mathbf{1}, \mathfrak{i}\}$ [15] mit $\mathfrak{i}^2 = -\mathbf{1}$ bzw. $\mathfrak{i}^2 = 0$ gewählt und damit $\mathbb{L}$ mit $\mathbb{K} \times \mathbb{K}$ identifiziert. Hier gilt also $\mathbf{1} = (1, 0)$ und $\mathfrak{i} = (0, 1)$. Die anormal-komplexen Zahlen haben wir dagegen als direkte Summe $\mathbb{K} \times \mathbb{K}$ des Körpers $\mathbb{K}$ dargestellt. Hier gilt also $\mathbf{1} = (1, 1)$.

Die Arithmetik in $\mathbb{L}$ umfaßt folgende Operationen:

1. Addition in $\mathbb{L}$.

2. Multiplikation in $\mathbb{L}$.

3. Skalarmultiplikation mit einem Element aus $\mathbb{K}$.

4. Berechnung der Negation in $\mathbb{L}$.

5. Berechnung der konjugierten Elemente in $\mathbb{L}$.

6. Berechnung der Inversen bezüglich der Multiplikation in $\mathbb{L}$.

Wir haben in unserem Programm Addition und Multiplikation des Grundkörpers $\mathbb{K} = \mathbb{Z}_p$ in üblicher Weise modulo der Primzahl p durchgeführt.

Für Potenzen k^n mit $k \in \mathbb{K}^*,\ n \in \mathbb{N}$ benützen wir die folgende schnelle Methode:

Ohne Einschränkung betrachten wir $n < p$, da $k^{n+p-1} \equiv k^n \ mod\ p$. [16]

Es sei nun $n = \sum_{i=0}^{r} n_i 2^i,\ n_i \in \{0, 1\}$ die Binärdarstellung von n. Es gilt dann:

$$k^n = (k^{2^0})^{n_0}(k^{2^1})^{n_1} \ldots (k^{2^r})^{n_r} = \prod_{0 \le i \le r,\ n_i = 1} k^{2^i}.$$

2.6 Digitale Unterschrift

Eine weitere Klasse von Sicherheitsmechanismen dient der sicheren Identifizierung eines Absenders. Authentisierung ist der Schutz von Daten vor unbefugter

[15] $\mathbf{1}$ bezeichne hier das Einselement der Algebra $\mathbb{L}$.

[16] Nach dem kleinen Satz von Fermat gilt $k^{p-1} \equiv 1 \ mod\ p$ für $k \in \mathbb{Z}$ und jede Primzahl $p \in \mathbb{N}$.

Veränderung in einer ungesischerten Umgebung z.B, im Internet. Unter Authentizität versteht man, dass

1. die Daten durch einen Angreifer nicht verändert werden (Datenintegrität).
2. die Daten wirklich von demjenigen herkommen, der als Absender angegeben ist (Datenauthentizität).

Jedes Chiffriersystem kann man auf folgende Weise als Authentikationsystem auffassen. Es sei (E, D) ein Chiffriersystem. Der Absender verschlüsselt die Nachricht m mit dem Schlüssel k und sendet $c := E_k(m)$. Der Empfänger verifiziert die Nachricht und den Absender, indem er die Entschlüsselungsfunktion D_k anwendet: $D_k(c) = D_k E_k(m) = m$. Genau dann stammt die Nachricht vom Absender, wenn sich ein sinnvoller Text ergibt (vgl. [23], Seite 169).

Aus Zeitgründen wird oft vorgeschlagen, die eigentliche Nachricht nicht zu verschlüsseln, sondern im Klartext zu übertragen und nur eine verschlüsselte Prüfsumme („Digitale Unterschrift “) anzuhängen, die vom gesamten Klartext abhängt (vgl. z.B. [5], Seite 201). Hierauf beruht das folgende Verfahren eines Authentikationssystems, das das in (6.4) entworfene Chiffriersystem verwendet. Man kann dazu etwa wie folgt verfahren: Der Absender verschlüsselt die Nachricht m mit dem Schlüssel k und sendet m zusammen mit dem letzten Punkt c_n von $E_k(m)$ als digitale Unterschrift. Aufgrund des Verschlüsselungsalgorithmus kann man nämlich n als Prüfsumme auffassen.

Durch dieses Verfahren wird ein *cartesisches* Authentikationsverfahren,

$f : M \times K \to N$ definiert (vgl. [5], [28]), d.h. M, K, N sind endliche Mengen, so dass gilt:

(i) f ist surjektiv.

(ii) Für $m_1, m_2 \in M$ mit $m_1 \neq m_2$ ist $f(\{m_1\} \times K) \cap f(\{m_2\} \times K) = \emptyset$.

M bzw. K bzw. N heißt Menge der *Daten* bzw. der *Schlüssel* bzw. *Nachrichten*.

Im obigen Beispiel ist $M = \bigcup_{i \geq 2} P(\mathbb{L})^i$, $K = K'''$ und $N = M \times P(\mathbb{L})$ sowie $f(\mathfrak{m}, k) = (\mathfrak{m}, pr_i \circ E_k(\mathfrak{m}))$ für $\mathfrak{m} \in P(\mathbb{L})^i$, wobei pr_i die Projektion auf die i-te Komponent bezeichne.

Hier wollen wir nun noch ein anderes, mit Hilfe der Vierkreisrelation konstruiertes Verfahren vorstellen.

Es sei $\mathfrak{B} := (P, \mathfrak{K}, \mathfrak{G})$ eine Möbius-Ebene. Es seien weiter $C \in \mathfrak{K}$ ein fester Kreis, $D := C^{(2)}$ die Datenmenge, $K := (P \backslash C)^{(3)}$ die Schlüsselmenge, $N := C^{(2)} \times P$ die Nachrichtenmenge. Es seien $k := (k_1, k_2, k_3) \in K$ und $(a, b) \in M$. Nach Korollar 1.2.1 und Lemma 1.2.3(2) gibt es genau ein $c \in P$ mit $(a, k_1, b, k_2, c, k_3) \in V$, das wir mit $E_k(a, b) := c$ bezeichnen. Nach Lemma 1.2.4(1) gilt $c \neq a, b, k_1, k_2$.

Wir betrachten nun $f : M \times K \to N,\ (a, b, k) \mapsto (a, b, E_k(a, b))$. Wegen Korollar 1.2.1 ist f surjektiv, d.h. es gilt (i). Nach Definition von f gilt auch (ii). Damit ist f ein cartesisches Authentikationssystem. Der Empfänger akzeptiert die Nachricht (a, b, c) als authentisch genau dann wenn er $c = E_k(a, b)$ errechnet.

Für $(a, b, c) \in N$ sei $K(a, b, c) := \{k \in K \mid c = E_k(a, b)\}$. Wegen Korollar 1.2.1 und Lemma 1.2.3(2) gilt $|K(a, b, c)| = \begin{cases} (p^2 - p)(p^2 - p - 1) & falls \quad c \in C \\ (p^2 - p - 1)(p^2 - p - 2) & falls \quad c \notin C \end{cases}$

Wegen $|K| = (p^2 - p)(p^2 - p - 1)(p^2 - p - 2)$ gilt damit nach [28] für die Wahrscheinlichkeit $Ws(k \in K(a, b, c)) = \begin{cases} \frac{1}{p^2 - p - 2} & falls \quad c \in C \\ \frac{1}{p^2 - p} & falls \quad c \notin C \end{cases}$

Da $Ws(k \in K(a, b, c)) \neq \sqrt{|K|}$ ist dies Authentikationssystem nicht perfekt (vgl. [5] Seite 204). In [5] haben A. Beutelspacher und U. Rosenbaum mit Hilfe einer proktiven Ebene der Ordnung p ein perfektes Authentikationssystem angegeben, wobei die Betrugswahrscheinlichkeit $Ws = \frac{1}{p}$ ist. Unser mit Hilfe einer Möbius-Ebene der Ordnung p definiertes Authentikationssystem ist zwar nicht perfekt, aber die Betrugswahrscheinlichkeit $Ws \leq \frac{1}{p^2 - p - 2} < \frac{1}{p}$.

Wir haben dieses Verfahren in Programm 3 implementiert. Zur Analyse machen wir abschließend die folgende Bemerkung.

Es gilt $(a, k_1, b, k_2, c, k_3) \in V \Leftrightarrow Dv(k_2, a, b, k_1) = Dv(c, a, b, k_1) \cdot Dv(k_3, a, b, k_1)$ (vgl. [21] Seite 79).

Damit gilt $(a, k_1, b, k_2, c, k_3) \in V \Leftrightarrow \frac{(k_2-a)(b-k_1)}{(k_2-k_1)(b-a)} = \frac{(c-a)(b-k_1)}{(c-k_1)(b-a)} \cdot \frac{(k_3-a)(b-k_1)}{(k_3-k_1)(b-a)}$, d.h.

$(a, k_1, b, k_2, c, k_3) \in V \Leftrightarrow (k_2-a)(c-k_1)(k_3-k_1) = (k_2-k_1)(c-a)(b-k_1)(k_3-a)$

Nach Routinerechnungen ergibt sich, dass das Verfahren nicht linear ist.

Literatur

[1] E. Artin, *Geometric Algebra*. Interscience Publishers, New York 1957.

[2] H. Becker & F.Piper, *Chipher systems*. Northwood Books, London 1982.

[3] W. Benz, *Vorlesungen über Geometrie der Algebren*. Springer, Berlin-Heidelberg-New York 1973.

[4] A. Beutelspacher, *Kryptologie*, 6. Aufl. Vieweg, Wiesbaden 1996.

[5] A. Beutelspacher & U. Rosenbaum, *Projektive Geometrie*. Vieweg, Wiesbaden 1992.

[6] C. Capellaro, *Anwendungen endlicher Kreisgeometrien in der Kryptologie*. Dissertation, TU München, 1994.

[7] Y. Chen, *Der Satz von Miquel in der Möbiusebene*. Math. Ann. **186** (1970), 81–100.

[8] T. ElGamal, *A public key cryptosystem and signature scheme based on discrete logariths*. IEEE Trans. Inform. Theory **IT-31** (1985), 469–473.

[9] W. Fumy & H. P. Riess, *Kryptographie*, 2. Aufl. R. Oldenbourg Verlag, München 1994.

[10] R. Halder & W. Heise, *Einführung in die Kombinatorik*. München-Wien 1976.

[11] W. Heise & H. Karzel, *Symmetrische Minkowski-Ebenen.* J. Geom. **3** (1973), 5–20.

[12] W. Heise & H. Seybold, *Das Existenzproblem der Möbius-, Laguerre- und Minkouski-Erweiterungen endlicher affiner Ebenen.* Sitz. Ber. Bayer. Akad. Wiss. Math.-Nat. K1 (1976), 43–58.

[13] C. Hering, *Eine Klassifikation der Möbius-Ebenen.* Math.Z. **87** (1965), 252–262.

[14] D. Hilbert, *Grundlagen der Geometrie.* 1. Aufl. Berlin 1899, 11. Aufl. Stuttgart 1972.

[15] G. Kaerlein, *Der Satz von Miquel in der pseudo-euklidischen (Minkowskischen) Geometrie.* Dissertation, Bochum, 1970.

[16] H. Karzel, K. Sörensen & D. Windelberg, *Einführung in die Geometrie.* Vandenhoeck, Göttingen 1973.

[17] M. Klein & H.-J. Kroll, *On Minkowski planes with transitive groups of homotheties.* Abh. Math. Sem. Univ. Hamburg **64** (1994), 303–313.

[18] R. Kleinewillinghöfer, *Eine Klassifikation der Laguerre-Ebenen nach $\mathfrak{L}$-Streckungen und $\mathfrak{L}$-Translationen.* Arch. Math. **34** (1980), 469–480.

[19] H.-J. Kroll, *Anordnungsfragen in Benz-Ebenen.* Abh. Math. Semin. Univ. Hamb. **46** (1977), 217–255.

[20] H.-J. Kroll & S. G. Taherian, *Bemerkungen zum Beweis des Darstellungssatzes für miquelsche Möbius-Ebenen von A. Lenard.* Abh. Math. Sem. Univ. Hamburg **69** (1999), 159–166.

[21] A. Lenard, *Ein neuer Beweis des Darstellungssatzes für Miquelsche Möbius-Ebenen.* Abh. Math. Sem. Univ. Hamburg **65** (1995), 57–82.

[22] K. Meyberg, *Algebra Teil 1,2.* Carl Hanser Verlag, München Wien 1980.

[23] K. Pommerening, *Datenschutz und Datensicherheit.* B.I. Wissenschaftsverlag, München Wien Zürich 1991.

[24] R. L. Rivest, A. Schamir & L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems.* Communication of the ACM **21**(1978), 120–126.

[25] H.-J. Samaga, *A unified approach to Miquel's theorem and its degenerations. In Geometry and Differential Geometry*, Lecture Notes in Math., vol. 792, Springer, 1980, pp. 132–142.

[26] H.-J. Samaga, *Miquel Sätze in Minkowski-Ebennen II.* Results Math. **25** (1994), 341–356.

[27] E. Schröder, *Ein neuer Winkelbegriff für die Elementargeometrie?* Praxis Math. **24** (1982), 257–269.

[28] K. Sörensen, Vorlessung über projektive Geometrie und ihre Anwendungen in der Kryptologie, WS 1999/2000.

[29] B. L. van der Waerden & L. J. Smid, *Eine Axiomatik der Kreisgeometrie und der Laguerregeometrie.* Math. Ann. **110** (1935), 753–776.

[30] G. S. Vernam, *Cipher printing telegraph systems for secret wire and radio telegraphic communications.* J. AIEE **45** (1926), 109–115.

Anhang:

/∗**Programm.1**: Das im Kapitel 2.2 beschriebene Verschluesselungsalgorithmus wurde in der Programmiersprache C implementiert. ∗/

```
# include <stdio.h>
# include <string.h>
# include <stdlib.h>
# include <stddef.h>
struct point {
   unsigned long int x;
   unsigned long int y;
} ;
struct Benzpt {
   int type;
   struct point value;
} ;
# define prime 32027UL
# define q 10L
# define Pmax 1000UL
# define Dmax 1000UL
# define inf 0
# define fin 1

int veadd (struct point *k, struct point *l, struct point *res)
{
  (*res).x = ((*k).x + (*l).x) % prime;
  (*res).y = ((*k).y + (*l).y) % prime;
  return 0;
}

int vesub (struct point *k, struct point *l, struct point *res)
{
  (*res).x = ((*k).x + prime - (*l).x) % prime;
  (*res).y = ((*k).y + prime - (*l).y) % prime;
  return 0;
}

int vemult (struct point *k, struct point *l, int m, struct point *res)
{
unsigned long int k1, k2, l1, l2, h1, h2;
  k1 = (*k).x;
  k2 = (*k).y;
  l1 = (*l).x;
  l2 = (*l).y;
  h1 = (k1 * l1) % prime;
  h2 = (k2 * l2) % prime;
  if(m==0){
```

```
    (*res).x = (h1 + prime - h2) % prime;
    (*res).y = (k1 * l2 + k2 * l1) % prime;
   }
   else if(m==1){
    (*res).x = (h1) % prime;
    (*res).y = (k1 * l2 + k2 * l1) % prime;
   }
   else if(m==2){
    (*res).x = h1;
    (*res).y = h2;
   }
   return 0;
}
int vecomp (struct point *a, struct point *res)
{
   unsigned long int a1, a2;
   a1 = (*a).x;
   a2 = (*a).y;
   (*res).x = a1;
   (*res).y = (prime - a2) % prime;
   return 0;
}
int scvemul (unsigned long int *k, struct point *a, struct point *res)
{
   unsigned long int a1, a2;
    a1 = (*a).x;
    a2 = (*a).y;
    (*res).x = ((*k) * a1) % prime;
    (*res).y = ((*k) * a2) % prime;
    return 0;
}
int scmult (unsigned long int *k,unsigned long int *l, unsigned long int *res)
{
    *res = ((*k) * (*l)) % prime;
    return 0;
}
int scpow (unsigned long int *k, unsigned int n, unsigned long int *res)
{
unsigned long int m, h, h1, h2;
m = n;
    h = (*k);
    *res = 1;
    while (m!=0) {
     if (m&1) {
```

```
      scmult (res, &h, &h1);
      *res = h1;
     }
    scmult (&h, &h, &h2);
    h = h2;
    m = m >>1;
   }
    return 0;
}
int scinvel (unsigned long int *k, unsigned long int *res)
{
   unsigned int n;
   n = (int) prime - 2;
   scpow (k, n, res);
  return 0;
}
int veinvel (struct point *a, int m, struct point *res)
{
  struct point ca, cb;
  unsigned long int h1, h2, h3, h4;
  if(m!=2){
    vecomp (a, &ca);
    vemult (a, &ca, m, &cb);
    h1 = (cb).x;
    scinvel(&h1, &h2);
    scvemul (&h2, &ca, res);
  } else{
    h1 = (*a).x;
    h2 = (*a).y;
    scinvel(&h1, &h3);
    scinvel(&h2, &h4);
    (*res).x=h3;
    (*res).y=h4;
  }
  return 0;
}
int krypt (struct Benzpt *p1, int k, struct point *a1, struct point *b1, struct
point *c1 , struct point *d1, struct Benzpt *q4)
{
   struct point h1, h2, h3, h4, xx, yy;
   if ((*p1).type == fin){
    xx.x=(*p1).value.x;
    xx.y=(*p1).value.y;
    vemult(&xx, c1, k, &h1);
```

```
 veadd(&h1, d1, &h3);
 vemult(&xx, a1, k, &h2);
 veadd(&h2, b1, &h4);
} else if((*p1).type == inf){
 if ((*p1).value.x == 2){
 yy.x=0;
 yy.y=(*p1).value.y;
 vemult(d1, &yy, k, &h1);
 veadd(&h1, c1, &h3);
 vemult(b1, &yy, k, &h2);
 veadd(&h2, a1, &h4);
} else if ((*p1).value.x == 1){
 yy.y=0;
 yy.x=(*p1).value.y;
 vemult(d1, &yy, k, &h1);
 veadd(&h1, c1, &h3);
 vemult(b1, &yy, k, &h2);
 veadd(&h2, a1, &h4);
} else if ((*p1).value.x == 0 && (*p1).value.y == 2){
 yy.x=0;
 yy.y=1;
 xx.x=1;
 xx.y=0;
 vemult(d1, &yy, k, &h1);
 vemult(&xx, c1, k, &h2);
 veadd(&h1, &h2, &h3);
 vemult(b1, &yy, k, &h1);
 vemult(&xx, a1, k, &h2);
 veadd(&h1, &h2, &h4);
} else if ((*p1).value.x == 0 && (*p1).value.y == 1){
 yy.x=1;
 yy.y=0;
 xx.x=0;
 xx.y=1;
 vemult(d1, &yy, k, &h1);
 vemult(&xx, c1, k, &h2);
 veadd(&h1, &h2, &h3);
 vemult(b1, &yy, k, &h1);
 vemult(&xx, a1, k, &h2);
 veadd(&h1, &h2, &h4);
 }
}
if((k==0 && (h3.x !=0 || h3.y !=0)) || (k==1&& h3.y !=0)|| (k==2 &&h3.x!=0
&& h3.y!=0)){
veinvel(&h3, k, &h1);
```

```
    vemult(&h4, &h1, k, &h2);
     (*q4).type=fin;
     (*q4).value.x=h2.x;
     (*q4).value.y=h2.y;
    } else if((k==0 && h3.x==0 && h3.y==0) || (k==1 && h3.y==0)){
     veinvel(&h4,k, &h1);
     vemult(&h3, &h1, k, &h2);
     (*q4).type=inf;
     (*q4).value.x=2;
     (*q4).value.y=h2.y;
    } else if(k==2 && h4.x!=0 && h4.y!=0){
     veinvel(&h4,k,&h1);
     vemult(&h3, &h1, k, &h2);
    if (h2.x==0){
     (*q4).type=inf;
     (*q4).value.x=2;
     (*q4).value.y=h2.y;
    }
    else{
     (*q4).type=inf;
     (*q4).value.x=1;
     (*q4).value.y=h2.x;
    }
    } else if(h4.x==1 && h4.y==0 && h3.x==0 && h3.y==1){
    (*q4).type=inf;
    (*q4).value.x=0;
    (*q4).value.y=2;
    }
   else if (h4.x==0 && h4.y==1 && h3.x==1 && h3.y==0){
     (*q4).type=inf;
     (*q4).value.x=0;
     (*q4).value.y=1;
    } return 0;
}
int delta (int key1, struct point *k2, struct point *k3, struct point *k4, struct
Benzpt *p)
{
   struct point pp, x1, x2, x3, x4;
   vemult(k2, k3, key1, &pp);
   vesub(k4, &pp, &x1);
   if (key1==0 || key1==1 ){
    x3.x = (1 + prime - (*k2).x) % prime;
    x3.y = (prime - (*k2).y) % prime;
   }
   else {
```

```
    x3.x = (1 + prime - (*k2).x) % prime;
    x3.y = (1 + prime - (*k2).y) % prime;
   }
   vemult(k4, k3, key1, &pp);
   vemult(&x3, &pp, key1, &x2);
   x2.x = (prime - x2.x) % prime;
   x2.y = (prime - x2.y) % prime;
   vemult(k2, k4, key1, &pp);
   vesub(&pp, k3, &x4);
   krypt (p, key1, &x1, &x2, &x3, &x4, p);
   return 0;
}
int zz( struct Benzpt *p, unsigned long int *z)
{
    if ((*p).type ==fin)
     (*z) = ((*p).value.y) * prime + (*p).value.x;
    else if ((*p).type ==inf && (*p).value.x == 0){
    if ( (*p).value.y == 1)
     (*z) = prime * prime + 2*prime;
    else
     (*z) = prime * prime + prime;
   }
   else if ((*p).type==inf && (*p).value.x == 2)
    (*z) = prime * prime + (*p).value.y;
   else if ((*p).type==inf && (*p).value.x == 1)
    (*z) = prime * prime + prime + (*p).value.y;
   return 0;
}
main()
{
struct Benzpt p[Pmax], q[Pmax], rr[Pmax];
int i, j, key1;
struct point pq, aa1, bb1, cc1, dd1,a1, b1, c1, d1, d2, a12, d12, det, key2, key3,
key4, key5, key6, key7;
unsigned long int c[Dmax], s[Dmax], z[Dmax], pp, h, f;
size_t dlength;
int sorry;
signed char *t, *d, letter;
h=1;
a1.x=11;
a1.y=56;
b1.x=23;
b1.y=222;
c1.x=2;
```

```
c1.y=11;
d1.x=412;
d1.y=91;
aa1.x=12;
aa1.y=562;
bb1.x=232;
bb1.y=22;
cc1.x=29;
cc1.y=191;
dd1.x=42;
dd1.y=111;
key2.x=23;
key2.y=121;
key3.x=120;
key3.y=34;
key4.x=2600;
key4.y=1629;
key5.x=2;
key5.y=21;
key6.x=170;
key6.y=4300;
key7.x=2300;
key7.y=19;
printf("Please give one of the integers 0 or 1 or 2 as the first key \n" );
scanf("% 1d", &key1);
vemult(&a1,&d1,key1, &a12);
vemult(&b1,&c1,key1, &d12);
vesub(&a12,&d12, &det);
if ((key1==0 && det.x==0 && det.y==0)|| (key1==1&&det.x==0)|| (key1==2
&&(det.x==0 || det.y==0))){
    printf(" illegal key!!\n");
    h=0;
}
vemult(&aa1,&dd1,key1, &a12);
vemult(&bb1,&cc1,key1, &d12);
vesub(&a12,&d12, &det);
if ((key1==0 && det.x==0 && det.y==0)|| (key1==1&&det.x==0)|| (key1==2
&&(det.x==0 || det.y==0))){
   printf(" illegal key!!\n");
   h=0;
}
if (h!=0){
printf ("this program is for chiffern. please give a text with at least 4 characters
\n");
printf ("\n");
```

```
printf("the calculation is modulo % u\n", prime);
d = (signed char *) malloc (Dmax);
sorry=0;
do{
printf ("\n");
for (i=0; i<Dmax-1 && (letter=getchar())!=EOF ; i++)
   d[i] = letter;
d[i] = '\0';
printf ("\n");
printf ("\n");
printf ("\n");
if (i % 4 == 0)
    dlength = i;
else
    dlength = (i/4 + 1) * 4;
if(dlength >4)
   printf("a plaintext with % d characters: \n" , i);
else{
    sorry=1;
    printf("Sorry ! we accept only a text with more than 4     characters. ");
   }
}
while(dlength<=4);
/* padding */
for (j=i+1; j<dlength; j++)
d[j] = '.';
printf("% s\n", d);
/* put four characters in one unsigned long integer. */
for (i=0; i<dlength/4;i++) {
c[i] = d[4*i];
for (j=1; j<4; j++) {
    c[i] = c[i] << 7;
    c[i] += d[4*i+j];
   }
}
/* the integers c[i] are mapped into Z(p^2+key1*p+(key1+1)% 2)   */
pp = prime * prime + key1*prime + ((key1+1)% 2);
z[0] = c[0];
for (i=1; i<dlength/4; i++)
   z[0]= (z[0] + c[i]) % pp;
for (i=1; i<dlength/4; i++)
   z[i] = (z[i-1] + c[i]) % pp;
/* the integers Z[i] are mapped into the Benz-plane */
for (i=0; i<dlength/4; i++) {
   if ( z[i]< prime * prime ){
```

```
      p[i].type = fin;
      p[i].value.x = z[i] % prime;
      p[i].value.y = z[i] / prime;
    } else if (z[i] == prime * prime){
      p[i].type = inf;
      p[i].value.x = 2;
      p[i].value.y = 0;
    } else if (prime * prime< z[i] && z[i]<prime * prime + prime ){
     p[i].type = inf;
     p[i].value.x = 2;
     p[i].value.y = z[i] % prime;
     } else if (z[i] == prime * prime + prime ){      p[i].type = inf;
     p[i].value.x = 0;
     p[i].value.y = 2;
    } else if (prime * prime + prime< z[i] && z[i]<prime * prime + 2*prime ){
     p[i].type = inf;
     p[i].value.x = 1;
     p[i].value.y = z[i] % prime;
    } else if (z[i] == prime * prime + 2*prime ){
     p[i].type = inf;
     p[i].value.x = 0;
     p[i].value.y = 1;
     }
}
delta (key1, &key2, &key3, &key4, &p[0]);
krypt (&p[0], key1, &a1, &b1, &c1, &d1, &p[0]);
for (i=1; i<dlength/4; i++){
    if (i% 2==0){
     pq.x=p[i-1].value.x;
     pq.y=p[i-1].value.y;
     vesub (&key4, &pq, &det);
    if ((key1==0 && det.x==0 && det.y==0)|| (key1==1 && det.x==0)||(key1==2
&&(det.x==0||det.y==0))){
      delta (key1, &key2, &key4, &key3, &p[i]);
      for (j=0; j<i+1; j++){
       krypt (&p[i], key1, &a1, &b1, &c1, &d1, &p[i]);
      }
     }
    else {
     delta (key1, &key2, &key4, &pq, &p[i]);
      for (j=0; j<i+1; j++){
      krypt (&p[i], key1, &a1, &b1, &c1, &d1, &p[i]);
     }
     }
    }
```

```
    else {
     pq.x= p[i-1].value.x;
     pq.y= p[i-1].value.y;
     vesub (&key3, &pq, &det);
      if ((key1==0 && det.x==0 && det.y==0)|| (key1==1 && det.x==0)||
(key1==2 &&(det.x==0||det.y==0))){
       delta (key1, &key2, &key3, &key4, &p[i]);
       for (j=0; j<i+1; j++){
        krypt (&p[i], key1, &a1, &b1, &c1, &d1, &p[i]);
       }
      }
     else {
      delta (key1, &key2, &key3, &pq, &p[i]);
      for (j=0; j<i+1; j++){
       krypt (&p[i], key1, &a1, &b1, &c1, &d1, &p[i]);
      }
     }
    }
}
for (i=0; i<dlength/4; i++){
    rr[i].type = p[i].type;
    rr[i].value.x = p[i].value.x;
    rr[i].value.y = p[i].value.y;
}    zz (&p[i-1], &f);
   f = f % q;
   pq.x = p[i-1].value.x;
   pq.y = p[i-1].value.y;
   vesub (&key7, &pq, &det);
   if ((key1==0 && det.x==0 && det.y==0)|| (key1==1 && det.x==0)||(key1==2
&&(det.x==0||det.y==0))){
   delta (key1, &key5, &key7, &key6, &p[0]);
   for (j=0; j<f+1;j++)
    krypt (&p[0], key1, &aa1, &bb1, &cc1, &dd1, &p[0]);
   }
   else {
    delta (key1, &key5, &key7, &pq, &p[0]);
    for (j=0; j<f+1; j++)
     krypt (&p[0], key1, &aa1, &bb1, &cc1, &dd1, &p[0]);
   }
   for (i=1; i<dlength/4; i++){
    if (i% 2==0){
     zz (&rr[i-1], &f);
     pq.x= rr[i-1].value.x;
     pq.y= rr[i-1].value.y;
     f = f % q;
```

```
      vesub (&key7, &pq, &det);
     if ((key1==0 && det.x==0 && det.y==0)|| (key1==1 &&det.x==0)||(key1==2
&&(det.x==0||det.y==0))){
      delta (key1, &key5, &key7, &key6, &p[i]);
      for (j=0; j<f+1;j++){
       krypt (&p[i], key1, &aa1, &bb1, &cc1, &dd1, &p[i]);
      }
     }
     else {
      delta (key1, &key5, &key7, &pq, &p[i]);
      for (j=0; j<f+1; j++){
       krypt (&p[i], key1, &aa1, &bb1, &cc1, &dd1, &p[i]);
      }
     }
    }
    else {
    zz (&p[i-1], &f);
    pq.x= p[i-1].value.x;
    pq.y= p[i-1].value.y;
    f = f % q;
    vesub (&key6, &pq, &det);
   if ((key1==0 && det.x==0 && det.y==0)|| (key1==1 &&     det.x==0)||(key1==2
&&(det.x==0||det.y==0))){
      delta (key1, &key5, &key6, &key7, &p[i]);
      for (j=0; j<f+1; j++){
       krypt (&p[i], key1, &aa1, &bb1, &cc1, &dd1, &p[i]);
      }
     }
      else {
      delta (key1, &key5, &key6, &pq, &p[i]);
       for (j=0; j<f+1; j++){
        krypt (&p[i], key1, &aa1, &bb1, &cc1, &dd1, &p[i]);
       }
      }
     }
   }
printf ("\n");
printf("ciphertext: \n");
printf ("\n");
printf ("\n");
for (i=0; i<dlength/4; i++)
   zz (&p[i], &z[i]);
   for (i=0; i<dlength/4; i+=5) {
    for (j=0; j<5; j++){
    if(i+j<dlength/4)
```

```
    printf ("% 10d ", z[i+j]);
    }
    printf ("\n");
   }
printf ("\n");
printf ("\n");
free(d);
free(t);
}
else
   return 0;
return 0;
}
```

/∗**Programm.2**: Das im Kapitel 2.2 beschriebene Entschluesselungsalgorithmus wurde in der Programmiersprache C implementiert. ∗/

```
# include <stdio.h>
# include <string.h>
# include <stdlib.h>
# include <stddef.h>
struct point {
   unsigned long int x;
   unsigned long int y;
} ;
struct Benzpt {
   int type;
   struct point value;
} ;
# define prime 32027UL
# define q 10L
# define Pmax 1000UL
# define Dmax 1000UL
# define inf 0
# define fin 1
int veadd (struct point *k, struct point *l, struct point *res)
{
   (*res).x = ((*k).x + (*l).x) % prime;
   (*res).y = ((*k).y + (*l).y) % prime;
   return 0;
}
int vesub (struct point *k, struct point *l, struct point *res)
{
   (*res).x = ((*k).x + prime - (*l).x) % prime;
   (*res).y = ((*k).y + prime - (*l).y) % prime;
   return 0;
}
int vemult (struct point *k, struct point *l, int m, struct point *res)
{
unsigned long int k1, k2, l1, l2, h1, h2;
k1 = (*k).x;
k2 = (*k).y;
l1 = (*l).x;
l2 = (*l).y;
h1 = (k1 * l1) % prime;
h2 = (k2 * l2) % prime;
if(m==0){
   (*res).x = (h1 + prime - h2) % prime;
```

```
    (*res).y = (k1 * l2 + k2 * l1) % prime;
}
else if(m==1){
    (*res).x = (h1) % prime;
    (*res).y = (k1 * l2 + k2 * l1) % prime;
}
else if(m==2){
    (*res).x = h1;
    (*res).y = h2;
}
return 0;
}
int vecomp (struct point *a, struct point *res)
{
    unsigned long int a1, a2;
    a1 = (*a).x;
    a2 = (*a).y;
    (*res).x = a1;
    (*res).y = (prime - a2) % prime;
    return 0;
}
int scvemul (unsigned long int *k, struct point *a, struct point *res)
{
    unsigned long int a1, a2;
    a1 = (*a).x;
    a2 = (*a).y;
    (*res).x = ((*k) * a1) % prime;
    (*res).y = ((*k) * a2) % prime;
    return 0;
}
int scmult (unsigned long int *k,unsigned long int *l, unsigned long int *res)
{
    *res = ((*k) * (*l)) % prime;
    return 0;
}
int scpow (unsigned long int *k, unsigned int n, unsigned long int *res)
{
    unsigned long int m, h, h1, h2;
    m = n;
    h = (*k);
    *res = 1;
    while (m!=0) {
      if (m& 1) {
       scmult (res, & h, & h1);
```

```
      *res = h1;
      }
     scmult (& h, & h, & h2);
     h = h2;
    m = m >>1;
    }
    return 0;
}
int scinvel (unsigned long int *k, unsigned long int *res)
{
    unsigned int n;
    n = (int) prime - 2;
    scpow (k, n, res);
     return 0;
}
int veinvel (struct point *a, int m, struct point *res)
{
struct point ca, cb;
unsigned long int h1, h2, h3, h4;
if(m!=2){
     vecomp (a, & ca);
     vemult (a, & ca, m, & cb);
     h1 = (cb).x;
     scinvel(& h1, & h2);
     scvemul (& h2, & ca, res);
} else{
     h1 = (*a).x;
     h2 = (*a).y;
     scinvel(& h1, & h3);
     scinvel(& h2, & h4);
     (*res).x=h3;
     (*res).y=h4;
}
return 0;
}
int krypt (struct Benzpt *p1, int k, struct point *a1, struct point *b1, struct
point *c1 , struct point *d1, struct Benzpt *q4)
{
struct point h1, h2, h3, h4, xx, yy;
if ((*p1).type == fin){
     xx.x=(*p1).value.x;
     xx.y=(*p1).value.y;
     vemult(& xx, c1, k, & h1);
     veadd(& h1, d1, & h3);
```

```
    vemult(& xx, a1, k, & h2);
    veadd(& h2, b1, & h4);
} else if((*p1).type == inf){
    if ((*p1).value.x == 2){
    yy.x=0;
    yy.y=(*p1).value.y;
    vemult(d1, & yy, k, & h1);
    veadd(& h1, c1, & h3);
    vemult(b1, & yy, k, & h2);
    veadd(& h2, a1, & h4);
} else if ((*p1).value.x == 1){
    yy.y=0;
    yy.x=(*p1).value.y;
    vemult(d1, & yy, k, & h1);
    veadd(& h1, c1, & h3);
    vemult(b1, & yy, k, & h2);
    veadd(& h2, a1, & h4);
} else if ((*p1).value.x == 0 & & (*p1).value.y == 2){
    yy.x=0;
    yy.y=1;
    xx.x=1;
    xx.y=0;
    vemult(d1, & yy, k, & h1);
    vemult(& xx, c1, k, & h2);
    veadd(& h1, & h2, & h3);
    vemult(b1, & yy, k, & h1);
    vemult(& xx, a1, k, & h2);
    veadd(& h1, & h2, & h4);
} else if ((*p1).value.x == 0 & & (*p1).value.y == 1){
    yy.x=1;
    yy.y=0;
    xx.x=0;
    xx.y=1;
    vemult(d1, & yy, k, & h1);
    vemult(& xx, c1, k, & h2);
    veadd(& h1, & h2, & h3);
    vemult(b1, & yy, k, & h1);
    vemult(& xx, a1, k, & h2);
    veadd(& h1, & h2, & h4);
}
}
if((k==0 & & (h3.x !=0 || h3.y !=0)) || (k==1& & h3.y !=0)|| (k==2 & & h3.x!=0
& & h3.y!=0)){
   veinvel(& h3, k, & h1);
   vemult(& h4, & h1, k, & h2);
```

```
    (*q4).type=fin;
    (*q4).value.x=h2.x;
    (*q4).value.y=h2.y;
} else if((k==0 & & h3.x==0 & & h3.y==0) || (k==1 & & h3.y==0)){
   veinvel(& h4,k, & h1);
   vemult(& h3, & h1, k, & h2);
   (*q4).type=inf;
   (*q4).value.x=2;
   (*q4).value.y=h2.y;
} else if(k==2 & & h4.x!=0 & & h4.y!=0){
   veinvel(& h4,k,& h1);
   vemult(& h3, & h1, k, & h2);
   if (h2.x==0){
    (*q4).type=inf;
    (*q4).value.x=2;
    (*q4).value.y=h2.y;
   }
   else{
    (*q4).type=inf;
    (*q4).value.x=1;
    (*q4).value.y=h2.x;
   }
} else if(h4.x==1 & & h4.y==0 & & h3.x==0 & & h3.y==1){
   (*q4).type=inf;
   (*q4).value.x=0;
   (*q4).value.y=2;
   }
else if (h4.x==0 & & h4.y==1 & & h3.x==1 & & h3.y==0){     (*q4).type=inf;
   (*q4).value.x=0;
   (*q4).value.y=1;
} return 0;
}
int delta (int key1, struct point *k2, struct point *k3, struct point *k4, struct
Benzpt *p)
{
struct point pp, x1, x2, x3, x4;
vemult(k2, k3, key1, & pp);
vesub(k4, & pp, & x1);
if (key1==0 || key1==1 ){
    x3.x = (1 + prime - (*k2).x) % prime;
x3.y = (prime - (*k2).y) % prime;
}
else {
   x3.x = (1 + prime - (*k2).x) % prime;
   x3.y = (1 + prime - (*k2).y) % prime;
```

```
}
vemult(k4, k3, key1, & pp);
vemult(& x3, & pp, key1, & x2);
x2.x = (prime - x2.x) % prime;
x2.y = (prime - x2.y) % prime;
vemult(k2, k4, key1, & pp);
vesub(& pp, k3, & x4);
krypt (p, key1, & x1, & x2, & x3, & x4, p);
return 0;
}
int zz( struct Benzpt *p, unsigned long int *z)
{
if ((*p).type ==fin)
   (*z) = ((*p).value.y) * prime + (*p).value.x;
else if ((*p).type ==inf & & (*p).value.x == 0){
   if ( (*p).value.y == 1)
     (*z) = prime * prime + 2*prime;
   else (*z) = prime * prime + prime;
} else if ((*p).type==inf & & (*p).value.x == 2)
    (*z) = prime * prime + (*p).value.y;
else if ((*p).type==inf & & (*p).value.x == 1)
    (*z) = prime * prime + prime + (*p).value.y;
return 0;
}
main()
{
struct Benzpt p[Pmax], q[Pmax], rr;
int i, j, key1;
struct point pq, aa1, bb1, cc1, dd1,a1, b1, c1, d1, d2, a12, d12, aa12, dd12, det,
x1, x2, x3, x4, key2, key3, key4, key5, key6, key7;
unsigned long int c[Dmax], s[Dmax], z[Dmax], pp, h, f;
size_t dlength;
signed char *t, *d;
h=1;
a1.x=11;
a1.y=56;
b1.x=23;
b1.y=222;
c1.x=2;
c1.y=11;
d1.x=412;
d1.y=91;
aa1.x=12;
aa1.y=562;
```

```
bb1.x=232;
bb1.y=22;
cc1.x=29;
cc1.y=191;
dd1.x=42;
dd1.y=111;
key2.x=23;
key2.y=121;
key3.x=120;
key3.y=34;
key4.x=2600;
key4.y=1629;
key5.x=2;
key5.y=21;
key6.x=170;
key6.y=4300;
key7.x=2300;
key7.y=19;
printf("Please give one of the integers 0 or 1 or 2 as the first key \n");
scanf("%1d", &key1);
vemult(&a1,&d1,key1, &a12);
vemult(&b1,&c1,key1, &d12);
vesub(&a12,&d12, &det);
if ((key1==0 && det.x==0 && det.y==0)|| (key1==1 && det.x==0)|| (key1==2
&&(det.x==0 || det.y==0))){
printf(" illegal key!!\n");
h=0;
}
vemult(&aa1,&dd1,key1, &a12);
vemult(&bb1,&cc1,key1, &d12);
vesub(&a12,&d12, &det);
if ((key1==0 && det.x==0 && det.y==0)|| (key1==1&&det.x==0)|| (key1==2
&&(det.x==0 || det.y==0))){
    printf(" illegal key!!\n");
    h=0;
}
if (h!=0){
printf("calculation modulo %u\n", prime);
printf ("\n");
printf("this program is for decryption. \n");
printf ("\n");
d = (signed char *) malloc (Dmax);
for (i=0; i<Dmax-1 ; i+=5){
   scanf("%10d%10d%10d%10d%10d", &z[i], &z[i+1], &z[i+2], &z[i+3], &z[i+4]);
    if (z[i]== -1||z[i+1]== -1||z[i+2]== -1||z[i+3]== -1||z[i+4]== -1)
```

```
    break;
}
if (z[i]== -1){
    z[i]='\0';
    dlength = 4*i;
}
else if (z[i+1]== -1){
    z[i+1]='\0';
    dlength = 4*(i+1);
}
else if (z[i+2]== -1){
    z[i+2]='\0';
    dlength = 4*(i+2);
}
else if (z[i+3]== -1){
    z[i+3]='\0';
    dlength = 4*(i+3);
}
else if (z[i+4]== -1){
    z[i+4]='\0';
    dlength = 4*(i+4);
}
pp = prime * prime + key1*prime + ((key1+1)%2);
printf ("\n");
/* the integers Z[i] are mapped into the Benz-plane */
for (i=0; i<dlength/4; i++) {
  if ( z[i]<prime * prime ){
     p[i].type = fin;
     p[i].value.x = z[i] % prime;
     p[i].value.y = z[i] / prime;
  }else if (z[i] == prime * prime){
    p[i].type = inf;
    p[i].value.x = 2;
    p[i].value.y = 0;
  }else if (prime * prime< z[i] && z[i]<prime * prime + prime ){
    p[i].type = inf;
    p[i].value.x = 2;
    p[i].value.y = z[i] % prime;
  }else if (z[i] == prime * prime + prime ){
    p[i].type = inf;
    p[i].value.x = 0;
    p[i].value.y = 2;
  }else if (prime * prime + prime< z[i] && z[i]<prime * prime + 2*prime ){
    p[i].type = inf;
    p[i].value.x = 1;
```

```
    p[i].value.y = z[i] % prime;
   }else if (z[i] == prime * prime + 2*prime ){
    p[i].type = inf;
    p[i].value.x = 0;
    p[i].value.y = 1;
   }
}
/* decryption */
d12.x=(prime-(a1.x))%prime;
d12.y=(prime-(a1.y))%prime;
a12.x=(prime-(d1.x))%prime;
a12.y=(prime-(d1.y))%prime;
dd12.x=(prime-(aa1.x))%prime;
dd12.y=(prime-(aa1.y))%prime;
aa12.x=(prime-(dd1.x))%prime;
aa12.y=(prime-(dd1.y))%prime;
for (i=1; i<dlength/4; i++){
  if (i%2==0){
    pq.x= q[i-1].value.x;
    pq.y= q[i-1].value.y;
    zz (&q[i-1], &f);
    f = f % prime2;
    vesub (&key7, &pq, &det);
    if ((key1==0 && det.x==0 && det.y==0)|| (key1==1 && det.x==0)||(key1==2
&&(det.x==0||det.y==0))){
    krypt (&p[i], key1, &aa12, &bb1, &cc1, &dd12, &q[i]);
    for (j=0; j<f; j++)
     krypt (&q[i], key1, &aa12, &bb1, &cc1, &dd12, &q[i]);
    delta (key1, &key5, &key6, &key7, &q[i]);
    }
    else {
     krypt (&p[i], key1, &aa12, &bb1, &cc1, &dd12, &q[i]);
     for (j=0; j<f; j++)
      krypt (&q[i], key1, &aa12, &bb1, &cc1, &dd12, &q[i]);
    delta (key1, &key5, &pq, &key7, &q[i]);
    }
   }
  else {
    pq.x= p[i-1].value.x;
    pq.y= p[i-1].value.y;
    zz (&p[i-1], &f);
    f = f % prime2;
    vesub (&key6, &pq, &det);
    if ((key1==0 && det.x==0 && det.y==0)|| (key1==1 && det.x==0)||(key1==2
&&(det.x==0||det.y==0))){
```

```
     krypt (&p[i], key1, &aa12, &bb1, &cc1, &dd12, &q[i]);
    for (j=0; j<f; j++)
     krypt (&q[i], key1, &aa12, &bb1, &cc1, &dd12, &q[i]);
     delta (key1, &key5, &key7, &key6, &q[i]);
   }
   else {
     krypt (&p[i], key1, &aa12, &bb1, &cc1, &dd12, &q[i]);
    for (j=0; j<f; j++)
      krypt (&q[i], key1, &aa12, &bb1, &cc1, &dd12, &q[i]);
    delta (key1, &key5, &pq, &key6, &q[i]);
     }
  }
}
for (i=1; i<dlength/4; i++){
   p[i].type = q[i].type;
   p[i].value.x = q[i].value.x;
   p[i].value.y = q[i].value.y;
}
zz (&p[i-1], &f);
f = f % prime2;
pq.x= p[i-1].value.x;
pq.y= p[i-1].value.y;
vesub (&key7, &pq, &det);
if ((key1==0 && det.x==0 && det.y==0)|| (key1==1 && det.x==0)||(key1==2
&&(det.x==0 ||det.y==0))){
   for (j=0; j<f+1; j++)
    krypt (&p[0], key1, &aa12, &bb1, &cc1, &dd12, &p[0]);
   delta (key1, &key5, &key6, &key7, &p[0]);
   }
else {
   for (j=0; j<f+1; j++)
    krypt (&p[0], key1, &aa12, &bb1, &cc1, &dd12, &p[0]);
    delta (key1, &key5, &pq , &key7, &p[0]);
}
krypt (&p[0], key1, &a12, &b1, &c1, &d12, &q[0]);
delta (key1, &key2, &key4, &key3, &q[0]);
for (i=1; i<dlength/4; i++){
  pq.x= p[i-1].value.x;
  pq.y= p[i-1].value.y;
  if (i%2==0){
   vesub (&key4, &pq, &det);
   if ((key1==0 && det.x==0 && det.y==0)|| (key1==1 && det.x==0)||(key1==2
&&(det.x==0||det.y==0))){
   krypt (&p[i], key1, &a12, &b1, &c1, &d12, &q[i]);
   for (j=0; j<i; j++)
```

```
    krypt (&q[i], key1, &a12, &b1, &c1, &d12, &q[i]);
   delta (key1, &key2, &key3, &key4, &q[i]);
}
else {
   krypt (&p[i], key1, &a12, &b1, &c1, &d12, &q[i]);
   for (j=0; j<i; j++)
     krypt (&q[i], key1, &a12, &b1, &c1, &d12, &q[i]);
   delta (key1, &key2, &pq, &key4, &q[i]);
   }
}
else {
    vesub (&key3, &pq, &det);
   if ((key1==0 && det.x==0 && det.y==0)|| (key1==1 && det.x==0)||(key1==2
&&(det.x==0||det.y==0))){
    krypt (&p[i], key1, &a12, &b1, &c1, &d12, &q[i]);
    for (j=0; j<i; j++)
     krypt (&q[i], key1, &a12,&b1, &c1, &d12, &q[i]);
    delta (key1, &key2, &key4, &key3, &q[i]);
   }
   else {
    krypt (&p[i], key1, &a12, &b1, &c1, &d12, &q[i]);
    for (j=0; j<i; j++){
     krypt (&q[i], key1, &a12, &b1, &c1, &d12, &q[i]);
   }
    delta (key1, &key2, &pq, &key3, &q[i]);
   }
  }
}
for (i=0; i<dlength/4; i++){
   p[i].type = q[i].type;
   p[i].value.x = q[i].value.x;
   p[i].value.y = q[i].value.y;
} for (i=0; i<dlength/4; i++)
    zz (&p[i], &z[i]);
s[0] = (2*z[0] + pp - z[i-1]) % pp;
for (i=1; i<dlength/4; i++)    s[i] = (z[i] + pp -z[i-1]) % pp;
t = (signed char *) malloc (dlength + 1);
for(i=0; i<dlength/4; i++) {
  for(j=0; j<4; j++) {
   h = s[i];
   h = h >> (21 - j * 7);
   t[4*i+j] = (int) h;
   s[i] = s[i] -(h << (21 - j * 7));
  }
}
```

```
t[dlength] = '\0';
  printf ("\n");
  printf("decrypted ciphertext: \n");
  printf ("\n");
  printf("%s\n", t);
  printf ("\n");
  free(d);
  free(t);
}
else
   return 0;
return 0;
}
```

Programm 3: Der im Kapitel 2.6 beschriebene Authentikationssystem wurde in der Programmiersprache C implementiert.*/

```
#include <stdio.h>
#include <string.h>
#include <stdlib.h>
#include <stddef.h>

struct scalar {
   int type;
   unsigned long int value;
};
struct point {
   unsigned long int x;
   unsigned long int y;
};
struct moept {
   int type;
   struct point value;
};
#define prime 32027UL
#define Pmax 40000UL
#define Dmax 40000UL
#define infin 0
#define finit 1

int scadd (struct scalar *k,struct scalar *l,struct scalar *res)
{
unsigned long int v1, v2;
if ((*k).type == infin || (*l).type == infin)
   (*res).type = infin;
else {
   v1 = (*k).value;
   v2 = (*l).value;
   (*res).type = finit;
   (*res).value = (v1 + v2) % prime;
  }
return 0;
}

int scsub (struct scalar *k, struct scalar *l, struct scalar *res)
{
  unsigned long int v1, v2;
  if ((*k).type == infin || (*l).type == infin)
    (*res).type = infin;
  else {
    v1 = (*k).value;
    v2 = (*l).value;
```

```
    (*res).type = finit;
    (*res).value = (v1 + prime - v2) % prime;
   }
return 0;
}
int veadd (struct moept *k, struct moept *l, struct moept *res)
{
  unsigned long int k1, k2, l1, l2;
  if ((*k).type == infin || (*l).type == infin)
    (*res).type = infin;
  else {
    k1 = (*k).value.x;
    k2 = (*k).value.y;
    l1 = (*l).value.x;
    l2 = (*l).value.y;
    (*res).type = finit;
    (*res).value.x = (k1 + l1) % prime;
    (*res).value.y = (k2 + l2) % prime;
  }
return 0;
}
int vesub (struct moept *k, struct moept *l, struct moept *res)
  {
  unsigned long int k1, k2, l1, l2;
  if ((*k).type == infin || (*l).type == infin)
    (*res).type = infin;
  else {
    k1 = (*k).value.x;
    k2 = (*k).value.y;
    l1 = (*l).value.x;
    l2 = (*l).value.y;
    (*res).type = finit;
    (*res).value.x = (k1 + prime - l1) % prime;
    (*res).value.y = (k2 + prime - l2) % prime;
   }
return 0;
}
int vemult (struct moept *k, struct moept *l, struct moept *res)
{
  unsigned long int k1, k2, l1, l2, h1, h2;
  if ((*k).type == finit && (*l).type == finit) {
    k1 = (*k).value.x;
    k2 = (*k).value.y;
    l1 = (*l).value.x;
```

```
    l2 = (*l).value.y;
    (*res).type = finit;
    h1 = (k1 * l1) % prime;
    h2 = (k2 * l2) % prime;
    (*res).value.x = (h1 + prime - h2) % prime;
    (*res).value.y = (k1 * l2 + k2 * l1) % prime;
    }
    else if ((*k).type == infin && (*l).type == finit) {
     if((*l).value.x == 0 && (*l).value.y == 0) {
     (*res).type = finit;
     (*res).value.x = 1;
     (*res).value.y = 0;
    }
    else
     (*res).type = infin;
    }
    else if ((*l).type == infin && (*k).type == finit) {
    if((*k).value.x == 0 && (*k).value.y == 0) {
     (*res).type = finit;
     (*res).value.x = 1;
     (*res).value.y = 0;
    }
    else
     (*res).type = infin;
    }
    else {
    (*res).type = infin;
    }
return 0;
}
int vecomp (struct moept *a, struct moept *res)
{
  unsigned long int a1, a2;
  if ((*a).type == infin)
     (*res).type = infin;
   else {
     a1 = (*a).value.x;
     a2 = (*a).value.y;
     (*res).type = finit;
     (*res).value.x = a1;
     (*res).value.y = (prime - a2) % prime;
    }
return 0;
}
```

```
int scvemul (struct scalar *k, struct moept *a, struct moept *res)
{
   unsigned long int l, a1, a2;
   if ((*k).type == finit && (*a).type == finit) {
    l = (*k).value;
    (*res).type = finit;
    a1 = (*a).value.x;
    a2 = (*a).value.y;
    (*res).value.x = (l * a1) % prime;
    (*res).value.y = (l * a2) % prime;
   }
   else if ((*k).type == infin && (*a).type == finit) {
    if((*a).value.x == 0 && (*a).value.y == 0){
    (*res).type = finit;
    (*res).value.x = 1;
    (*res).value.y = 0;
    }
   else
    (*res).type = infin;
   }
   else if ((*a).type == infin && (*k).type == finit) {
    if((*k).value == 0) {
    (*res).type = finit;
    (*res).value.x = 1;
    (*res).value.y = 0;
   }
    else
    (*res).type = infin;
   }
   else {
    (*res).type = infin;
   }
return 0;
}
int scmult (struct scalar *k, struct scalar *l, struct scalar *res)
{
   unsigned long int v1, v2;
   if ((*k).type == finit && (*l).type == finit) {
    v1 = (*k).value;
    v2 = (*l).value;
    (*res).type = finit;
    (*res).value = (v1 * v2) % prime;
   }
   else if ((*k).type == infin && (*l).type == finit) {
    if ((*l).value == 0) {
```

```
    (*res).type = finit;
    (*res).value = 1;
   }
   else
    (*res).type =infin;
   }
   else if ((*l).type == infin && (*k).type == finit) {
    if ((*k).value == 0) {
     (*res).type = finit;
     (*res).value = 1;
    }
   else
    (*res).type =infin;
   }
   else {
    (*res).type =infin;
   }
return 0;
}
int scpow (struct scalar *k, unsigned int n, struct scalar *res)
{
   struct scalar h, h1, h2;
   unsigned long int m;
   if ((*k).type == infin)
    (*res).type = infin;
   else {
    m = n;
    h = *k;
    (*res).type = finit;
    (*res).value = 1;
    while (m!=0) {
    if (m&1) {
    scmult (res, &h, &h1);
    *res = h1;
    }
   scmult (&h, &h, &h2);
    h = h2;
    m = m >>1;
    }
   }
return 0;
}
int scinvel (struct scalar *k, struct scalar *res)
{
```

```
   unsigned int n;
   if ((*k).type == infin) {
    (*res).type = finit;
    (*res).value = 0;
   }
   else if ((*k).value == 0) {
    (*res).type = infin;
   }
   else {
    n = (int) prime - 2;
    scpow(k, n, res);
   }
return 0;
}
int veinvel (struct moept *a, struct moept *res) {
   struct moept ca, aa;
   struct scalar h1, h2;
   if ((*a).type == finit) {
    if((*a).value.x == 0 && (*a).value.y == 0)       (*res).type = infin;
    else {
     vecomp (a, &ca);
     vemult (a, &ca, &aa);
     h1.type = aa.type;
     h1.value = aa.value.x;
     scinvel(&h1, &h2);
     scvemul (&h2, &aa, res);
    }
   }
   else {
    (*res).type = finit;
    (*res).value.x = 0;
    (*res).value.y = 0;
}
return 0;
}
int circular (struct moept *a, struct moept *b, struct moept *c)
{
   struct scalar h1, h2, h3, h4, h5, h6, a1, a2, b1, b2, c1, c2;
   if ((*a).type == infin || (*b).type == infin ||    (*c).type == infin)
    return 1;
   else {
    a1.type = finit;
    a1.value = (*a).value.x;
    a2.type = finit;
```

```
    a2.value = (*a).value.y;
    b1.type = finit;
    b1.value = (*b).value.x;
    b2.type = finit;
    b2.value = (*b).value.y;
    c1.type = finit;
    c1.value = (*c).value.x;
    c2.type = finit;
    c2.value = (*c).value.y;
    scsub (&c1, &a1, &h1);
    scsub (&b2, &a2, &h2);
    scmult (&h1, &h2, &h3);
    scsub (&c2, &a2, &h4);
    scsub (&b1, &a1, &h5);
    scmult (&h4, &h5, &h6);
    if (h3.value == h6.value)
     return 1;
    else
     return 0;
  }
}
int cirisct (struct moept *a, struct moept *b, struct moept *point, struct moept
*k, struct moept *l, struct moept *res)
{
  struct scalar zero = {finit,0}, one = {finit,1};
  struct moept zeropt = {finit,{0,0}}, onept = {finit,{1,0}};
  struct moept q1, q2, q3, q4, hp1, hp2, hp3, knew, bp, ap,    bk, lp, al, ak, kp,
bl, ac, bc, pk;
  struct scalar eta2, q11, q12, q21, q22, q31, q32, q41, q42,    h1, h2, h3, h4, h5,
h6, h7, h8, den;
  if (circular (point, k, l) == 0) {
    vesub (b, point, &bp);
    vesub (a, point, &ap);
    vesub (b, k, &bk);
    vesub (l, point, &lp);
    vesub (a, l, &al);
    vesub (k, point, &kp);
    vesub (b, l, &bl);
    vesub (a, k, &ak);
    vemult (&bl, &ap, &hp1);
    vemult (&hp1, &kp, &q1);
    vemult (&al, &bp, &hp1);
    vemult (&hp1, &kp, &q2);
    vemult (&bk, &ap, &hp1);
    vemult (&hp1, &lp, &q3);
```

```
  vemult (&ak, &bp, &hp1);
  vemult (&hp1, &lp, &q4);
  q11.type = finit;
  q11.value = q1.value.x;
  q12.type = finit;
  q12.value = q1.value.y;
  q21.type = finit;
  q21.value = q2.value.x;
  q22.type = finit;
  q22.value = q2.value.y;
  q31.type = finit;
  q31.value = q3.value.x;
  q32.type = finit;
  q32.value = q3.value.y;
  q41.type = finit;
  q41.value = q4.value.x;
  q42.type = finit;
  q42.value = q4.value.y;
  scmult (&q31, &q42, &h1);
  scmult (&q41, &q32, &h2);
  scsub (&h1, &h2, &den);
  if (den.type == finit && den.value == 0) {
   eta2.type = finit;
   eta2.value = 0;
  }
  else {
   scmult (&q22, &q11, &h1);
   scmult (&q12, &q21, &h2);
   scsub(&h1, &h2, &h3);
   scinvel (&den, &h4);
   scmult (&h3, &h4, &eta2);
  }
  vemult (k, &lp, &hp1);
  scvemul (&eta2, &hp1, &hp2);
  vesub (&zeropt, &hp2, &hp1);
  vemult (l, &kp, &hp2);
  veadd (&hp1, &hp2, &hp3);
  scvemul (&eta2, &lp, &hp1);
  vesub (&zeropt, &hp1, &hp2);
  veadd (&kp, &hp2, &hp1);
  veinvel (&hp1, &hp2);
  vemult (&hp2, &hp3, res);
 }
else {
  if ((*k).type == infin) {
```

```
      knew.type = (*l).type;
      knew.value.x = (*l).value.x;
      knew.value.y = (*l).value.y;
   }
else {
   knew.type = (*k).type;
   knew.value.x = (*k).value.x;
   knew.value.y = (*k).value.y;
}
   vesub (a, point, &ap);
   vesub (b, point, &bp);
   vesub (point, &knew, &pk);
   vesub (a, &knew, &ak);
   vesub (b, &knew, &bk);
   vemult (&ap, &pk, &q1);
   vemult (&pk, &bp, &q2);
   vemult (&bk, &ap, &q3);
   vemult (&ak, &bp, &q4);
   q11.type = finit;
   q11.value = q1.value.x;
   q12.type = finit;
   q12.value = q1.value.y;
   q21.type = finit;
   q21.value = q2.value.x;
   q22.type = finit;
   q22.value = q2.value.y;
   q31.type = finit;
   q31.value = q3.value.x;
   q32.type = finit;
   q32.value = q3.value.y;
   q41.type = finit;
   q41.value = q4.value.x;
   q42.type = finit;
   q42.value = q4.value.y;
   scmult (&q31, &q42, &h1);
   scmult (&q41, &q32, &h2);
   scsub (&h1, &h2, &den);
   if (den.type == finit && den.value == 0) {
    eta2.type = finit;
    eta2.value = 0;
   }
   else {
    scmult (&q22, &q11, &h1);
    scmult (&q12, &q21, &h2);
    scsub(&h1, &h2, &h3);
```

```
    scinvel (&h3, &h4);
    scmult (&den, &h4, &eta2);
  }    scvemul (&eta2, &pk, &hp1);
  veadd (&hp1, &knew, res);
} return 0;
}
int V ( struct moept *a1, struct moept *a2, struct moept *b1, struct moept *b2,
struct moept *c1, struct moept *c2)
{
  int i, j;
  struct moept h[6];
  cirisct (c2, b2, a1, c1, b1, &h[0]);
  cirisct (c2, a2, b1, c1, a1, &h[1]);
  cirisct (b2, a2, c1, b1, a1, &h[2]);
  cirisct (b2, a1, c2, b1, a2, &h[3]);
  cirisct (a1, c2, b2, a2, c1, &h[4]);
  cirisct (b1, c2, a2, b2, c1, &h[5]);
  for (i=0; i<6; i++){
   for (j=i+1; j<6; j++){
    if (h[i].type == h[j].type ||h[i].value.x == h[j].value.x ||h[i].value.y == h[j].value.y)
     return 0;
   }
  }
  return 1;
}
main()
{
  struct moept p[Pmax], q[Pmax], key[Pmax], a;
  unsigned long int c[Dmax], s[Dmax], z[Dmax];
  size_t dlength;
  signed char *t, *d, letter;
  printf("calculation modulo %u\n", prime);
  a.type = finit;
  a.value.x = 2;
  a.value.y = 5;
  for (i=0; i<3*dlength; i++) {
   (key[i]).type = a.type;
   (key[i]).value.x = a.value.x + 2*i;
   (key[i]).value.y = a.value.y + i;
  }
  d = (signed char *) malloc (Dmax);
  for (i=0; i<Dmax-1 && (letter=getchar())!=EOF ; i++)
   d[i] = letter;
  d[i] = '\0';
  printf ("\n");
```

```
printf("plaintext with %d letters: \n" , i);
if (i%8 == 0)
 dlength = i;
else
 dlength = (i/8 + 1) * 8;
/* padding */
for (j=i+1; j<dlength; j++)
 d[j] = 'a' + j % 8;
printf ("\n");
printf("%s\n", d);
printf ("\n");
/* put four characters in one unsigned long integer */
for (i=0; i<dlength/4; i++) {
 c[i] = d[4*i];
 for (j=1; j<4; j++) {
  c[i] = c[i] << 7;
  c[i] += d[4*i+j];
 }
}
/* the integers c[i] are mapped into Z(p+1) */
z[0] = c[0] % (prime +1);
for (i=1; i<dlength/4; i++) {
 z[i] = (z[i-1] + c[i]) % (prime+1);
}
/* the integers Z[i] are mapped into the Moebius-plane */
for (i=0; i<dlength/4; i++) {
 if (z[i] == prime)
  p[i].type = infin;
 else {
  p[i].type = finit;
  p[i].value.x = z[i] % prime;
  p[i].value.y = 0;
 }
}
j = 0;
for (i=0; i<dlength/4; i+=2) {
 cirisct (&p[i+1], &key[j], &key[j+2], &key[j+1], &p[i], &q[i+1]);
 cirisct (&key[j], &key[j+1],&q[i+1], &p[i], &p[i+1], &q[i]);
 j+=3;
}
/* pirnt signature */
printf ("signature:\n");
for (i=0; i<dlength/4;i+=2)
 printf("%u",q[i].value.x);
free (d);
```

```
    free (t);
    return 0;
}
```