

Technische Universität München  
Fakultät für Mathematik

# Pythagoreische und euklidische Körper

Diplomarbeit von **Thomas Ganter**

Aufgabensteller: Prof. Dr. H. Wähling  
Abgabedatum: 15. November 1996

Ich erkläre hiermit, daß ich diese Arbeit alleine und nur mit den angegebenen Hilfsmitteln angefertigt habe.

(Prien am Chiemsee, den 15.November 1996, Thomas Ganter)

# Inhaltsverzeichnis

<b>1</b>	<b>Vorbereitungen</b>	<b>5</b>
1.1	Die Theorie von Artin und Schreier . . . . .	6
1.2	Algebraische Galoiserweiterungen . . . . .	10
1.3	Die maximale $p$ -Erweiterung eines Körpers . . . . .	11
1.4	Potenzreihenkörper . . . . .	12
<b>2</b>	<b>Pythagoreische Körper</b>	<b>23</b>
2.1	Die pythagoreische Hülle eines Körpers . . . . .	24
2.2	Eigenschaften pythagoreischer Körper . . . . .	30
2.3	Pythagoreische Körper und formale Potenzreihen . . . . .	34
2.4	Level und Pythagoraszahl eines Körpers . . . . .	36
<b>3</b>	<b>Euklidische Körper</b>	<b>38</b>
3.1	Erste Eigenschaften . . . . .	39
3.2	Euklidische Hüllen . . . . .	44
3.3	Der Satz von Whaples mit Folgerungen . . . . .	49
3.4	Die euklidischen Unterkörper von $\mathbb{R}$ . . . . .	51
3.5	Formale Potenzreihenkörper über euklidischen Körpern . . . . .	55

# Einleitung

Die vorliegende Arbeit befasst sich mit einigen Aspekten der Theorie der euklidischen und pythagoreischen Körpern. Im wesentlichen stützen wir uns dabei auf die Arbeiten von Becker, hier insbesondere [Bec73] und von Diller und Dress, nämlich den Artikel [DD65].

Die Theorie der euklidischen und pythagoreischen Körper ist eine verhältnismäßig junge, die maßgeblichen Erkenntnisse stammen allesamt aus der zweiten Hälfte unseres Jahrhunderts. Grundlage dafür waren die Arbeiten von Artin und Schreier zu Beginn dieses Jahrhunderts, die erstmals Untersuchungen über *formal reelle* Körper anstellten. Einen Einstieg in die Theorie der formal reellen Körper werden wir in Kapitel 1 im ersten Abschnitt geben. Wir nennen einen Körper formal reell, wenn die  $-1$  des Körpers nicht als Summe von endlich vielen Quadraten des Körpers geschrieben werden kann (vgl. (1.6)). Artin und Schreier haben gezeigt, daß dies genau dann der Fall ist, wenn  $K$  eine Anordnung besitzt (vgl. (1.7)). Darüberhinaus werden Kriterien angegeben, unter welchen Voraussetzungen sich eine solche Anordnung auf algebraische Körpererweiterungen fortsetzen lassen. Da die Arbeiten von Artin und Schreier inzwischen zu den Standardwerken zählen, aber auch um den Umfang dieser Arbeit in Grenzen zu halten wurde im ersten Abschnitt des ersten Kapitels auf Beweise verzichtet; stattdessen verweisen stets ein oder mehrere Literaturangaben auf entsprechende Stellen in Standardwerken.

Einen wichtigen Satz über  $p$ -Erweiterungen und insbesondere die maximale  $p$ -Erweiterung eines Körpers werden wir im dritten Abschnitt des ersten Kapitels beweisen (vgl. (1.21)). Unter einer maximalen  $p$ -Erweiterung des Körpers  $K$  verstehen wir das Kompositum aller algebraischen Galois-Erweiterungen  $E$  von  $K$ , deren Grad über  $K$  eine  $p$ -Potenz ist (vgl. (1.19)). Wir

werden zum einen zeigen, daß die maximale  $p$ -Erweiterung bereits die Vereinigung dieser Erweiterungskörper ist; zum anderen werden wir nachweisen, daß genau dann, wenn die maximale  $p$ -Erweiterung von  $K$  nicht bereits mit  $K$  übereinstimmt, also eine echte Erweiterung ist,  $K$  eine zyklische algebraische Galoiserweiterung vom Grad  $p$  besitzt. Vor allem diese letzte Aussage wird später in dieser Arbeit mehrmals von Bedeutung sein.

Schließlich werden wir im vierten Abschnitt des ersten Kapitels eine Einführung in die Theorie der formalen Potenzreihen geben. Insbesondere werden wir Körper formaler Potenzreihen untersuchen und der Frage nachgehen, welches die Quadrate in einem solchen Körper sind. Wir werden erkennen, daß diese Frage vollständig zu beantworten ist und in (1.35) eine Charakterisierung der Quadrate in Körpern formaler Potenzreihen geben.

In den folgenden zwei Kapiteln werden wir stets von formal reellen Körpern reden. Auf diese wichtige Generalvoraussetzung wird auch im Text noch an mehreren Stellen hingewiesen werden.

## pythagoreische Körper

Im zweiten Kapitel werden wir uns mit *pythagoreischen* Körpern befassen. Wir nennen einen Körper  $K$  pythagoreisch, wenn die Summe einer endlichen Zahl von Quadraten aus  $K^\times$  stets wieder ein Quadrat aus  $K^\times$  ist (vgl. (2.1)); dabei beschränken wir uns allerdings lediglich auf formal reelle Körper, da ansonsten, wie wir kurz folgern, der Körper bereits quadratisch abgeschlossen wäre und folglich die Eigenschaft *pythagoreisch* nichts besonderes mehr an sich hätte.

Neben einigen weiteren Charakterisierungen pythagoreischer Körper werden wir zunächst untersuchen, wann ein Körper einen Erweiterungskörper besitzt, der pythagoreisch ist. Wir werden den Begriff der *pythagoreischen Hülle* in (2.4) einführen und dann erkennen, daß jeder formal reelle Körper eine pythagoreische Hülle besitzt; die pythagoreische Hülle ist sogar bis auf Isomorphie eindeutig (vgl. (2.5)). Schließlich gelingt es uns sogar, eine Konstruktion für die pythagoreische Hülle eines Körpers  $K$  explizit anzugeben (vgl. (2.9)).

Durch die Untersuchung der Anordnungen der pythagoreischen Hülle eines Körpers werden wir in der Lage sein zu folgern, daß sich jede Anordnung

eines Körpers  $K$  stets auf seine pythagoreische Hülle fortsetzen läßt (vgl. (2.12)); die pythagoreische Hülle ist sogar die größte 2-Erweiterung von  $K$ , auf die sich alle Anordnungen von  $K$  fortsetzen lassen. In (2.16) werden wir ferner feststellen, daß, wenn  $K$  eine Körpererweiterung  $E$  von endlichem Grad besitzt, die pythagoreisch ist, bereits  $K$  selbst pythagoreisch ist.

Schließlich werden wir noch der Frage nachgehen, wann ein Körper formaler Potenzreihen über einem Körper  $K$  pythagoreisch ist; wir werden erkennen, daß dies genau dann der Fall ist, wenn bereits  $K$  ein pythagoreischer Körper ist. Mit dieser Untersuchung schließen wir das zweite Kapitel und betrachten im folgenden euklidische Körper als Erweiterungen pythagoreischer Körper mit speziellen zusätzlichen Eigenschaften.

### euklidische Körper

Einen pythagoreischer Körper, der genau eine Anordnung besitzt, nennen wir *euklidisch* (vgl. (3.1)). Nach (3.2) sind das genau die Körper, deren Quadrate eine Anordnung bilden. Wir folgern dann sofort die Existenz euklidischer Oberkörper. Neben einem weiteren Kennzeichnungssatz werden wir die Exaktheit einer Sequenz zwischen verschiedenen Quadratklassenkörpern erhalten (3.5), aus der wir einige nützliche Erkenntnisse folgern können. Wie bereits für pythagoreische Körper können wir auch für euklidische Körper folgern, daß Unterkörper mit endlichem Grad bereits euklidisch sein müssen.

Schließlich werden wir den Begriff der *euklidischen Hülle* erklären als einen minimalen euklidischen Oberkörper. Euklidische Körper besitzen genau eine Anordnung, und wir werden sehen, daß zu jeder Anordnung eines Körpers sogar eine euklidische Hülle existiert, die diese Anordnung fortsetzt (vgl. (3.13)).

Einigen Raum wird die Untersuchung der Anzahl euklidischer Teilkörper von  $\mathbb{R}$  einnehmen. Wir werden erkennen, daß die Zahl solcher Teilkörper sogar der Gesamtzahl von Teilmengen in  $\mathbb{R}$  entspricht. Wie schon bei den pythagoreischen Körpern werden wir unsere Betrachtungen mit Überlegungen zu den Körpern formaler Potenzreihen über euklidischen Körpern beenden.

# Kapitel 1

## Vorbereitungen

Dieses einführende Kapitel dient der Klärung der Definitionen und soll dem Leser die zugrundeliegenden Schreibweisen und Sätze näherbringen. Der Umfang einer klassischen Algebra-Vorlesung wird dabei als bekannt vorausgesetzt. Der interessierte Leser sei außerdem auf die entsprechende Fachliteratur im Literaturverzeichnis hingewiesen, hier besonders die Arbeit von Priess-Crampe<sup>1</sup> und Jacobson<sup>2</sup>, deren Schreibweise hier weitestgehend gefolgt wird.

In allen Kapiteln bezeichne stets, falls es nicht ausdrücklich anders erklärt wird,  $K$  einen Körper mit einer Charakteristik  $\neq 2$ , sowie  $K^2 := \{x^2 : x \in K^\times\}$  die Menge der Quadrate in  $K^\times$ ,  $\sigma(K)$  bezeichne alle Summen von Elementen aus  $K^2$ , das sind alle Elemente, die sich als Summe von Quadraten in  $K^\times$  schreiben lassen.

Körper der Charakteristik 2 werden wir bewußt ausschließen, da für diese in unserem Zusammenhang kaum sinnvolle Ergebnisse erzielt werden können.

Wir werden „ $\subset$ “ bzw. „ $\supset$ “ schreiben, um anzuzeigen, daß es sich um eine **echte** Teilmenge resp. Obermenge handelt. Soll auch die Gleichheit zulässig sein, so werden wir stattdessen die Symbole „ $\subseteq$ “ bzw. „ $\supseteq$ “ verwenden.

---

<sup>1</sup>[PC83]

<sup>2</sup>[Jac80a]

## 1.1 Die Theorie von Artin und Schreier

Da wir im Zusammenhang mit pythagoreischen und euklidischen Körpern stets wissen müssen, welches die positiven Elemente eines Körpers sind, benötigen wir zuallererst eine Definition des Begriffs der Anordnung.

**Definition 1.1** *Unter einer Anordnung eines Körpers  $K$  versteht man eine Teilmenge  $P \subset K$  mit folgenden Eigenschaften:*

- a)  $0 \notin P$ ,
- b) Für  $0 \neq x \in K$  gilt entweder  $x \in P$  oder  $-x \in P$ ,
- c)  $P$  ist abgeschlossen unter Addition und Multiplikation.

*Die Elemente von  $P$  werden als positive Elemente bezeichnet.*

Mit dieser Definition sagen wir kurz auch  $P$  ist eine Anordnung von  $K$ . Gleichbedeutend mit Definition 1.1 ist folgende Charakterisierung:

**Satz 1.2** *Für eine Anordnung  $P$  eines Körpers  $K$  gilt:*

- a)  $P$  ist abgeschlossen unter Addition und Multiplikation,
- b)  $P \cap (-P) = \emptyset$ ,     und
- c)  $P \cup (-P) = K^\times$ ,

*wobei hier wie üblich  $(-P) := \{p : (-p) \in P\}$  sei.*

ANMERKUNG: *Es ist ebenfalls nicht unüblich, die Null des Körpers als Element der Anordnung zuzulassen. Bei Bourbaki<sup>3</sup> etwa wird eine Anordnung durch die drei Eigenschaften: 1.  $P + P \subseteq P$ , 2.  $PP \subseteq P$ , 3.  $P \cap (-P) = \{0\}$  erklärt, wobei die Anordnung total genannt wird, wenn 4.  $P \cup (-P) = K$  erfüllt ist.*

---

<sup>[1.1]</sup>Siehe [Lam73, chap.8, Def.1.2], [Jac80a, Def.5.1] oder auch [PC83, II.§1 Satz 1]

<sup>3</sup>[Bou88]

Da es allerdings in unserem Zusammenhang stets umständlich wäre, die Null separat zu behandeln, wollen wir mit obiger Definition arbeiten.  $\diamond$

Da ein Körper  $K$  mitunter mehrere Anordnungen besitzt, werden Elemente, die positiv unter allen Anordnungen sind, *total positiv* genannt. Aus  $a \cdot a = a^2 = (-a)(-a)$  für ein  $a \in K^\times$  folgt sofort, daß alle Quadrate total positiv sind. Mit (1.1) wird sofort klar:

**Lemma 1.3** *Es sei  $K$  ein Körper mit mindestens einer Anordnung. Die total positiven Elemente eines Körpers  $K$  sind dann genau die Summen von Quadraten in  $K$ , also  $\sigma(K)$ .*

Teilmengen von Anordnungen, die lediglich die Abgeschlossenheitsrelationen erfüllen, nennen wir Präordnungen:

**Definition 1.4** *Unter einer Präordnung eines Körpers  $K$  verstehen wir eine Teilmenge  $P \subset K^\times$ , die sowohl additiv, als auch multiplikativ abgeschlossen ist; für die also  $P \cdot P \subseteq P$ ,  $P + P \subseteq P$  gilt.*

Der folgende Satz, der auf Artin zurückgeht, begründet die Namenswahl „Präordnung“:

**Satz 1.5 (Artin)** *Jede Präordnung eines Körpers ist der Durchschnitt von Anordnungen.*

Artin und Schreier haben den Begriff der formal reellen Körper eingeführt und eine Theorie entwickelt, auf deren Basis Artin später eines der Hilbertschen Probleme lösen konnte<sup>4</sup>.

**Definition 1.6** *Ein Körper  $K$  heißt formal reell, wenn  $(-1) \in K$  nicht Summe von Quadraten aus  $K$  ist. Mit dem zuvor eingeführten Symbol bedeutet dies:*

$$K \text{ formal reell} \iff (-1) \notin \sigma(K)$$

---

<sup>4</sup>Es war dies Hilberts siebzehntes Problem, das die Frage nach der Positivität spezieller rationaler Funktionen in  $n$  Unbestimmten stellte. Vergleiche hierzu etwa [Jac80b].

[<sup>1-6</sup>]Siehe [Lam73, chap.8,p.223] sowie [Jac80b, Def.11.1]

Nun ist offenkundig ein Körper, der eine Anordnung besitzt, formal reell. Artin und Schreier haben gezeigt, daß die Umkehrung ebenfalls gilt:

**Satz 1.7 (Artin/Schreier)** *Ein Körper  $K$  besitzt genau dann eine Anordnung, wenn  $K$  formal reell ist.*

Besitzt ein Körper nun eine Anordnung, so ist als nächstes die Frage interessant, ob und auf welche Körpererweiterungen sich die Anordnung fortsetzen läßt. Diese Frage beantwortet zu Teilen der folgende Satz:

**Satz 1.8** *Sei  $K$  ein Körper mit einer Anordnung  $P$ : sei ferner  $f$  ein irreduzibles Polynom aus  $K[x]$ . Existieren  $a, b \in K$  so, daß  $f(a)f(b) < 0$ , dann existiert eine Fortsetzung von  $P$  auf  $L := K[x]/(f)$ .*

Dieser Satz erlaubt es uns, leicht zu charakterisieren, wann eine Anordnung auf einen Erweiterungskörper fortsetzbar ist:

Zunächst betrachten wir als einfache Folgerung aus (1.8) das folgende Lemma:

**Lemma 1.9** *Sei  $K$  ein Körper, versehen mit einer Anordnung  $P$ ; sei ferner  $L = K(\gamma)$  mit einer Nullstelle  $\gamma$  von  $x^2 - c$ ,  $0 < c \in K$ . Dann existiert eine Fortsetzung der Anordnung von  $K$  auf  $L$ , d.h. eine Anordnung  $P'$  von  $L$ , mit  $P' \cap K = P$ .*

Auch das nachstehende Lemma ist eine Folgerung aus (1.8):

**Lemma 1.10** *Sei  $K$  ein Körper, versehen mit einer Anordnung  $P$ . Sei ferner  $L$  eine Erweiterung ungeraden Grades über  $K$ . Dann existiert eine Fortsetzung der Anordnung von  $K$  auf  $L$ .*

---

<sup>[1.7]</sup>Siehe [Lam73, chap.8,cor.1.10], [PC83, 11.§2 Satz 2] sowie [Jac80b, Th.11.1]

<sup>[1.8]</sup>Siehe [PC83, II.§2 Lemma 4] oder [Jac80b, p.633 Lemma 2]

<sup>[1.9]</sup>Siehe [PC83, II.§2 Lemma 5]

<sup>[1.10]</sup>Siehe [PC83, II.§2 Lemma 6]

Wir wollen ebenfalls beachten, daß mit dem Satz von Artin/Schreier also jede Körpererweiterung gemäß (1.9) und (1.10) eines formal reellen Körpers wieder formal reell ist.

Die Eigenschaft *formal reell* läßt es weiter zu, den Begriff der Abgeschlossenheit wie folgt einzuführen:

**Definition 1.11** *Sei  $K$  ein formal reeller Körper, der keine echt algebraische Erweiterung besitzt, die formal reell ist. Dann heißt  $K$  reell abgeschlossen.*

In einem reell abgeschlossenen Körper hat jedes positive Element bereits eine Quadratwurzel in  $K$ , oder anders geschrieben:

**Satz 1.12** *Sei  $K$  ein reell abgeschlossener Körper, versehen mit der Anordnung  $P$ . Dann ist  $P = K^2$ . Insbesondere ist  $P$  eindeutig bestimmt.*

Wie immer interessieren bei algebraischen Eigenschaften stets Existenz und Eindeutigkeit. Darüber verschaffen uns die folgenden zwei Sätze einen Überblick:

**Satz 1.13** *Zu jedem formal reellen Körper  $K$  gibt es eine algebraische Erweiterung  $L$  so, daß  $L$  reell abgeschlossen ist und sich die Anordnung  $P$  von  $K$  zu einer Anordnung  $P_L$  von  $L$  fortsetzen läßt. Außerdem ist  $L$  bis auf  $K$ -Isomorphie eindeutig bestimmt.*

Der Beweis dieses Satzes macht Gebrauch vom Zorn'schen Lemma. Die folgende Definition ist damit in natürlicher Weise gegeben:

**Definition 1.14** *Es seien die Beziehungen wie in Satz 1.13 gegeben. Der Körper  $L$  wird dann reeller Abschluß von  $K$  genannt.*

Darüber hinaus macht man sich leicht klar, daß folgendes Lemma gilt:

**Lemma 1.15** *Die Anordnung in einem reellen Abschluß sind genau seine Quadrate.*

---

<sup>[1.11]</sup>Siehe [Lam73, chap.8,Def.1.8] oder [PC83, Seite 23f.]

<sup>[1.12]</sup>Siehe [PC83, II.§2, Lemma 7, Satz 8] sowie [Lam73, chap.8, Th.1.8]

<sup>[1.13]</sup>Siehe [PC83, II.§Satz 3] oder auch [Jac80b, Th.11.4] sowie [Lam73, chap.8 prop.1.9]

Es folgt noch ein letzter Satz, der einen Zusammenhang zwischen reell abgeschlossenen und algebraisch abgeschlossenen Körpern herstellt:

**Satz 1.16** *Genau dann ist  $K$  reell abgeschlossen, wenn  $K(i)$  algebraisch abgeschlossen ist, wobei hier  $i$  eine Wurzel des Polynoms  $X^2 + 1$  bezeichnet.*

## 1.2 Algebraische Galoiserweiterungen

Dieser Abschnitt soll noch einmal diejenigen Tatsachen über algebraische Galoiserweiterungen zusammenstellen, die in dieser Arbeit benötigt werden.

**Definition 1.17** *Es seien  $E, K$  Körper, wobei  $E$  eine Erweiterung von  $K$  sein soll.*

*Ein Element  $e$  von  $E$  heißt algebraisch über  $K$ , wenn  $e$  die Wurzel eines Polynoms mit Koeffizienten aus  $K$  ist; ansonsten heißt  $e$  transzendent.*

*$E$  heißt eine algebraische Erweiterung von  $K$ , wenn jedes Element von  $E$  algebraisch über  $K$  ist.*

Einige einfache und bekannte Aussagen fassen wir in dem folgenden Lemma zusammen. Die Beweise sind in jedem ausreichend umfassenden Algebra-Buch zu finden.

**Lemma 1.18** *Seien  $E, K$  Körper mit  $E \supseteq K$ . Ist  $e \in E$  algebraisch über  $K$ , so existiert ein eindeutig bestimmtes irreduzibles normiertes Polynom  $f_e \in K[X]$ , zu dem  $e$  eine Wurzel ist.*

*Sei  $f$  ein weiteres normiertes Polynom in  $K[X]$  mit Wurzel  $e$ , so gilt:  $f_e | f$ .*

## 1.3 Die maximale $p$ -Erweiterung eines Körpers

**Definition 1.19** Sei  $K$  ein Körper sowie  $p$  eine Primzahl. Unter der maximalen  $p$ -Erweiterung  $K_p$  von  $K$  versteht man das Kompositum aller endlichen Galoiserweiterungen  $E \subset \overline{K}$  von  $K$ , dessen Grad über  $K$  eine  $p$ -Potenz ist.

Wieder ist es möglich, einen Abschlußbegriff einzuführen:

**Definition 1.20** Ein Körper  $K$  heißt  $p$ -abgeschlossen, wenn  $K = K_p$ .

Wir werden in dieser Arbeit mehrmals mit 2-abgeschlossenen Körpern befaßt sein und benötigen dafür Aussagen über diese. Im folgenden Satz werden wir deshalb allgemeine Aussagen für ein beliebiges  $p$  erklären und beweisen, da dies keinen weiteren Aufwand erfordert:

**Satz 1.21** Für die maximale  $p$ -Erweiterung eines Körpers gilt:

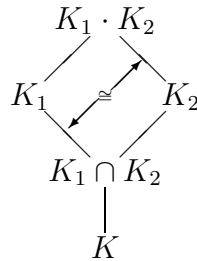
- a)  $K_p$  ist die Vereinigung  $V$  aller der oben beschriebenen Körper  $E$ .
- b)  $K_p/K$  ist galoissch.
- c) Genau dann ist  $K$   $p$ -abgeschlossen, wenn  $K$  keine zyklische Erweiterung vom Grad  $p$  besitzt.

**BEWEIS:** Zum Beweis von a) genügt zu zeigen, daß mit  $a$  und  $b$  aus zwei endlichen Galoiserweiterungen vom Grad einer  $p$ -Potenz über  $K$  eine Galoiserweiterung existiert, die beide enthält und deren Grad über  $K$  ebenfalls eine  $p$ -Potenz ist: Seien  $a \in K_1$  und  $b \in K_2$  mit den eben genannten Eigenschaften. Dann ist  $K_1 \cap K_2$  Erweiterungskörper vom Grad einer  $p$ -Potenz über  $K$  (und eventuell mit  $K$  identisch).  $K_1/K$  ist galoissch. Mit dem Translationsatz folgt, daß  $K_1 \cdot K_2/K_2 \cong K_1/K_1 \cap K_2$ . Da der Grad von  $K_1/K_1 \cap K_2$  ebenfalls eine  $p$ -Potenz ist, folgt somit die Behauptung.

---

[1.19] Siehe [Bec73, Seite 42 Nr.1]

[1.21] Siehe [Bec73, Seite 42 Nr.1]



Mit Teil a) folgt der Nachweis von b) sofort: Bekanntlich ist eine Körpererweiterung genau dann galoissch, wenn sie normal und separabel ist (Artin). Jedes Element  $a \in K_p$  ist bereits enthalten in einer endlichen Galoiserweiterung  $E$ , da  $K_p$  eine Vereinigung solcher Erweiterungskörper ist. Mit  $E$  ist aber  $a$  bereits separabel über  $K$ . Betrachten wir ein beliebiges irreduzibles Polynom  $\phi(x) \in K[x]$ , das eine Nullstelle  $a$  in  $K_p$  besitzt. Mit a) ist aber  $a$  schon enthalten in einer endlichen Galoiserweiterung  $E$ , so daß  $\phi(x)$  in  $E[x] \subset K_p[x]$  bereits in Linearfaktoren zerfällt. Also ist  $K_p/K$  galoissch.

Für Teil c) ist nur zu zeigen, daß im Fall  $K \neq K_p$  in  $K_p$  stets eine zyklische Erweiterung von  $K$  mit Grad  $p$  enthalten ist. Die Gegenrichtung ist trivial. Nehmen wir also an:  $K_p \neq K$ . Dann existiert mindestens eine endliche Galoiserweiterung  $E$  von  $K$ , deren Grad über  $K$  eine  $p$ -Potenz ist, etwa  $p^n$ . Wir wissen, daß die Galoisgruppe von  $E/K$  eine Untergruppe vom Index  $p$  besitzt. Diese ist wiederum ein Normalteiler, so daß mit dem Hauptsatz der Galoistheorie  $K$  einen endlich-galoisschen Erweiterungskörper vom Grad  $p$  besitzt, und dieser ist zyklisch.  $\square$

## 1.4 Potenzreihenkörper

Die Einführung von Körpern formaler Potenzreihen geht zurück auf Hilbert und Hahn. Wir benötigen diese jedoch nur in einer sehr allgemeinen Form. Daher schildern wir eine Konstruktion, die von B.H. Neumann stammt. Die dafür notwendigen Erkenntnisse werden wir im folgenden kurz schildern. Außerdem werden wir eine eigene Charakterisierung der Quadrate in Körpern

formaler Potenzreihen gewinnen, die uns die Handhabung dieser Körper in den von uns benötigten Fällen bedeutend vereinfacht. Wir stützen uns bei unseren Ausführungen sowie bei Sätzen, die wir nicht beweisen, stets auf [Wäh92], [Kal89] sowie [Tsc81].

**Definition 1.22** Sei  $G = (G, +, \leq)$  eine angeordnete Gruppe, sowie  $K$  ein Schiefkörper. Jede Abbildung  $p : G \rightarrow K$ , deren Träger  $T(p) := \{x \in G \mid p(x) \neq 0\}$  bezüglich „ $\leq$ “ wohlgeordnet ist, heiÙe eine formale Potenzreihe auf  $G$  über  $K$  (oder auch mit Koeffizienten aus  $K$ ). Wir schreiben  $p$  in der Form  $\sum_{x \in T(p)} t^x p_x$ , wobei  $p_x := p(x)$ . Die Menge aller formalen Potenzreihen auf  $K$  über  $G$  sei bezeichnet mit  $H(G, K)$ .

Für den Rest dieses Abschnitts bezeichne nun  $G$  stets eine angeordnete Gruppe, sowie  $K$  einen Schiefkörper. Offensichtlich ist die folgende Aussage:

**Satz 1.23**  $(H(G, K), +)$  mit der inneren Verknüpfung  $+$ , definiert durch

$$(p + q)(x) := p(x) + q(x), \quad x \in G, p, q \in H(G, K)$$

ist eine abelsche Gruppe.

Bevor eine Verknüpfung, die als Multiplikation angesehen werden kann, definiert wird, müssen wir den Begriff des *Faktorensystems* kennenlernen:

**Definition 1.24** Man nennt zwei Abbildungen  $f : G \times G \rightarrow K^\times$ ,  $\omega : G \rightarrow \text{Aut } K$  ein Faktorensystem, wenn die folgenden Bedingungen erfüllt sind:

$$(I) \quad f(a, b) \cdot d^{\omega(a)\omega(b)} = d^{\omega(a+b)} f(a, b)$$

$$(II) \quad f(a + b, c) f(a, b)^{\omega(c)} = f(a, b + c) f(b, c)$$

$$(III) \quad f(e, x) = 1 = f(x, e), \quad \omega(e) = \text{Id}$$

jeweils mit  $a, b, c, x \in G$ ,  $d \in K$ . Für  $p, q \in H(G, K)$  werde dann  $pq$  definiert durch

$$(pq)(z) := \sum_{\substack{x+y=z \\ (x,y) \in T(p) \times T(q)}} f(x, y) p(x)^{\omega(y)} q(y). \quad (*)$$

---

[1.22] Siehe [Wäh92, Seite 44]

[1.23] Siehe [Wäh92, Seite 45]

[1.24] Siehe [Wäh92, Seite 45]

Für (\*) bleibt die Wohldefiniertheit noch zu zeigen. Diese folgt aber sofort aus dem folgenden Lemma:

**Lemma 1.25** *Für wohlgeordnete Teilmengen  $S, T$  von  $G$  gilt:*

( $\alpha$ )  $S + T$  ist wohlgeordnet.

( $\beta$ ) Zu jedem  $z \in S + T$  existieren nur endlich viele Paare  $(x, y) \in S \times T$  mit  $x + y = z$ .

So daß wir schließlich folgenden Satz erhalten:

**Satz 1.26** *Die für  $p, q \in H(G, K)$  durch (\*) erklärte innere Verknüpfung ist wohldefiniert und der Träger von  $(pq)$  wohlgeordnet.*

(\*) besagt im wesentlichen:

$$t^x p_x \cdot t^y p_y = t^{x+y} f(x, y) p_x^{\omega(y)} p_y$$

Also in der üblichen Summenschreibweise

$$\left( \sum_{x \in T(p)} t^x p_x \right) \cdot \left( \sum_{y \in T(q)} t^y p_y \right) = \sum_{z \in T(p \cdot q)} t^z \left( \sum_{\substack{x+y=z \\ (x,y) \in T(p) \times T(q)}} f(x, y) p(x) q(y) \right).$$

Offenbar erfüllt immer das triviale Faktorensystem  $f : (x, y) \mapsto 1$ ,  $\omega : \tau \mapsto \text{Id}_K$  die Bedingungen (I), (II) und (III). Für ein spezielles Faktorensystem wollen wir im folgenden  $H(G, K)$  genauer durch  $H_{f,\omega}(G, K)$  bezeichnen.

Der folgende Satz wurde für triviale Faktorensysteme bereits 1907 von H.Hahn und F.Hausdorff bewiesen; die allgemeine Fassung allerdings stammt von B.H.Neumann:

**Satz 1.27 (Neumann 1949)** *Es sei  $G = (G, +, \leq)$  eine angeordnete Gruppe,  $K$  ein Schiefkörper und  $(f, \omega)$  ein Faktorensystem. Dann ist die Menge der formalen Potenzreihen auf  $K$  über  $G$ , bezeichnet durch  $H_{f,\omega}(G, K)$ , ein Schiefkörper.*

---

[1.25] Siehe [Wäh92, Seite 45]

[1.26] Siehe [Wäh92, (2)]

[1.27] Siehe [Wäh92, (4)]

Man kann sogar noch etwas weiter gehen und zeigen, daß *jeder* angeordnete Schiefkörper  $K$  in einen angeordneten Schiefkörper  $H$  einbettbar ist. Es ist sogar jeder Schiefkörper  $K$  in jeden Schiefkörper formaler Potenzreihen über  $K$  einbettbar.

Da wir in dieser Arbeit allerdings unser Augenmerk stets auf Körper gerichtet haben, ist es interessant und notwendig zu wissen, unter welchen Einschränkungen ein Körper  $K$  wieder einen Körper  $H_{f,\omega}(G, K)$  liefert. Dazu beweisen wir folgenden Satz:

**Satz 1.28** *Unter den Voraussetzungen von (1.27) ist  $H = H_{f,\omega}(G, K)$  genau dann kommutativ, wenn  $K$  und  $G$  kommutativ sind,  $f$  symmetrisch ist und  $\omega(x) = \text{Id}$  für alle  $x \in G$ .*

BEWEIS: Die Notwendigkeit folgt sofort aus (\*), so daß nur „ $\Rightarrow$ “ zu zeigen bleibt. Sei also  $H$  kommutativ. Da eine Einbettung von  $K$  in  $H$  existiert (s. Bemerkung nach 1.27), ist auch  $K$  kommutativ. Mit den speziellen Potenzreihen  $t^a$  und  $t^b$  etwa erhalten wir aus (\*): Es ist  $t^a t^b(a+b) = f(a,b)$  und  $t^a t^b(x) = 0$  für  $x \neq a+b$ . Für das vertauschte lautende Produkt erhalten wir  $t^b t^a(b+a) = f(b,a)$  und  $t^b t^a(x) = 0$  mit  $x \neq b+a$ , so daß wegen der Kommutativität von  $H$  sofort aus der Gleichheit der beiden  $a+b = b+a$  und  $f(a,b) = f(b,a)$  zwingend erforderlich wird.

Für  $k \in K$  und  $x \in G$  gilt:

$$(\epsilon(k) \cdot \tau(x)) = f(e, x)\epsilon(k)(e)^{\omega(x)} \cdot \tau(x)(x) = k^{\omega(x)}$$

und

$$(\tau(x) \cdot \epsilon(k)) = f(x, e)\tau(x)(x)^{\omega(e)} \cdot \epsilon(k)(e) = k.$$

Das schließlich zeigt  $\omega(x) = \text{Id}$ . □

Wir werden im folgenden mit  $H_f(G, K)$  einen Körper formaler Potenzreihen bezeichnen, dabei sei  $G = (G, +, \leq)$  eine angeordnete Gruppe,  $K$  ein Körper und  $f : G \times G \rightarrow K^\times$  eine symmetrische Abbildung. Gemäß unseren bisherigen Erkenntnisse ist  $H_f(G, K)$  ein Körper. Für  $p, q \in H_f(G, K)$  ist dann  $(p+q)(x) = p(x) + q(x)$ ,  $(p \cdot q)(x) = \sum_{\substack{z+y=x \\ (z,y) \in T(p) \times T(q)}} f(z, y)p(z)q(y)$  mit  $x \in G$ .

---

[1.28] Siehe [Wäh92, (8)]

Nach der nun folgenden Untersuchung der Quadrate in  $H_f(G, K)$  werden wir noch eine weitere Forderung an  $f$  stellen müssen:  $f(a, b)$  wird dann als  $G \times G \rightarrow P_K$  mit  $P_K$  einer Anordnung von  $K$  erklärt werden.

An dieser Stelle ist es zweckmäßig, zwei weitere Abbildungen zu definieren:

$$\text{ord} : H_f(G, K) \rightarrow G, \quad \text{sowie} \quad \text{anf} : H_f(G, K) \rightarrow K$$

Definitionen und Sätze werden dadurch erheblich besser lesbar sein:

Ist  $p$  aus  $H_f(G, K)$ , und ist  $x_0 = \min T(p)$  das kleinste Element des Trägers von  $p$ , so werden wir  $t^{x_0}p_{x_0}$  als den *Anfangsterm von  $p$*  bezeichnen;  $\text{anf}(p) := p_{x_0}$  als den *Anfangskoeffizienten*, sowie  $\text{ord}(p) := x_0$  als dessen Ordnung.

Für die leere Potenzreihe setzen wir als Ordnung  $\text{ord}(0) := \infty$ , sowie den Anfangskoeffizienten  $\text{anf}(0) = 0_K$ .

Es ist maßgeblich vom Anfangskoeffizienten, so werden wir sogleich sehen, abhängig, ob  $p$  ein Quadrat ist oder nicht:

**Lemma 1.29** *Es sei  $p \in H_f(G, K)^\times$  mit dem Anfangskoeffizienten  $p_{x_0}$ . Ist  $p$  ein Quadrat, so existiert ein  $y \in G$ , so daß  $x_0 = 2y$  und  $p_{x_0}/f(y, y) \in K^2$ .*

BEWEIS: Sei  $q \in H_f(G, K)^\times$ , und sei  $t^y q_y$  der Anfangsterm von  $q$ , so ist der Anfangsterm von  $q \cdot q$  gemäß (\*) gleich  $f(y, y)t^{2y}q_y^2$ .  $\square$

Bevor wir uns auf die Suche nach allen Quadraten in  $H_f(G, K)$  machen, wollen wir nur kurz folgendes mengentheoretische Lemma einfügen, das im Beweis benötigt wird und welches in [PC83] auch bewiesen wird.

**Lemma 1.30** *Sei  $S$  eine wohlgeordnete Teilmenge des Positivitätsbereichs einer angeordneten abelschen Gruppe  $(G, \cdot)$ . Sei ferner  $T := \bigcup_{n \in \mathbf{N}} S^n$  die von  $S$  erzeugte Unterhalbgruppe. Dann ist  $T$  eine wohlgeordnete Teilmenge von  $G$ .*

Die folgenden vier Lemmata dienen der Kennzeichnung der Quadrate in  $H_f(G, K)$ .

---

<sup>[1.30]</sup>Siehe [PC83, II,§5, Lemma 14]

**Lemma 1.31** Für  $p, p' \in H_f(G, K)$  mit  $\text{ord}(p) = 0 = \text{ord}(p')$  und  $\text{anf}(p) = \text{anf}(p')$  gilt:

$$\text{ord}(p^2 - p'^2) = \text{ord}(p - p')$$

**BEWEIS:** Es bezeichne  $r := p - p' \in H_f(G, K)$ , sowie  $s := p^2 - p'^2 \in H_f(G, K)$ . Nach den Voraussetzungen gilt:  $\text{ord}(r) > 0$ ; und zwar bestimmt sich die Ordnung von  $r$  als das kleinste Element  $m$  in  $T(p) \cup T(p')$ , für das  $p_m \neq p'_m$  ist.

Mit Hilfe von (\*) erhalten wir für  $s(m)$ :

$$s(m) = \sum_{\substack{(\alpha, \beta) \in T(p) \times T(p) \\ \alpha + \beta = m}} f(\alpha, \beta) p_\alpha p_\beta - \sum_{\substack{(\alpha, \beta) \in T(p') \times T(p') \\ \alpha + \beta = m}} f(\alpha, \beta) p'_\alpha p'_\beta.$$

Aufgrund der Voraussetzungen ist  $p(\alpha) = 0 = p'(\alpha)$  für alle  $\alpha < 0$ , ferner ist  $p(\alpha) = p'(\alpha)$  für  $\alpha < m$ . Daraus allerdings folgt sofort:  $p_\alpha p_\beta = p'_\alpha p'_\beta$  für alle  $\alpha, \beta < m$ , für die auch  $\alpha + \beta < m$ . Also bestehen die Summen in der obigen Gleichung jeweils lediglich aus den beiden Termen zu den Tupeln  $(0, m)$  und  $(m, 0)$ , so daß wir erhalten:

$$s(m) = 2f(0, m)p_0p_m - 2f(0, m)p'_0p'_m = 2f(0, m)p_0(p_m - p'_m) \neq 0$$

und daher  $m \in T(s)$ .

Angenommen, es existiere ein  $n \in T(s)$  mit  $n < m$ . Dann existieren  $0 \leq n_1, n_2 \leq n$  in  $T(p)$  oder  $T(p')$  so, daß  $n_1 + n_2 = n$ . Außerdem gilt dann  $p_{n_i} \neq p'_{n_i}$  für  $i$  gleich 1 oder 2, da sonst der resultierende Term in der Differenz verschwände. Dies allerdings widerspricht wiederum der Minimalität von  $m$ .  $\square$

Sei nun ein  $q \in H_f(G, K)$  gegeben mit  $\text{ord}(q) = 0$ ,  $\text{anf}(q) = 1$ , so bezeichne  $A$  die von  $T(q)$  erzeugte Unterhalbgruppe von  $G$ . Mit  $T(q)$  ist nach (1.30) auch  $A$  wohlgeordnet:

**Lemma 1.32** Zu jedem  $\epsilon \in A$  existiert genau ein  $p_\epsilon \in H_f(G, K)$  mit den Eigenschaften

- a)  $T(p_\epsilon) \subseteq A$ ,
- b)  $p_\epsilon(\gamma) = 0$  für jedes  $\gamma > \epsilon$ ,

$$c) \text{ ord}(q - p_\epsilon^2) > \epsilon .$$

BEWEIS: *Existenz:* Es sei  $\epsilon' \in A$  gegeben, und die Behauptung sei richtig für jedes  $\epsilon < \epsilon'$  aus  $A$ . Im Fall  $\epsilon' = 0$  ist  $p_0 := 1$  die eindeutig bestimmte Lösung. Im Fall  $\epsilon' > 0$  sind zwei Fälle zu unterscheiden:

1. Fall:  $\epsilon'$  hat in  $A$  einen unmittelbaren Vorgänger  $\epsilon$ . Dann sei  $p'$  definiert als  $p' := p_\epsilon$ .
2. Fall:  $\epsilon'$  ist Limeszahl in  $A$  (d.h. es gibt in  $A$  keinen unmittelbaren Vorgänger). Dann sei  $p'$  erklärt durch

$$p'(\alpha) := \begin{cases} p_\alpha(\alpha) & \text{für jedes } \alpha < \epsilon' \text{ aus } A, \\ 0 & \text{sonst.} \end{cases}$$

Seien nun  $\alpha, \beta \in A$  mit  $\alpha \leq \beta < \epsilon'$ . Mit den Voraussetzungen folgt aus  $\text{ord}(q - p_\alpha^2) > \alpha$  und  $\text{ord}(q - p_\beta^2) > \alpha$  sofort:  $\text{ord}(p_\beta^2 - p_\alpha^2) > \alpha$  und damit (nach Lemma 1.31) auch  $\text{ord}(p_\beta - p_\alpha) > \alpha$ . Damit ist offensichtlich  $p_\alpha(\gamma) = p_\beta(\gamma)$  für alle  $\gamma < \alpha$ . Aus  $\beta < \epsilon'$  folgt damit  $p_\beta(\alpha) = p_\alpha(\alpha) \stackrel{!}{=} p'(\alpha)$ , und deshalb  $\text{ord}(p' - p_\beta) > \beta$ . Wiederum mit (1.31) erhält man sofort  $\text{ord}(p'^2 - q) > \beta$ . Für  $p'$  und für  $\alpha \leq \beta < \epsilon'$ ,  $\alpha, \beta \in A$  haben wir also gezeigt:

$$(I) \quad p'(\alpha) = p_\alpha(\alpha) \stackrel{!}{=} p_\beta(\alpha) \Rightarrow \text{ord}(p' - p_\beta) > \beta \stackrel{(1.31)}{\Rightarrow} \text{ord}(p'^2 - q) > \beta$$

Jetzt setzen wir

$$p_\epsilon(\gamma) := \begin{cases} p'(\gamma) & \text{für } \gamma < \epsilon, \\ \frac{1}{2f(0, \epsilon')} \left( q(\epsilon') - \sum_{\substack{\alpha, \beta \in T(p') \\ \alpha + \beta = \epsilon'}} f(\alpha, \beta) p'(\alpha) p'(\beta) \right) & \text{für } \gamma = \epsilon, \\ 0 & \text{sonst.} \end{cases}$$

Mit  $\alpha, \beta \in T(p')$  und  $T(p') \subseteq A$  (nach Voraussetzung) ist auch der Träger von  $p_\epsilon$  von  $T(p')$  erzeugt; liegt also in  $A$ .  $p'(\gamma) = 0$  für jedes  $\gamma > \epsilon'$  nach Konstruktion; also ist damit auch  $p_\epsilon(\gamma) = 0$  für jedes  $\gamma > \epsilon'$ . Einfache Anwendung der Produktformel (\*) schließlich liefert ( $\omega$  ist trivial) mit  $\text{ord}(p'^2 - q) > \beta$  (I) für alle  $\beta < \epsilon'$  zunächst  $\text{ord}(p'^2 - q) \geq \epsilon'$ , also auch  $\text{ord}(p_\epsilon^2 - q) \geq \epsilon'$ . Jetzt nutzen wir die spezielle Konstruktion von  $p_\epsilon^2(\epsilon')$  aus und erhalten damit:

$$p_\epsilon^2(\epsilon') = 2f(0, \epsilon') \frac{1}{2f(0, \epsilon')} \left( q(\epsilon') - \sum_{\substack{\alpha, \beta \in T(p') \\ \alpha + \beta = \epsilon'}} f(\alpha, \beta) p'(\alpha) p'(\beta) \right) +$$

$$+ \sum_{\substack{\alpha, \beta \in T(p') \\ \alpha + \beta = \epsilon'}} f(\alpha, \beta) p'(\alpha) p'(\beta) = q(\epsilon')$$

Dies schließlich läßt uns  $\text{ord}(q - p_\epsilon^2) > \epsilon$  gewinnen; die Bedingungen aus (1.32) gelten also auch für  $\epsilon'$  mit  $p_\epsilon$ . Transfinite Induktion begründet die Existenz der  $p_\epsilon$  mit den Eigenschaften a)–c).

*Eindeutigkeit:* Angenommen,  $p_\epsilon$  und  $p'_\epsilon$  erfüllen beide die Eigenschaften. Aus  $\text{ord}(q - p_\epsilon^2) > \epsilon$  und  $\text{ord}(q - p_\epsilon'^2) > \epsilon$  erhält man zunächst  $\text{ord}(p_\epsilon'^2 - p_\epsilon^2) > \epsilon$  und dann mit (1.31) sofort auch  $\text{ord}(p'_\epsilon - p_\epsilon) > \epsilon$ . Da aber nach Eigenschaft (b)  $p_\epsilon(\gamma) = p'_\epsilon(\gamma) = 0$  für alle  $\gamma > \epsilon$  gilt, verschwindet die Differenz vollständig;  $p'_\epsilon$  und  $p_\epsilon$  sind also gleich.  $\square$

Jetzt erklärt man  $p \in H_f(G, K)$  durch

$$p(\epsilon) := \begin{cases} p_\epsilon(\epsilon) & \text{für } \epsilon \in A, \\ 0 & \text{sonst.} \end{cases}$$

Es sei dabei  $p_\epsilon$  wie eben in (1.32) gewonnen. Dann ist nach den Bedingungen aus (1.32)  $T(p) \subseteq A$ , so daß  $p \in H_f(G, K)$ . Für jedes  $\epsilon' \in A$  und  $A \ni \epsilon \leq \epsilon'$  gilt, wiederum mit (1.31) und den Bedingungen aus (1.32), wie auch in (I):  $p(\epsilon) = p_\epsilon(\epsilon) = p_{\epsilon'}(\epsilon)$ . Damit erhalten wir sofort  $\text{ord}(q - p^2) > \epsilon$ .

Mit der Definition von  $A$  und der Konstruktion von  $p$  ist andererseits  $T(q) \subseteq A$  sowie auch  $T(p^2) \subseteq A$ . Daraus folgt  $(q - p^2)(\epsilon) = 0$  für jedes  $\epsilon \in G \setminus A$ . Damit folgt  $p^2 = q$  sofort.

Damit ist gezeigt:

**Lemma 1.33** *Jedes  $q \in H_f(G, K)$  mit  $\text{ord}(q) = 0$ ,  $\text{anf}(q) = 1$  ist ein Quadrat. Die multiplikative Untergruppe  $Q_f^e(G, K)$  aller solcher  $q$  wollen wir die [Gruppe der] Elementarquadrate nennen.*

Wir werden nun versuchen, eine möglichst große Klasse von Elementen von  $H_f(G, K)$  auf Quadrate in  $Q_f^e(G, K)$  zurückzuführen. Dazu benötigen wir folgendes Lemma:

**Lemma 1.34** *Jedes Element  $p \in H_f^\times(G, K)$  hat die Gestalt  $t^{\text{ord}(p)} \text{anf}(p) \cdot q$  mit  $q \in Q_f^e(G, K)$ .*

**BEWEIS:** Es sei  $p \in H_f(G, K)$ . Wir bezeichnen die Ordnung von  $p$  mit  $\alpha := \text{ord}(p)$ . Dann sei  $q$  definiert als  $q := p \cdot t^{-\alpha} \frac{1}{f(-\alpha, \alpha) \text{anf}(p)}$ . Unter Anwendung von (\*) ergibt sich

$$q(\gamma) = \sum_{\substack{\beta \in T(p) \\ -\alpha + \beta = \gamma}} f(-\alpha, \beta) \frac{1}{f(-\alpha, \alpha) \text{anf}(p)} p(\beta) .$$

Das heißt  $q(0) = f(-\alpha, \alpha) \frac{1}{f(-\alpha, \alpha) p(\alpha)} p(\alpha)$ , also  $\text{anf}(q) = 1$ , sowie  $\text{ord}(p) \leq 0$ . Wäre  $\text{ord}(q) = \epsilon < 0$ , so existierte ein  $\beta \in T(p)$  mit  $\beta - \alpha = \epsilon$ , also  $\beta < \alpha$  im Widerspruch zur Definition von  $\alpha$ . Also  $\text{ord}(q) = 0$ . Das zeigt  $q \in Q_f^e(G, K)$ .

Dann ergibt wiederum  $t^\alpha \text{anf}(p) \cdot q$  mit (\*):

$$\begin{aligned} (t^\alpha \text{anf}(p) \cdot q)(\gamma) &= \sum_{\substack{\beta \in T(q) \\ \alpha + \beta = \gamma}} f(\alpha, \beta) \text{anf}(p) q(\beta) = \\ &= \sum_{\substack{\beta \in T(q) \\ \alpha + \beta = \gamma}} f(\alpha, \beta) \text{anf}(p) \sum_{\substack{\delta \in T(p) \\ -\alpha + \delta = \beta}} f(-\alpha, \delta) \frac{1}{f(-\alpha, \alpha) \text{anf}(p)} p(\delta) = \end{aligned}$$

[Wichtig ist es, an dieser Stelle zu beachten, daß jede der beiden Summen genau aus einem Term besteht, so erhalten wir  $\beta := \gamma - \alpha$  und  $\delta = \beta$ ]

$$\begin{aligned} f(\alpha, \gamma - \alpha) \text{anf}(p) f(-\alpha, \gamma) \frac{1}{f(-\alpha, \alpha) \text{anf}(p)} p(\gamma) &= \\ \frac{f(\alpha, \gamma - \alpha) f(-\alpha, \gamma)}{f(-\alpha, \alpha)} p(\gamma) &= p(\gamma) \end{aligned}$$

Das Verschwinden des Bruchs im vorletzten Term überlegt man sich schnell selbst mit (II) und (III) aus (1.24) sowie  $a := \gamma$ ,  $b := -\alpha$ ,  $c := \alpha$  und  $\omega := 1_G$ . □

Mit (1.33) und (1.34) erhält man unmittelbar

**Satz 1.35** *Es sei  $p \in H_f(G, K)^\times$  mit dem Anfangsterm  $t^{x_0} p_{x_0}$ .  $p$  ist genau dann ein Quadrat, wenn ein  $y \in G$  existiert, so daß  $x_0 = 2y$  und  $p_{x_0}/f(y, y) \in K^2$ .*

**BEWEIS:** Die Richtung „ $\Rightarrow$ “ ist bereits in (1.29) gezeigt worden.

Für die Gegenrichtung betrachten wir

$$(t^y p_y)^2 = t^{2y} f(y, y) p_y^2 .$$

Zusammen mit (1.33) und (1.34) ergibt sich die obige Behauptung; denn nach (1.34) ist jedes  $p \in H_f(G, K)^\times$  ein Produkt eines  $t^y p_y$  und eines Elementarquadrats nach (1.33).  $\square$

Im folgenden werden wir noch der Frage nach den Anordnungen von  $H_f(G, K)$  nachgehen. Dabei werden wir versuchen, eine bestehende Anordnung  $P_K$  von  $K$  zu einer Anordnung  $P$  von  $H_f(G, K)$  fortzusetzen. Um überhaupt multiplikativ abgeschlossene Teilmengen zu erhalten, werden wir allerdings, wie bereits angekündigt, eine zusätzliche Anforderung an  $f$  stellen:  $f(x, y) \geq 0$  für alle  $x, y \in G$ . **Ein zulässiges  $f$  wird also von nun an auch über diese vierte Eigenschaft verfügen.**

Es sei nun  $K$  ein Körper, sowie  $P_K$  eine Anordnung von  $K$ . Betrachten wir nun die Menge  $P$ , definiert durch

$$P := \{p \in H_f(G, K) : \text{anf}(p) \in P_K\} .$$

Man macht sich sehr leicht selbst klar, daß  $P$  additiv abgeschlossen ist. Die multiplikative Abgeschlossenheit überprüfen wir sehr leicht mittels (\*). Da für alle  $p \in H_f(G, K)^\times$  gilt:  $\text{anf}(p) \in K^\times$ , ist offensichtlich genau  $p \in P$  oder  $(- )p \in P$ . Zusammen mit  $\text{anf}(p) = 0_K \iff p = 0_{H_f(G, K)}$  ergibt das:  $P$  ist eine Anordnung von  $H_f(G, K)$ . Wir wollen diese Erkenntnis noch als Satz formulieren:

**Satz 1.36** *Ist  $K$  ein Körper, sowie  $P_K$  eine Anordnung von  $K$ . Dann ist*

$$P := \{p \in H_f(G, K) : \text{anf}(p) \in P_K\}$$

*eine Anordnung von  $H_f(G, K)$ , genannt die von  $K$  kommende Anordnung.  $P$  ist eine Fortsetzung der Anordnung  $P_K$  der Einbettung von  $P$  in  $H_f(G, K)$ .*

Mit (1.36) schließlich haben wir die Erkenntnis gewonnen, daß sich auf  $H_f(G, K)$  bestehende Anordnungen von  $K$  fortsetzen lassen. Andererseits können wir  $K$  in kanonischer Weise in  $H_f(G, K)$  einbetten, so daß jede Anordnung von  $H_f(G, K)$  eingeschränkt auf diese Einbettung eine Anordnung von  $K$  liefert. Beide Aussagen zusammen erlauben uns folgende Folgerung:

**Korollar 1.37** *Es sei  $K$  irgendein nicht notwendigerweise formal reeller Körper. Genau dann ist  $H_f(G, K)$  formal reell, wenn auch  $K$  formal reell ist.*

# Kapitel 2

## Pythagoreische Körper

In diesem Kapitel betrachten wir Eigenschaften pythagoreischer Körper, das sind Körper, in denen jede Summe von Quadraten bereits wieder ein Quadrat ist. Als einfache Beispiele betrachte man den Körper der reellen Zahlen; als Gegenbeispiel etwa den Körper der rationalen Zahlen.

**Definition 2.1** *Ein Körper  $K$  heißt pythagoreisch, wenn die Summe von zwei Quadraten in  $K$  bereits wieder ein Quadrat ist.*

Das folgende Lemma ist trivial:

**Lemma 2.2** *Ein Körper  $K$  ist genau dann pythagoreisch, wenn  $1+x^2 \in K^2$  für jedes  $x \in K$ .*

**BEWEIS:** Is  $K$  pythagoreisch, so folgt  $1+x^2 \in K^2, \forall x \in K^\times$ , sofort. Gelte andererseits für jedes  $x \in K^\times: 1+x^2 \in K^2$ , dann ist bereits  $K$  pythagoreisch; anderenfalls existierte ein  $x^2+y^2=c$ , welches kein Quadrat ist, und wir erhalten mit  $1+\left(\frac{y}{x}\right)^2 = \frac{c}{x^2} \notin K^2$  sofort einen Widerspruch.  $\square$

Ebenfalls leicht einzusehen ist, daß für einen beliebigen Körper  $K$  der algebraische Abschluß  $\overline{K}$  pythagoreisch ist.

**Lemma 2.3**  *$\overline{K}$  und, wenn  $K$  formal reell ist, jeder reelle Abschluß von  $K$  ist pythagoreisch für jeden Körper  $K$ .*

**BEWEIS:** Zum Beweis der ersten Aussage machen wir uns lediglich klar, daß ansonsten  $\phi(x) := x^2 - (1 + y^2)$  für ein  $y \in \overline{K}$  über  $\overline{K}$  nicht zerfallen würde. Die zweite Aussage folgt sofort mit 1.12.  $\square$

Das folgende, einfache Beispiel liegt auf der Hand:

**BEISPIEL: [Pythagoreische Oberkörper von  $\mathbf{Q}$ ]**

Wir nehmen in diesem Beispiel einen pythagoreischen Körper  $P$  annehmen, der  $\mathbf{Q}$  umfaßt. Ein solcher Körper existiert mit (2.3) stets. Aus (2.2) erhalten wir sofort, daß  $1^2 + 1^2 = 2$  ein Quadrat in  $P$  sein muß; mit Induktion sogar, daß  $\mathbf{N}$  Quadrate in  $P$  sein müssen. Aufgrund der Beschaffenheit der Elemente von  $\mathbf{Q}$  als Quotient eines Elements aus  $\mathbf{Z}$  durch eine Natürliche Zahl wird sofort klar, daß  $\mathbf{Q}^\times \subseteq P_P$ , wenn  $P_P$  die Anordnung auf  $P$  bezeichnet.  $\lrcorner$

Wir wollen uns in dieser Arbeit, falls es nicht ausdrücklich anders angegeben ist, nur auf formal reelle Körper beschränken. Ansonsten wäre nämlich bereits jedes Element aus  $K^\times$  ein Quadrat: Sei  $(-1) \in K - K$  ist pythagoreisch — die Summe von Quadraten und somit wieder ein Quadrat, etwa  $b^2 = -1$ , dann erhalten wir als Konsequenz:

$$a = \underbrace{\left(\frac{a+1}{2}\right)^2}_{=:a_1} - \underbrace{\left(\frac{a-1}{2}\right)^2}_{=:a_2} = a_1^2 + (-1)a_2^2 = a_1^2 + (ba_2)^2 \in K^2 \quad \forall a \in K^\times,$$

d.h.  $K$  ist quadratisch abgeschlossen und damit uninteressant.

## 2.1 Die pythagoreische Hülle eines Körpers

**Definition 2.4 (Hülle und Abschluß)** Sei  $K$  ein (nicht notwendigerweise formal reeller) Körper. Ein  $K$  umfassender Körper  $K_\Pi$  heißt pythagoreische Hülle (oder pythagoreischer Abschluß) von  $K$ , wenn für jeden Zwischenkörper  $L$  mit  $K \subseteq L \subseteq K_\Pi$  gilt:

$$L \text{ pythagoreisch} \iff L = K_\Pi$$

Offensichtlich ist  $K_\Pi$  in  $\overline{K}$ , dem algebraischen Abschluß von  $K$ , enthalten. Damit folgt sofort der erste Teil von

**Satz 2.5 (Existenz und Eindeutigkeit)** *Jeder Körper  $K$  besitzt einen pythagoreischen Abschluß, und dieser ist (bis auf  $K$ -Isomorphie) eindeutig.*

Die Eindeutigkeit bis auf  $K$ -Isomorphie, erlaubt es uns, von *dem* pythagoreischen Abschluß zu sprechen. Im folgenden Lemma werden wir dann auch den pythagoreischen Abschluß konstruieren.

**BEWEIS:** Wir wissen, daß  $\overline{K}$  pythagoreisch ist. Wir bezeichnen den Durchschnitt aller pythagoreischen Zwischenkörper  $K_i$  ( $i \in I$ ) von  $\overline{K}/K$  mit  $K_p$ .

**$K_p$  ist pythagoreisch:** Wählen wir ein  $x \in K_p$  beliebig, so ist bereits  $x \in K_i$  für alle  $i \in I$ . Damit ist auch  $(1 + x^2) \in K_i^2$  für alle  $i \in I$ , da die  $K_i$  sämtlich pythagoreisch sind. Dies zeigt  $(1 + x^2) \in K_p^2$ , also pythagoreisch. Konstruktiongemäß existiert kein weiterer echter Zwischenkörper von  $K_p/K$ , der pythagoreisch ist, also ist  $K_p$  ein pythagoreischer Abschluß von  $K$ .

**$K_\Pi$  ist eindeutig:** Gemäß Konstruktion ist  $K_p$  der einzige in  $\overline{K}$  enthaltene pythagoreische Abschluß von  $K$ . Mit der Eindeutigkeit des algebraischen Abschlusses  $\overline{K}$  von  $K$  bis auf  $K$ -Isomorphie ist auch  $K_p$  bis auf  $K$ -Isomorphie eindeutig und somit auch  $K_\Pi$ .  $\square$

Im folgenden ist es nützlich, über eine abkürzende Schreibweise für alle pythagoreischen Unterkörper eines Körpers  $K$  zu verfügen:

**Definition 2.6** *Sei  $K$  ein Körper. Dann bezeichnet*

$$\mathcal{P}_K := \{P \subseteq K : P \text{ pythagoreisch und formal reell} \}$$

*die Menge aller pythagoreischen Teilkörper von  $K$ .*

*Ist  $L$  ein Erweiterungskörper von  $K$ , so bezeichnet  $\mathcal{P}_K^L$  die Menge*

$$\mathcal{P}_K^L := \{K \subseteq P \subseteq L : P \text{ pythagoreisch und formal reell} \}.$$

Mit dieser Definition wollen wir nun zwei Aussagen über Durchschnitte pythagoreischer Unterkörper eines festen Körpers  $K$  gewinnen:

**Lemma 2.7** *Sei  $K$  ein Körper und sei  $\mathcal{M} \subseteq \mathcal{P}_K$ . Dann ist  $P := \bigcap_{M \in \mathcal{M}} M$  ein pythagoreischer Körper.*

**BEWEIS:** Sei  $x \in P$  beliebig, so gilt  $x \in M$  für alle  $M \in \mathcal{M}$ . Damit ist auch  $x^2$  und also  $1 + x^2$  in all diesen  $M$  enthalten.  $1 + x^2$  ist Summe von Quadraten in allen  $M \in \mathcal{M}$ ; sie besitzt dort nach Voraussetzung auch eine Wurzel, nämlich dieselbe in allen  $M \in \mathcal{M}$ . Also ist  $P$  pythagoreisch.  $\square$

Es ist außerdem interessant zu untersuchen, wie der Durchschnitt aller pythagoreischer Zwischenkörper eines Körpers  $K$  und eines pythagoreischen Erweiterungskörpers  $L$  von  $K$  aussieht:

**Korollar 2.8** *Ist  $L$  ein pythagoreischer Erweiterungskörper eines Körpers  $K$ . Dann ist der Durchschnitt*

$$P := \bigcap_{M \in \mathcal{P}_K^L} M = \bigcap_{\substack{K \subseteq M \subseteq L \\ M \text{ pythagoreisch}}} M$$

der eindeutig bestimmte pythagoreische Abschluß von  $K$ .

**BEWEIS:** Mit (2.7) ist  $P$  pythagoreisch. Definitionsgemäß ist der pythagoreische Abschluß von  $K$  —  $K_{\Pi}$  — in  $P$  enthalten. Gegen die Annahme  $K_{\Pi} \subset P$  spricht, daß auch  $K_{\Pi}$  in  $\mathcal{P}_K^L$  enthalten sein muß. Die Existenz eines  $p \in P$  mit  $p \notin K_{\Pi}$  führt dann sofort zu einem Widerspruch.  $\square$

Bisher ist uns nur die Existenz und die Eindeutigkeit von  $K_{\Pi}$  bekannt. Mit den bisherigen Mitteln ist es allerdings nicht möglich,  $K_{\Pi}$  explizit anzugeben. Mit dem nun folgenden Lemma wird uns dies allerdings schon bald möglich sein; außerdem werden wir erkennen, daß der pythagoreische Abschluß eine Galoiserweiterung ist.

**Lemma 2.9 (Konstruktion)** *Sei  $K$  ein (nicht notwendigerweise formal reeller) Körper. Es bezeichne  $X$  die Menge aller Zwischenkörper  $L$  von  $\overline{K}/K$ , zu denen ein Körperturm*

$$K = K_0 \subset K_1 \subset \dots \subset K_{n-1} \subset K_n = L \quad (*)$$

existiert, so daß  $K_i = K_{i-1}(\sqrt{x_i^2 + y_i^2})$ ,  $i = 1, \dots, n$ , für geeignete  $x_i, y_i \in K_{i-1}$ . Es ist dann

$$E := \bigcup_{L \in X} L$$

der pythagoreische Abschluß von  $K$ .

Ferner ist  $E$  galoissch über  $K$ .

**BEWEIS:** Es seien  $x, y \in E^\times$  beliebig. Dann gibt es Unterkörper  $L, L' \in X$  von  $\overline{K}$  so, daß  $x \in L$  und  $y \in L'$ . Gemäß der Konstruktion von  $E$  existieren zu  $L$  und  $L'$  Körturtürme  $K = K_0 \subset K_1 \subset \dots \subset K_r = L$  und  $K = K'_0 \subset K'_1 \subset \dots \subset K'_s = L'$  derart, daß  $K_i = K_{i-1}(\sqrt{x_i^2 + y_i^2})$  für  $i = 1, \dots, r$  und  $K'_i = K'_{i-1}(\sqrt{x_i'^2 + y_i'^2})$  für  $i = 1, \dots, s$  gilt, mit  $x_i, y_i \in K_{i-1}$  und  $x'_i, y'_i \in K'_{i-1}$ . Wir bilden nun einen Körturturm als das Kompositum der beiden Körturtürme zu  $L$  und  $L'$  durch

$$K = K_0 \subset K_1 \subset \dots \subset K_r \subset \\ \subset K_r(\sqrt{x_1'^2 + y_1'^2}) \subset \dots \subset K_r(\sqrt{x_1'^2 + y_1'^2}, \dots, \sqrt{x_s'^2 + y_s'^2}) = L \cdot L' =: F .$$

Da  $F$  ein Körper ist und sowohl  $L$  als auch  $L'$  umfaßt, sind mit  $x$  und  $y$  auch  $x \pm y, x \cdot y$  und  $x^{-1}, y^{-1}$  in  $F$  enthalten.  $F$  wiederum ist aufgrund seiner Konstruktion enthalten in  $X$ , so daß  $E$   $F$  umfaßt, also  $E \supset F$ . Aus der freien Wahl von  $x$  und  $y$  folgt damit sofort, daß  $E$  ein Teilkörper von  $\overline{K}$  ist.

Es ist leicht einzusehen, daß die  $L \in X$  in jedem pythagoreischen Zwischenkörper von  $\overline{K}|K$  enthalten sein müssen, und somit auch  $E$ , was uns  $E \subseteq K_\Pi$  liefert.

Zum Beweis von  $E \supseteq K_\Pi$  genügt es zu zeigen, daß  $E$  pythagoreisch ist. Angenommen, es gäbe eine Summe von Quadraten in  $E$  so, daß diese nicht in  $E^2$  enthalten ist. Dann existieren  $x, y \in E^\times$  mit  $x^2 + y^2 \notin E^2$ . Mit der oben durchgeführten Konstruktion aber haben wir gezeigt, daß es ein  $L \in X$  gibt, in dem sowohl  $x$ , als auch  $y$  enthalten sind. Dann aber existiert auch für  $L' := L(\sqrt{x^2 + y^2})$  ein Körturturm gemäß (\*) und folglich ist  $L' \in X$ , also  $L' \subset E$ .

Schließlich müssen wir noch zeigen, daß  $E = K_\Pi$  galoissch ist über  $K$ , die Erweiterung soll also normal und separabel sein. Bereits aus der Konstruktion von  $E$  wird klar, daß  $E$  separabel ist: Jedes Element  $a \in E$  ist bereits in einem  $L$  enthalten, das offensichtlich separabel ist.

Sei  $\tau$  ein  $K$ -Homomorphismus von  $E$  in  $\overline{K}$ . Dann wird jeder Körturturm

$$K = K_0 \subset K_1 \subset \dots \subset K_n = L$$

durch  $\tau$  in einen Körturturm

$$\tau(K) = \tau(K_0) \subset \tau(K_1) \subset \dots \subset \tau(K_n) = \tau(L)$$

derselben Art übergeführt. Es folgt  $\tau(L) \subseteq E$  und mithin  $\tau(E) \subseteq E$ . Es gilt also  $\tau(E) = E$  für jeden  $K$ -Homomorphismus  $\tau$ . Das allerdings bedeutet  $E$  ist normal.  $\square$

Durch diese Konstruktion wird sofort klar:

**Korollar 2.10** *Die pythagoreische Hülle  $K_{\Pi}$  zu einem Körper  $K$  ist eine galoissche 2-Erweiterung.*

Eine wesentliche Eigenschaft der pythagoreischen Hülle ist es, daß diese für formal reelle Körper weiterhin formal reell ist:

**Satz 2.11** *Sei  $K$  irgendein Körper. Ist  $K$  formal reell, so ist auch  $K_{\Pi}$  formal reell.*

Da wir uns in den Vorbemerkungen zu diesem Kapitel darauf verständigt haben, nur formal reelle Körper zu betrachten, sind somit auch, falls es nicht anders vermerkt wird, alle pythagoreischen Hüllen stets formal reell.

**BEWEIS:** Sei  $K$  im Beweis von (2.9) formal reell. Dann sind auch alle  $L \in X$  formal reell gemäß (1.9) und der Bemerkung nach (1.10), da Quadrate stets in der Anordnung enthalten sind. Konstruktionsgemäß kann also die  $(-1) \in E = K_{\Pi}$  nicht Summe von endlich vielen Quadraten sein, weil diese in einem Zwischenkörper  $L \in X$  lägen — im Widerspruch zur Eigenschaft von  $L$ , formal reell zu sein.  $\square$

Gemäß der Generalvoraussetzung ist ein Körper  $K$  für uns stets formal reell, besitzt also mindestens eine Anordnung. In den Vorbereitungen wurde gezeigt, unter welchen Voraussetzungen sich diese Anordnungen auf Körpererweiterungen fortsetzen. Man sieht sehr leicht ein, daß ein Zusammenhang zwischen endlichen 2-Erweiterungen eines Körpers  $K$  und  $K_{\Pi}$  besteht:

**Lemma 2.12** *Es sei  $L$  eine endliche 2-Erweiterung von  $K$ . Lassen sich alle Anordnungen von  $K$  auf  $L$  fortsetzen, dann ist  $L \subseteq K_{\Pi}$ .*

**BEWEIS:** Ist  $L$  eine 2-Erweiterung von  $K$ , so existiert ein galoisscher Zwischenkörper  $L \supseteq M \supset K$ , der über  $K$  den Grad 2 besitzt. Dann allerdings existiert ein  $a \in K$  so, daß  $M = K(\sqrt{a})$ . Damit ist  $a$  ein Quadrat

in  $M$ , also bereits total positiv in  $K$ , und mithin Summe von Quadraten:  
 $a = x_1^2 + x_2^2 + \dots + x_n^2$ .

Dann existiert ein Körperturm

$$K = K_1 \subseteq K_2 \subseteq \dots \subseteq K_n = L \subseteq K_{\Pi}$$

mit den Bezeichnungen

$$\begin{aligned} K_i &:= K_{i-1} \left( \sqrt{\gamma_{i-1}^2 + x_i^2} \right), \\ \gamma_0 &:= 0, \\ \gamma_i &:= \sqrt{\gamma_{i-1}^2 + x_i^2} = \sqrt{x_1^2 + x_2^2 + \dots + x_i^2}. \end{aligned}$$

Es ist damit  $M \subseteq L$  und deshalb  $M \subseteq K_{\Pi}$ . Da  $L$  eine endliche 2-Erweiterung von  $K$  war, ist  $L$  eine 2-Erweiterung von geringerem Grad über  $M$ . In endlich vielen Schritten wiederholt man den Beweis und zeigt damit die Behauptung.  $\square$

Es sei  $K$  ein formal reeller Körper. Bekanntlich ist seine pythagoreische Hülle konstruktionsgemäß in der maximalen 2-Erweiterung  $K_2$  von  $K$  enthalten. Daß man die pythagoreische Hülle eines Körpers auch über die Eigenschaften der 2-Erweiterungen von  $K$  bestimmen kann, zeigt der folgende Satz:

**Satz 2.13** *Die pythagoreische Hülle eines formal reellen Körpers ist die größte 2-Erweiterung, auf die sich jede Anordnung von  $K$  fortsetzen läßt.*

BEWEIS: Bekanntlich ist die pythagoreische Hülle eines Körpers eine 2-Erweiterung. Sei  $\mathcal{P}$  die Familie der Anordnungen von  $K$ . Mit (1.9) zusammen mit (2.9) erhalten wir sofort: *Alle Anordnungen von  $K$  lassen sich auf  $K_{\Pi}$  fortsetzen.*

Es bezeichne nun  $L$  eine 2-Erweiterung von  $K$ , auf die sich alle Anordnungen aus  $\mathcal{P}$  fortsetzen lassen und die  $K_{\Pi}$  echt umfaßt:  $L \supset K_{\Pi}$ . Dann allerdings ist  $L$  auch eine 2-Erweiterung von  $K_{\Pi}$ , da 2-Erweiterungen galoissch sind.

Mit (1.21) existiert dann bereits ein zyklischer Erweiterungskörper  $M$  vom Grad 2 über  $K_{\Pi}$ , für den  $L \supseteq M \supset K_{\Pi}$  gilt. Dann existieren für alle

Anordnungen aus  $\mathcal{P}$  auch Fortsetzungen auf  $M$ , da  $P \in \mathcal{P}$  auf  $L$  fortgesetzt werden kann und die Einschränkung auf den Teilkörper  $M$  von  $L$  wiederum eine Anordnung liefert.  $M$  ist eine endliche 2-Erweiterung von  $K_{\Pi}$ , auf die sich alle Anordnungen von  $K_{\Pi}$  fortsetzen lassen, also in der pythagoreischen Hülle von  $K_{\Pi}$  enthalten.

Da die pythagoreische Hülle von  $K_{\Pi}$  gleich  $K_{\Pi}$  ist, folgt:  $M$  ist keine Erweiterung vom Grad 2 über  $K_{\Pi}$ , somit kann  $L$  kein echter Oberkörper von  $K_{\Pi}$  sein.  $\square$

## 2.2 Eigenschaften pythagoreischer Körper

Im Text direkt vor (1.3) wurde der Begriff *total positiv* eingeführt als die Eigenschaft einer Zahl, in allen Anordnungen eines Körpers enthalten zu sein. Weiter haben wir erkannt, daß zumindest  $\sigma(K) \subseteq P_K$  für jeden Körper  $K$  und jede Anordnung  $P_K$  von  $K$ . Im Fall von pythagoreischen Körpern können wir darauf basierend noch eine weitere Charakterisierung angeben:

**Lemma 2.14** *Es sei  $K$  ein Körper. Genau dann ist  $K$  pythagoreisch, wenn  $K^2$  alle total positiven Elemente von  $K$  stellt.*

Zunächst wollen wir eine nützliche Aussage darüber gewinnen, welche Elemente in der Menge der Quadrate von  $K$  stets enthalten sein müssen, damit  $K$  pythagoreisch sein kann. Und zwar werden wir feststellen, daß zumindest  $\mathbb{N} \subseteq K^2$  erfüllt sein muß:

**Lemma 2.15** *Sei  $K$  ein Körper. Ist  $K$  pythagoreisch, dann ist  $\mathbb{N} \subseteq K^2$ .*

BEWEIS: Da  $K$  stets formal reell ist, gilt  $\mathbb{N} \subseteq K$ . Ist  $K$  pythagoreisch und nehmen wir an,  $\mathbb{N} \not\subseteq K^2$ . Dann existiert ein kleinstes  $n \in \mathbb{N}$ , mit  $n \notin K^2$  und  $n > 1 \in K^2$ . Dann ist aber auch  $(n - 1) \notin K^2$ , da ansonsten mit (2.2) sofort  $1 + (n - 1) = n$  einen Widerspruch ergäbe. Dies wiederum ist aber selbst ein Widerspruch zur Minimalität von  $n$ .  $\square$

Eine weitere Konsequenz, die wir im folgenden sofort anwenden werden, ist, daß damit auch alle  $\frac{1}{n}$ , mit  $n \in \mathbb{N}$ , Quadrate in  $K$  sind.

Eine bemerkenswerte Eigenschaft pythagoreischer Körper ist, daß alle Unterkörper, über denen ein pythagoreischer Körper  $L$  endlichen Grad hat, bereits pythagoreisch sein müssen. Wir werden gleich sehen, daß der Beweis dazu nicht allzu kompliziert verläuft. Vorher jedoch führen wir uns vor Augen, daß hierfür lediglich Erweiterungen vom Grad einer 2-Potenz untersucht werden müssen; andere Erweiterungen fallen offensichtlich bei der Bildung von Summen von Quadraten nicht ins Gewicht. Auch genügt es, den Beweis für Erweiterungen vom Grad 2 zu führen, da (wir sind im Endlichen) dies beliebig oft wiederholt werden kann:

**Satz 2.16** *Ist ein Körper  $L$  pythagoreisch und eine endliche Erweiterung eines Körpers  $K$ , so ist auch  $K$  pythagoreisch.*

BEWEIS: Wir nehmen an, daß  $K$  nicht pythagoreisch ist und werden im folgenden kurz begründen, warum es genügt, den Fall  $[K_{\Pi} : K] = 2$  zu betrachten:

Wir haben in (2.8) gesehen, daß  $K_{\Pi}$  in jedem pythagoreischen Oberkörper von  $K$  enthalten ist. Ist  $K$  also ein Unterkörper von  $L$ , so ist  $K_{\Pi}$  ebenfalls ein Unterkörper von  $L$ . Wie wir in (2.10) gesehen haben, ist  $K_{\Pi}$  eine 2-Erweiterung von  $K$ . Und nach der Konstruktion von  $K_{\Pi}$ , wie sie in (2.9) durchgeführt wurde, existiert bereits ein  $K'$  mit  $K \subseteq K' \subset K_{\Pi}$  mit  $[K_{\Pi} : K'] = 2$ .

Da  $K$  nicht pythagoreisch ist, existiert nach (2.2) ein  $a \in K$  mit  $1 + a^2 = b \notin K^2$ , so daß  $K_{\Pi} = L := K(\sqrt{b})$ . Dann allerdings ist  $\frac{a^2}{2} \in L^2$ , sowie  $\frac{1}{2}(1 + \sqrt{1 + a^2})^2 \in L^2$ , also muß auch

$$\begin{aligned} \frac{a^2}{2} + \frac{1}{2}(1 + \sqrt{1 + a^2})^2 &= \frac{a^2}{2} + \frac{1}{2}(2 + 2\sqrt{1 + a^2} + a^2) = \\ a^2 + 1 + \sqrt{1 + a^2} &= b + \sqrt{b} \in L^2 \quad \text{sein.} \end{aligned}$$

Daraus folgt  $c := \sqrt{b + \sqrt{b}} \in L$ .

Betrachten wir nun

$$L \ni \frac{a\sqrt{b}}{c} = \sqrt{\frac{a^2b}{b + \sqrt{b}}} = \sqrt{\frac{(a^2b)(b - \sqrt{b})}{(b + \sqrt{b})(b - \sqrt{b})}} =$$

---

[2.16] Siehe [DD65]; Korollar 1. Dort ist unser Satz eine Folgerung aus einem weitergehenden Satz, dessen Aussage wir im folgenden darstellen werden.

$$\sqrt{\frac{a^2b^2 - a^2b\sqrt{b}}{b^2 - b}} = \sqrt{\frac{(b - \sqrt{b})(a^2b)}{b(b - 1)}} = \sqrt{\frac{(b - \sqrt{b})(a^2b)}{ba^2}} = \sqrt{b - \sqrt{b}} =: d.$$

Aus den vier Linearfaktoren schließlich erzeugen wir durch Multiplikation das Polynom  $f := X^4 - 2bX^2 + b^2 - b$ ; dieses besitzt die Wurzeln  $\pm d$  sowie  $\pm c$ , wie wir uns leicht selbst klarmachen. Ferner ist  $f$  über  $K$  irreduzibel: Die Faktorisierung von  $f$  über  $L$  lautet natürlich

$$\begin{aligned} f(X) &= (X - d)(X + d)(X - c)(X + c) \\ &= \left(X - \sqrt{b - \sqrt{b}}\right) \left(X + \sqrt{b - \sqrt{b}}\right) \left(X - \sqrt{b + \sqrt{b}}\right) \left(X + \sqrt{b + \sqrt{b}}\right). \end{aligned}$$

Zum Nachweis der Irreduzibilität genügt es also, Produkte zweier dieser Faktoren zu betrachten, da die einzelnen Faktoren und damit auch die Produkte dreier dieser Faktoren keine Polynome über  $K$  darstellen:

$$\begin{aligned} (X - d)(X + d) &= \left(X - \sqrt{b - \sqrt{b}}\right) \left(X + \sqrt{b - \sqrt{b}}\right) = X^2 - (b - \sqrt{b}) \\ &\implies (X - d)(X - d), (X - c)(X + c) \notin K[X] \\ (X - d)(X - c) &= \left(X - \sqrt{b - \sqrt{b}}\right) \left(X - \sqrt{b + \sqrt{b}}\right) \\ &= X^2 - X \left(\sqrt{b + \sqrt{b}} + \sqrt{b - \sqrt{b}}\right) + \sqrt{b^2 - b} \\ (X - d)(X + c) &= \left(X - \sqrt{b - \sqrt{b}}\right) \left(X + \sqrt{b + \sqrt{b}}\right) \\ &= X^2 + X \left(\sqrt{b + \sqrt{b}} - \sqrt{b - \sqrt{b}}\right) - \sqrt{b^2 - b} \end{aligned}$$

$$\begin{aligned} b^2 - b &= (1 + a^2)^2 - (1 + a^2) = 1 + 2a^2 + a^4 - (1 + a^2) = a^2 + a^4 = a^2(1 + a^2) \notin K^2 \\ &\implies (X - d)(X + c), (X + d)(X - c), (X - d)(X - c), (X + d)(X + c) \notin K[X] \end{aligned}$$

Damit sind  $\pm d$  und  $\pm c$  konjugiert, die Erweiterung  $L$  hat also mindestens Grad 4 über  $K$ , im Widerspruch zur Annahme.  $\square$

Aus dem Beweis wird außerdem sofort klar:

**Korollar 2.17** *Sei  $K$  formal reell und nicht pythagoreisch. Dann enthält der pythagoreische Abschluß von  $K$  auch einen Teilkörper, der über  $K$  zyklisch ist und den Grad 4 besitzt.*

BEWEIS: Mit den Bezeichnungen aus dem vergangenen Beweis:  $K(c, d)$  ist eine Erweiterung vom Grad 4 über  $K$  und in  $K_{\Pi}$  enthalten. Außerdem ist  $\tau$ , definiert durch

$$\tau : K(c, d) \rightarrow K(c, d) : \begin{cases} c \mapsto d \\ d \mapsto -c \end{cases},$$

ein Automorphismus von  $K(c, d)$ , der  $K$  fixiert und der zyklisch von Ordnung 4 ist.  $\square$

Diese bemerkenswerte Erkenntnis läßt sich sogar noch erweitern. Bisher wissen wir, daß der pythagoreische Abschluß eines Körpers keine echte endliche Erweiterung sein kann, da ansonsten der Körper bereits pythagoreisch und mit seinem Abschluß identisch wäre. Sehr leicht kann man den vergangenen Satz zu einer allgemeineren Aussage erweitern:

**Satz 2.18** *Es sei  $K$  ein Körper. Genau dann ist  $K$  pythagoreisch, wenn  $K$  keine zyklische Erweiterung vom Grad 4, wohl aber vom Grad 2 besitzt.*

BEWEIS: **1.** Sei  $K$  pythagoreisch und  $E$  eine zyklische Erweiterung von  $K$  vom Grad 4 mit dem Zwischenkörper  $L$ . Dann gibt es  $a, b, c \in K$  mit

$$L = K(\sqrt{a}), \quad E = L(\sqrt{b + c\sqrt{a}}).$$

Wir bezeichnen abkürzend  $\sqrt{b + c\sqrt{a}} =: e$ .

Sei ferner  $\tau$  ein Erzeugendes der Galoisgruppe  $G(E : K)$ , die nach Voraussetzung zyklisch ist. Dann sind die Bilder von  $e$  unter  $\tau$ :

$$\begin{aligned} \tau & : \tau(e^2) = \tau(b + c\sqrt{a}) = b + c\tau(\sqrt{a}) = b - c\sqrt{a} \Rightarrow \tau(e) = \sqrt{b - c\sqrt{a}}, \\ \tau^2 & : \tau^2(e) = (-e) \text{ da } \tau^4 = \text{Id} \text{ ,} \\ \tau^3 & : \tau^3(e) = \tau(\tau^2(e)) = (-\tau(e)) = \left(-\sqrt{b - c\sqrt{a}}\right) \text{ ,} \end{aligned}$$

---

<sup>[2.17]</sup>Siehe [DD65]; Satz 1 Teil b)

<sup>[2.18]</sup>Siehe [DD65]; Satz 1 Teil a)

also

$$(e\tau(e))^2 = e^2\tau(e^2) = (b + c\sqrt{a})(b - c\sqrt{a}) = b^2 - c^2a \in K \cap E^2,$$

und daher ist  $e\tau(e)$  ein Element von Grad 2 über  $K$  mit Minimalpolynom  $f = X^2 + c^2a - b^2$ . Die Erweiterung  $K(e\tau(e)) := L'$  ist also quadratisch. Außerdem ist  $E^2 = L^2 \cup eL^2$ , und mit  $e^2 \in L$  folgt  $L' \subseteq L$ . Dieselbe Überlegung läßt uns weiter schließen:

$$(e\tau(e))^2 = b^2 - c^2a \in K \cap L^2 = K^2 \cup aK^2.$$

Ist jetzt  $(e\tau(e))^2 \in K^2$ , so folgern wir zunächst  $e\tau(e) \in K$  und damit dann  $\tau(e\tau(e)) = e\tau(e)$ , was uns folgendes liefert:

$$\tau(e)\tau^2(e) = \tau(e\tau(e)) = e\tau(e)$$

Mit  $\tau^2(e) = e$  stellt das allerdings einen Widerspruch zu  $\tau^2(e) = (-e)$  und  $e \neq 0$  dar.

Ist andererseits  $(e\tau(e))^2 \in aK^2$ , so existiert ein  $x \in K$  mit  $b^2 - c^2a = x^2a$ . Daraus aber folgt  $b^2 = a(x^2 + c^2)$ , und das führt mit  $(x^2 + c^2) \in K^2$ , da  $K$  pythagoreisch ist, dazu, daß  $a \in K^2$  im Widerspruch zu  $K \neq L$  steht. Also kann  $K$  keine zyklische Erweiterung vom Grad 4 besitzen.

$K$  besitzt mit  $K(i)$  einen Erweiterungskörper vom Grad 2.

2. Es existiere zu  $K$  keine zyklische Erweiterung vom Grad 4. Existiert zu  $K$  keine Erweiterung von Grad 2, so ist  $K = K(i)$ , und  $K$  ist nicht formal reell. Besitze also  $K$  eine Erweiterung vom Grad 2 und sei aber  $K$  selbst nicht pythagoreisch. Nach (2.5) existiert zu  $K$  ein pythagoreischer Abschluß  $K_{\Pi}$ , und nach (2.17) existiert ein Erweiterungskörper  $E$  von  $K$  mit  $K \subseteq E \subseteq K_{\Pi}$  und  $[E : K] = 4$  im Widerspruch zur Annahme. Damit ist  $K$  bereits pythagoreisch.  $\square$

## 2.3 Pythagoreische Körper und formale Potenzreihen

Im einführenden Kapitel haben wir gesehen, daß unter gewissen zusätzlichen Anforderungen an das Faktorensystem der Schiefkörper der formalen Potenzreihen über einem Körper  $K$  sogar kommutativ ist. Im folgenden werden wir

der interessanten Frage nachgehen, ob und welche zusätzlichen Forderungen notwendig sind, damit die formalen Potenzreihen über einen pythagoreischen Körper wieder einen pythagoreischen Körper bilden.

Bereits in (2.2) haben wir gesehen, daß es ausreicht,  $1 + p^2$  für  $p \in H_f(G, K)$  zu betrachten. In (1.35) haben wir gezeigt, daß es genügt, die Anfangsterme der formalen Potenzreihen zu kennen, um bereits all ihre Quadrate zu kennen.

Die 1 in  $H_f(G, K)$  ist bekanntlich die Abbildung

$$x \mapsto \begin{cases} 1 & \text{für } x = 0, \\ 0 & \text{sonst,} \end{cases}$$

der Anfangskoeffizient also von der Ordnung 0. Sei der Anfangskoeffizient von  $p^2$  von der Ordnung  $x_0$ .

Im Fall  $x_0 < 0$  ist auch der Anfangskoeffizient der Summe mit dem von  $p^2$  identisch, so daß offensichtlich wieder ein Quadrat vorliegt.

Im Fall  $x_0 = 0$  muß, da  $K$  pythagoreisch ist, der neue Anfangskoeffizient ein Quadrat in  $K$  sein, denn man kann  $f(0, 0)$  aus der Summe ausklammern und erhält wieder die in (1.35) geforderte Form.

Im Fall  $x_0 > 0$  ist natürlich der neue Anfangskoeffizient, nämlich  $f(0, 0)1$ , ein Quadrat. Wir haben also folgendes

**Lemma 2.19** *Formale Potenzreihenkörper über einem pythagoreischen Körper sind pythagoreisch.*

Man macht sich ebenso leicht klar, daß auch die Umkehrung gilt:

Ist  $H_f(G, K)$  pythagoreisch, so muß folglich bereits  $K$  pythagoreisch sein, da ansonsten Summen von Quadraten der Einbettung von  $K$  in  $H_f(G, K)$  nicht wieder Quadrate sein können. Zusammenfassend haben wir folgenden Satz:

**Satz 2.20** *Es sei  $K$  ein formal reeller Körper.  $H_f(G, K)$  ist genau dann pythagoreisch, wenn  $K$  pythagoreisch ist.*

---

<sup>[2.20]</sup>Siehe [Rib92]; Paragraph 5.

ANMERKUNG: Dieses Ergebnis wird in [Rib92] zwar auch erzielt, allerdings auf eine gänzlich andere Weise. Ribenboim betrachtet nämlich eine charakteristische Größe von  $K$  als auch von  $H_f(G, K)$ , die sogenannte Pythagoraszahl, und kann dann mittels zweier Ungleichungen deren Gleichheit beweisen.

◇

## 2.4 Level und Pythagoraszahl eines Körpers

Dieser Abschnitt soll einen Ausblick auf weitere Aspekte unseres Themas ermöglichen. Die darin enthaltenen Themen werden daher nicht annähernd erschöpfend behandelt oder bewiesen sondern dienen lediglich zur Information der Leser.

Mit Hilfe der Pythagoraszahl eines Körpers läßt sich der Begriff des pythagoreischen Körpers ebenfalls einführen. Dieser Weg wird zum Beispiel bei Ribenboim<sup>1</sup> besprochen. Die Pythagoraszahl eines Körpers ist erklärt als die kleinste natürliche Zahl  $n$ , für die die Summe von  $n$  Quadraten (nicht notwendigerweise von Null verschieden) stets wieder ein Quadrat ist:

**Definition 2.21** Sei  $K$  ein Körper, dann bezeichnet  $K^2$  die Menge seiner Quadrate. Es sei  $\square[n]_K := \{\sum_{i=1}^n x_i : x_i \in K^2 \cup \{0\}\}$ ,  $n \in \mathbf{N}$ , die Menge aller Summen von bis zu  $n$  Quadraten.

Die Pythagoraszahl  $PN(K)$  ist definiert als die kleinste natürliche Zahl  $n$ , für die  $\square[n]_K = \sigma(K) \cup \{0\}$ . Falls es keine natürliche Zahl mit dieser Eigenschaft gibt, so ist  $PN(K) := \infty$ .

Mit dieser Definition ist ein Körper  $K$  genau dann pythagoreisch, wenn  $PN(K) = 1$ :

**Lemma 2.22** Es sei  $K$  ein formal reeller Körper. Genau dann ist  $PN(K) = 1$ , wenn  $K$  pythagoreisch ist.

---

<sup>1</sup>[Rib92]

**BEWEIS:** Ist  $PN(K) = 1$ , dann ist jede Summe von Quadraten bereits ein Quadrat, also  $K$  pythagoreisch. Ist andererseits  $K$  pythagoreisch, so ist  $\square_n_K = \sigma(K) \cup \{0\}$ .  $\square$

Eine weitere wichtige Größe in diesem Zusammenhang ist der *Level*  $\lambda(K)$  eines Körpers  $K$ , definiert wie folgt:

**Definition 2.23** *Sei  $K$  ein Körper. Dann sei der Level  $\lambda(K)$  des Körpers erklärt als*

$$\lambda(K) := \begin{cases} \infty & \text{falls } K \text{ formal reell ist} \\ l \leq 1 & \text{minimal, so daß } \square_l_K \ni (-1) \end{cases} .$$

Offensichtlich folgt bereits aus dieser Definition:  $\lambda(K) = 1$  dann und nur dann, wenn  $-1 \in K^2$ ; speziell bedeutet das, die Charakteristik von  $K$  ist 2.

Das folgende Lemma geht auf Pfister zurück:

**Lemma 2.24 (Pfister)** *Ist  $K$  nicht formal reell, dann ist  $\lambda(K)$  eine Potenz von 2.*

Für den Beweis verweisen wir auf [Rib72, Bem. nach Definition 2].

Ist  $K$  ein nicht formal reeller Körper, dessen Charakteristik nicht 2 ist, so kann man sehr leicht folgendes zeigen:

**Lemma 2.25** *Sei  $K$  ein Körper mit Charakteristik  $\neq 2$  und  $\lambda(K) < \infty$ . Dann ist jedes  $x \in K$  Summe von genau  $1 + \lambda(K)$  Quadraten.*

**BEWEIS:** Bekanntlich ist

$$x = \left(\frac{x+1}{2}\right)^2 - \left(\frac{x-1}{2}\right)^2 .$$

$\lambda(K) = n$  bedeutet definitionsgemäß, daß die  $(-1)$  Summe von  $n$  Quadraten aus  $K$  ist:  $(-1) = r_1^2 + r_2^2 + \dots + r_n^2$ . Das bedeutet

$$x = \left(\frac{x+1}{2}\right)^2 + (r_1^2 + r_2^2 + \dots + r_n^2) \left(\frac{x-1}{2}\right)^2 = \left(\frac{x+1}{2}\right)^2 + \sum_{i=1}^n \left(\frac{r_i(x-1)}{2}\right)^2$$

$\square$

# Kapitel 3

## Euklidische Körper

In diesem Kapitel untersuchen wir die Eigenschaften euklidischer Körper. Dabei handelt es sich um spezielle pythagoreische Körper, und zwar solche, die nur eine Anordnung besitzen. Dies wollen wir zunächst als Definition formulieren:

**Definition 3.1** *Ein Körper  $K$  heißt euklidisch, wenn er pythagoreisch mit genau einer Anordnung ist.*

Offensichtlich gleichwertig dazu ist die folgende Charakterisierung:

**Lemma 3.2** *Ein formal reeller Körper  $K$  ist genau dann euklidisch, wenn  $K^2$  eine (die!) Anordnung von  $K$  bildet.*

BEWEIS: Ist  $K^2$  eine Anordnung von  $K$ , so ist  $K$  pythagoreisch, da  $K$  formal reell und  $K^2$  additiv abgeschlossen ist. Angenommen, es existiert eine weitere Anordnung  $P$ , sowie  $a \in P \setminus K^2 \neq \emptyset$ . Dann ist  $(-a) \in K^2$ , also  $b := \sqrt{-a} \in K$ . Da  $P$  multiplikativ abgeschlossen sein muß, folgt mit  $b^2 = (-a) \notin P$  und  $(-b)^2 = b^2 \notin P$  sofort  $P = K^2$ .

Ist andererseits  $K$  euklidisch, so ist  $K$  formal reell. Da  $K$  insbesondere auch pythagoreisch ist, ist  $K^2$  abgeschlossen unter Addition und Multiplikation, bildet also eine Präordnung. Da — nach dem Satz von Artin —  $K^2$  also Durchschnitt von Anordnungen ist,  $K$  aber wegen der Eigenschaft, euklidisch zu sein, nur eine Anordnung  $P$  besitzt, stimmt  $K^2$  mit  $P$  überein.  $\square$

ANMERKUNG: In der Literatur wird euklidisch überwiegend so definiert: Ein Körper  $K$  ist euklidisch, wenn  $K^2$  seine Anordnung ist.  $\diamond$

BEISPIEL: Der Körper  $\mathbb{R}$  der reellen Zahlen ist euklidisch: Die Quadrate von  $\mathbb{R}$  bilden eine Anordnung, da für alle  $x \in \mathbb{R}^\times$  entweder  $x$  oder  $(-x)$  in  $\mathbb{R}^2$  enthalten ist und die Quadrate abgeschlossen unter Multiplikation und Addition sind.  $\lrcorner$

Ähnlich wie schon bei den pythagoreischen Körpern, wo es offensichtlich war, daß zu jedem Körper ein pythagoreischer Oberkörper existiert, läßt sich auch zu jedem Körper ein euklidischer Oberkörper finden:

**Satz 3.3** *Zu jedem Körper  $K$  existiert ein euklidischer Körper  $E$  so, daß  $K \subseteq E$ .*

BEWEIS: Die Aussage folgt direkt aus (1.13) mit (1.12): Zu  $K$  existiert ein reeller Abschluß  $L$ , und die Anordnung  $P_L$  von  $L$  ist mit  $L^2$  identisch und eindeutig.  $\square$

**Es ist wichtig**, hierbei zu beachten, daß gemäß unserer Generalvoraussetzung, falls es nicht explizit anders betont wird, stets nur von formal reellen Körpern die Rede ist.

## 3.1 Erste Eigenschaften

Eine Kennzeichnung euklidischer Körper gibt der folgende Satz:

**Satz 3.4** *Für einen formal reellen Körper  $K$  sind folgende Aussagen äquivalent:*

- a)  $K$  ist euklidisch,
- b)  $K(i)$  ist die einzige quadratische Erweiterung,
- c)  $K$  besitzt keine formal reellen quadratischen Erweiterungen.

---

<sup>[3.4]</sup>Siehe [Bec73, Satz 1]. Der Satz enthält noch weitere Aussagen über den Witttring  $W(K)$  von  $K$ , die wir in diesem Zusammenhang nicht behandeln wollen.

**BEWEIS:** b) $\Rightarrow$ c) ist bekannt. c) $\Rightarrow$ a): Sei  $P$  eine Anordnung von  $K$  und  $a \in P \setminus K^2$ . Nach (1.9) ist  $K(\sqrt{a})$  formal reell, also  $P \setminus K^2 = \emptyset$ , und somit  $P = K^2$ . a) $\Rightarrow$ b): Angenommen,  $K$  besitze eine quadratische Erweiterung  $L = K(\sqrt{a})$ , so folgt  $a \notin K^2$ , also  $a \notin P$ , folglich  $a \in (-P)$ , und damit  $L \equiv K(i)$ .  $\square$

Es sei  $K$  ein Körper von einer Charakteristik  $\neq 2$ ,  $L = K(\sqrt{a})$  eine quadratische Erweiterung, sowie  $\bar{a} := aK^2$  die Quadratklasse zu  $a$ . Sei ferner  $j := \{1, \bar{a}\} \rightarrow K^\times/K^2$  die natürliche Inklusion,  $j'$  sei der von der Inklusion  $K^\times \rightarrow L^\times$  induzierte Homomorphismus  $K^\times/K^2 \rightarrow L^\times/L^2$  sowie  $n$  der zu der Normabbildung gelieferte Epimorphismus  $L^\times/L^2 \rightarrow N/K^2$ , wobei  $N$  die zu  $L$  gehörende Normuntergruppe von  $K$  ist.

**Lemma 3.5** *Mit den soeben eingeführten Bezeichnungen gilt:*

$$N = K^2 \iff K \text{ pythagoreisch, } L = K(i).$$

*Des weiteren ist die Sequenz*

$$1 \longrightarrow \{1, \bar{a}\} \xrightarrow{j} K^\times/K^2 \xrightarrow{j'} L^\times/L^2 \xrightarrow{n} N/K^2 \longrightarrow 1$$

*exakt.*

**BEWEIS:** Für die erste Aussage folgt „ $\Leftarrow$ “ sofort: Ist  $L = K(i)$ , so ist für ein beliebiges  $L \ni b = \alpha + \beta i$  die Norm  $N(b) = \alpha^2 + \beta^2$  und somit, da  $K$  pythagoreisch ist, ein Quadrat.

Für „ $\Rightarrow$ “ folgt mit  $N \ni N(\sqrt{a}) = -a \in K^2$  sofort  $L = K(i)$  sowie  $K^2 = K^2 + K^2$ ;  $(-1)$  ist also nicht Quadratsumme, somit ist  $K$  formal reell und pythagoreisch.

Für die zweite Aussage beachten wir, daß  $j$  definitionsgemäß injektiv ist.  $a$  ist ein Quadrat in  $L$ , also fallen die Quadratklassen von 1 und  $a$  in  $L$  zusammen. Das aber bedeutet  $\text{Bild}(j) \subseteq \text{Kern}(j')$ . Sei nun  $a' \in \text{Kern}(j')$ . Dann ist  $a'K^2 \in L^2$ . Und das bedeutet  $a' = 1$  oder  $a' = \bar{a}$ . Also ist sogar  $\text{Bild}(j) \subseteq \text{Kern}(j')$ .

Um schließlich den Kern von  $n$  zu bestimmen betrachten wir nun ein  $b \in L$  mit  $n(b) = 1$ . Mit dem „Satz 90“ von Hilbert ist das genau dann der Fall,

---

<sup>[3.5]</sup>Siehe [Bec73, Lemma 1]

wenn  $b$  von der Form  $\frac{b'}{\tau b}$  ist, wobei  $\tau$  ein Element der Galoisgruppe von  $L$  über  $K$  sein soll. Dann ist  $b$  von der Gestalt

$$b = \frac{\alpha + \beta\sqrt{a}}{\alpha - \beta\sqrt{a}} = \frac{1}{(\alpha - \beta\sqrt{a})^2}(\alpha^2 - \beta^2 a);$$

mithin folgt  $b \in dL^2$  mit einem  $d \in K^\times$ . □

Bezeichnet  $q_F$  die Quadratklassenzahl  $[F^\times : F^2]$ , so läßt sich aus (3.5) folgern:

**Korollar 3.6** *Mit den soeben eingeführten Bezeichnungen folgt:*

$$q_L = \frac{1}{2}q_K[N : K^2],$$

$$L \text{ formal reell} \Rightarrow q_L \geq q_K,$$

$$L \text{ ist nicht euklidisch.}$$

BEWEIS: 1. Für die erste Aussage betrachten wir zunächst folgende Homomorphie:

$$\text{Bild}(j') \cong (K^\times/K^2)/\text{Kern}(j') = (K^\times/K^2)/\text{Bild}(j)$$

Zusätzlich folgt mittels Homomorphiesatz außerdem

$$\begin{aligned} \text{Bild}(n) &\cong (L^\times/L^2)/\text{Kern}(n) = (L^\times/L^2)/\text{Bild}(j') \\ \implies |\text{Bild}(n)| &= \frac{|L^\times/L^2|}{|\text{Bild}(j')|}, \end{aligned}$$

so daß wir zusammenfassend

$$\begin{aligned} [L^\times : L^2] &= |L^\times/L^2| = |\text{Bild}(n)| |\text{Bild}(j')| = \\ &= [N : K^2] \frac{|K^\times/K^2|}{|\text{Bild}(j)|} = [N : K^2] \frac{[K^\times : K^2]}{2} \end{aligned}$$

erhalten.

---

<sup>[3.6]</sup>Siehe [Bec73, Folgerungen aus Lemma 1]

2. Mit der in Punkt 1 behandelten Gleichung folgt die Behauptung sofort mit der nachstehenden Überlegung: Ist  $L$  formal reell, so erhalten wir mit (3.5)  $N \neq K^2 \iff [N : K^2] > 1$  und damit das Behauptete.

3. Wir dürfen davon ausgehen, daß  $L$  formal reell ist. Wäre nämlich  $L$  nicht formal reell, so kann  $L$  nicht euklidisch sein. Mit 2. allerdings folgt dann sofort  $q_L \geq q_K$ . Die Quadratklassenzahl eines euklidischen Körpers ist offensichtlich stets 2, und man macht sich leicht klar, daß jeder formal reelle Körper mit Quadratklassenzahl 2 bereits euklidisch ist.

Nehmen wir jetzt an,  $L$  sei euklidisch, so erhalten wir mit (1.) zunächst

$$2 = \frac{1}{2}q_K[N : K^2].$$

Dann ist aber  $L$  bereits formal reell, und (2.) bedeutet für uns, daß  $q_K \leq 2$ . Das allerdings läßt uns für  $[N : K^2]$  nur die beiden Möglichkeiten  $[N : K^2] = 2$ , falls  $q_K = 2$  oder  $[N : K^2] = 4$ , falls  $q_K = 1$ .

Der Fall  $q_K = 2$  bedeutet aber:  $K$  ist euklidisch, und mithin pythagoreisch, was wiederum sofort  $[N : K^2] = 1$  liefert.

Der Fall  $q_K = 1$  aber bedeutet,  $K$  ist quadratisch abgeschlossen und daher nicht formal reell. Dann ist aber auch  $L$  als quadratische Erweiterung von  $K$  natürlich auch nicht formal reell im Widerspruch zur Annahme.

Zusammengefaßt erhalten wir:  $L$  kann nicht euklidisch sein.  $\square$

Die nun folgende Aussage gilt ebenso für pythagoreische Körper; wir haben sie in (2.16) bereits für diesen Fall bewiesen.

**Satz 3.7** *Ist  $E$  euklidisch und eine endliche Erweiterung des Körpers  $K$ , so ist auch  $K$  bereits euklidisch.*

Da es sich hierbei um einen zentralen Satz handelt, werden wir mehrere Beweise behandeln:

**BEWEIS:** [1] Aus (2.16) sowie der Tatsache, daß alle euklidischen Körper definitionsgemäß pythagoreisch sind, folgt sofort:  $K$  ist pythagoreisch. Es bleibt zu zeigen: Für jedes  $x \in K^\times$  gilt entweder  $x \in K^2$  oder  $(-x) \in K^2$ .

---

<sup>[3.7]</sup>Siehe [Bec73, Lemma 2]

Sei  $P$  eine Anordnung von  $K$  und sei  $n \in \mathbb{N}$  der Grad von  $E$  über  $K$ . Dann existiert ein  $n_0 \in \mathbb{N}$  so, daß  $2^{n_0} > n$ . Angenommen, es sei  $x \in P$  mit  $x \notin K^2$ . Dann existiert ein  $e \in E$  mit  $e \notin K$  und  $e^{2^{n_0}} = x$ . Die daraus resultierende Folgerung  $[K(e) : K] = 2^{n_0}$  steht in direktem Widerspruch zur Annahme,  $E$  sei euklidisch.  $\square$

**BEWEIS:** [2] Mit (3.6), insbesondere der dritten Aussage dort, folgt sofort: Ist  $L$  eine quadratische Erweiterung eines Körpers  $K$ , so ist  $L$  nicht euklidisch. Ist  $E$  euklidisch und eine endliche Erweiterung des Körpers  $K$ , so kann  $E$  keine 2-Erweiterung von  $K$  sein, da sonst ein quadratischer Unterkörper existieren würde. Dann allerdings kann  $E$  nicht euklidisch sein.

Ist  $E$  keine 2-Erweiterung von  $K$ , und ist  $E$  euklidisch, so ist damit auch bereits  $K$  euklidisch.  $\square$

Als nächstes wollen wir die Automorphismengruppe eines euklidischen Körpers näher untersuchen. Zunächst betrachten wir die Gruppe  $\text{Aut}_K(E)$  der  $K$ -Automorphismen eines Körpers  $E$ , der euklidisch und eine algebraische Erweiterung eines Körpers  $K$  ist.

**Lemma 3.8** *Ist ein euklidischer Körper  $E$  algebraisch über einem Körper  $K$ , so ist jeder  $K$ -Automorphismus von  $E$  die Identität.*

**BEWEIS:** Da der Positivitätsbereich von  $E$  gerade die Quadrate in  $E$  sind, muß jeder Automorphismus auch die Anordnung von  $E$  erhalten. Sei jetzt  $\tau \in \text{Aut}_K(E)$  ein  $K$ -Automorphismus von  $E$ . Dann folgt sofort aus  $\tau(1) = 1$ , daß  $\tau(\lambda) = \lambda$  für alle  $\lambda \in K$ .

Seien nun  $\alpha \in E$  algebraisch über  $K$  sowie  $f \in K[X]$  das Minimalpolynom von  $\alpha$ . Wir erkennen durch die Überlegung  $f^\tau = f$  sofort, daß  $\tau(\alpha)$  unter den Konjugierten von  $\alpha$  zu finden sein muß.

Seien  $\alpha_1, \dots, \alpha_n$  die zu  $\alpha$  Konjugierten (mit  $1 \leq i \leq n$ ), so dürfen wir ohne Beschränkung der Allgemeinheit annehmen, daß  $\alpha_1 < \alpha_2 < \dots < \alpha_n$  zutrifft. Die Tatsache, daß  $\tau$  anordnungserhaltend auf  $E$  ist, bedeutet

$$\tau(\alpha_1) < \tau(\alpha_2) < \dots < \tau(\alpha_n),$$

was unter der Annahme  $\tau(\alpha_j) \neq \alpha_j$  sofort zu einem Widerspruch führt (mit  $1 \leq j \leq n$ ): Angenommen,  $\tau(\alpha_1) = \alpha_j \neq \alpha_1$ . Dann muß es ein  $2 \leq k \leq n$

geben mit  $\tau(\alpha_k) = \alpha_1$ . Nach der Anordnung der  $\alpha_i$  aber gilt dann für  $\alpha_k$ :

$$\tau(\alpha_1) < \tau(\alpha_k) \quad \text{und daher} \quad \alpha_j < \tau(\alpha_1)$$

im Widerspruch zur Anordnungstreue von  $\tau$ . Dies zeigt  $\tau(\alpha_1) = \alpha_1$ , und der Rest folgt ebenso in  $n - 1$  Schritten.  $\square$

Ist nun  $E$  ein euklidischer Körper, so betrachten wir die Automorphismengruppe von  $E$ . Nehmen wir an, es existiere ein Torsionselement  $\tau$ . Wir dürfen ohne Beschränkung der Allgemeinheit annehmen, daß ein  $x \in E$  existiert mit  $\tau(x) < x$ . Dann gilt allerdings aufgrund der Anordnungstreue von  $\tau$ , daß  $\tau^i(x) < \tau^{i-1}(x)$  im Widerspruch zur Annahme,  $\tau$  sei eine Torsion.

Mit den soeben gewonnenen Erkenntnissen haben wir schließlich folgenden Satz:

**Satz 3.9** *Ist ein euklidischer Körper  $E$  algebraisch über einem Körper  $K$ , so ist jeder  $K$ -Automorphismus von  $E$  die Identität.*

*Die Automorphismengruppe eines euklidischen Körpers ist torsionsfrei.*

*Jeder über  $\mathbf{Q}$  algebraische euklidische Körper besitzt eine triviale Automorphismengruppe.*

## 3.2 Euklidische Hüllen

Wie bereits im Kapitel über pythagoreische Körper wird auch für euklidische Körper der Begriff einer Hülle als bezüglich der Inklusion minimaler euklidischer Erweiterungskörper definiert:

**Definition 3.10** *Es sei  $K$  ein Körper. Ein euklidischer Erweiterungskörper  $E$  heißt euklidische Hülle von  $K$ , wenn es keinen echten Zwischenkörper von  $E/K$  gibt, der euklidisch ist.*

ANMERKUNG: *Es ist wichtig anzumerken, daß es in der Regel tatsächlich mehrere euklidische Hüllen zu einem Körper gibt. Die pythagoreische Hülle eines Körpers ist bis auf  $K$ -Isomorphie eindeutig, aber euklidische Hüllen*

---

<sup>[3.9]</sup>Siehe [Bec73, Satz 2]

existieren mehrere, die nicht isomorph sind. Wir werden später zeigen, daß zu jeder Anordnung des Körpers eine euklidische Hülle existiert; und ferner, daß die pythagoreische Hülle eines Körpers der Durchschnitt seiner euklidischen Hüllen ist.  $\diamond$

Jetzt wollen wir einen Satz über die Existenz der euklidischen Hüllen eines Körpers betrachten.

**Satz 3.11** *Ein formal reeller Körper besitzt euklidische Hüllen, und zwar liegt in jedem euklidischen Erweiterungskörper genau eine. Euklidische Hüllen sind algebraische Erweiterungen.*

BEWEIS: Sei  $K$  ein formal reeller Körper. Nach (3.3) besitzt  $K$  mindestens einen euklidischen Oberkörper, etwa  $E'$ . Auf allen Zwischenkörpern von  $E'/K$  induzieren wir die von  $E'$  stammende Anordnung. Ferner definieren wir  $K_0 := K$ ,  $K_{i+1} := K_i(\sqrt{a_i})$  mit  $0 < a_i \in K_i$  für  $i \in \mathbb{N}$ . Wir bilden  $E$  als die Vereinigung aller  $K_i$ , also  $E := \bigcup_{i \in \mathbb{N}} K_i$ .

Konstruktionsgemäß besitzt  $E$  keine weiteren reellen quadratischen Erweiterungen,  $E(i)$  ist die einzige quadratische Erweiterung von  $E$ , so ist mit (3.4)  $E$  euklidisch.

Ein euklidischer Zwischenkörper von  $E'/K$ , etwa  $E_0$ , besitzt nur eine Anordnung, nämlich die von  $E'$  induzierte. Also ist mit  $E$  auch auf den Körpern  $K_i$  die Anordnung von  $E'$  induziert. Ferner ist auch  $K_i \subseteq E_0$  für alle  $i \in \mathbb{N}$ .

$E$  kann keinen echten Unterkörper enthalten, der euklidisch ist. Ein solcher Unterkörper wäre von der Gestalt  $\bigcup_{i \in \mathbb{N} \setminus I} K_i$ , mit  $I$  einer nichtleeren Ausnahmemenge. Dann allerdings enthielte  $E$  positive Elemente, die keine Quadrate sind, und ist daher nicht euklidisch. Folglich ist  $E$  eine euklidische Hülle von  $K$ , und zwar die einzige, die in  $E'$  enthalten ist.

Die letzte Aussage folgt direkt aus der hier vorgeführten Konstruktion.  $\square$

Euklidische Körper zeichnen sich dadurch aus, daß sie genau eine Anordnung besitzen. Natürlich ist die Einschränkung der Anordnung eines euklidischen Körpers auf einen Unterkörper dort auch eine Anordnung. Im folgenden

---

<sup>[3.11]</sup>Siehe [Bec73, Satz 5]

wollen wir die Zusammenhänge zwischen den Anordnungen eines Körpers sowie seinen euklidischen Hülle untersuchen. Dazu benötigen wir zunächst folgende Bezeichnung:

**Definition 3.12** *Sei  $K$  ein Körper, versehen mit einer Anordnung  $P$ . Eine euklidische Hülle  $E$  von  $K$  heißt zu  $P$  gehörend oder auch Hülle zu  $P$ , wenn  $P$  die von  $E$  auf  $K$  induzierte Anordnung ist:*

$$P = K \cap E^2$$

Es ist nun eine interessante Frage, ob sich zu jeder Anordnung eines Körpers auch eine euklidische Hülle finden läßt. Interessanterweise läßt sich diese Frage stets mit „Ja“ beantworten:

**Satz 3.13** *Zu jeder Anordnung  $P$  eines formal reellen Körpers  $K$  gibt es euklidische Hüllen.*

**BEWEIS:** Sei  $P$  eine beliebige Anordnung auf  $K$ . Dann ist  $K(\sqrt{P}) := K(W)$  mit  $W := \{\sqrt{x} | x \in P\}$ , also ein Erweiterungskörper von  $K$ , auf den  $P$  mit (1.9) fortsetzbar ist. Mit (3.11) folgt sofort die Existenz einer euklidischen Hülle, die  $K(\sqrt{P})$  umfaßt und deren Anordnung eine Fortsetzung der Anordnung von  $K(\sqrt{P})$  ist; also eine Fortsetzung von  $P$  ist.  $\square$

**Satz 3.14** *Zur Anordnung  $P$  eines formal reellen Körpers  $K$  gehöre die euklidische Hülle  $E$ ;  $E'$  sei ein euklidischer Erweiterungskörper, der  $P$  auf  $K$  induziere. Bei diesen Voraussetzungen besitzt jeder anordnungstreue Monomorphismus  $\tau : K \rightarrow E'$  eine eindeutige Fortsetzung  $\sigma : E \rightarrow E'$ ;  $\sigma$  ist anordnungstreu.*

**BEWEIS:** Ein Monomorphismus zwischen zwei euklidischen Körpern ist natürlich stets anordnungstreu, da die Anordnung hier durch die Quadrate definiert wird.

Sei  $M$  die Menge aller Paare  $(L, \sigma_L)$ , bestehend aus einem Zwischenkörper  $L$  von  $E$  über  $K$  und einer Fortsetzung  $\sigma_L : L \rightarrow E'$  von  $\tau$ , die anordnungstreu

---

<sup>[3.13]</sup>Siehe [Bec73, Satz 7]

<sup>[3.14]</sup>Siehe [Bec73, Satz 8]

und ein Monomorphismus ist. Auf  $M$  führen wir nun unter der Bezeichnung  $\triangleleft$  eine Ordnungsrelation wie folgt ein:

$$(L_1, \sigma_{L_1}) \triangleleft (L_2, \sigma_{L_2}) \iff L_1 \subset L_2 \wedge \sigma_{L_1} = \sigma_{L_2}|_{L_1}.$$

Zu jeder bezüglich  $\triangleleft$  aufsteigende Kette  $\mathcal{K}$ ,  $(L_1, \sigma_{L_1}) \triangleleft (L_2, \sigma_{L_2}) \triangleleft \dots$  betrachten wir zunächst  $L_S := \bigcup_i L_i$ , sowie  $\sigma_{L_S}$ , das wir wie folgt definieren:

$$\forall l \in L_S : \exists (L, \sigma_L) \in \mathcal{K} \Rightarrow \sigma_{L_S}(l) := \sigma_L(l);$$

$\sigma_{L_S}$  ist wohldefiniert:

Angenommen, es sei  $l \in L_1 \cap L_2$  mit  $(L_1, \sigma_{L_1}), (L_2, \sigma_{L_2}) \in \mathcal{K}$ , so ist entweder  $L_1 \subset L_2$  oder  $L_1 \supset L_2$ . Es sei ohne Beschränkung der Allgemeinheit der erste Fall gegeben. Dann ist  $\sigma_{L_1} = \sigma_{L_2}|_{L_1}$ , also ist  $\sigma_{L_1}(l) = \sigma_{L_2}(l)$ . Damit existiert in  $M$  zu jeder Kette  $\mathcal{K}$  mit  $(L_S, \sigma_{L_S})$  eine obere Schranke.

Deshalb existiert in  $M$  nach Zorn mindestens ein maximales Element, nennen wir es  $(L, \sigma_L)$ .

Ist dieses  $L$  nicht euklidisch, so existiert ein  $0 < a \in (L^\times \cup E^2) \setminus L^2$ . Auf die Erweiterung  $L(\sqrt{a})$  aber, die in  $E$  enthalten ist, läßt sich nach (1.9) die Anordnung von  $L$  fortsetzen. Für das Bild von  $a$  unter  $\sigma_L$  gilt also mit  $a$  auch  $\sigma_L(a) > 0$ . Das Bild ist also ein Quadrat  $\sigma_L(a) = b^2$ , da  $E'$  euklidisch ist. Die Abbildung  $\sigma_L$  läßt sich durch  $\sigma_{L'}(x + y\sqrt{a}) \mapsto \sigma_L(x) + \sigma_L(y)b$  ebenfalls fortsetzen, so daß  $L$  im Widerspruch zur Annahme nicht maximal gewählt war. Also ist  $L$  euklidisch und daher mit  $E$  identisch; das aber bedeutet  $\sigma = \sigma_L$ .

Nach (3.11) existiert in  $E'$  genau eine euklidische Hülle von  $\tau(K)$ , diese ist also  $\sigma(E)$ . Die Erkenntnis, daß  $E$  keine  $K$ -Automorphismen besitzt, folgt sofort aus der Tatsache, daß man von  $K$  durch  $K^{(0)} := K, K^{(i+1)} := K(\sqrt{a}); a \in K^{(i)}$  bis zu  $E$  aufsteigen kann.  $\square$

Sofort folgt damit das folgende

**Korollar 3.15** *Je zwei euklidische Hüllen zu einer Anordnung  $P$  des reellen Körpers  $K$  sind über  $K$  isomorph.*

<sup>[3.15]</sup>Siehe [Bec73, Satz 8, Korollar 1]

Bereits die Definition der euklidischen Körper hat angedeutet, daß eine engere Beziehung zwischen euklidischen und pythagoreischen Körpern bestehen muß. Jeder pythagoreische Erweiterungskörper von  $K$  enthält die pythagoreische Hülle  $K_{\Pi}$ , also umfaßt auch jeder euklidische Erweiterungskörper  $E$  von  $K$  als Teilkörper  $K_{\Pi}$ . Es ist nicht schwer zu sehen, daß der Durchschnitt aller euklidischen Hüllen von  $K$  sogar mit  $K_{\Pi}$  übereinstimmt:

**Satz 3.16** *Die pythagoreische Hülle  $K_{\Pi}$  eines formal reellen Körpers  $K$  ist der Durchschnitt aller euklidischen Hüllen.*

BEWEIS: Ganz klar ist die pythagoreische Hülle von  $K$  definitionsgemäß in jeder euklidischen Hülle von  $K$  enthalten, also auch in deren Schnitt. Es ist also lediglich zu zeigen, daß der Schnitt nicht echt größer ist:

Der pythagoreische Abschluß  $K_{\Pi}$  ist nach (2.13) die größte 2-Erweiterung, auf die sich alle Anordnungen von  $K$  fortsetzen lassen. Damit sind die euklidischen Hüllen von  $K_{\Pi}$  mit denen von  $K$  identisch.

Es sei  $L$  der Durchschnitt aller euklidischer Hüllen von  $K$ ;  $L$  ist normal und, mit den euklidischen Hüllen, auch separabel, also galoissch, und somit eine 2-Erweiterung von  $K_{\Pi}$ .

Es sei  $L \neq K_{\Pi}$ . Nach (1.21) existiert dann ein quadratischer Erweiterungskörper  $L_0 = K_{\Pi}(\sqrt{a})$  mit  $L \subseteq L_0$ . Dann aber besitzt  $L_0$  nicht mehr alle Anordnungen von  $K$ , also gibt es eine Anordnung  $P$  von  $K$ , deren euklidische Hülle  $E_P$  kein Erweiterungskörper von  $L_0$  ist. Dies steht im Widerspruch zur Annahme,  $L$  sei der Durchschnitt aller euklidischer Hüllen von  $K$ , also kann  $L$  nicht echt größer als  $K_{\Pi}$  sein.  $\square$

Als direkte Folgerung des letzten Satzes erhalten wir sogar:

**Korollar 3.17** *Sei  $\mathcal{E}$  eine Familie von euklidischen Körpern. Dann ist  $\bigcap_{E \in \mathcal{E}} E$  pythagoreisch.*

BEWEIS: Es sei  $K := \bigcap_{E \in \mathcal{E}} E$ . Dann ist mit den Bezeichnungen des zweiten Kapitels, insbesondere von Definition (2.6),

$$K = \bigcap_{E \in \mathcal{E}} E = \bigcap_{P \in \mathcal{P}_K} P.$$

Mit (2.7) folgt das Behauptete.  $\square$

---

<sup>[3.16]</sup>Siehe [Bec73, Satz 10]

### 3.3 Der Satz von Whaples mit Folgerungen

Auf *G. Whaples* geht ein Kennzeichnungssatz für euklidische Körper zurück, den wir im folgenden in mehreren Schritten erarbeiten und beweisen wollen. Betrachten wir zunächst folgendes Lemma:

**Lemma 3.18** *Es sei  $K$  ein euklidischer Körper. Dann ist  $K_2 = K(i)$ .*

BEWEIS: Der Beweis ist denkbar einfach:

Sei  $K$  euklidisch. Nach (3.4) besitzt  $K$  nur eine einzige quadratische Erweiterung, nämlich  $K(i)$ .  $K(i)$  allerdings besitzt keine weitere quadratische Erweiterung. Mit (1.21) bedeutet dies:  $K_2 = K(i)$ .  $\square$

Als nächsten Schritt überlegen wir uns, was es bedeutet, wenn die maximale 2-Erweiterung eines Körpers  $K$  einen endlichen Grad über  $K$  besitzt. Wir werden erkennen, daß dann bereits  $K$  euklidisch ist und  $[K_2 : K] = 2$  folgt.

**Lemma 3.19** *Sei  $K$  ein formal reeller Körper mit Charakteristik  $\neq 2$ . Ist  $[K_2 : K]$  endlich, so gilt:  $K$  ist ein euklidischer Körper.*

BEWEIS:  $K_2/K$  ist eine galoissche Körpererweiterung nach (1.21). Deshalb gibt es einen Zwischenkörper  $E$  von  $K_2/K$  mit  $[K_2 : E] = 2$ . Dieser ist dann allerdings  $K_2 = E(i)$ . Dies wiederum besagt:  $E$  ist euklidisch (etwa mit (3.4)), und mit (3.7) ist dann sogar  $K$  euklidisch. Mit Lemma (3.18) bedeutet das:  $K = E$ ; und mithin ist  $K$  euklidisch.  $\square$

Das eben bewiesene Lemma stellt einen Teil des Kennzeichnungssatzes von *G. Whaples* dar. Der vollständige Satz, den wir nachstehend behandeln, stellt keinerlei Anforderungen mehr an den zugrundeliegenden Körper. Dies allerdings macht den Beweis derart kompliziert, da dann im Fall von Körpern ohne  $p$ -te Einheitswurzeln große Probleme auftreten. Wir werden daher in dieser Arbeit nicht den vollständigen Beweis für den Satz von Whaples liefern; er kann in der Literatur, etwa in [Bec73] gut nachvollzogen werden.

---

<sup>[3.18]</sup>Siehe [Bec73, Satz 3; 2.Hälfte]

**Satz 3.20 (Satz von Whaples)** *Sei  $K$  ein Körper. Ist für eine Primzahl  $p$  die maximale  $p$ -Erweiterung  $K_p$  von  $K$  eine echte, aber endliche Erweiterung, so folgt:  $p = 2$ ,  $K$  ist euklidischer Körper und  $K_2 = K(i)$ . Umgekehrt gilt für jeden euklidischen Körper  $K_2 = K(i)$ .*

**BEWEIS:** Sei zunächst die Charakteristik von  $K$  von  $p$  verschieden. Nehmen wir an,  $p \neq 2$ .  $K$  enthält dann eine primitive  $p$ -te Einheitswurzel  $\zeta$ . Ohne Einschränkung dürfen wir annehmen, daß  $K_p/K$  zyklisch vom Grad  $p$  ist.  $K(\sqrt[p]{\zeta})$  ist eine  $p$ -Erweiterung von  $K$ , somit  $\eta = \sqrt[p]{\zeta} \in K_p$ . Entweder liegt  $\eta$  bereits wieder in  $K$ , oder aber es ist  $X^p - \zeta = 0$  das Minimalpolynom zu  $\eta$  über  $K$ . Da  $p$  ungerade ist, ergibt sich in jedem Fall:  $N_{K_p/K} = \zeta$ . Ziehen wir [Alb38, chap.IX,§6,Th.11] zu Hilfe, so erkennen wir, daß dann  $K$  allerdings eine zyklische Erweiterung vom Grad  $p^2$  besitzen muß. Das ist ein Widerspruch.

Der Fall  $p = 2$  wurde bereits in (3.19) behandelt.

Auf den Beweis des allgemeinen Falls wird hier mit Hinweis auf die angegebene Literatur verzichtet.  $\square$

Als Folgerung von (3.20) gewinnen wir sofort folgenden Kennzeichnungssatz:

**Satz 3.21** *Es sei  $K$  ein Körper sowie  $E$  eine Erweiterung von  $K$ . Dann sind äquivalent:*

- a)  $K$  ist formal reell, und  $E$  ist eine euklidische Hülle von  $K$ ,
- b)  $E$  ist euklidisch und in  $K_2$  enthalten,
- c)  $E \subset K_2$ ,  $[K_2 : E] = 2$ ,
- d)  $E \subset K_2$ ,  $1 < [K_2 : E] < \infty$ .

---

[3.20]Siehe [Bec73, Satz 3]. Hier wird direkt aus einer Arbeit von G.Whaples zitiert.

[3.21]Siehe [Bec73, Satz 6]

**BEWEIS:** **a)⇒b):** Nach der Konstruktion in (3.11) ist  $E \subseteq K_2$  sofort klar.  
**b)⇒c):** Nach (3.4) ist  $E(i)$  die einzige quadratische Erweiterung von  $E$ . Daraus folgt allerdings:  $E(i)$  ist 2-abgeschlossen, also  $K_2 \subseteq E(i)$ . Das zeigt  $E \subset K_2$  und  $[K_2 : E] = 2$ .  
**c)⇒d):** Die Aussage ist trivial.  
**d)⇒a):** Wäre  $E$  2-abgeschlossen, so folgte mit  $E \subset K_2$  sofort  $E = K_2$  und mithin  $[K_2 : E] = 1$ . Also ist  $E_2 \neq E$ , und wir erhalten außerdem  $1 < [E_2 : E] < \infty$ . Mit dem Satz von Whaples (3.20) ist  $E$  euklidisch.  $K$  ist notwendigerweise formal reell, sonst wäre  $E$  als Erweiterungskörper nicht euklidisch. Es bleibt zu zeigen, daß  $E$  eine euklidische Hülle und mithin minimal ist. Angenommen, es sei  $E'$  eine euklidische Hülle von  $K$ , aber ein echter Unterkörper von  $E$ . Dann gilt für  $E'$  mit (3.4) ebenfalls  $K_2 = E'(i)$ , also  $E' = E$  im Widerspruch zur Annahme.  $\square$

### 3.4 Die euklidischen Unterkörper von $\mathbb{R}$

Dieser Abschnitt behandelt kurz die Frage nach den euklidischen Zwischenkörpern zwischen  $\mathbb{Q}$  und  $\mathbb{R}$ .

**Lemma 3.22** *Der euklidische Abschluß von  $\mathbb{Q}$  ist echt kleiner als der reelle Abschluß von  $\mathbb{Q}$ .*

**BEWEIS:** Der euklidische Abschluß von  $\mathbb{Q}$  ist eine 2-Erweiterung von  $\mathbb{Q}$ ; daher ist jedes Element in  $\mathbb{Q}$  algebraisch über  $\mathbb{Q}$ , und die dazugehörige Ordnung ist eine Potenz von 2.

Der reelle Abschluß umfaßt allerdings alle reellen algebraischen Erweiterungen von  $\mathbb{Q}$ , ist also echt größer.  $\square$

Mit dieser Eigenschaft folgt außerdem sofort:

**Korollar 3.23** *In  $\mathbb{R}$  ist ein euklidischer Teilkörper enthalten, der echt kleiner ist.*

Damit allein wollen wir uns allerdings nicht begnügen. Bekanntlich existiert eine Transzendenzbasis  $\mathcal{B}$  von  $\mathbb{R}$  über  $\mathbb{Q}$ . Die Mächtigkeit von  $\mathcal{B}$  ist gleich der Mächtigkeit von  $\mathbb{R}$ . Mit dieser Tatsache können wir leicht folgendes Lemma beweisen:

**Lemma 3.24** *Die Familie der euklidischen Teilkörper von  $\mathbb{R}$  ist zu  $\mathbb{R}$  mindestens gleichmächtig.*

**BEWEIS:** Seien  $b_1, b_2 \in \mathcal{B}$  Elemente der Transzendenzbasis. Dann sind  $b_1$  und  $b_2$  algebraisch unabhängig über  $\mathbb{Q}$  und mithin transzendent. Aufgrund der algebraischen Unabhängigkeit sind dann auch  $\mathbb{Q}(b_1)$  und  $\mathbb{Q}(b_2)$  verschiedene echte Erweiterungen von  $\mathbb{Q}$ .

Beide Körpererweiterungen sind eingebettet in  $\mathbb{R}$  und besitzen daher eine Anordnung, sind also formal reell. Es genügt nun zu zeigen: Die euklidischen Hüllen  $E_1$  von  $\mathbb{Q}(b_1)$  und  $E_2$  von  $\mathbb{Q}(b_2)$  sind verschieden.

Angenommen, es sei  $E_1 = E_2$  für irgendwelche  $b_1, b_2 \in \mathcal{B}$ . Dann existiert ein Zwischenkörper  $L$  von  $\mathbb{Q}(b_1) \subset L \subseteq E_1$  und  $\mathbb{Q}(b_2) \subset L \subseteq E_2$ .  $L$  ist in der euklidischen Hülle von  $\mathbb{Q}(b_1)$  enthalten und daher eine 2-Erweiterung von  $\mathbb{Q}(b_1)$ .  $b_2$  ist deshalb algebraisch und von endlichem Grad (sogar einer Potenz von 2) über  $\mathbb{Q}(b_1)$ .

Sei  $f \in \mathbb{Q}(b_1)[X]$  das Minimalpolynom zu  $b_2$  über  $\mathbb{Q}(b_1)$ . Dann ist  $f$  von der Gestalt

$$f(X) = X^n + X^{n-1}a_{n-1} + \dots + X^1a_1 + a_0,$$

dabei läßt sich jedes  $a_i \in \mathbb{Q}(b_1)$  schreiben als  $a_i := \alpha_i + \beta_i b_1$ . Damit hat das Polynom  $g \in \mathbb{Q}[X, Y]$  mit

$$g(X, Y) := X^n + X^{n-1}\alpha_{n-1} + X^{n-1}Y\beta_{n-1} + X^{n-2}\alpha_{n-2} + X^{n-2}Y\beta_{n-2} + \dots + X^1\alpha_1 + X^1Y\beta_1 + Y\beta_0 + \alpha_0$$

die Wurzel  $(b_1, b_2)$ . Da  $\mathcal{B}$  allerdings eine Transzendenzbasis ist, folgt damit bereits  $b_1 = b_2$ .  $\square$

Die letzte Aussage konnten noch sehr leicht elementar bewiesen werden. Wir werden sofort erkennen, daß dieselbe Strategie auch für einen sehr viel allgemeineren Fall zum Ziel führt. Bevor wir uns allerdings daran machen können, dieses Ergebnis so allgemein als möglich zu formulieren, wird es erforderlich, kurz ein Lemma über algebraisch unabhängige Systeme und transzendente Erweiterungskörper zu beweisen:

**Lemma 3.25** *Es sei  $K$  ein Körper, sowie  $\mathcal{T}$  ein über  $K$  algebraisch unabhängiges System. Seien ferner  $B \subseteq \mathcal{T}$  eine Teilmenge sowie  $b \in \mathcal{T}$  irgendein Element von  $\mathcal{T}$ . Offensichtlich ist  $E := K(B)$  ein  $B$  umfassender*

Erweiterungskörper von  $K$ , sowie  $L := E(b)$  ein Erweiterungskörper von  $E$ , der  $b$  enthält, und es gilt:

Genau dann ist  $b$  algebraisch über  $E$ , wenn  $b \in B$ .

**BEWEIS:** Ist  $b \in B$ , so ist selbstverständlich  $b$  algebraisch über  $E$ ; der Erweiterungskörper  $L$  von  $E$  ist dann nämlich kein echter. Es bleibt also nur die Gegenrichtung zu zeigen:

Ist  $L$  keine echte algebraische Erweiterung von  $E$ , so ist natürlich  $b$  nicht algebraisch über  $E$ , und mithin nicht in  $B$  enthalten.

So sei also  $L$  im folgenden eine echte algebraische Erweiterung von  $E$ ; es ist dann  $b$  algebraisch über  $E$ , also existiert ein Minimalpolynom mit Koeffizienten  $\lambda_i$  aus  $E$  zu  $b$ :

$$\sum_{i=0}^n \lambda_i b^i = 0$$

Bekanntlich läßt sich jedes Element einer algebraischen Körpererweiterung schreiben als Quotient zweier Polynome über dem Grundkörper, so daß die Koeffizienten aus obigem Polynom etwa von folgender Gestalt sind:

$$\lambda_i = \frac{\sum_{j=0}^m l_{j_1^j, \dots, j_r^j}^{\lambda_i} b_1^{j_1^j} \cdot \dots \cdot b_r^{j_r^j}}{\sum_{k=0}^o h_{k_1^k, \dots, k_r^k}^{\lambda_i} b_1^{k_1^k} \cdot \dots \cdot b_r^{k_r^k}} \quad b_1, \dots, b_r \in B, l_{j_1^j, \dots, j_r^j}^{\lambda_i}, h_{k_1^k, \dots, k_r^k}^{\lambda_i} \in K$$

Der bemerkenswerte und wichtige Gesichtspunkt dabei ist, daß hier jeweils nur *endlich* viele Elemente aus  $B$  bei der Bildung eines der Koeffizienten  $\lambda_i$  beteiligt sind; deswegen dürfen wir uns auch erlauben, für beide Polnome in allen  $n$  Koeffizienten  $\lambda_1, \dots, \lambda_n$  dieselbe  $r$ -Elementige Teilmenge von  $B$  zugrunde zu legen.

Setzen wir diese allgemeine Form für die  $\lambda_i$  in das Minimalpolynom von  $b$  ein, so erhalten wir:

$$\sum_{i=0}^n \frac{\sum_{j=0}^m l_{j_1^j, \dots, j_r^j}^{\lambda_i} b_1^{j_1^j} \cdot \dots \cdot b_r^{j_r^j}}{\sum_{k=0}^o h_{k_1^k, \dots, k_r^k}^{\lambda_i} b_1^{k_1^k} \cdot \dots \cdot b_r^{k_r^k}} b^i = 0$$

Nun Multiplizieren wir dieses Polynom mit allen im Nenner auftretenden Polynomen und erhalten:

$$\sum_{i=0}^n \left( \left( \sum_{j=0}^m l_{j_1, \dots, j_r}^{\lambda_j} b_1^{j_1} \cdot \dots \cdot b_r^{j_r} \right) \cdot \prod_{\substack{p=1 \\ p \neq i}}^n \left( \sum_{k=0}^o h_{k_1, \dots, k_r}^{\lambda_p} b_1^{k_1} \cdot \dots \cdot b_r^{k_r} \right) \right) b^i = 0$$

Da die Menge der Polynome in  $b_1, \dots, b_r$  über  $K$  Ringstruktur besitzt, ist auch das Produkt der  $n$  Polynome in der letzten Gleichung wieder ein Polynom der gleichen Gestalt, so daß wir schließlich wie folgt schreiben können:

$$\sum_{i=0}^n \left( \sum_{j=0}^m \gamma_{k_{i,j,1}, \dots, k_{i,j,r}} b_1^{k_{i,j,1}} \cdot \dots \cdot b_r^{k_{i,j,r}} \right) b^i = 0 \quad \gamma_{k_{0,0,1}, \dots, k_{n,m,r}} \in K$$

Und mithin

$$\sum_{i=0}^n \sum_{j=0}^m \gamma_{k_{i,j,1}, \dots, k_{i,j,r}} b_1^{k_{i,j,1}} \cdot \dots \cdot b_r^{k_{i,j,r}} \cdot b^i = 0 \quad \gamma_{k_{0,0,1}, \dots, k_{n,m,r}} \in K$$

Da jetzt allerdings die Menge  $B \cup \{b\} \subseteq \mathcal{T}$  algebraisch unabhängig ist kann diese letzte Gleichheit nur bedeuten, daß entweder alle  $k_{0,0,1}, \dots, k_{n,m,r}$  verschwinden, oder daß bereits  $b \in B$ . Den ersten Fall können wir ausschließen, da der Polynomring über einem Körper nullteilerfrei ist, so daß  $b \in B$  als einzige Möglichkeit verbleibt. Damit allerdings ist die Aussage bewiesen.  $\square$

Jetzt sind wir in der Lage, die allgemeinste mögliche Aussage über die Anzahl der euklidischen Unterkörper von  $\mathbb{R}$  zu formulieren:

**Satz 3.26** *Es bezeichne  $\mathcal{E} := \mathcal{E}_{\mathbb{Q}}^{\mathbb{R}}$  die Menge der euklidischen Zwischenkörper von  $\mathbb{Q}$  und  $\mathbb{R}$ . Dann ist  $|\mathcal{E}| = 2^{|\mathbb{R}|}$ .*

BEWEIS: Wir werden den Satz in zwei Schritten beweisen, von denen der zweite trivial ist:

1.  $|\mathcal{E}| \geq 2^{|\mathbb{R}|}$  werden wir zeigen, indem wir nachweisen:

$$\tau : \wp(\mathcal{B}) \rightarrow \mathcal{E} \quad : \quad B \mapsto \tau(B),$$

ist eine Injektion der Potenzmenge von  $\mathcal{B}$  in  $\mathcal{E}$ , wobei  $\tau(B)$  die euklidische Hülle zur von  $\mathbb{R}$  auf  $\mathbf{Q}(B)$  induzierten Anordnung von  $\mathbf{Q}(B)$  sei. Seien dazu  $B_1, B_2 \in \mathcal{B}$  zwei beliebige Teilmengen von  $\mathcal{B}$ , für die wir  $B_1 \neq B_2$  annehmen; im anderen Fall wäre nichts zu zeigen.

Es genügt zu zeigen: Die euklidischen Hüllen von  $\mathbf{Q}(B_1)$  und  $\mathbf{Q}(B_2)$  sind verschieden; das bedeutet, daß mindestens eine der beiden Hüllen Elemente enthält, die nicht in der anderen enthalten sind. Wir werden die beiden verschiedenen Teilmengen  $B_1, B_2$  von  $\mathcal{B}$  dazu benutzen, ein solches Element nachzuweisen.

Aus Symmetriegründen ist es offensichtlich, daß wir annehmen dürfen, es existiere ein  $b \in B_1$ , welches nicht bereits in  $B_2$  enthalten ist. Dann ist  $b$  auch nicht in  $\mathbf{Q}(B_2)$  enthalten, da dann  $b$  algebraisch wäre über  $\mathbf{Q}(B_2)$ , und dies mit (3.25) der Voraussetzung  $b \notin B_2$  widerspricht.

Da wir in (3.11) bereits bewiesen haben, daß euklidische Hüllen algebraische Erweiterungen sind, muß aber  $b$  algebraisch über  $\mathbf{Q}(B_2)$  sein, wenn die euklidischen Hüllen von  $\mathbf{Q}(B_1)$  und  $\mathbf{Q}(B_2)$  gleich sein sollen. Dieser offensichtliche Widerspruch begründet die Aussage.

2.  $|\mathcal{E}| \leq 2^{|\mathbb{R}|}$  ist trivial, da  $\mathbb{R}$  nicht mehr Teilmengen enthalten kann als die Potenzmenge Elemente enthält.  $\square$

### 3.5 Formale Potenzreihenkörper über euklidischen Körpern

Wie bereits im Kapitel über pythagoreische Körper wollen wir auch hier zunächst die Frage behandeln, wie sich Körper formaler Potenzreihen über euklidischen Körpern verhalten. Wir hatten zuvor gesehen, daß dies im Fall der pythagoreischen Körper äußerst einfach war: Ohne Einschränkungen war  $H_f(G, K)$  genau dann pythagoreisch, wenn dies bereits auch auf  $K$  zutrifft. Wollen wir ein ähnliches Resultat auch für einen euklidischen Körper  $K$  erzielen, so müssen wir zunächst die Frage nach den Anordnungen von  $H_f(G, K)$  stellen.

Im folgenden sei stets  $K$  euklidisch. Ist nun aber  $K$  euklidisch, so ist auch jedes  $x \in P_K$  ein Quadrat und  $P_K$  ist die einzige Anordnung von  $K$

nach (3.2). In (1.35) haben wir für die Menge der Quadrate in  $H_f(G, K)$  erkannt, daß dafür sowohl die Quadrate in  $K$ , als auch die Struktur von  $G$  von gleichwertiger Bedeutung sind: Mit der Bezeichnung  $G_2 := \{2g : g \in G\}$  läßt sich das so formulieren:  $p \in H_f(G, K)$  ist ein Quadrat genau dann, wenn  $\text{ord}(p) \in G_2$  und  $\text{anf}(p) \in f(\text{ord}(p)/2, \text{ord}(p)/2)K^2$ . Außerdem findet man leicht, daß im Fall  $G_2 \neq G$  sofort  $[G : G_2] = 2$  folgt.

Mit dieser Charakterisierung folgt sofort folgendes Lemma:

**Satz 3.27** *Es sei  $K$  ein beliebiger Körper.  $H_f(G, K)$  ist genau dann euklidisch, wenn  $G = G_2$  und  $K$  euklidisch ist.*

BEWEIS: Ist  $H_f(G, K)$  euklidisch, so besitzt  $H_f(G, K)$  nach (3.2) genau eine Anordnung, und das sind die Quadrate in  $H_f(G, K)$ . Also existiert auch eine Anordnung auf der Einbettung von  $K$  in  $H_f(G, K)$ : Für jedes  $x \in K^\times$  ist entweder  $t^0x$  oder  $(-t^0)x$  in der Anordnung, und damit in der Menge der Quadrate von  $H_f(G, K)$  enthalten. Damit ist aber auch für jedes  $x \in K^\times$  entweder  $x$  oder  $(-x)$  ein Quadrat nach unserer Vorüberlegung;  $K$  ist notwendigerweise euklidisch. Sei nun  $G_2 \neq G$ , so betrachten wir die formale Potenzreihe  $t^g \in H_f(G, K)$  mit  $g \in G \setminus G_2$ . Entweder  $t^g$  oder  $(-t^g)$  muß ein Quadrat sein, und folglich wiederum gemäß unserer Vorüberlegung  $g \in G_2$ .

Die Umkehrung ist trivial. □

BEISPIEL 1:  $H_f(\mathbb{Z}, \mathbb{R})$  ist nicht euklidisch:

Ganz klar verletzt  $\mathbb{Z}$  die Bedingung  $\mathbb{Z}_2 = \mathbb{Z}$ . ┘

BEISPIEL 2:  $H_f(\mathbb{Q}, \mathbb{R})$  ist euklidisch:

$\mathbb{R}$  ist euklidisch (siehe Beispiel nach (3.2)), und für  $\mathbb{Q}$  gilt offensichtlich  $\mathbb{Q}_2 = \mathbb{Q}$ . ┘

Wir haben im zweiten Kapitel erkannt, daß  $H_f(G, K)$  für pythagoreisches  $K$  stets wieder pythagoreisch ist. Folglich ist  $H_f(G, K)$  auch für euklidisches  $K$  zumindest pythagoreisch — besitzt aber unter Umständen mehr als eine Anordnung, nämlich genau dann, wenn  $G \neq G_2$ . Die Frage, von welcher Gestalt die dann zwangsläufig existierenden weiteren Anordnungen (neben der von  $K$  kommenden) von  $H_f(G, K)$  aussehen, läßt sich ebenfalls sehr leicht beantworten:

**Lemma 3.28** Sei  $K$  ein euklidischer Körper sowie  $H_f(G, K)$  ein Körper formaler Potenzreihen über  $K$ . Ist  $G_2 \neq G$ , so definiert

$$Q := \{p \in H_f(G, K)^\times : p \in H_f(G, K)^2 \vee (\text{ord}(p) \notin G_2 \wedge \text{anf}(p) \notin P_K)\}$$

eine Anordnung auf  $H_f(G, K)$ , wobei  $P_K$  wie üblich die Anordnung auf  $K$  bezeichnet.

Diese Konstruktion ist denkbar einfach und liegt auf der Hand: Die Quadrate sind in jeder Anordnung eines Körpers enthalten. Unter allen formalen Potenzreihen mit „ungerader“ Ordnung erklären wir diejenigen als positiv, welche einen in  $K$  negativen Anfangskoeffizienten besitzen.

BEWEIS: Zum Nachweis der Behauptung betrachte man:

Die Eigenschaften  $Q \cap (-Q) = \emptyset$  sowie  $Q \cup (-Q) = H_f(G, K)^\times$  sind offensichtlich. Ebenfalls offensichtlich ist die additive Abgeschlossenheit von  $Q$ . Für die multiplikative Abgeschlossenheit beachte man die Produktformel und erhält:

- Das Produkt zweier Quadrate ist wieder ein Quadrat, liegt also in  $Q$ .
- Das Produkt zweier Nicht-Quadrate ist ebenfalls ein Quadrat und damit in  $Q$ .
- Das Produkt von Quadrat und Nicht-Quadrat ist kein Quadrat, da die Ordnung nicht in  $G_2$  liegt. Außerdem ist der Anfangskoeffizient negativ, das Ergebnis liegt also wieder in  $Q$ .

Dabei ist es wichtig, sich vor Augen zu halten, daß in  $K$  jede positive Zahl ein Quadrat ist, so daß ohne Beschränkung der Allgemeinheit  $f$  trivial angenommen werden darf. Außerdem geht hier wiederum maßgeblich die zusätzliche Bedingung  $f(a, b) > 0 \forall a, b \in G$  ein. □

# Schlußbemerkungen

Die Theorie der pythagoreischen und euklidischen Körper ist bei weitem noch nicht abgeschlossen. Viele Fragen sind noch offen oder gar noch überhaupt nicht formuliert worden, so daß hier noch Potential für Untersuchungen vorhanden ist. Wir wollen an dieser Stelle noch einen kurzen Überblick über einige Veröffentlichungen der letzten Jahr geben, die ebenfalls mit den hier behandelten Themen befaßt sind oder weitergehende Untersuchungen anstellen; diese Auflistung steht hier selbstverständlich ohne Anspruch auf Vollständigkeit, sie soll vielmehr als Anregung für das weiterführende Lesen und als Einstieg in die fortführende Literatur auf diesem Gebiet dienen.

Diller und Dress untersuchen in [DD65] die Galoisgruppe solcher Körpererweiterungen eines pythagoreischen Körpers, die eine Erweiterung vom Grade  $2^n$  sind, durch eine Charakterisierung der Quadratklassenstruktur des Grundkörpers.

Eine genauere Untersuchung des pythagoreischen Abschlusses spezieller Körper unternimmt Griffin in [Gri76]; und zwar widmet er sich nach eingehender Betrachtung allgemeiner Körper zunächst solchen, die unter speziellen Bewertungen abgeschlossen sind, und sodann globalen Körpern.

In seinem Artikel [Brö76] geht Bröcker auf die sogenannten *erblich pythagoreischen Körper* ein. Das sind solche Körper, die pythagoreisch sind und die keine formal reellen endlich-algebraischen Erweiterungen besitzen, die nicht auch pythagoreisch sind. Als  $\Omega$ -pythagoreisch werden ferner Körper bezeichnet, die erblich pythagoreisch innerhalb eines  $p$ -abgeschlossenen Körpers  $\Omega$  sind. Bröcker stellt unter anderem Zusammenhänge zwischen Fächern und  $\Omega$ -pythagoreischen Körpern her. Eine schwächere Eigenschaft ist die folgende: Ist zu einem pythagoreischen Körper bereits jeder formal reelle qua-

dratische Erweiterungskörper pythagoreisch, dann heißt der Körper *strikt-pythagoreisch*. Solche Körper werden in [Brö72] durch Bröcker behandelt.

Auf die Arbeiten von Bröcker aufbauend hat Jacob ebenfalls die Struktur pythagoreischer Körper bewertungstheoretisch ergründet und seine Ergebnisse in [Jac81c] veröffentlicht. Weitergehende, galoistheoretische Eigenschaften pythagoreischer Körper finden sich darüberhinaus in [Jac81b]. In der Arbeit [Jac81a] schließlich verallgemeinert Jacob einen Kennzeichnungssatz von Bröcker und Brown für *superpythagoreische Körper*; das sind pythagoreische Körper, deren Quadrate einen (starken) Fächer bilden. Superpythagoreische Körper werden auch manchmal als *strikt-pythagoreisch* bezeichnet.

Das Konzept der Vererbung kann auch auf euklidische Körper übertragen werden. So heißt ein Körper *erblich euklidisch*, wenn er und alle endlich algebraischen Erweiterungskörper euklidisch sind. Solche Körper untersuchen Prestel und Ziegler in [PZ73] und charakterisieren sie außerdem bewertungstheoretisch sowie galoistheoretisch.

Die Struktur der Galoisgruppe  $K_{\Pi}/K$  wird von Ware in [War83] unter Zuhilfenahme der Theorie der Quadratischen Formen untersucht. Dabei legt der Autor besonderen Wert auf die Betrachtung der Beziehungen zur Torsionsuntergruppe des Witttrings  $W(K)$ .

Von Becker wurden solche Körper untersucht, für die die Galoisgruppe gewisser Körpererweiterungen abelsch ist. In [Bec78] führt das den Autor zu einer Untersuchung der Summen von Quadraten, weiteren  $2^n$ -ten Potenzen und deren Zusammenhänge mit pythagoreischen Körpern.

Bei der Suche nach nicht formal reellen Körpern mit nichttrivialem Kaplansky-Radikal konnte Berman in [Ber79] durch Betrachtung spezieller Erweiterungen pythagoreischer Körper und dem Raum deren Anordnungen ebenfalls einige bemerkenswerte Ergebnisse erzielen.

Am Ende dieser Arbeit möchte ich den verbleibenden Platz noch nutzen, um einige Danksagungen auszusprechen:

Recht herzlich möchte ich meinem Aufgabensteller und Betreuer, Herrn Professor Dr. Heinz Wähling, für die Unterstützung während der letzten sechs Monate danken. Seiner Inspiration ist es nicht nur zuzuschreiben, daß die Theorie der Körper formaler Potenzreihen nicht nur zur Konstruktion von Beispielen verwendet wurde sondern daß tatsächlich echte Aussagen über die

Zusammenhänge von Körpern und ihren Potenzreihenkörper möglich wurden, sondern auch, daß es zu den Betrachtungen über die Anzahl der euklidischen Teilkörper von  $\mathbb{R}$  kam.

Meinen Eltern und meinen zwei Brüdern möchte ich dafür danken, daß sie mich so sehr moralisch unterstützt und mir auch sonst alle möglichen Steine aus dem Weg geräumt haben.

Schließlich gilt meine Dankbarkeit noch einer Reihe von Menschen, die ich mich freue meine Freunde nennen zu dürfen, deren Geduld ich wohl in der letzten Zeit durch Unanwesenheit oder chronische Übermüdung stark strapaziert habe doch die alle einzeln zu nennen der Platz hier aber leider nicht ausreicht.

Thomas Ganter

# Literaturverzeichnis

- [Alb38] ADRIAN A. ALBERT. „Modern Higher Algebra“. Cambridge University Press, London, 2. Auflage (1938).
- [Bec73] EBERHARD BECKER. Euklidische Körper und euklidische Hüllen von Körpern. *Journal für Mathematik* **268/269**, 41–52 (1973).
- [Bec78] EBERHARD BECKER. hereditary pythagorean fields, infinite harison-primes and sums of  $2^n$ th powers. *bulletin of the american mathematical society* **84**(2), 278–280 (1978).
- [Ber79] LAWRENCE BERMAN. Pythagorean Fields and the Kaplanski Radical. *journal of algebra* **61**, 497–507 (1979).
- [Bou88] NICOLAS BOURBAKI. „Algebra II“. Elements of mathematics. Springer Verlag, Berlin, Heidelberg, New York, U.S. Auflage (1988).
- [Brö72] LUDWIG BRÖCKER. Über eine Klasse pythagoreischer Körper. *Arch. Math.* **XXIII**, 405–407 (1972).
- [Brö76] LUDWIG BRÖCKER. Characterization of Fans and Hereditary Pythagorean Fields. *Mathematische Zeitschrift* **151**, 149–163 (1976).
- [DD65] JUSTUS DILLER UND ANDREAS DRESS. Zur Galoistheorie pythagoreischer Körper. *Arch.Math.* **XVI**, 148–152 (1965).
- [Gri76] MALCOM P. GRIFFIN. the pythagorean closure of fields. *math. scand.* **38**, 177–191 (1976).

- [Hei91] WERNER HEISE. Induktives Beweisen und Definieren. Pamphlet wider die These vom göttlichen Ursprung der natürlichen Zahlen, Mathematisches Institut der TU München (1991).
- [Jac80a] NATHAN JACOBSON. „Basic Algebra“, Band I. W.H.Freeman and Company, San Francisco (1980).
- [Jac80b] NATHAN JACOBSON. „Basic Algebra“, Band II. W.H.Freeman and Company, San Francisco (1980).
- [Jac81a] BILL JACOB. Fans, real valuations, hereditary-pythagorean fields. *pacific journal of mathematics* **93**(1), 95–105 (1981).
- [Jac81b] BILL JACOB. The Galois cohomology of Pythagorean Fields. *inventiones mathematicae* **65**, 97–113 (1981).
- [Jac81c] BILL JACOB. On the structure of pythagorean fields. *Journal of Algebra* **68**, 247–267 (1981).
- [Jud93] THOMAS W. JUDSON. „Abstract algebra: theory and application“. the Prindle, Weber & Schmidt series in advanced mathematics. PWS Publishing Company, Boston, Massachusetts (1993).
- [Kal89] FRANZ B. KALHOFF. Anordnungsräume und Witttringe projektiver Ebenen. Habilitationsschrift, Universität Dortmund (1988/89).
- [Lam73] T.Y. LAM. „The algebraic theory of quadratic forms“. W.A.Benjamin, Inc., Reading, Massachusetts (1973).
- [Leu93] ARMIN LEUTBECHER. Elementare Zahlentheorie. Skriptum zur Vorlesung im Wintersemester 1992/1993 TUM-MATH-04-93-00-300/1.-FM, Fakultät für Mathematik der TU München (April 1993).
- [PC83] SIBYLLA H.G. PRIESS-CRAMPE. „Angeordnete Strukturen: Gruppen, Körper, projektive Ebenen“. Nummer 98 in Ergebnisse der Mathematik und ihrer Grenzgebiete. Springer Verlag, Berlin, Heidelberg, New York (1983).
- [PZ73] ALEXANDER PRESTEL UND MARTIN ZIEGLER. Erblich euklidische Körper. *Journal für Mathematik* **274/275**, 196–205 (1973).

- [Rib72] PAOLO RIBENBOIM. „L'Arithmétique des Corps“. Herman, Paris (1972).
- [Rib74] PAOLO RIBENBOIM. Pfister's dimension and the level of fields. *math.scand.* **35**, 311–318 (1974).
- [Rib92] PAOLO RIBENBOIM. Fields: Algebraically closed and others. *manuscripta mathematica* **75**, 115–150 (1992).
- [RS90] FRITZ REINHARDT UND HEINRICH SOEDER. „dtv-Atlas zur Mathematik“, Band 1. Deutscher Taschenbuch-Verlag GmbH & Co. KG, München, 8. Auflage (1990).
- [Tsc81] A. TSCHIMMEL. Über Anordnungsräume von Schiefkörpern. Dissertationsschrift, Universität Münster (1981).
- [Wäh92] HEINZ WÄHLING. Angeordnete algebraische Strukturen. Skriptum zur Vorlesung im Sommersemester 1992, Mathematisches Institut der TU München (1992).
- [War83] ROGER WARE. Quadratic forms and pro 2-groups II: The galois group of the pythagorean closure of a formally real field. *Journal of Pure and Applied Algebra* **30**, 95–107 (1983).