



universität
wien

DIPLOMARBEIT

Titel der Diplomarbeit

„Einheiten in total definiten Quaternionenalgebren“

Verfasser

Ludwig Geroldinger

angestrebter akademischer Grad

Magister der Naturwissenschaften (Mag.rer.nat)

Wien, Dezember 2009

Studienkennzahl lt. Studienblatt: A 405

Studienrichtung lt. Studienblatt: Mathematik

Betreuer: Prof. Dr. Joachim Schwermer

Zuallererst möchte ich mich bei Professor Joachim Schwermer für das Thema und die Betreuung bedanken. Er hat mir einen Einblick in ein hochaktuelles Forschungsgebiet ermöglicht. Dr. Harald Grobner, Professor Joachim Mahnkopf und Dr. Christoph Waldner hatten für meine Fragen bei der Erstellung der Diplomarbeit immer ein offenes Ohr: Herzlichen Dank.

Viele Vorlesungen - von Linearer Algebra bis zu zahlentheoretischen Spezialvorlesungen - habe ich bei Professor Johannes Schoißengeier gehört, der für mich ein wichtiger Ansprechpartner während des ganzen Studiums war. Auch ihm ein aufrichtiges Dankeschön.

Inhaltsverzeichnis

1	Quaternionenalgebren	1
1.1	Grundlegende Eigenschaften von Quaternionenalgebren	1
1.2	Das Verzweigungsverhalten von Quaternionenalgebren	6
1.3	Ordnungen in Quaternionenalgebren	10
1.4	Topologische Eigenschaften von Quaternionenalgebren	14
2	Adele und Ideale	19
2.1	Das eingeschränkte direkte Produkt	19
2.2	Topologische Eigenschaften der Adele von Quaternionenalgebren	24
2.3	Topologische Eigenschaften der Ideale	26
3	Einheiten in total definiten Quaternionenalgebren	29
3.1	Der Dirichlet'sche Einheitensatz für S -Einheiten	29
3.2	Eine Verallgemeinerung des Dirichlet'schen Einheitensatzes auf total definite Quaternionenalgebren	33
3.3	Interpretation des Hauptsatzes	37

Einleitung

Es sei K ein algebraischer Zahlkörper und $\mathcal{O}_K$ sein Ganzheitsring. Wir bezeichnen die Menge aller nichtäquivalenten Bewertungen auf K mit $\Omega(K)$ und nennen die Elemente von $\Omega(K)$ auch die Stellen von K . Für $v \in \Omega(K)$ bezeichne K_v die Vervollständigung von K bezüglich eines zur Stelle v gehörigen Absolutbetrages. Für eine endliche Stelle $v \in \Omega(K)$ notieren wir den Bewertungsring von K_v mit R_v .

Es sei nun r die Anzahl der reellen Stellen von K , s die Anzahl der komplexen Stellen von K und μ_K die Gruppe der Einheitswurzeln in K . Nach dem Dirichlet'schen Einheitensatz gibt es einen Isomorphismus abelscher Gruppen:

$$\mathcal{O}_K^* \cong \mu_K \times \mathbb{Z}^{r+s-1},$$

oder äquivalent, eine exakte Sequenz abelscher Gruppen

$$1 \longrightarrow \mu_K \longrightarrow \mathcal{O}_K^* \longrightarrow \mathbb{Z}^{r+s-1} \longrightarrow 1,$$

womit die Struktur der Einheitengruppe $\mathcal{O}_K^*$ bestimmt ist.

Es sei A Quaternionenalgebra (siehe Definition 1.1.1) über einem Zahlkörper K . Eine $\mathcal{O}_K$ -Ordnung $\mathcal{O}$ in A ist ein endlich erzeugter $\mathcal{O}_K$ -Modul, welcher ein Teilring von A ist, und eine K -Basis von A enthält.

Eine Quaternionenalgebra A über einem Zahlkörper K erfüllt die Eichlerbedingung, falls es eine archimedische Stelle $v \in \Omega(K)$ gibt, sodass $A \otimes_K K_v$ keine Divisionsalgebra ist. Die Quaternionenalgebra A heißt total definit, falls sie nicht die Eichlerbedingung erfüllt, also für alle archimedischen Stellen $v \in \Omega(K)$ $A \otimes_K K_v$ eine Divisionsalgebra ist.

Bei der Untersuchung der Einheitengruppe $\mathcal{O}^*$ in einer total definiten Quaternionenalgebra A orientieren wir uns an dem adelischen Zugang zum Dirichlet'schen Einheitensatz. Wir werden die Existenz folgender exakter Sequenz topologischer Gruppen beweisen

$$1 \longrightarrow \text{Tor}(\mathcal{O}^*) \longrightarrow \mathcal{O}^* \longrightarrow \mathbb{Z}^{r+s-1} \longrightarrow 1,$$

wobei $\text{Tor}(\mathcal{O}^*)$ die Torsionsgruppe von $\mathcal{O}^*$ ist und r wieder die Anzahl der reellen Stellen und s die Anzahl der komplexen Stellen von K bezeichnet. Diese Sequenz ist eine Verallgemeinerung des Dirichlet'schen Einheitensatzes auf Ordnungen in Quaternionenalgebren. Aufgrund der Nichtkommutativität der Gruppen spaltet sie jedoch im Allgemeinen nicht. Insbesondere ist $\mathcal{O}^*$ nicht notwendigerweise isomorph zum direkten Produkt von $\text{Tor}(\mathcal{O}^*)$ mit einer freien abelschen Gruppe. Etwas allgemeiner als gerade formuliert werden wir die Struktur der S -Einheitengruppe $\mathcal{O}_S^*$ beschreiben, siehe 3.2.3.

Im folgenden beschreiben wir den Zusammenhang dieser Arbeit mit der Theorie zentral einfacher Algebren.

In der nichtkommutativen Algebra werden zentral einfache (nicht kommutative) Algebren über algebraischen Zahlkörpern untersucht. Analog zur algebraischen Zahlentheorie wird die Arithmetik dieser Algebren studiert. Dabei wird die Rolle des Ganzheitsringes $\mathcal{O}_K$ durch Ordnungen

(das sind vollständige $\mathcal{O}_K$ -Gitter, welche zugleich Teilringe der Algebra sind) eingenommen. Wie in der klassischen Theorie werden die Ideale und die Einheitengruppe solcher Ordnungen untersucht.

Die Idealtheorie ist weitgehend bekannt. Da zentral einfache Algebren nicht notwendigerweise kommutativ sind, muss man zwischen zweiseitigen und einseitigen Idealen unterscheiden. Man zeigt wie bei Dedekindringen, dass die Menge der zweiseitigen Ideale eine freie abelsche Gruppe bildet, die von der Menge der von Null verschiedenen Primideale erzeugt wird. Die Theorie der einseitigen Ideale ist komplizierter. Erfüllt die Algebra die Eichlerbedingung, kann man aber folgendes tun: Man führt auf der Menge der einseitigen Ideale (in einer maximalen Ordnung) eine Äquivalenzrelation ein, sodass die Menge der Ideale modulo dieser Relation isomorph zu einer Strahlklassengruppe ist (Satz von Swan). Mit diesem Ergebnis ist man auch in der Lage alle konjugierten maximalen Ordnungen anzugeben. Diese Theorie findet sich in [11]. Wenn die Eichlerbedingung nicht erfüllt ist, ist die Theorie weniger glatt. Für Algorithmen zur Berechnung gewisser Invarianten siehe [6].

Die Einheitentheorie ist nicht so gut erforscht. Einen guten Überblick dieser Theorie findet sich in [7]. Dort wird bewiesen, dass die Einheitengruppe endlich präsentiert ist.

Die vorliegende Arbeit behandelt die Einheitengruppe einer Ordnung in einer total definiten zentral einfachen Algebra über einem Zahlkörper (Quaternionenalgebren sind genau die vierdimensionalen zentral einfachen Algebren).

Kapitel 1

Quaternionenalgebren

In diesem Kapitel sei K ein Körper mit $\text{char}K \neq 2$.

1.1 Grundlegende Eigenschaften von Quaternionenalgebren

Es seien $a, b \in K^*$. Wir konstruieren im folgenden eine vierdimensionale K -Algebra $A = A(a, b|K)$. Zunächst betrachten wir die zweidimensionale kommutative K -Algebra $B := K[X]/(X^2 - a)$ und identifizieren K mit der Unteralgebra $K1$. Als Vektorraum über K hat B die Basis $1 = (X^2 - a)$, $i := X + (X^2 - a)$, und die Multiplikation auf B wird durch $i^2 := a1$ festgelegt. Die Abbildung

$$B \longrightarrow B, \quad x \mapsto \bar{x} \quad \text{mit} \quad \overline{u + iv} = u - iv, \quad \text{für } u, v \in K$$

ist ein Isomorphismus von B als K -Algebra. Nun definieren wir auf $A = A(a, b|K) := B \times B$ durch komponentenweise Addition und der folgenden Multiplikation

$$(x, y) \cdot (x', y') := (xx' + by\bar{y}', xy' + y\bar{x}'), \quad \text{für } x, y, x', y' \in B$$

eine Ringstruktur. Es zeigt

$$(x, 0)(x', y') = (xx', xy') \quad \text{und} \quad (x', y')(x, 0) = (x'x, y'\bar{x}),$$

dass $B \longrightarrow A, \quad x \mapsto (x, 0)$ ein injektiver Ringhomomorphismus ist und wir dadurch B mit seinem Bild in A identifizieren können. Außerdem sieht man durch die letzte Gleichung, dass K im Zentrum von A liegt, womit A zu einer K -Algebra wird.

Definition 1.1.1. Eine Algebra A über K heißt *Quaternionenalgebra*, falls $a, b \in K^*$ existieren, sodass A zu $A(a, b|K)$ als K -Algebra isomorph ist. Wir sprechen dann auch von der durch a und b gegebenen Quaternionenalgebra.

Ab nun bezeichne A eine Quaternionenalgebra. Wir werden $A = A(a, b|K)$ schreiben, wenn wir betonen wollen, dass A durch a und b gegeben ist.

Man kann obige Konstruktion auch in Charakteristik 2 ausführen. Es ist dann aber die Abbildung $x \mapsto \bar{x}$, die Identität und die Multiplikation kommutativ. Also erhält man in Charakteristik 2 mit obiger Konstruktion kein Analogon zu den Hamiltonschen Quaternionen, siehe 1.1.9. Deshalb betrachten wir hier nur den Fall $\text{char}K \neq 2$.

Proposition 1.1.2. 1. Es ist $1 = (1, 0)$, $i = (i, 0)$, $j := (0, 1)$, $k := (0, i)$ eine Basis von $A(a, b|K)$ über K , und es gilt: $i^2 = a1$, $j^2 = b1$, $k^2 = -ab$, $ij = -ji = k$, $jk = -kj = -bi$, $ki = -ik = -aj$.

2. Es seien $a, b \in K^*$. Weiters sei T eine vierdimensionale K -Algebra mit einer Basis e_0, e_1, e_2, e_3 , so dass $e_0 = 1$, $e_1^2 = a1$, $e_2^2 = b1$ und $e_1e_2 = -e_2e_1 = e_3$. Dann ist durch $1 \mapsto e_0$, $i \mapsto e_1$, $j \mapsto e_2$, $k \mapsto e_3$ ein K -Algebrenisomorphismus von $A(a, b|K)$ nach T gegeben.

Beweis. Einfache Rechnung. □

Die Basis $\{1, i, j, k\}$ aus 1.1.2 bezeichnen wir im Folgenden als die Standardbasis von A über K .

Proposition 1.1.3. 1. Für $(a, b) \neq (0, 0)$ ist $K1$ das Zentrum von $A(a, b|K)$. (A ist eine zentrale Algebra.)

2. Für $a, b \neq 0$ sind (0) und $A(a, b|K)$ die einzigen zweiseitigen Ideale in $A(a, b|K)$. (A ist eine einfache Algebra.)

Beweis. 1. Für $x, y \in A(a, b|K)$ definieren wir den Kommutator durch $[x, y] := xy - yx$. Bezüglich der Standardbasis hat x die Form $x = x_01 + x_1i + x_2j + x_3k$ mit allen $x_r \in K$, sodass sich mittels 1.1.2 folgendes ergibt:

$$[i, x] = x_0i + x_1i^2 + x_2ij + x_3ik - x_0i - x_1i^2 - x_2ji - x_3ki = 2x_2k + 2x_3aj$$

$$[j, x] = x_0j + x_1ji + x_2j^2 + x_3jk - x_0j - x_1ij^2 - x_2ij - x_3kj = -2x_1k - 2x_3bi$$

$$[k, x] = x_0k + x_1ki + x_2kj + x_3k^2 - x_0k - x_1ik - x_2jk - x_3k^2 = -2ax_1j + 2bx_2i$$

Aus der Konstruktion von $A(a, b|K)$ folgt $K \subseteq Z(A(a, b|K))$. Ist umgekehrt $x \in Z(A(a, b|K))$ dann folgt $[i, x] = [j, x] = [k, x] = 0$, sodass sich wegen $\text{char} K \neq 2$ und $a \neq 0$, $b \neq 0$ $x_1 = x_2 = x_3 = 0$ ergibt, und wir $Z(A(a, b|K)) \subseteq K$ erhalten.

2. Es sei I ein (zweiseitiges) Ideal in $A(a, b|K)$ und $x \in I$, $x \neq 0$. Dann sind auch die folgenden Elemente in I :

$$[j, [i, x]] = [j, (2x_3a)j + (2x_2)k] = (-4x_2b)i$$

$$[k, [j, x]] = [k, (-2x_3b)i + (-2x_1)k] = (4x_3ab)j$$

$$[i, [k, x]] = [i, (2bx_2)i - (2ax_1)j] = (-4x_1a)k.$$

Ist einer der Koeffizienten x_1, x_2, x_3 von x ungleich 0, so enthält I nach obiger Rechnung eine Einheit. Falls $x_1 = x_2 = x_3 = 0$ enthält I ebenfalls eine Einheit, da dann $x = x_0 \in K^*$ gilt. Es folgt in beiden Fällen $I = A(a, b|K)$. □

Proposition 1.1.4. Es seien $a, b \in K^*$. Die Algebra $A = A(a, b|K)$ ist entweder eine Divisionsalgebra oder isomorph zur Matrizenalgebra $M_2(K)$.

Beweis. Es sei A keine Divisionsalgebra. Dann existiert ein Element $x \in A \setminus \{0\}$, welches keine Einheit ist. Weiters ist das Linksideal $I := Ax$ ungleich A und ungleich (0) . Als Vektorraum über K gibt es für die Dimension von I nur die Möglichkeiten $\dim_K I = 1, 2$ oder 3 .

Gilt $\dim_K I = 1$, so ist $I = Ax = Kx$. Somit gibt es für jedes $d \in A$ ein $\lambda_d \in K$ mit $dx = \lambda_d x$. Wegen $\lambda_1 = 1$ ist die Abbildung $\lambda : A \rightarrow K$, $d \mapsto \lambda_d$ ein Epimorphismus. Der Kern von λ ist ein zweiseitiges Ideal der Dimension drei in A , was einen Widerspruch zu 1.1.3 gibt. Somit kann der Fall $\dim_K I = 1$ nicht eintreten.

Der Fall $\dim_K I = 3$ lässt sich analog wie der erste Fall ausschließen, indem man den eindimensionalen Vektorraum A/I betrachtet.

Sei nun $\dim_K I = 2$ und v_1, v_2 eine K -Basis von I . Die Linksmultiplikation mit $q \in A$ ist eine K -lineare Abbildung $I \rightarrow I$, $x \mapsto qx$. Wir bezeichnen mit $\mu(q)$ die Matrix dieser linearen Abbildung bezüglich der Basis v_1, v_2 . Dann ist $\mu : A \rightarrow M_2(K)$ ein Algebrenhomomorphismus. Er ist injektiv, weil A einfach ist, und wegen $\dim_K A = \dim_K M_2(K) = 4$ ist er auch surjektiv. $\square$

Bemerkung 1.1.5. 1. Wir können obige Proposition auch mithilfe des Wedderburn'schen Struktursatz für zentrale einfache Algebren beweisen. Nach diesem existiert genau eine positive ganze Zahl r und bis auf Isomorphie genau eine Divisionsalgebra D sodass $A \cong M_r(D)$. Aus $4 = \dim_K A = r^2 \dim_K D$ folgt dann entweder $r = 2$ und $D = K$, also $A \cong M_2(K)$, oder $r = 1$ und $A \cong D$, also A eine Divisionsalgebra.

2. Der Satz von Skolem-Noether besagt, dass je zwei Algebrenhomomorphismen zentral einfacher Algebren durch ein Element aus A konjugiert sind. Man kann mithilfe des Wedderburnschen Satzes und dem Satz von Skolem-Noether zeigen, dass jede vierdimensionale zentrale einfache Algebra über K eine Quaternionenalgebra ist.

Proposition 1.1.6. Für alle $a, b, \lambda, \mu \in K^*$ gilt:

$$A(a, b|K) \cong A(b, a|K) \cong A(a, -ab|K) \cong A(a\lambda^2, b\mu^2|K)$$

Beweis. Wir zeigen, dass die letzten drei Quaternionenalgebren isomorph zur ersten sind, indem wir geeignete e_0, e_1, e_2, e_3 wie in 1.1.2 angeben. Es sei $\{1_1, i_1, j_1, k_1\}$ die Standardbasis von $A(b, a|K)$. Wir setzen $e_0 = 1$, $e_1 = j_1$, $e_2 = i_1$, $e_3 = -k_1$, womit sich die erste Behauptung ergibt. Weiters sei $\{1_2, i_2, j_2, k_2\}$ bzw. $\{1_3, i_3, j_3, k_3\}$ die Standardbasis von $A(a, -ab|K)$ bzw. $A(ax^2, by^2|K)$. Dann setzt man $e_0 = 1$, $e_1 = i_2$, $e_2 = a^{-1}k_2$, $e_3 = j_2$ bzw. $e_0 = 1$, $e_1 = \lambda^{-1}i_3$, $e_2 = \mu^{-1}j_3$, $e_3 = \lambda^{-1}\mu^{-1}k_3$, womit sich auch die zweite und die dritte Behauptung ergibt und die Proposition bewiesen ist. $\square$

Einem Quaternion $x = x_0 1 + x_1 i + x_2 j + x_3 k$ ordnet man sein konjugiertes Quaternion

$$\bar{x} := x_0 1 - x_1 i - x_2 j - x_3 k$$

zu. Für je zwei Elemente $x, y \in A(a, b|K)$ gilt dann

$$\overline{x + y} = \bar{x} + \bar{y} \quad \text{und} \quad \overline{xy} = \bar{y} \bar{x},$$

wobei die erste Identität offensichtlich ist. Die zweite Gleichheit prüft man zunächst auf den Basiselementen nach. Dann folgt die Identität für beliebige Elemente mit Hilfe der Distributiv- und Assoziativgesetze. Weiters kann man nachrechnen, dass

$$\bar{x}x = x\bar{x} = (x_0^2 - ax_1^2 - bx_2^2 + abx_3^2) \cdot 1$$

gilt, womit wir $\bar{x}x$ als Element von K auffassen können.

Definition 1.1.7. 1. Die Abbildung $n : A \longrightarrow K$, $x \longmapsto n(x) := \bar{x}x$ heißt (*reduzierte*) *Normabbildung* von A .

2. Die Abbildung $sp : A \longrightarrow K$, $x \longmapsto sp(x) := \bar{x} + x$ heißt (*reduzierte*) *Spurabbildung* von A .

Proposition 1.1.8. *Es gilt: $x \in A^* \iff n(x) \in K^*$.*

Beweis. Die Normabbildung ist multiplikativ:

$$n(xy) = xy\bar{xy} = xn(y)\bar{x} = n(y)x\bar{x} = n(x)n(y).$$

Ist $xy = 1$ dann folgt $n(x)n(y) = n(xy) = n(1) = 1$.

Sei umgekehrt $n(x) \in K^*$ dann ist $x^{-1} = \bar{x}n(x)^{-1}$. □

Beispiel 1.1.9. 1. Im Fall $K = \mathbb{R}$ und $a = b = -1$ nennen wir $\mathbb{H} := A(-1, -1|\mathbb{R})$ die Hamiltonschen Quaternionen. Da in diesem Fall die Normabbildung durch $n(x) = x_0^2 + x_1^2 + x_2^2 + x_3^2$ gegeben ist, sieht man aus obiger Proposition, dass $\mathbb{H}$ eine Divisionsalgebra ist. Wegen $i^2 = -1$ können wir $\mathbb{C}$ in $\mathbb{H}$ einbetten.

Es gilt zudem $\mathbb{H} \cong \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in M_2(\mathbb{C}) \mid a, b \in \mathbb{C} \right\}$. Da letztere Menge eine vierdimensionale $\mathbb{R}$ -Algebra ist, können wir 1.1.2 verwenden. Wir setzen

$$e_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad e_1 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad e_3 = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}.$$

Es gilt dann $e_1^2 = -e_0$, $e_2^2 = -e_0$, $e_3 = e_1e_2 = -e_2e_1$, womit die Isomorphie gezeigt ist.

2. Die Normabbildung der Quaternionenalgebra $A(1, b|K)$ hat die Form $n(x) = x_0^2 - x_1^2 - bx_2^2 + bx_3^2$. Es ist $n(1 + i + j + k) = 0$ und somit $A(a, b|K) \cong M_2(K)$ nach 1.1.8 und 1.1.4. Durch die folgende Zuordnung ist ein solcher Isomorphismus gegeben:

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad j \mapsto \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix}, \quad k \mapsto \begin{pmatrix} 0 & 1 \\ -b & 0 \end{pmatrix}.$$

3. Ist K ein endlicher Körper und A eine K -Quaternionenalgebra, so gilt $A \cong M_2(K)$.

Beweis: Die multiplikative Gruppe von K ist zyklisch, also ist $K^* = \{u, u^2, \dots, u^{p^f-1}, u^{p^f} = 1\}$, für ein $u \in K^*$, eine Primzahl p und eine positive natürliche Zahl f . Wir betrachten also $A = A(u^i, u^j|K)$ für $1 < i, j < p^f - 1$. Für i oder j gerade, ist nach 1.1.6 und Punkt (2) $A(u^i, u^j|K) \cong A(1, u^j|K) \cong M_2(K)$. Sind i und j ungerade so folgt $A(u^i, u^j|K) \cong A(u, u|K) \cong A(u, -u^2|K)$. Wenn -1 ein Quadrat ist, folgt wegen $A(u, -u^2|K) \cong A(u, 1|K) \cong M_2(K)$ die Behauptung. Wegen $\text{char} K = p \neq 2$ ist -1 immer ein Quadrat: Indirekt angenommen $-1 = u^{2k+1}$ dann folgt $1 = u^{4k+2}$. Weil $4k+2$ gerade ist, teilt p^f nicht $4k+2$, ein Widerspruch.

Bemerkung 1.1.10. Es sei $\alpha \in A$. Dann definiert $r_\alpha(x) := \alpha x$ eine K -lineare Abbildung auf A . Man definiert häufig $N_{A/K}(\alpha) := \det(r_\alpha) = \det(\alpha)$ und $Sp_{A/K}(\alpha) := Sp(r_\alpha) = sp(\alpha)$. Diese Definitionen stimmen aber nicht mit obiger Norm- und Spurabbildung überein. Es lässt sich zeigen, dass $2sp(\alpha) = Sp_{A/K}(\alpha)$ und $n(\alpha)^2 = N_{A/K}(\alpha)$ gilt. Wenn jedoch $A = K(\alpha)$ eine quadratische Körpererweiterung von K ist, gilt:

$$n|_{K(\alpha)} = N_{K(\alpha)/K}(\alpha).$$

Eine zentrale Frage in der Theorie der Quaternionenalgebren ist, ob für gegebene $a, b \in K^*$ die Algebra $A(a, b|K)$ eine Divisionsalgebra ist, oder $A \cong M_2(K)$ gilt. Diese Frage steht in direktem Zusammenhang mit der Lösbarkeit einer binären quadratischen Form. Deshalb definieren wir:

Definition 1.1.11. Es seien $a, b \in K$. Dann definieren wir das *Hilbert-Symbol* von a und b durch:

$$(a, b) := \begin{cases} 1 & ax^2 + by^2 - z^2 = 0 \text{ hat eine nichttriviale Lösung in } K, \\ -1 & ax^2 + by^2 - z^2 = 0 \text{ hat keine nichttriviale Lösung in } K. \end{cases}$$

Bevor wir den Hauptsatz dieses Abschnitts beweisen, erinnern wir an folgende Begriffe. Es sei V ein K -Vektorraum und $q : V \times V \rightarrow K$ eine symmetrische Bilinearform. Dann nennen wir (V, q) einen quadratischen Vektorraum. Ein Element $x \in V \setminus \{0\}$ heißt isotrop, falls $q(x) = 0$ gilt, und (V, q) heißt isotrop, falls V isotrope Elemente enthält.

Theorem 1.1.12. Sei $A(a, b|K)$ eine Quaternionenalgebra. Die folgenden Aussagen sind äquivalent:

1. Die Algebra $A(a, b|K)$ ist eine Matrizenalgebra, also $A(a, b|K) \cong M_2(K)$.
2. Es gibt ein $x \in A, x \neq 0$ mit $n(x) = 0$. (Der quadratische Vektorraum (A, n) ist isotrop).
3. Für $L = K(\sqrt{b})$, ist $a \in N_{L/K}(L)$.
4. Es ist $(a, b) = 1$.

Beweis. Die Äquivalenz $(1) \iff (2)$ folgt aus 1.1.8.

$(2) \Rightarrow (3)$: Es sei $x = x_0 + x_1i + x_2j + x_3k \in A \setminus \{0\}$ mit $n(x) = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2 = 0$. Wir setzen $v = x_0 + x_2\sqrt{b}$ und $w = x_1 + \sqrt{b}x_3$, wodurch wir folgende Identität erhalten:

$$N_{L/K}(v) = x_0^2 - bx_2^2 = a(x_1^2 - bx_3^2) = aN_{L/K}(w).$$

Aus $x \neq 0$ folgt $v \neq 0$ oder $w \neq 0$. Weil $w = 0$ nach obiger Identität auch $N_{L/K}(w) = 0$ und $N_{L/K}(v) = 0$ impliziert, folgt dann wegen $N_{L/K}(L^*) \subseteq K^*$ auch $v = 0$. Somit ist $w \neq 0$. Wir setzen $q := vw^{-1}$, sodass $a = N_{L/K}(q) \in N_{L/K}(L)$ gilt.

$(3) \Rightarrow (4)$: Sei $q = q_1 + q_2\sqrt{b} \in L = K(\sqrt{b})$ mit $N_{L/K}(q) = q_1^2 - bq_2^2 = a$, dann ist $(1, q_2, q_1)$ eine nichttriviale Lösung der Gleichung $ax^2 + by^2 - z^2 = 0$. Also ist $(a, b) = 1$.

$(4) \Rightarrow (1)$: Es sei $(x_0, y_0, z_0) \in K^3$ eine nichttriviale Lösung der Gleichung $ax^2 + by^2 - z^2 = 0$. Ist $x_0 = 0$ so gilt $by_0^2 = z_0^2$. Aus $(y_0, z_0) \neq (0, 0)$ folgt also $y_0 \neq 0$ und $z_0 \neq 0$, womit $b = (z_0/y_0)^2$ ein Quadrat in K ist. Nach 1.1.6 und 1.1.9 gilt dann $A(a, b|K) \cong A(a, 1|K) \cong A(1, a|K) \cong M_2(K)$.

Im Fall $y_0 = 0$ folgt, dass $a = (z_0/x_0)^2$ ein Quadrat in K ist, und $z_0 = 0$ impliziert, dass $-ab = (y_0b/x_0)^2$ ein Quadrat in K ist. Im letzteren Fall bedenkt man noch $A(a, b|K) \cong A(a, -ab|K)$, sonst argumentiert man analog.

Es bleibt der Fall, dass $x_0 \neq 0, y_0 \neq 0, z_0 \neq 0$. Es löst dann $x_1 := x_0/z_0 \neq 0$ und $y_1 := y_0/z_0 \neq 0$ die Gleichung $ax^2 + by^2 = 1$. Wir setzen nun $e_0 := 1, e_1 := x_1i + y_1j, e_2 := k$ und $e_3 := e_1e_2 = (x_1i + y_1j)k = ax_1j - by_1i$. Ist $a \neq -b$ so ist e_3 kein Vielfaches von e_1 und die Elemente e_0, e_1, e_2, e_3 bilden eine Basis von $A(a, b|K)$. Es gilt

$$e_1^2 = (x_1i + y_1j)^2 = ax_1^2 + by_1^2 = 1, \quad e_2^2 = k^2 = -ab, \quad e_3^2 = e_1e_2 = -e_2e_1.$$

Nun folgt aus 1.1.2 und 1.1.9 dass

$$A(a, b|K) \cong A(1, -ab|K) \cong M_2(K).$$

Im Fall $a = -b$ hat $ax^2 + by^2 - z^2 = 0$ die Lösung $(1, 1, 0)$, sodass wir wie weiter oben argumentieren können. $\square$

Beispiel 1.1.13. 1. Es ist $(1, 1, 0)$ eine Lösung von $ax^2 - ay^2 - z^2 = 0$, womit $A(a, -a|K) \cong M_2(K)$ gilt.

2. Es sei $a \neq 1$. Dann ist $(1, 1, 1)$ eine Lösung von $ax^2 + y^2 - ay^2 - z^2 = 0$, womit $A(a, 1-a|K) \cong M_2(K)$ gilt.

3. Für $p \equiv 1 \pmod{4}$ gilt $A(-1, p|K) \cong M_2(K)$, für $p \equiv 3 \pmod{4}$ hingegen ist $A(-1, p|K)$ eine Divisionsalgebra:

Wir wissen aus der elementaren Zahlentheorie, dass die Pell'sche Gleichung $x^2 - py^2 = -1$ für $p \equiv 1 \pmod{4}$ eine Lösung besitzt, womit $-x^2 + py^2 - z^2 = 0$ ebenso lösbar ist. Es folgt die erste Behauptung. Da sich Primzahlen $p \equiv 3 \pmod{4}$ nicht als Summe zweier Quadrate darstellen lassen, besitzt die Gleichung $-x^2 + py^2 \equiv z^2 \pmod{4}$ keine Lösung. Somit ist auch $-x^2 + py^2 - z^2 = 0$ unlösbar und die zweite Behauptung folgt.

1.2 Das Verzweigungsverhalten von Quaternionenalgebren

Es sei in diesem Abschnitt K ein algebraischer Zahlkörper mit $[K : \mathbb{Q}] = n$. Wir notieren die n Einbettungen von K mit $\sigma_1, \dots, \sigma_r, \sigma_{r+1}, \dots, \sigma_{r+s}, \sigma_{r+s+1} = \overline{\sigma_{r+1}}, \dots, \sigma_{r+2s} = \overline{\sigma_{r+s}}$, wobei die ersten r Einbettungen reell sind und die σ_i mit $r < i \leq s$ komplex und paarweise nicht konjugiert sind. Es bezeichne $R = \mathcal{O}_K$ den Ring der ganzen Zahlen in K .

Aus der Algebra wissen wir, dass die Menge der nichtäquivalenten archimedischen Absolutbeträge auf K durch $|\sigma_1|, \dots, |\sigma_r|, |\sigma_{r+1}|^2, \dots, |\sigma_{r+s}|^2$ repräsentiert wird. Die nichtarchimedischen Absolutbeträge auf K sind durch die Menge der Primideale in $\mathcal{O}_K$ gegeben. Wir bezeichnen ab nun die Menge aller nichtäquivalenten Bewertungen auf K mit $\Omega(K)$ und nennen die Elemente von $\Omega(K)$ auch die Stellen von K . Die Menge der archimedischen Stellen nennen wir die unendlichen Stellen und notieren sie mit $\Omega_\infty \subseteq \Omega(K)$. Eine unendliche Stelle, deren Absolutbetrag durch eine reelle (bzw. komplexe) Einbettung repräsentiert wird, heißt auch reelle (bzw. komplexe) Stelle. Die Menge der nichtarchimedischen Stellen nennen wir auch die endlichen Stellen. Wir verwenden die Konvention, dass $v \in \Omega(K)$ bzw. $v_\infty \in \Omega_\infty(K)$ bzw. $v_f \in \Omega_f(K)$ eine beliebige

Stelle bzw. eine unendliche Stelle bzw. eine endliche Stelle bezeichnet. Für $v \in \Omega(K)$ bezeichne K_v die Vervollständigung von K bezüglich einem zur Stelle v gehörigen Absolutbetrages. Ist v_∞ eine reelle (bzw. komplexe) Stelle so gilt $K_{v_\infty} \cong \mathbb{R}$ (bzw. $K_{v_\infty} \cong \mathbb{C}$). Für $v \in \Omega_f(K)$ notieren wir den Bewertungsring von K_v mit R_v . Dieser ist die Vervollständigung von R bezüglich einem zur Stelle v gehörigen Absolutbetrages.

Die Eigenschaften des Körpers K hängen eng mit den Eigenschaften der Körper K_v für $v \in \Omega(K)$ zusammen. Diesen Zusammenhang nennt man das algebraische lokal-global Prinzip.

Proposition 1.2.1. 1. Für $a, b \in \mathbb{C}^*$ gilt: $A(a, b|\mathbb{C}) \cong M_2(\mathbb{C})$.

2. Für $a, b \in \mathbb{R}^*$ gilt: $a < 0$ und $b < 0 \iff A(a, b|\mathbb{R}) \cong \mathbb{H}$.

Beweis. 1. Da $\mathbb{C}$ algebraisch abgeschlossen ist, lassen sich a und b als Quadrat darstellen. Somit folgt aus 1.1.6 und 1.1.9: $A(a, b|\mathbb{C}) \cong A(1, 1|\mathbb{C}) \cong M_2(\mathbb{C})$.

2. Nach 1.1.6 ist jede Quaternionenalgebra entweder zu $A(1, 1|\mathbb{R})$ oder zu $A(-1, -1|\mathbb{R})$ oder zu $A(1, -1|\mathbb{R})$ isomorph. Aus 1.1.9 oder 1.1.12(4) erhalten wir $A(1, 1|\mathbb{R}) \cong M_2(\mathbb{R})$, $A(-1, -1|\mathbb{R}) \cong \mathbb{H}$ und $A(1, -1|\mathbb{R}) \cong M_2(\mathbb{R})$. $\square$

Definition 1.2.2. Es sei A eine Quaternionenalgebra über K . Für $v \in \Omega(K)$ setzen wir $A_v := A \otimes_K K_v$ und nennen A_v die Lokalisierung von A an der Stelle v .

Die Lokalisierung A_v ist in kanonischer Weise eine K_v -Algebra. Mithilfe der universellen Abbildungseigenschaft des Tensorproduktes von Algebren zeigt man leicht

$$A(a, b|K) \otimes_K K_v \cong A(a, b|K_v).$$

Ist allgemeiner $\sigma : K \rightarrow K_v$ eine Körpereinbettung, dann ist $\sigma(K)$ ein Teilkörper von K_v , und wir können K mit $\sigma(K)$ identifizieren. Somit macht folgende Notation Sinn:

$$A(a, b|K)_\sigma := A(\sigma(a), \sigma(b)|K) \otimes_{\sigma(K)} K_v \cong A(\sigma(a), \sigma(b)|K_v).$$

Sei $\sigma : K \rightarrow \mathbb{C}$ eine komplexe Einbettung. Dann ist $K_v \cong \mathbb{C}$ und es gilt:

$$A(a, b|K)_\sigma = A(\sigma(a), \sigma(b)|\mathbb{C}) \cong M_2(\mathbb{C}).$$

Für $\sigma : K \rightarrow \mathbb{R}$ ist $K_v \cong \mathbb{R}$ und

$$A(a, b|K)_\sigma = A(\sigma(a), \sigma(b)|\mathbb{R}) \cong \mathbb{H} \text{ oder } M_2(\mathbb{R}).$$

Definition 1.2.3. Sei $v \in \Omega(K)$ eine Stelle von K und A eine Quaternionenalgebra über K . Wir sagen, A verzweigt an der Stelle v , wenn A_v eine Divisionsalgebra über K_v ist. Andernfalls sagen wir, dass A an der Stelle v spaltet. Die Menge der Stellen, an denen A verzweigt, bezeichnen wir mit $\text{Ram}(A) \subseteq \Omega(K)$.

Bemerkung 1.2.4. Es sei $v \in \text{Ram}(A)$ eine reelle Stelle. Dann ist A eine Divisionsalgebra.

Beweis. Wegen $v \in \text{Ram}(A)$ ist A_v eine Divisionsalgebra. Weil $M_2(K)$ nichttriviale Nullteiler besitzt und $A \subseteq A_v$ ist, folgt aus 1.1.4, dass auch A eine Divisionsalgebra ist. $\square$

Man kann zeigen, dass es über K_v bis auf Isomorphie höchstens eine Divisionsalgebra gibt. Im archimedischen Fall wissen wir das aus 1.2.1.

Aus 1.2.1 und 1.1.12 ergibt sich nun:

Korollar 1.2.5. *Es sei $A(a, b|K)$ eine Quaternionenalgebra und σ eine reelle Einbettung mit dazugehöriger reeller Stelle v . Dann sind die folgenden Aussagen äquivalent:*

1. *Die Quaternionenalgebra $A(a, b|K)$ verzweigt an der Stelle v .*
2. *Für die reellen Einbettung σ gilt $\sigma(a) < 0$ und $\sigma(b) < 0$.*
3. *Das Hilbert-Symbol von $\sigma(a)$ und $\sigma(b)$ ist negativ, also $(\sigma(a), \sigma(b)) = -1$.*

Beispiel 1.2.6. Es sei $a = \sqrt{2 - \sqrt{5}}$ und $K = \mathbb{Q}(a)$. Wir behaupten $f(X) = X^4 - 4X^2 - 1 = (X - a)(X - \bar{a})(X - \sqrt{2 + \sqrt{5}})(X + \sqrt{2 + \sqrt{5}})$ ist das Minimalpolynom von a über $\mathbb{Q}$. Da $f(a) = 0$ und f normiert ist, genügt es zu zeigen, dass f irreduzibel über $\mathbb{Q}$ ist: Das sieht man dadurch, dass das Produkt von je zwei Linearfaktoren von $f(X)$ nicht in $\mathbb{Q}[X]$ liegt.

Somit hat K eine komplexe Stelle und zwei reelle Stellen, deren Einbettungen durch $\sigma(a) = \pm\sqrt{2 + \sqrt{5}}$ gegeben sind.

Sei $x \in \mathbb{Q}$ mit $x < -\sqrt{2 + \sqrt{5}}$. Dann verzweigt $A(-1, x + a|K) = A(-1, x + \sqrt{2 - \sqrt{5}}|K)$ an beiden reellen Stellen nach 1.2.5(3). Nach 1.2.1 spaltet $A(-1, x + a|K)$ (wie jede Quaternionenalgebra) an ihrer komplexen Stelle.

Die nächsten beiden Beispiele befassen sich mit Quaternionenalgebren, die an allen archimedischen Stellen verzweigen. Diese spezielle Klasse von Algebren werden wir im dritten Kapitel genauer betrachten.

Beispiel 1.2.7. Sei d eine positive, natürliche, quadratfreie Zahl und $K = \mathbb{Q}(\sqrt{d})$. Es ist $[K : \mathbb{Q}] = 2$ und $G(K/\mathbb{Q}) = \{id, \tau\}$, wobei τ durch $\sqrt{d} \mapsto -\sqrt{d}$ gegeben ist. Es seien $a := x + y\sqrt{d}$ und $b := u + v\sqrt{d}$ mit $x, y, u, v \in \mathbb{Q}$. Wir betrachten $A(a, b|K)$. Dann ist

$$A(a, b|K)_{id} = A(a, b|\mathbb{R}), \quad \text{und}$$

$$A(a, b|K)_{\tau} = A(\tau(a), \tau(b)|\mathbb{R}) = A(x - y\sqrt{d}, u - v\sqrt{d}|\mathbb{R}).$$

Also gilt $A(a, b|K)_{id} \cong A(a, b|K)_{\tau} \cong \mathbb{H}$ genau dann wenn

$$x + y\sqrt{d} < 0, \quad x - y\sqrt{d} < 0, \quad u + v\sqrt{d} < 0, \quad u - v\sqrt{d} < 0.$$

Insbesondere verzweigt $A(-1, -1|K)$ an den beiden reellen Stellen von K . Wir werden dieses Beispiel in 3.3.6 wieder aufgreifen.

Beispiel 1.2.8. Um ein interessanteres Beispiel zu konstruieren, betrachten wir den maximal reellen Teilkörper eines Kreisteilungskörpers:

Es sei $n \in \mathbb{N}$, $\zeta := e^{2\pi i/n}$ und $L := \mathbb{Q}(\zeta)$ der n -te Kreisteilungskörper. Dann ist $L/\mathbb{Q}$ galoissch, und es gibt genau einen Gruppenisomorphismus

$$f: G(L/\mathbb{Q}) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$$

mit folgender Eigenschaft: Ist $1 \leq k \leq n$ mit $\text{ggT}(k, n) = 1$ und $\tau_k: L \rightarrow L$ mit $\tau_k(\zeta) = \zeta^k$, so ist $f(\tau_k) = k + n\mathbb{Z}$. Insbesondere ist dann $G(L/\mathbb{Q}) = \{\tau_k \mid 1 \leq k \leq n, \text{ggT}(k, n) = 1\}$.

Nun setzen wir $\theta := \zeta + \zeta^{-1} = 2\text{Re}\zeta$, und $K := \mathbb{Q}(\theta)$. Dann ist $K \subseteq \mathbb{Q}(\zeta) \cap \mathbb{R} \subsetneq \mathbb{Q}(\zeta)$. Weil ζ dem Polynom $X^2 - \theta X + 1 \in K[X]$ genügt, ist $[L : K] = 2$, $G(L/K) = \{id_L, \tau_{n-1}\}$ (es ist τ_{n-1} die Komplexkonjugation) und K ist der maximal reelle Teilkörper von L .

Wir können aus $G(L/\mathbb{Q})$ und $G(L/K)$ die Galoisgruppe $G(K/\mathbb{Q})$ berechnen. Die Abbildung

$$\phi: G(L/\mathbb{Q})/G(L/K) \rightarrow G(K/\mathbb{Q}), \quad \tau_i G(L/K) \mapsto \tau_i|_K$$

ist ein Gruppenisomorphismus. Der Körper K hat also $\varphi(n)/2$ reelle Körpereinbettungen, welche als die auf K eingeschränkten Automorphismen von $G(L/K)$ gegeben sind. Dabei gilt für $\tau_i, \tau_j \in G(L/\mathbb{Q})$ mit $\tau_i \neq \tau_j$:

$$\tau_i|_K = \tau_j|_K \iff \tau_i - \tau_j \in G(L/K) \iff \tau_i = \overline{\tau_j}.$$

Wir konstruieren nun Quaternionenalgebren über $K = \mathbb{Q}(\theta)$, die an alle reellen Stellen verzweigen. Da die Eulersche φ -Funktion nur gerade Werte annimmt, und wir den Fall des quadratischen reellen Zahlkörpers schon behandelt haben, setzen wir $\varphi(n) \geq 6$ voraus.

Es gilt $n = 7$, $\varphi(7) = 6$ und $G(L : \mathbb{Q}) = \{\tau_1 = id, \tau_2, \tau_3, \tau_4, \tau_5, \tau_6\}$. Es ist $\tau_1 = \overline{\tau_6}$, $\tau_2 = \overline{\tau_5}$, $\tau_3 = \overline{\tau_4}$ und somit $G(K : \mathbb{Q}) = \{\tau_1|_K = id|_K, \tau_2|_K, \tau_3|_K\}$. Die Körpererweiterung $K/\mathbb{Q}$ hat die Basis $\{1, \theta = 2\cos(2\pi/7), \theta^2 = 4\cos(2\pi/7)^2\}$, sodass für $a, b \in K^*$ und rationale Zahlen $x, y, z, u, v, w \in \mathbb{Q}$ existieren mit $a = x + y\theta + z\theta^2$ und $b = u + v\theta + w\theta^2$. Wir betrachten $A(a, b|K)$ und erhalten

$$\begin{aligned} A(a, b|K)_{\tau_1} &= A(a, b|\mathbb{R}) \\ A(a, b|K)_{\tau_2} &= A(x + y\tau_2(\theta) + z\tau_2(\theta^2), u + v\tau_2(\theta) + w\tau_2(\theta^2)|\mathbb{R}) \\ A(a, b|K)_{\tau_3} &= A(x + y\tau_3(\theta) + z\tau_3(\theta^2), u + v\tau_3(\theta) + w\tau_3(\theta^2)|\mathbb{R}) \end{aligned}$$

mit

$$\begin{aligned} \tau_2(\theta) &= \tau_2(\zeta + \zeta^{-1}) = \zeta^2 + \zeta^{-2} = 2\text{Re}(\zeta^2) = 2\cos(4\pi/7), \\ \tau_2(\theta^2) &= \tau_2(\zeta^2 + \zeta^{-2} + 2) = \zeta^4 + \zeta^{-4} + 2 = 2\text{Re}(\zeta^4) + 2 = 2\cos(8\pi/7) + 2, \\ \tau_3(\theta) &= \tau_3(\zeta + \zeta^{-1}) = \zeta^3 + \zeta^{-3} = 2\text{Re}(\zeta^3) = 2\cos(6\pi/7) \text{ und} \\ \tau_3(\theta^2) &= \tau_3(\zeta^2 + \zeta^{-2} + 2) = \zeta^6 + \zeta^{-6} + 2 = 2\text{Re}(\zeta^6) + 2 = 2\cos(12\pi/7) + 2. \end{aligned}$$

Offenbar gibt es unendlich viele Möglichkeiten für $x, y, z, u, v, w \in \mathbb{Q}$, sodass $A(a, b|K)_{\tau_1} \cong A(a, b|K)_{\tau_2} \cong A(a, b|K)_{\tau_3} \cong \mathbb{H}$ gilt und $A(a, b|K)$ an allen reellen Stellen verzweigt.

1.3 Ordnungen in Quaternionenalgebren

Es sei in diesem Abschnitt K ein algebraischer Zahlkörper mit $[K : \mathbb{Q}] = n$ und $R = \mathcal{O}_K$ sein Ganzheitsring. Für eine Stelle $v \in \Omega(K)$ bezeichne K_v die Vervollständigung von K bezüglich einem zu v gehörigen Absolutbetrages. Für eine endliche Stelle $v \in \Omega_f(K)$ bezeichnen wir den zu K_v gehörigen Bewertungsring mit R_v .

Es sei T ein nicht notwendig kommutativer Ring und S ein kommutativer Teilring. Ein Element $x \in T$ heißt ganz über S , wenn x einem normierten Polynom über S genügt oder äquivalent der Modul $S[x]$ in T endlich erzeugt ist.

Wir wollen in A Idealtheorie betreiben. Es liegen folgende zueinander analoge Situationen vor:



Es stellt sich die Frage, welches Objekt die Rolle von $\mathcal{O}_K$ in A einnimmt.

Die naheliegenste Idee, den ganzen Abschluss von R in A zu betrachten, führt nicht zum Ziel, da dieser, wegen der Nichtkommutativität von A im allgemeinen kein Ring ist:

Proposition 1.3.1. *Die folgenden Aussagen sind äquivalent:*

1. Ein Element $\alpha \in A$ ist ganz über R .
2. Die Norm $n(\alpha)$ und die Spur $sp(\alpha)$ von α liegen in R .

Beweis. (2) $\Rightarrow$ (1) Da jedes $\alpha \in A$ dem normierten Polynom $X^2 - sp(\alpha)X + n(\alpha) \in R[X]$ genügt, ist α ganz über R .

(1) $\Rightarrow$ (2) Nun sei α ganz über R und $\alpha \in K$. Da R ganz abgeschlossen ist, liegt α in R und die Behauptung folgt.

Sei also $\alpha \in A \setminus K$. Wir bezeichnen mit $K(\alpha)$ die kleinste kommutative K -Algebra die K und α enthält. Nun unterscheiden wir zwei Fälle:

Fall 1: Es sei A eine Divisionsalgebra. Dann ist $K(\alpha)/K$ eine quadratische Körpererweiterung, weil α algebraisch über K ist. Das konjugierte Element von α in der Körpererweiterung ist $\bar{\alpha}$ welches ebenfalls ganz über R ist. Wenn nun $\mathcal{O}_{K(\alpha)}$ den Ganzheitsring von $K(\alpha)$ bezeichnet, dann gilt $\alpha, \bar{\alpha} \in \mathcal{O}_{K(\alpha)}$. Es folgt dann $n(\alpha), sp(\alpha) \in \mathcal{O}_{K(\alpha)} \cap K = R$.

Fall 2: Es sei $A \cong M_2(K)$. Dann ist α konjugiert zu einem Element der Form $\begin{pmatrix} u & v \\ 0 & w \end{pmatrix}$, $u, v, w \in K$. Es sei $p \in R[X]$ mit $p(\alpha) = 0$. Dann ist wegen $p[\begin{pmatrix} u & v \\ 0 & w \end{pmatrix}] = g^{-1}p[\alpha]g = 0$, für alle $g \in M_2(K)$ auch $\begin{pmatrix} u & v \\ 0 & w \end{pmatrix}$ ganz. Wegen $\begin{pmatrix} u & v \\ 0 & w \end{pmatrix}^n = \begin{pmatrix} u^n & * \\ 0 & w^n \end{pmatrix}$ genügen auch u und w dem Polynom p . Da R ganz abgeschlossen ist, liegen u und w in R . Also ist nach 1.1.10 $n(\alpha), sp(\alpha) \in R$. $\square$

Beispiel 1.3.2. Wir betrachten $A(-1, 3|\mathbb{Q})$, mit der Standardbasis $\{1, i, j, k\}$. Mithilfe obiger Proposition können wir zeigen, dass $\alpha = j$ und $\beta = (3j + 4ij)/5$, aber nicht $\alpha + \beta$ und $\alpha\beta$ ganz über $R = \mathbb{Z}$ sind. Es ist

$$N(\alpha) = 3 \in \mathbb{Z}, \quad Sp(\alpha) = 0 \in \mathbb{Z},$$

$$N(\beta) = (3j + 4ij)(-3j - 4ij)/25 = 3 \in \mathbb{Z}, \quad Sp(\beta) = 0 \in \mathbb{Z}, \quad \text{aber}$$

$$Sp(\alpha\beta) = (9 + 4jij)/5 = 18/5 \notin \mathbb{Z} \quad \text{und} \quad N(\alpha + \beta) = (8j + 4ij)(-8j - 4ij)/25 = 144/25 \notin \mathbb{Z}.$$

Wir müssen andere Objekte suchen, die $\mathcal{O}_K$ ersetzen können. Wir werden sehen, dass es solche Objekte gibt und werden ihnen den Namen Ordnung geben. Zur Einstimmung betrachten wir zunächst Ordnungen in K :

Definition 1.3.3. Eine *Ordnung* $\mathfrak{o}$ von K ist ein freier $\mathbb{Z}$ -Modul, welcher Teilring von $\mathcal{O}_K$ ist, und eine $\mathbb{Z}$ -Basis der Länge n besitzt. Den Ring $\mathcal{O}_K$ nennen wir die maximale Ordnung von K .

Proposition 1.3.4. Es seien $a_1, \dots, a_n \in \mathcal{O}_K$ und $K = \mathbb{Q}(a_1, \dots, a_n)$. Dann ist $\mathfrak{o} = \mathbb{Z}[a_1, \dots, a_n]$ eine Ordnung von K . Umgekehrt haben alle Ordnungen diese Form.

Beweis. Als Untermodul des freien $\mathbb{Z}$ -Moduls $\mathcal{O}_K$ besitzt $\mathfrak{o}$ eine $\mathbb{Z}$ -Basis, die wegen $\mathbb{Q} \cdot \mathfrak{o} := \{\sum_{i=1}^n q_i o_i \mid q_i \in \mathbb{Q}, o_i \in \mathfrak{o}, n \geq 0\} = K$ gleichzeitig eine Basis von K über $\mathbb{Q}$ sein muss, also Länge n hat.

Es sei umgekehrt $\mathfrak{o} \subseteq \mathcal{O}_K$ eine Ordnung in K und $b_1, \dots, b_n \in \mathcal{O}_K$ eine $\mathbb{Z}$ -Basis. Weil $b_1, \dots, b_n$ linear unabhängig über $\mathbb{Z}$ sind, sind sie es auch über $\mathbb{Q}$ und es gilt $K = \mathbb{Q}(b_1, \dots, b_n)$. $\square$

Proposition 1.3.5. Eine Ordnung $\mathfrak{o}$ von K ist ein noetherscher Integritätsbereich in welchem jedes von (0) verschiedene Primideal ein maximales Ideal ist. Ordnungen sind im allgemeinen nicht ganz abgeschlossen.

Beweis. [9] Kap.1 §12. $\square$

Da die Eigenschaft dedekindsch zu sein, äquivalent mit der eindeutigen Primidealzerlegung ist, gilt diese in Ordnungen (im allgemeinen) nicht mehr. Die einzige Ordnung mit dieser gewünschten Eigenschaft ist die maximale Ordnung, der Ring $\mathcal{O}_K$.

Mit diesem Wissen im Hintergrund verallgemeinern wir nun den Begriff der Ordnung auf Quaternionenalgebren.

Definition 1.3.6. Es sei V ein Vektorraum über K . Ein endlich erzeugter R -Modul L in V heißt *R-Gitter*. Weiters heißt L ein *vollständiges R-Gitter*, falls $K \otimes_R L \cong V$.

Bemerkung 1.3.7. Die Abbildung, die durch

$$K \otimes_R L \xrightarrow{\sim} K \cdot L, \quad k \otimes_R l \mapsto k \cdot l,$$

gegeben ist, und linear fortgesetzt werden kann, ist ein K -Vektorraumisomorphismus. Also ist ein R -Gitter L genau dann vollständig wenn $K \cdot L \cong V$ gilt.

Definition 1.3.8. 1. Ein *Ideal* I in A ist ein vollständiges R -Gitter.

2. Eine *Ordnung* $\mathcal{O}$ in A ist ein Ideal, welches auch ein Teilring von A mit Eins ist.

3. Eine Ordnung $\mathcal{O}$ ist *maximal*, falls sie maximal bezüglich $\subseteq$ ist.

Bemerkung 1.3.9. Falls R ein Hauptidealring ist (das ist genau dann der Fall, wenn R faktoriell ist), sind R -Ordnungen frei: Nach [4, Kapitel VII. Satz 8.6 (b)] ist jeder torsionsfreie endlich erzeugte R -Modul frei. Also genügt es zu zeigen, dass $\mathcal{O}$ torsionsfrei ist. Sei also $a \in R \setminus \{0\}$, $x \in \mathcal{O}$ und $ax = 0$. Für $q \in K$ ist dann $qax = 0$ und mit $q := a^{-1}$ erhalten wir $1x = x = 0$, womit die Behauptung folgt. Analog zeigt man, dass R -Gitter frei sind. Also gilt für jede Ordnung $\mathcal{O}$ und jedes R -Gitter I : $\dim_R \mathcal{O} = \dim_R I = \dim_K A$. (Weil R_v ein Hauptidealring ist, überlegt man sich analog, dass R_v -Ordnungen frei sind.)

Bevor wir zeigen, dass wir mit obiger Definition wirklich Ordnungen in K verallgemeinert haben, brauchen wir ein Lemma.

Lemma 1.3.10. *Es sei L ein vollständiges R -Gitter in V und M ein R -Untermodul von V . Dann ist M ein vollständiges R -Gitter genau dann, wenn ein $d \in R \setminus \{0\}$ existiert mit $dL \subseteq M \subseteq d^{-1}L$.*

Beweis. Angenommen, es gibt ein $d \in R \setminus \{0\}$ mit obiger Eigenschaft. Dann ist $V = K \cdot L = \frac{K}{d} \cdot dL \subseteq K \cdot M$, und es folgt $V = K \cdot M$. Somit ist M vollständig. Als endlich erzeugter R -Modul über einem noetherschen Ring ist $d^{-1}L$ noethersch, sodass wegen $M \subseteq d^{-1}L$ auch M endlich erzeugt ist.

Es sei $n := \dim_K V$ und $\langle m_1, \dots, m_r \rangle_R = M$ und $\langle l_1, \dots, l_s \rangle_R = L$. Es ist $r = s = n$ da sonst $K \cdot M = V$ bzw. $K \cdot L = V$ verletzt wäre. Da K der Quotientenkörper von R ist, existieren a_i, b_i, c_i, d_i mit $m_i = \frac{a_i}{b_i}$ und $l_i = \frac{c_i}{d_i}$ für $1 \leq i \leq n$. Für $d := \prod_{1 \leq i \leq n} b_i d_i$ gilt $dL \subseteq M \subseteq d^{-1}L$. $\square$

Proposition 1.3.11. *Ein Teilring $\mathcal{O} \subseteq A$ ist eine Ordnung genau dann, wenn $R \subseteq \mathcal{O}$ gilt, alle Elemente aus $\mathcal{O}$ ganz über R sind und $K \cdot \mathcal{O} = A$ ist.*

Beweis. Es sei $\mathcal{O}$ Ordnung. Wenn wir R mit $R1$ identifizieren, folgt $R \subseteq \mathcal{O}$. Es sei $\alpha \in \mathcal{O}$. Dann ist $R[\alpha]$ als R -Untermodul von $\mathcal{O}$ endlich erzeugt und somit α ganz über R . Und die letzte Behauptung ist gerade 1.3.7.

Es sei umgekehrt $\mathcal{O} \subseteq A$ ein Teilring, der die drei obigen Eigenschaften erfüllt. Es genügt die Bedingung in 1.3.10 nachzuweisen. Es sei $\{x_1, x_2, x_3, x_4\}$ eine Basis von A mit $x_i \in \mathcal{O}$ und $(1, i, j, k) = (y_1, y_2, y_3, y_4)$ die Standardbasis. Sei weiters $A := (Sp(x_i x_j))_{1 \leq i, j \leq 4}$ und $B := Sp((y_i y_j))_{1 \leq i, j \leq 4} = \Delta(2, 2a, 2b, -2ab)$. Es gibt eine invertierbare Matrix $M \in GL_2(K)$ mit $M \cdot \{x_1, x_2, x_3, x_4\}^t = \{y_1, y_2, y_3, y_4\}$. Dann ist $MBM^t = A$. Nach 1.3.1 ist $A \in M_2(R)$ und somit $d := \det A = \underbrace{\det M}_{\neq 0} \cdot \underbrace{\det B}_{\neq 0} \cdot \underbrace{\det M}_{\neq 0} \in R \setminus \{0\}$. Wir setzen $L := \{\sum_{i=1}^4 a_i x_i \mid a_i \in R\}$. Dann gilt

$dL \subseteq L \subseteq \mathcal{O}$. Nun sei $\alpha \in \mathcal{O}$, $\alpha = \sum_{i=1}^4 b_i x_i$ mit $b_i \in K$. Für jedes j ist $\alpha x_j \in \mathcal{O}$, sodass nach 1.3.1 $Sp(\alpha x_j) = \sum_{i=1}^4 b_i Sp(x_i x_j) \in R$ ist. Also ist jede Komponente von $A \cdot \{b_1, b_2, b_3, b_4\}^t \in R$. Es bezeichne A^* die Adjungierte von A . Nach dem Satz von Lagrange gilt $AA^* = A^*A = \det A \cdot I_n$. Somit folgt $b_i \in (1/d)R$ und $\mathcal{O} \subseteq (1/d)L$. $\square$

Proposition 1.3.12. *Jede Ordnung ist in einer maximalen Ordnung enthalten.*

Beweis. Wir betrachten die Menge $\mathbf{O} := \{\mathcal{O} \subseteq A \mid \mathcal{O} \text{ ist Ordnung in } A\}$ und zeigen, dass jede totalgeordnete Teilmenge eine obere Schranke hat. Sei $\{\mathcal{O}_i\}_{i \in I}$ eine totalgeordnete Teilmenge von $\mathbf{O}$. Dann ist $\bigcup_{i \in I} \mathcal{O}_i$ wegen 1.3.11 eine Ordnung und somit eine obere Schranke von $\{\mathcal{O}_i\}_{i \in I}$. Aus dem Zornschen Lemma folgt, dass es in $\mathbf{O}$ ein maximales Element gibt. $\square$

- Beispiel 1.3.13.** 1. Sei $\{x_1, x_2, x_3, x_4\}$ eine K -Basis von A . Dann ist der freie R -Modul $R[x_1, x_2, x_3, x_4]$ ein Ideal in A .
2. Wenn wir $A(a, b|K)$ betrachten können wir nach 1.1.6 annehmen, dass $a, b \in R$ gilt. Es ist dann $R[1, i, j, k]$ eine Ordnung in A .
3. Der Modul $M_2(R)$ ist eine maximale Ordnung in $M_2(K)$:
Indirekt angenommen $\mathcal{O}$ ist eine Ordnung, mit $M_2(R) \subsetneq \mathcal{O}$. Dann enthält $\mathcal{O}$ ein Element der Form $\begin{pmatrix} x & y \\ z & w \end{pmatrix}$ mit mindestens einem Eintrag nicht in R . Durch geeignete Addition und Multiplikation mit Elementen aus $M_2(R)$ können wir annehmen, dass $\mathcal{O}$ ein Element der Form $\alpha := \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ enthält, mit $a \notin R$. Da R ganz abgeschlossen ist, ist $R[a]$ und dann auch $R[\alpha]$ kein endlich erzeugter R -Modul. Da $\mathcal{O}$ als endlich erzeugter R -Modul über einem noetherschen Ring noethersch ist, erhalten wir einen Widerspruch.
4. Wir betrachten $A(-1, -1|\mathbb{Q})$, die Hamilton'schen Quaternionen über $\mathbb{Q}$. Die Ordnung $\mathbb{Z}[1, i, j, k]$ ist nicht maximal. Sie ist echt in der Ordnung $\mathbb{Z}[1, i, j, (1+i+j+k)/2]$ enthalten. Man kann zeigen, dass $\mathbb{Z}[1, i, j, (1+i+j+k)/2]$ eine maximale Ordnung ist.
5. Es sei I ein Ideal in A . Dann sind die Ordnungen zur Linken und zur Rechten von I definiert durch:

$$\mathcal{O}_l(I) := \{\alpha \in A \mid \alpha I \subseteq I\}, \quad \mathcal{O}_r(I) := \{\alpha \in A \mid I\alpha \subseteq I\}.$$

Wir zeigen, dass $\mathcal{O}_l(I)$ und $\mathcal{O}_r(I)$ wirklich Ordnungen sind:

Offensichtlich ist $\mathcal{O}_l(I)$ ein Teilring und ein R -Untermodul von A . Für $y \in A$ ist yI ein vollständiges R -Gitter in A , sodass nach 1.3.10 ein $d \in R \setminus \{0\}$ existiert mit $dyI \subseteq I$. Es ist dann $dy \in \mathcal{O}_l(I)$ und wir erhalten $K \cdot \mathcal{O}_l(I) = A$. Wir zeigen nun, dass $\mathcal{O}_l(I)$ endlich erzeugt ist: Da I ein vollständiges R -Gitter ist, gibt es ein $k \in K$ mit $k1_K \in I$ und dann auch ein $s \in R$ mit $s1_R \in I$. Daraus folgt $\mathcal{O}_l(I)(s1_R) \subseteq I$ und somit $\mathcal{O}_l(I) \subseteq s^{-1}I$. Da $s^{-1}I$ ein Gitter ist und R noethersch ist, folgt dass $\mathcal{O}_l(I)$ ebenfalls ein Gitter ist.

Analog zeigt man, dass $\mathcal{O}_r(I)$ eine Ordnung ist.

Lemma 1.3.14. *Es sei V ein endlichdimensionaler Vektorraum über K und L ein R -Gitter in V . Dann gilt*

$$L = \bigcap_{v \in \Omega_f} R_v L.$$

Beweis. Offensichtlich ist die linke Seite in der Rechten enthalten. Es sei $x_1, \dots, x_r$ ein Erzeugendensystem von L über R , und dann auch eines von $R_v L$ über R für $v \in \Omega_f$.

Es sei nun $x \in \bigcap_{v \in \Omega_f} R_v L$. Wir betrachten das Ideal

$$J := \{y \in R \mid yx \in L\}.$$

Es sei $v \in \Omega_f$ und es bezeichne $\mathfrak{p}$ das zu v gehörige Primideal. Nun ist $x = \sum_{k=1}^r a_k x_k$ mit $a_k = b_k/c_k$, wobei $b_k, c_k \in R$ und $c_k \notin \mathfrak{p}$. Es ist dann auch $c := c_1 c_2 \dots c_r \notin \mathfrak{p}$, aber $c \in J$. Somit liegt J in keinem Primideal, weshalb schon $J = R$ gilt. Also ist $1 \in J$ und $x \in L$. $\square$

Definition 1.3.15. Es sei $\mathcal{O}$ eine R -Ordnung in A . Für $v \in \Omega_f$ setzen wir $\mathcal{O}_v := \mathcal{O} \otimes_R R_v$ und nennen $\mathcal{O}_v$ die Lokalisierung von $\mathcal{O}$ an der Stelle v .

Es ist $\mathcal{O}_v$ in kanonischer Weise eine R_v -Ordnung. Aus obigem Lemma und aus 1.3.7 folgt:

Korollar 1.3.16. *Es gilt:*

$$R = \bigcap_{v \in \Omega_f} R_v \quad \text{und} \quad \mathcal{O} = \bigcap_{v \in \Omega_f} \mathcal{O}_v.$$

1.4 Topologische Eigenschaften von Quaternionenalgebren

Es sei in diesem Abschnitt K ein algebraischer Zahlkörper und $R = \mathcal{O}_K$ sein Ganzheitsring. Für eine Stelle $v \in \Omega(K)$ bezeichne K_v die Vervollständigung von K bezüglich einem zu v gehörigen Absolutbetrages. Für eine endliche Stelle $v \in \Omega_f(K)$ bezeichnen wir den zu K_v gehörigen Bewertungsring mit R_v . Weiters sei A eine Quaternionenalgebra über K .

Es sei $v \in \Omega_f$ und $\mathfrak{p}$ das dazugehörige Primideal. Weil $\mathcal{O}_K$ ein Dedekindring ist, lässt sich für $x \in K$ das gebrochene Hauptideal (x) eindeutig als Produkt von Primidealen schreiben:

$$(x) = \prod_{\{0\} \neq \mathfrak{q} \triangleleft R \text{ prim}} \mathfrak{q}^{\nu_{\mathfrak{q}}(x)},$$

für eindeutige $\nu_{\mathfrak{q}}(x) \in \mathbb{Z}$. Es ist dann

$$\nu_{\mathfrak{p}} : K^* \longrightarrow \mathbb{Z}$$

die $\mathfrak{p}$ -adische Bewertung von K und K_v die Vervollständigung von K bezüglich folgendem Absolutbetrag:

$$|\cdot|_v : K \longrightarrow \mathbb{R}_+, \quad |x|_v := c^{-\nu_{\mathfrak{p}}(x)}$$

wobei $c := N(\mathfrak{p})$ die Norm des Primideals $\mathfrak{p}$ bezeichnet. Weiters ist

$$R_v = \{x \in K_v \mid |x|_v \leq 1\} = \{x \in K_v \mid |x|_v < N(\mathfrak{p})\}$$

der Bewertungsring von K_v und

$$\mathfrak{p}_v = \{x \in K_v \mid |x|_v < 1\} = \{x \in K_v \mid |x|_v \leq N(\mathfrak{p})^{-1}\}$$

das maximale Ideal in R_v .

Falls v eine reelle (bzw. komplexe) Stelle ist, bezeichnen wir mit $|\cdot|_v = |\cdot|$ (bzw. $|\cdot|_v = |\cdot|^2$) den gewöhnlichen Absolutbetrag auf $\mathbb{R}$ (bzw. $\mathbb{C}$).

Theorem 1.4.1. 1. Für $v \in \Omega$ ist K_v ein lokalkompakter topologischer Körper, und für $v \in \Omega_f$ ist R_v ein kompakter offener Teilring von K_v .

2. Für $v \in \Omega$ ist K_v^* bezüglich der Teilraumtopologie von K_v eine lokalkompakte offene Gruppe und für $v \in \Omega_f$ ist R_v^* eine kompakte offene Untergruppe von K_v^* .

Beweis. 1. Nach [1, Seite 402] ist die Vervollständigung eines Körpers bezüglich eines Absolutbetrages ein topologischer Körper. Um zu zeigen, dass K_v lokalkompakt ist, genügt es somit zu beweisen, dass jede Umgebung der $\{0\}$ eine kompakte Umgebung enthält.

Weil R_v das Urbild von $(-c, c)$ und $[-1, 1]$ unter $|\cdot|_v$ ist, ist R_v offen und abgeschlossen. Analog erhält man, dass für $r \in \mathbb{N}$ die $\mathfrak{p}_v^r$ offen und abgeschlossen sind. Da $\{\mathfrak{p}_v^r \mid r \in \mathbb{N}\}$ eine Umgebungsbasis der $\{0\} \in K_v$ bildet, genügt es für die restlichen Behauptungen zu zeigen, dass R_v kompakt ist.

Die Menge R_v aber, ist die Einheitskugel in dem vollständigen normierten Raum K_v . Wir erinnern uns aus der Funktionalanalysis, dass Einheitskugeln in endlichdimensionalen Banachräumen kompakt sind.

2. Weil die Menge $\{0\}$ abgeschlossen ist, ist $K_v^* = K_v \setminus \{0\}$ offen. Dass R_v^* offen und abgeschlossen ist, folgt aus

$$R_v^* = \{x \in K_v \mid |x|_v = 1\} = \{x \in K_v \mid |x|_v > c^{-1}\} \cap \{x \in K_v \mid |x|_v < c\}.$$

Als abgeschlossene Teilmenge von R_v ist R_v^* nach 1.4.5 kompakt. $\square$

Im nächsten Resultat zeigen wir, dass man wie auf K_v , auf quaternionischen Divisionalgebren A_v über K_v eine Bewertung definieren kann. Weiters stellt sich heraus, dass der Bewertungsring $\mathcal{O}_v$ offen und kompakt ist. Dies ist ein wichtiger Schritt um die Arithmetik solcher Algebren zu verstehen. (Wir haben hier die Objekte A_v und $\mathcal{O}_v$ nicht wie zuvor durch lokalisieren von A und $\mathcal{O}$ eingeführt. Da aber alle (hier betrachteten) lokalen Objekte von dieser Form sind, macht das nichts.)

Proposition 1.4.2. *Es sei A_v eine quaternionische Divisionsalgebra über K_v und es bezeichne $\nu : K^* \rightarrow \mathbb{Z}$ die v -adische Bewertung von K . Dann hat die Abbildung*

$$w : A_v^* \rightarrow \mathbb{Z}, \quad w(x) := \nu(n(x)).$$

folgende Eigenschaften:

1. $w(xy) = w(x) + w(y)$ für alle $x, y \in A_v^*$,
2. $w(x + y) \geq \min\{w(x), w(y)\}$ mit Gleichheit falls $w(x) \neq w(y)$ für alle $x, y \in A_v^*$.

Also definiert w eine Bewertung auf A_v und

$$|\cdot|_{A_v} : A_v^* \rightarrow \mathbb{R}_+, \quad |x|_{A_v} := |n(x)|_v = c^{-n(x)}$$

einen Absolutbetrag auf A_v .

Beweis. 1. Die Gleichung folgt aus der Definition von ν und aus der Multiplikativität der Normabbildung.

2. Es sei $x \in A_v \setminus K_v$. Weil A_v eine Divisionsalgebra ist und weil x algebraisch über K_v ist, ist $K_v(x)$ eine quadratische Körpererweiterung. Nach 1.1.10 gilt $n|_{K_v(x)} = N_{K_v(x)/K_v}$. Wir wissen aus der Algebra, dass $\nu \circ N_{K_v(x)/K_v}$ eine Bewertung von $K_v(x)$ ist. Somit gilt die Behauptung für $w|_{K_v(x)}$.

Nun seien $x, y \in A_v^*$. Wir wenden obige Überlegung auf $K_v(xy^{-1})$ an und erhalten:

$$w(x + y) - w(y) = w(xy^{-1} + 1) \geq \min\{w(xy^{-1}), w(1)\},$$

mit Gleichheit wenn $w(xy^{-1}) \neq w(1)$. Durch erneutes Anwenden von (1) ergibt sich die Behauptung. $\square$

Proposition 1.4.3. *Es sei A_v eine quaternionische Divisionsalgebra über K_v . Der Bewertungsringsring $\mathcal{O}_v = \{x \in A_v \mid |x|_{A_v} \leq 1\} = \{x \in A_v \mid |x|_{A_v}^2 \leq 1\}$ und seine Einheitengruppe $\mathcal{O}_v^* = \{x \in A_v \mid |n(x)|_v = 1\}$ sind offen und kompakt in A_v .*

Beweis. Weil $\mathcal{O}_v$ das Urbild von $(-c, c)$ unter $|\cdot|_{A_v}$ ist, ist $\mathcal{O}_v$ offen. Wir zeigen, dass $\mathcal{O}_v$ kompakt ist. Nach 1.4.2 ist A_v ein normierter Vektorraum. Es genügt zu zeigen, dass A_v vollständig ist, denn die Einheitskugeln in vollständigen normierten Vektorräumen sind kompakt. Das folgt aus einer allgemeinen Überlegung im Beweis des nächsten Theorem.

Wir stellen $\mathcal{O}_v^*$ als Urbild des Absolutbetrages dar und erkennen, dass $\mathcal{O}_v^*$ abgeschlossen und offen ist:

$$\mathcal{O}_v^* = \{x \in A \mid |x|_{A_v} = 1\} = \{x \in A \mid |x|_{A_v} > c^{-1}\} \cap \{x \in A \mid |x|_{A_v} < c\}.$$

Als abgeschlossene Teilmenge des kompakten Bewertungsrings $\mathcal{O}_v$ ist $\mathcal{O}_v^*$ kompakt. $\square$

Bemerkung 1.4.4. Aufgrund von 1.4.2 und 1.4.3 kann man die Elemente aus $\mathcal{O}_v$ wie jene aus R_v eindeutig in einer Potenzreihe darstellen. Genauer kann man zeigen:

Es sei $\pi \in \mathcal{O}_v$ ein Element mit Bewertung $w(\pi) = 1$. Dann gibt es für jedes $a \in \mathcal{O}_v$ eine eindeutige Darstellung der Form:

$$a = \sum_{i \geq 0} a_i \pi^i, \quad \text{mit } a_i \in \mathcal{O}_v, \quad i \in \mathbb{N}.$$

Die nächsten beiden Sätze sind grundlegend für die Konstruktionen in Kapitel 2.

Theorem 1.4.5. *Es sei A eine Quaternionenalgebra über K und $\mathcal{O}$ eine R -Ordnung in A . Dann ist für $v \in \Omega$ A_v in kanonischer Weise eine lokalkompakte K_v -Algebra, und für $v \in \Omega_f$ ist $\mathcal{O}_v$ eine kompakte, offene R_v -Ordnung.*

Beweis. Der Beweis dieses Theorems folgt einem allgemeinen Prinzip:

Es sei V ein n -dimensionaler Vektorraum über einem vollständigen nichttrivial bewerteten topologischen Körper L . Dann gibt es genau eine Hausdorfftopologie auf V sodass V ein topologischer Vektorraum wird. Diese erhält man durch die Produkttopologie auf L^n .

Man sieht leicht, dass A_v mit der Produkttopologie des K_v^4 zu einer topologischen K_v -Algebra wird. Aus den Eigenschaften von K_v erhält man, dass A_v eine vollständige, lokalkompakte, topologische K_v -Algebra ist. Falls A_v eine Divisionsalgebra ist, folgt aus der Eindeutigkeitsaussage für die Topologie, dass die von K_v induzierte Topologie mit der von der Bewertung induzierten Topologie übereinstimmt.

Nun sei $v \in \Omega_f$ und $\{x_1, \dots, x_4\}$ eine R_v -Basis von $\mathcal{O}_v$. Es ist dann $\{x_1, \dots, x_4\}$ auch eine K_v -Basis von A_v und nach Definition der Topologie auf A_v erhalten wir einen topologischen Vektorraumisomorphismus:

$$f : K_v^4 \longrightarrow A_v \quad f(a_1, \dots, a_4) := \sum_{1 \leq i \leq 4} a_i x_i$$

Dann ist $f(R_v^4) = \mathcal{O}_v$ und weil nach 1.4.1 R_v kompakt und offen ist, folgt die Behauptung. $\square$

Bemerkung 1.4.6. Durch die Produkttopologie des $\mathbb{R}^4$ erben die Hamilton'schen Quaternionen $\mathbb{H} = (-1, -1|\mathbb{R})$ eine $\mathcal{C}^\infty$ -Mannigfaltigkeitsstruktur. Genauer haben wir einen Diffeomorphismus $\{z \in \mathbb{H}^* \mid n(z) = 1\} \cong \{(x_1, x_2, x_3, x_4) \in \mathbb{R}^4 \mid x_1^2 + x_2^2 + x_3^2 + x_4^2 = 1\} = S^3$. Wegen $\mathbb{R}_{>0} \supseteq n(\mathbb{H}^*) \supseteq n(\mathbb{R}) \supseteq \mathbb{R}_{>0}$ erhalten wir $\mathbb{H}^* \cong S^3 \times \mathbb{R}_{>0}$.

Theorem 1.4.7. *Es sei A eine Quaternionenalgebra über K und $\mathcal{O}$ eine R -Ordnung in A .*

1. *Für $v \in \Omega$ ist A_v^* bezüglich der Teilraumtopologie von A_v eine lokalkompakte offene Gruppe.*
2. *Für $v \in \Omega_f$ ist $\mathcal{O}_v^*$ eine kompakte, offene Untergruppe von A_v^* .*

Beweis. 1. Zunächst bemerken wir, dass A_v^* offen ist: Falls A_v eine Divisionsalgebra ist, folgt das aus $A_v^* = A_v \setminus \{0\}$. Im anderen Fall ist $A_v^* = \text{GL}_2(K_v)$ das Urbild von $K_v \setminus \{0\}$ unter der stetigen Funktion $\det$, und somit offen.

Nun zeigen wir, dass A_v^* lokalkompakt ist. Wir behandeln zunächst den archimedischen Fall. Dann ist $A_v^* = \mathbb{H}^*, \text{GL}_2(\mathbb{R})$ oder $\text{GL}_2(\mathbb{C})$, je nachdem ob v reell ist und A über $\mathbb{R}$ verzweigt (oder nicht) oder ob v komplex ist. Diese drei Gruppen sind offene reelle Mannigfaltigkeiten ($\mathbb{H}^* = \mathbb{R}_{>0} \times S^3$, nach 1.4.6 und $\text{GL}_2(\mathbb{R})$ bzw. $\text{GL}_2(\mathbb{C})$ sind die Urbilder von $\mathbb{R} \setminus \{0\}$ unter der glatten Funktion $\det$) und daher lokal kompakt, denn: Sei $x \in A_v^*$ und (φ, U) eine Karte, so dass $x \in U$. Dann besitzt $\varphi(x)$ eine kompakte Umgebung in $\varphi(U)$ und ihr Urbild ist eine kompakte Umgebung von x in A_v^* .

Es sei nun v nicht-archimedisch. Weil A_v eine topologische K_v -Algebra ist, ist A_v^* eine topologische Gruppe und es genügt es zu zeigen, dass $\{1\}$ eine Umgebungsbasis aus kompakten Mengen besitzt.

Falls A_v eine Divisionsalgebra ist, wählen wir ein Element $\pi \in A_v$ mit Bewertung $w(\pi) = 1$ und betrachten den offenen und kompakten Bewertungsring $\mathcal{O}_v = \{x \in A_v \mid |x|_{A_v} \leq 1\}$ aus 1.4.3. Somit definiert

$$\{1 + \pi^r \mathcal{O}_v \mid r \in \mathbb{N}\}$$

eine kompakte (und offene) Umgebungsbasis der $\{1\}$ in A_v^* . (Weil Elemente aus $1 + \pi^r \mathcal{O}_v$ Bewertung 0 haben, liegen sie in $\mathcal{O}_v^*$, also insbesondere in A_v^* .)

Falls $A_v = M_2(K_v)$, ist

$$\{\mathbf{I}_2 + \pi^r M_2(R_v) \mid r \in \mathbb{N}\}$$

eine solche Umgebungsbasis, denn mit R_v ist auch $M_2(R_v)$ offen und kompakt. (Es ist leicht zu überprüfen, dass Matrizen aus $\mathbf{I}_2 + \pi^r M_2(R_v)$ invertierbar sind.)

2. Es sei $v \in \Omega_f$. Wir zeigen die Behauptung zunächst für maximale Ordnungen $\mathcal{O}_v$.

Es sei A_v eine Divisionsalgebra. Dann kann man zeigen (siehe [8, Seite 208]), dass $\mathcal{O}_v = \{x \in A_v \mid |x|_{A_v} \leq 1\}$ aus 1.4.3 die eindeutige maximale Ordnung von A_v ist. In 1.4.3 haben wir gezeigt, dass $\mathcal{O}_v^*$ offen und kompakt ist.

Es sei nun $A_v = M_2(K_v)$. Dann kann man zeigen (siehe [8, Seite 210]), dass alle maximalen Ordnungen zu $\mathcal{O}_v = M_2(R_v)$ konjugiert sind. Wegen der Stetigkeit der Multiplikation reicht es daher den Satz für $\mathcal{O}_v^* = GL_2(R_v)$ zu zeigen. Da R_v offen und kompakt in K_v ist, ist $M_2(R_v)$ offen und kompakt in A_v . Die Gruppe $GL_2(R_v)$ ist das Urbild der offenen und abgeschlossenen Menge R_v unter der stetigen Abbildung $\det$. Demnach ist $GL_2(R_v)$ offen und als abgeschlossene Teilmenge der kompakten Menge $M_2(R_v)$ selbst kompakt. Das zeigt die Behauptung.

Es sei nun $\mathcal{O}'_v$ eine beliebige Ordnung. Nach 1.3.12 ist $\mathcal{O}'_v$ in einer maximalen Ordnung $\mathcal{O}_v$ enthalten. Es genügt zu zeigen, dass $\mathcal{O}'_v$ offen ist. Denn dann ist $\mathcal{O}'_v$ auch abgeschlossen und als Teilmenge der kompakten Menge $\mathcal{O}_v$ kompakt. Wir zeigen, dass $\{1\}$ eine offene Umgebung in $\mathcal{O}'_v$ hat. Es hat dann jedes Element in $\mathcal{O}'_v$ eine offene Umgebung, womit $\mathcal{O}'_v$ offen ist.

Es sei A_v eine Divisionsalgebra. Dann liegt $\mathcal{O}'_v$ in der maximalen Ordnung $\mathcal{O}_v = \{x \in A_v \mid |x|_{A_v} \leq 1\}$. Wir wählen ein Element $\pi \in \mathcal{O}_v$ mit Bewertung $w(\pi) = 1$. Es ist dann $(\pi^n)_{n \in \mathbb{N}}$ eine Nullfolge in $\mathcal{O}_v$. Da $1 \in \mathcal{O}'_v$ und $\mathcal{O}'_v$ offen ist, existiert eine natürliche Zahl $m \in \mathbb{N}$ mit

$$U := 1 + \pi^m \mathcal{O}_v \subseteq \mathcal{O}'_v$$

Aus 1.4.4 folgt, dass U eine Untergruppe von $\mathcal{O}_v^*$ ist, womit U eine offene Umgebung der $\{1\}$ in $\mathcal{O}'_v$ ist.

Es sei nun $A_v = M_2(K_v)$. Weiters sei π ein uniformisierendes Element von R_v , also $\nu(\pi) = 1$. Dann existiert ein $m \in \mathbb{N}$ mit

$$U := \mathbf{I}_2 + \pi^m M_2(R_v) \subseteq \mathcal{O}'_v.$$

Man überzeugt sich leicht davon, dass U eine Untergruppe von $GL_2(K_v)$ ist. Somit ist U eine offene Umgebung der $\{1\}$ in $\mathcal{O}'_v$. $\square$

Bemerkung 1.4.8. Ersetzen wir in 1.4.3, 1.4.5 und 1.4.7 A durch K und in 1.4.5 und 1.4.7 $\mathcal{O}$ durch R , so erhalten wir jeweils die Aussagen von 1.4.1. Das Entscheidende an 1.4.5 und 1.4.7 ist, dass es uns erlaubt, Ordnungen zu studieren, die nicht von einer Bewertung kommen.

Kapitel 2

Adele und Ideale

In diesem Kapitel sei K ein algebraischer Zahlkörper und $R = \mathcal{O}_K$ sein Ganzheitsring. Weiters bezeichne $\Omega = \Omega(K)$ die Menge aller Stellen von K , Ω_∞ die Menge der unendlichen Stellen und Ω_f die Menge der endlichen Stellen. Für eine Stelle $v \in \Omega(K)$ bezeichne K_v die Vervollständigung von K bezüglich einem zu v gehörigen Absolutbetrages. Für eine endliche Stelle $v \in \Omega_f(K)$ bezeichnen wir den zu K_v gehörigen Bewertungsring mit R_v . Weiters sei A eine Quaternionenalgebra über K und $A_v = A \otimes_K K_v$.

2.1 Das eingeschränkte direkte Produkt

Definition 2.1.1 (Eingeschränktes direktes Produkt). Es sei Λ eine Menge und Λ_0 eine endliche Teilmenge. Weiter sei $\{G_\lambda \mid \lambda \in \Lambda\}$ eine Familie von lokalkompakten, hausdorff'schen topologischen Gruppen. Für $\lambda \in \Lambda \setminus \Lambda_0$ sei H_λ eine kompakte offene Untergruppe von G_λ . Das *eingeschränkte direkte Produkt* der Gruppen G_λ in Bezug auf H_λ ist die folgende Untergruppe des direkten Produktes:

$$G := \prod_{\lambda \in \Lambda \setminus \Lambda_0} [G_\lambda : H_\lambda] := \{x = (x_\lambda)_{\lambda \in \Lambda} \in \prod_{\lambda \in \Lambda} G_\lambda \mid x_\lambda \in H_\lambda \text{ für fast alle } \lambda \in \Lambda \setminus \Lambda_0\}.$$

Die Familie von Mengen

$$\{\prod_{\lambda \in \Lambda} U_\lambda \mid U_\lambda \text{ offene Umgebung der Einselemente in } G_\lambda \text{ und } U_\lambda = H_\lambda \text{ für fast alle } \lambda \in \Lambda \setminus \Lambda_0\}$$

definiert eine Umgebungsbasis des Einselementes in G .

Es sei S eine endliche Menge mit $\Lambda_0 \subseteq S \subseteq \Lambda$. Wir definieren eine Untergruppe von G :

$$G_S := \prod_{\lambda \in S} G_\lambda \times \prod_{\lambda \in \Lambda \setminus S} H_\lambda.$$

Nach Definition der Topologie auf G ist G_S offen in G .

Da ohnehin alle hier behandelten topologischen Objekte hausdorff'sch sind, werden wir, diese Voraussetzung in obiger Definition nicht wieder erwähnen. Für ein $x \in G$ bezeichne x_λ die Projektion von x auf die Komponente G_λ .

In den nächsten beiden Proposition untersuchen wir die Topologie von G .

Proposition 2.1.2. *Es sei S eine endliche Menge mit $\Lambda_0 \subseteq S \subseteq \Lambda$. Dann ist G_S eine lokalkompakte topologische Gruppe.*

Beweis. Es ist G_S ein endliches Produkt lokalkompakter topologischer Räume mit einem kompakten Raum. Also ist G_S mit der Produkttopologie eine lokalkompakter topologischer Raum. Offensichtlich ist G_S dann auch eine lokalkompakte topologische Gruppe, bezüglich der Produkttopologie.

Die Produkttopologie auf G_S ist identisch zu der Teilraumtopologie auf G_S , die durch die oben definierte Umgebungsbasis induziert wird.

Somit ist jede Untergruppe von G , die von der Form G_S ist, lokalkompakt bezüglich der Topologie, des eingeschränkten direkten Produktes. Da jedes Element von G in einer Untergruppe der Form G_S liegt, ist G lokalkompakter topologischer Raum. Die Topologie ist wieder mit der Gruppenstruktur verträglich. $\square$

Proposition 2.1.3. *Der topologische Abschluss einer Teilmenge $Z \subseteq G$ ist kompakt genau dann, wenn $Z \subseteq \prod_{\lambda \in \Lambda} Z_\lambda$ für kompakte Teilmengen $Z_\lambda \subseteq G_\lambda$ mit $Z_\lambda = H_\lambda$ für fast alle $\lambda \in \Lambda \setminus \Lambda_0$.*

Beweis. Es sei $\bar{Z} \subseteq G$ kompakt. Da G von offenen Mengen der Form G_S überlagert wird, gibt es eine endliche Teilüberlagerung die $\bar{Z}$ überlagert. Es gibt eine Menge S_0 sodass diese endliche Teilüberlagerung in G_{S_0} liegt. Also erhalten wir:

1. Für $\lambda \in \Lambda$ bezeichne $p_\lambda : G \longrightarrow G_\lambda$ die natürliche Projektion. Da die Topologie des eingeschränkten direkten Produktes auf $G_{S_0} \subseteq G$ mit der Produkttopologie übereinstimmt, sind die p_λ stetig auf G_{S_0} und somit ist $p_\lambda(Z)$ kompakt für alle $\lambda \in \Lambda$.
2. Es ist $p_\lambda(Z) \subseteq H_\lambda$ für fast alle $\lambda \in \Lambda$.

Die Behauptung folgt nun unmittelbar.

Es sei nun umgekehrt $\bar{Z}$ in einem Produkt der Form $\prod_{\lambda \in \Lambda} Z_\lambda$ enthalten, mit $Z_\lambda \subseteq G_\lambda$ kompakt und $Z_\lambda = H_\lambda$ für fast alle $\lambda \in \Lambda \setminus \Lambda_0$. Weil auf G_S die Topologie des eingeschränkten direkten Produktes mit der Produkttopologie übereinstimmt, ist $\bar{Z}$ kompakt in G_S . Dass $\bar{Z}$ kompakt in G ist folgt aus der Definition der Kompaktheit. $\square$

Wenn in obiger Definition die G_λ lokalkompakte topologische Ringe (bzw. Moduln) sind, und die H_λ kompakte, offene topologische Unterringe (bzw. Untermoduln) von G_λ sind, dann zeigt man leicht, dass $\prod_{\lambda \in \Lambda \setminus \Lambda_0} [G_\lambda : H_\lambda]$ ein lokalkompakter topologischer Ring (bzw. Modul) ist. Wir sprechen dann von einem *eingeschränkten direkten Produkt von Ringen (bzw. Moduln)*.

In den von uns betrachteten Situationen wird $\Lambda = \Omega$, die Menge aller Stellen von K sein und $\Lambda_0 = \Omega_\infty$ die Menge aller archimedischen Stellen sein. Es sei im folgenden S eine endliche Menge mit $\Omega_\infty \subseteq S \subseteq \Omega$.

Beispiel 2.1.4. 1. Für alle Stellen $v \in \Omega$ ist nach 1.4.5 K_v ein lokalkompakter topologischer Körper, und für $v \in \Omega_f$ ist R_v ein kompakter offener Unterring von K_v . Wir können also das eingeschränkte direkte Produkt der Ringe K_v in Bezug auf R_v bilden. Dieses nennen

wir den *Ring der Adele von K* . Wir bezeichnen ihn mit $\mathbf{A}_K$. Es sei $x \in K$. Dann ist $x \in K_v$ für alle $v \in \Omega$, und $x \in R_v$ für fast alle $v \in \Omega \setminus \Omega_\infty$. Also können wir K durch die Abbildung $x \mapsto (\dots, x, x, x, \dots, x, x, \dots)$ in $\mathbf{A}_K$ einbetten. Das Bild von K unter dieser Einbettung werden wir mit K bezeichnen. Die Untergruppe $\mathbf{A}_{K,S} := \prod_{v \in S} K_v \times \prod_{v \in \Omega \setminus S} R_v$ nennen wir die *S-Adele von K* .

2. Für alle Stellen $v \in \Omega$ ist nach 1.4.7 K_v^* eine lokalkompakte topologische Gruppe, und für $v \in \Omega_f$ ist R_v^* eine kompakte offene Untergruppe von K_v^* . Das eingeschränkte direkte Produkt von K_v^* in Bezug auf R_v^* nennen wir die *Gruppe der Idele von K* und notieren wir mit $\mathbf{I}_K$. Wir können $\mathbf{I}_K$ als Teilmenge von $\mathbf{A}_K$ auffassen. Tun wir dies, so ist $\mathbf{I}_K$ gerade die Menge der Einheiten von $\mathbf{A}_K$. Die Topologie von $\mathbf{I}_K$ als eingeschränktes direktes Produkt stimmt nicht mit der Teilraumtopologie von $\mathbf{A}_K$ überein, siehe 2.3.1. Die Untergruppe $\mathbf{I}_{K,S} := \prod_{v \in S} K_v^* \times \prod_{v \in \Omega \setminus S} R_v^*$ nennen wir die *S-Idele von K* .
3. Es sei A eine Quaternionenalgebra über K und $A_v = A \otimes_K K_v$. Weiters sei $\mathcal{O}$ R -eine Ordnung in A und $\mathcal{O}_v = \mathcal{O} \otimes_R R_v$. Nach 1.4.5 ist A_v für alle Stellen $v \in \Omega$ eine lokalkompakte topologische Algebra, und für $v \in \Omega_f$ ist $\mathcal{O}_v$ ein kompakter offener Unterring von A_v . Das eingeschränkte direkte Produkt der A_v in Bezug auf $\mathcal{O}_v$ bezeichnen wir mit $\mathbf{A}_A$ und nennen es den *Ring der Adele von A* . Wie in (1) können wir A und K wieder in $\mathbf{A}_A$ einbetten. Wir werden die Bilder unter dieser Einbettung mit A und K bezeichnen. Die Untergruppe $\mathbf{A}_{A,S} := \prod_{v \in S} A_v \times \prod_{v \in \Omega \setminus S} \mathcal{O}_v$ nennen wir die *S-Adele von A* .
4. Für alle Stellen $v \in \Omega$ ist nach 1.4.7 A_v^* eine lokalkompakte topologische Gruppe, und für $v \in \Omega_f$ ist $\mathcal{O}_v^*$ eine kompakte offene Untergruppe von A_v^* . Das eingeschränkte direkte Produkt der A_v^* in Bezug auf $\mathcal{O}_v^*$ bezeichnen wir mit $\mathbf{I}_A$, und nennen es die *Gruppe der Idele von A* . Die Topologie von $\mathbf{I}_A$ als eingeschränktes direktes Produkt stimmt nicht mit der Teilraumtopologie von $\mathbf{A}_A$ überein, siehe 2.3.1. Die Untergruppe $\mathbf{I}_{A,S} := \prod_{v \in S} A_v^* \times \prod_{v \in \Omega \setminus S} \mathcal{O}_v^*$ nennen wir die *S-Idele von A* .
5. Es sei E ein n -dimensionaler K -Vektorraum und $\{e_1, \dots, e_n\}$ eine Basis. Für $v \in \Omega$ ist dann $\{e_1 \otimes_K 1, \dots, e_n \otimes_K 1\}$ eine Basis des K_v -Vektorraums $E_v := E \otimes_K K_v$. Dieser ist lokalkompakt bezüglich der durch K_v induzierten Produkttopologie. Weil für $v \in \Omega_f$, R_v ein Hauptidealring ist, ist nach 1.3.9, das R_v -Erzeugnis von $\{e_1 \otimes_K 1, \dots, e_n \otimes_K 1\}$ ein freier R_v -Modul. Dieser, wir notieren ihn mit ε_v , ist offen und kompakt. Wir können also das eingeschränkte direkte Produkt der E_v in Bezug auf ε_v bilden, und notieren es mit $\mathbf{A}_{E/K}$.

Lemma 2.1.5. *Es seien $\prod_{\lambda \in \Lambda \setminus \Lambda_0} [G_\lambda : H_\lambda]$ und $\prod_{\lambda \in \Lambda \setminus \Lambda'_0} [G'_\lambda : H'_\lambda]$ zwei eingeschränkte direkte Produkte von topologischen Gruppen (bzw. Moduln). Für $\lambda \in \Lambda$ seien $f_\lambda : G_\lambda \longrightarrow G'_\lambda$ topologische Gruppenhomomorphismen (bzw. Modulhomomorphismen) mit $f_\lambda(H_\lambda) \subseteq H'_\lambda$. Dann ist auch die Einschränkung des topologischen Gruppenhomomorphismus (bzw. Modulhomomorphismus) $\prod_{\lambda \in \Lambda} f_\lambda$ auf $\prod_{\lambda \in \Lambda \setminus \Lambda_0} [G_\lambda : H_\lambda]$ ein solcher.*

Beweis. Das folgt aus der Definition des eingeschränkten direkten Produktes. □

Beispiel 2.1.6. Es bezeichne $n_v : A_v \longrightarrow K$ die Normabbildung von A_v . Nach 1.3.1 und 1.3.11 gilt $n_v(\mathcal{O}_v) \subseteq R_v$ für alle $v \in \Omega_f$. Also erhalten wir einen Morphismus $n_{\mathbf{A}} : \mathbf{A}_A \longrightarrow \mathbf{A}_K$. Diesen nennen wir die (reduzierte) Normabbildung von $\mathbf{A}_A$. Analog erhält man eine (reduzierte) Spurabbildung $sp_{\mathbf{A}} : \mathbf{A}_A \longrightarrow \mathbf{A}_K$.

Da die Gruppen K_v und A_v und jene aus 2.1.4 lokalkompakt sind, können wir die Konzepte der harmonischen Analysis verwenden um diese zu untersuchen.

Es sei G eine lokalkompakte Gruppe, μ ein Haar-Maß auf G und $\alpha \in \text{Aut}(G)$ ein topologischer Gruppenautomorphismus auf G . Dann definiert α ein Haar-Maß μ^α auf G , indem wir für jede messbare Funktion f auf G folgende Gleichung fordern:

$$\int_G f(g) d\mu(g) = \int_G f(\alpha(g)) d\mu^\alpha(g)$$

Da Haar-Maße auf lokalkompakten Gruppen bis auf Konstanten eindeutig bestimmt sind, existiert ein $c_\alpha \in \mathbb{R}$, sodass für alle messbaren Mengen $B \subseteq G$ die Gleichung $\mu^\alpha(B) = c_\alpha \mu(B)$ gilt. Wir nennen c_α den Modul von α und die Zuordnung $\alpha \mapsto c_\alpha$ die Modulabbildung. Offensichtlich gilt

$$c_{\alpha \circ \beta} = c_\alpha \cdot c_\beta,$$

für zwei topologische Gruppenautomorphismen $\alpha, \beta \in \text{Aut}(G)$. Somit ist der Begriff des Moduls unabhängig von dem zu Beginn gewählten Haar-Maß μ .

Definition 2.1.7. Falls T ein lokalkompakter Ring ist, ist für $x \in T^*$ die Linksmultiplikation $m_x : T \longrightarrow T$, $z \mapsto xz$ ein topologischer Ringautomorphismus auf T . Den Modul von m_x nennen wir den *Modul* von x und notieren ihn mit $\|x\|_T$. Weiters definieren wir für $x \in T \setminus T^*$: $\|x\|_T = 0$.

Es sei T ein lokalkompakter und σ -kompakter Ring (also Vereinigung von abzählbar vielen kompakten Teilmengen) und M ein freier, lokalkompakter topologischer Modul über T mit $\dim_T M = n$. Dann ist M mit T^n topologisch isomorph: Ist nämlich $f : T^n \longrightarrow M$ der algebraische Isomorphismus, so ist f stetig, und nach [3, Abstract Harmonic Analysis, Chapter II, (5.29)], auch offen.

Es definiert die komponentenweise Linksmultiplikation mit $x \in T^*$ einen Automorphismus auf M . Den Modul des von $x \in T^*$ induzierten Automorphismus auf M nennen wir den *Modul* von x auf M und notieren ihn mit $\|x\|_M$. Aus Fubini's Theorem folgt dann für $x \in T^*$:

$$\|x\|_M = \|x\|_T^n.$$

Bemerkung 2.1.8. Die topologischen Ringe K_v , A_v und $\mathbf{A}_K$ sind σ -kompakt.

1. Es sei $\mathfrak{p}_v$ das maximale Ideal von R_v , π ein uniformisierendes Element und $R_v/\mathfrak{p}_v = \{\nu_1, \dots, \nu_q\}$. Dann ist

$$K_v = \bigcup_{n \in \mathbb{N}} \bigcup_{\substack{\nu_i \in R_v/\mathfrak{p}_v \\ i \in \{-n, \dots, 0\}}} \sum_{-n \leq i \leq 0} \nu_i \pi^i + \mathfrak{p}_v^n,$$

und somit ist K_v σ -kompakt. Aufgrund des topologischen Isomorphismus $A_v \cong K_v^4$ ist auch A_v σ -kompakt.

2. Da es nur endlich viele archimedischen Stellen und nur abzählbar viele Primideale in R gibt, ist die Anzahl der Stellen von K_v abzählbar. Daraus, und aus (1) folgt, dass $\mathbf{A}_K$ σ -kompakt ist.

Theorem 2.1.9. *Es sei A eine Quaternionenalgebra über K und $v \in \Omega$. Dann gilt:*

1. $\|x\|_v := \|x\|_{K_v} = |x|_v$, für alle $x \in K_v$,
2. $\|x\|_{A_v} = \|n(x)\|_{K_v}^2$, für alle $x \in A_v^*$.

Falls A_v eine Divisionsalgebra ist, ist nach (2) und 1.4.2

$$\|x\|_{A_v} = |x|_{A_v}^2, \text{ für alle } x \in A_v.$$

Beweis. 1. Man sieht leicht, dass für eine reelle Stelle v $\|x\|_{\mathbb{R}} = |x| \stackrel{Def}{=} |x|_v$ und für eine komplexe Stelle v $\|x\|_{\mathbb{C}} = |x|^2 \stackrel{Def}{=} |x|_v$ gilt. Für den nichtarchimedischen Fall siehe [2, Proposition 3.2.9].

2. Nach 2.1.8 und der Überlegung davor, gilt:

$$\|n(x)\|_{A_v} = \|n(x)\|_{K_v}^4, \text{ für alle } x \in A_v^*.$$

Aus der Multiplikativität der Normabbildung und der Modulabbildung folgt:

$$\|n(x)\|_{A_v} = \|x\|_{A_v} \|\bar{x}\|_{A_v}, \text{ für alle } x \in A_v^*.$$

Somit genügt es für $x \in A_v^*$ die Identität $\|x\|_{K_v} = \|\bar{x}\|_{K_v}$ zu zeigen.

Es sei $m_x : A_v \rightarrow A_v$, $z \mapsto xz$ die Linksmultiplikation mit x und $\bar{id}_{A_v} : A_v \rightarrow A_v$ die Abbildung, die jedem Quaternion sein Konjugiertes zuordnet. Dann ist

$$m_{\bar{x}} = \bar{id}_{A_v} \circ m_x \circ id_{A_v}.$$

Somit genügt es zu zeigen, dass der Modul von $\bar{id}_{A_v}$ gleich 1 ist. Die Abbildung $\bar{id}_{A_v}$ ist aber offensichtlich maßerhaltend. $\square$

Den Rest des Abschnittes widmen wir der Verträglichkeit der Modulfunktion mit der Konstruktion des direkten Produktes. Das wird in der Arbeit nicht gebraucht werden, ist aber von ästhetischem Wert.

Proposition 2.1.10. *Es sei $G = \prod_{\lambda \in \Lambda \setminus \Lambda_0} [G_\lambda : H_\lambda]$ ein eingeschränktes direktes Produkt von Gruppen bzw. Ringen. Weiters seien dg_λ Haar-Maße auf G_λ mit folgender Normierung:*

$$\int_{H_\lambda} 1 \, dg_\lambda = 1$$

für fast alle $\lambda \in \Lambda \setminus \Lambda_0$. Dann gibt es genau ein Haar-Maß dg auf G , sodass für jede Menge S mit $\Lambda_0 \subseteq S \subseteq \Lambda$ die Einschränkung des Maßes dg_S von dg auf

$$G_S := \prod_{\lambda \in S} G_\lambda \times \prod_{\lambda \in \Lambda \setminus S} H_\lambda.$$

das Produktmaß ist.

Beweis. [10] Seite 185. □

Wir schreiben

$$dg = \prod_{\lambda \in \Lambda} dg_\lambda$$

für das in obiger Proposition definierte Maß, und nennen dg das durch die dg_λ induzierte Maß auf G .

Korollar 2.1.11. *Die Modulabbildung auf G ist das Produkt der Modulabbildungen auf G_λ :*

$$\| \cdot \|_G = \prod_{\lambda \in \Lambda} \| \cdot \|_{G_\lambda}$$

Beweis. Die Behauptung folgt aus 2.1.10. □

2.2 Topologische Eigenschaften der Adele von Quaternionenalgebren

Um die Arithmetik von K bzw. A zu verstehen, werden wir die topologischen Eigenschaften der eingeschränkten direkten Produkte aus 2.1.4 untersuchen.

Das Ziel dieses Abschnittes ist folgender Satz:

Theorem 2.2.1. *Es sei A eine Quaternionenalgebra über einem algebraischen Zahlkörper K . Dann gilt*

1. *Es ist K diskret und kokompakt in $\mathbf{A}_K$.*
2. *Es ist A diskret und kokompakt in $\mathbf{A}_A$.*

Wir stellen zunächst die notwendigen Teilresultate zusammen, und geben einen Beweis von 2.2.1 am Ende des Abschnittes.

Als erstes erinnern wir an die Konstruktion aus 2.1.4(5) und betrachten A als K -Vektorraum und K als $\mathbb{Q}$ -Vektorraum. Wir werden zeigen, dass die Topologien auf $\mathbf{A}_{K/\mathbb{Q}}$ und $\mathbf{A}_{\mathbb{Q}}$ übereinstimmen, womit schon fast alles getan ist, um die Behauptung auf den Fall $K = \mathbb{Q}$ zu reduzieren.

Lemma 2.2.2. *Es sei E ein n -dimensionaler Vektorraum über K . Wir fassen K als Vektorraum über sich selbst auf und bilden $\mathbf{A}_{E/K}$ und $\mathbf{A}_K$ wie in 2.1.4(5). Es ist dann $\mathbf{A}_{E/K}$ ein $\mathbf{A}_K$ -Modul und $\mathbf{A}_{E/K} \cong (\mathbf{A}_K)^n$ ein topologischer Modul-Isomorphismus.*

Beweis. Zunächst ist $\mathbf{A}_{E/K}$ durch komponentenweise Operation ein freier $\mathbf{A}_K$ -Modul. Somit haben wir einen algebraischen stetigen Isomorphismus $f : \mathbf{A}_{E/K} \xrightarrow{\sim} \mathbf{A}_K^n$. Nach 2.1.2 sind $\mathbf{A}_K$ und $\mathbf{A}_{E/K}$ lokalkompakt und nach 2.1.8 ist $\mathbf{A}_K$ σ -kompakt. Somit folgt die Behauptung aus folgendem allgemeinen Prinzip:

Es sei T ein lokalkompakter und σ -kompakter Ring und M ein freier, lokalkompakter topologischer Modul über T mit $\dim_T M = n$. Dann ist M mit T^n topologisch isomorph: Ist nämlich $f : T^n \rightarrow M$ der algebraische Isomorphismus, so ist f stetig, und nach [3, Abstract Harmonic Analysis, Chapter II, (5.29)], auch offen. □

Lemma 2.2.3. *Es sei K ein algebraischer Zahlkörper, L/K eine Körpererweiterung mit $[L : K] = n$ und v eine Stelle von K . Es bezeichne $\mathcal{O}_L$ den Ganzheitsring von L . Wir wählen $\{e_1, \dots, e_n\}$ mit der Eigenschaft $\langle e_1, \dots, e_n \rangle_R = \mathcal{O}_L$ und definieren $\varepsilon_v := \langle e_1, \dots, e_n \rangle_{R_v}$ für $v \in \Omega_f$. Dann existiert ein topologischer Vektorraumisomorphismus ψ_v sodass*

$$L \otimes_K K_v \cong \prod_{w|v}^{\psi_v} L_w, \quad \text{und} \quad \varepsilon_v \cong \prod_{w|v}^{\psi_v} (\mathcal{O}_L)_w$$

gilt, wobei w über alle Stellen von L läuft, die über v liegen.

Beweis. [10, Beweis von Lemma 5.10] Beim Nachlesen, erinnere man sich an den topologischen K_v -Vektorraumisomorphismus $L \otimes_K K_v \cong \prod_{i=1}^n K_v$ aus 1.4.5. $\square$

Proposition 2.2.4. *Es sei L/K eine Körpererweiterung. Dann sind die Konstruktionen aus 2.1.4(3) und 2.1.4(5) als topologische Moduln isomorph. Das heißt $\mathbf{A}_L \cong \mathbf{A}_{L/K}$, wobei:*

$$\mathbf{A}_L = \{x \in \prod_{w \in \Omega(L)} L_w \mid x_w \in (\mathcal{O}_L)_w \text{ für fast alle } w \in \Omega(L)\}$$

$$\mathbf{A}_{L/K} = \{x \in \prod_{v \in \Omega(K)} L \otimes_K K_v \mid x_v \in \varepsilon_v \text{ für fast alle } v \in \Omega(K)\}$$

Beweis. Es folgt aus 2.2.3 und 2.1.5, dass die Abbildung $(\psi_v)_{v \in \Omega(K)}$ aus 2.2.3 ein topologischer $\mathbf{A}_K$ -Modulisomorphismus zwischen $\mathbf{A}_L$ und $\mathbf{A}_{L/K}$ ist. $\square$

Proposition 2.2.5. *Es ist $\mathbb{Q}$ eine diskrete und kokompakte Untergruppe von $\mathbf{A}_{\mathbb{Q}}$.*

Beweis. Wir definieren

$$C := \{x \in \mathbf{A}_{\mathbb{Q}} \mid |x_{v_\infty}|_{v_\infty} \leq \frac{1}{2} \text{ und } |x_v|_v \leq 1 \text{ für alle } v \in \Omega_f\}.$$

Es genügt zu zeigen, dass $C \cap \mathbb{Q} = \{0\}$ und $\mathbf{A}_{\mathbb{Q}} = C + \mathbb{Q}$ gilt. Es sei $x \in C \cap \mathbb{Q}$. Wegen $x \in \mathbb{Z}_v$, für $v \in \Omega_f$ ist $x \in \mathbb{Z}$ und wegen $|x_{v_\infty}|_{v_\infty} \leq \frac{1}{2}$ ist $x = 0$.

Die Identität $\mathbf{A}_{\mathbb{Q}} = C + \mathbb{Q}$ beweisen wir in zwei Schritten. Zunächst zeigen wir, dass für $y \in \mathbf{A}_{\mathbb{Q}}$ ein $\delta \in \mathbb{Q}$ existiert mit $y_v - \delta \in \mathbb{Z}_v$ für $v \in \Omega_f$. Es sei $S \subseteq \Omega_f$ eine endliche Menge sodass $y_v \in \mathbb{Z}_v$ für $v \notin S$. Dann existiert ein $u = u(v) \in \mathbb{Q}$ mit folgender Eigenschaft:

$$y - u \in \mathbb{Z}_v, \text{ für } v \in S \quad \text{und} \quad u \in \mathbb{Z}_v \text{ für } v \notin S.$$

Nun setzen wir $\delta = \sum_{v \in S} u(v)$, womit der erste Schritt gezeigt ist.

Weiters existiert ein $\delta' \in \mathbb{Z}$ sodass $|y_\infty - \delta - \delta'|_\infty \leq \frac{1}{2}$ ist. Weil die Elemente $y_\infty - \delta$ und δ' in $\mathbb{Z}_v$ liegen, erhalten wir:

$$|y_\infty - \delta - \delta'|_\infty \leq \frac{1}{2} \quad \text{und} \quad |y_\infty - \delta - \delta'|_v \leq 1.$$

Somit ist $y = \underbrace{y_\infty - \delta - \delta'}_{\in C} + \underbrace{\delta + \delta'}_{\in \mathbb{Q}}$, womit das Theorem bewiesen ist. $\square$

Beweis von Theorem 2.2.1. 1. In 2.2.5 wurde der Fall $K = \mathbb{Q}$ gezeigt. Den allgemeinen Fall führen wir auf diesen zurück: Es sei $[K : \mathbb{Q}] = n$. Dann erhalten wir aus 2.2.2 und 2.2.4 einen Isomorphismus von topologischen $\mathbf{A}_{\mathbb{Q}}$ -Moduln $\mathbf{A}_K \cong \mathbf{A}_{\mathbb{Q}}^n$. Also gilt $\mathbf{A}_K/K \cong \mathbf{A}_{\mathbb{Q}}^n/\mathbb{Q}^n \cong (\mathbf{A}_{\mathbb{Q}}/\mathbb{Q})^n$, womit $\mathbf{A}_K/K$ kompakt und K diskret in $\mathbf{A}_K$ ist.

2. Aus 2.2.2 erhalten wir einen Isomorphismus von topologischen $\mathbf{A}_K$ -Moduln $\mathbf{A}_A \cong \mathbf{A}_K^4$. Also gilt $\mathbf{A}_A/A \cong \mathbf{A}_K^4/K^4 \cong (\mathbf{A}_K/K)^4$, womit $\mathbf{A}_A/A$ kompakt und A diskret in $\mathbf{A}_A$ ist. $\square$

2.3 Topologische Eigenschaften der Ideale

Wir wollen eine multiplikative Fassung von 2.2.1 beweisen. Es stellt sich jedoch heraus, dass weder K^* kokompakt in $\mathbf{I}_K$ noch A^* kokompakt in $\mathbf{I}_A$ liegt. In diesem Abschnitt liegt eine starke Analogie zwischen algebraischen Zahlkörpern und Quaternionenalgebren vor. Analoge Aussagen werden wir simultan beweisen. Es sei in diesem Abschnitt X ein algebraischer Zahlkörper oder eine Quaternionenalgebra über einem Zahlkörper. Aus 1.4.1 und 1.4.5 wissen wir, dass X_v lokalkompakt ist. Wir beginnen mit folgender Proposition:

Proposition 2.3.1. 1. Die Abbildung $\iota : \mathbf{I}_K \longrightarrow \mathbf{A}_K \times \mathbf{A}_K$, $\iota(x) = (x, x^{-1})$ ist ein topologischer Isomorphismus auf sein Bild.

2. Die Abbildung $\iota : \mathbf{I}_A \longrightarrow \mathbf{A}_A \times \mathbf{A}_A$, $\iota(x) = (x, x^{-1})$ ist ein topologischer Isomorphismus auf sein Bild.

Beweis. Es sei X ein algebraischer Zahlkörper oder eine Quaternionenalgebra über einem solchen und $Y = R$ falls $X = K$ oder $Y = \mathcal{O}$ eine Ordnung, falls $X = A$. Es sei $x \in \mathbf{I}_X$ und

$$\mathcal{U}_x = \left\{ \prod_{v \in \Omega} U_v \mid U_v \text{ offene Umgebungen von } x_v \in X_v \text{ und } U_v = Y_v \text{ für fast alle } v \in \Omega \setminus \Omega_{\infty} \right\}$$

eine Umgebungsbasis von x in $\mathbf{A}_X$. Weiters bezeichne

$$\mathcal{V}_x = \left\{ \prod_{v \in \Omega} V_v \mid V_v \text{ offene Umgebungen von } x_v \in X_v^* \text{ und } V_v = Y_v^* \text{ für fast alle } v \in \Omega \setminus \Omega_{\infty} \right\}$$

eine Umgebungsbasis von x in $\mathbf{I}_X$.

Wir zeigen nun, dass ι stetig ist. Dazu wählen wir ein $V \in \mathcal{V}_x$ und zeigen, dass $\iota(V)$ eine Umgebung von $\iota(x)$ in $\mathbf{A}_X^2$ ist. Es existiert eine endliche Menge $S \supseteq \Omega_{\infty}$ sodass $V = \prod_{v \in S} V_v \times \prod_{v \notin S} Y_v^*$ ist. Weil nach 1.4.7 X_v^* offen in X_v ist, sind die V_v offene Umgebungen von x_v in X_v . Folglich ist $V_1 = \prod_{v \in S} V_v \times \prod_{v \notin S} Y_v$ eine Umgebung von x in $\mathbf{A}_X$ und $V_2 = \prod_{v \in S} V_v^{-1} \times \prod_{v \notin S} Y_v$ eine Umgebung von x^{-1} in $\mathbf{A}_X$. Weil $\mathbf{A}_X \times \mathbf{A}_X$ die Produkttopologie trägt, ist $V_1 \times V_2$ eine Umgebung von (x, x^{-1}) in $\mathbf{A}_X^2$ und $V_1 \times V_2 \cap \iota(\mathbf{I}_X)$ eine Umgebung von $\iota(x)$. Aus $V_1 \times V_2 \cap \iota(\mathbf{I}_X) = \{(y, y^{-1}) \mid y \in V_1, y^{-1} \in V_2\} = \{(y, y^{-1}) \mid \prod_{v \in S} V_v \times \prod_{v \notin S} Y_v^*\} = \iota(V)$ folgt die Behauptung.

Wir zeigen nun, dass $\iota^{-1} : \iota(\mathbf{I}_X) \longrightarrow \mathbf{I}_X$ stetig ist. Wir wählen ein $U = U_1 \times U_2 \in \mathcal{U}_x \times \mathcal{U}_{x^{-1}}$ und zeigen, dass $\iota^{-1}(U)$ eine Umgebung von x in $\mathbf{I}_X$ ist. Es existieren endliche Mengen $S_1, S_2 \supseteq \Omega_{\infty}$ sodass $U_1 = \prod_{v \in S_1} U_{1v} \times \prod_{v \notin S_1} Y_v$ und $U_2 = \prod_{v \in S_2} U_{2v} \times \prod_{v \notin S_2} Y_v$ ist. Es ist $U'_1 = U_1 \cap \iota(\mathbf{I}_X) = \prod_{v \in S_1} U_{1v} \times \prod_{v \notin S_1} Y_v^*$ eine Umgebung von x in $\mathbf{I}_X$ und $U'_2 = U_2 \cap \iota(\mathbf{I}_X) = \prod_{v \in S_2} U_{2v}^* \times \prod_{v \notin S_2} Y_v^*$

eine Umgebung von x^{-1} in $\mathbf{I}_X$. Weiters ist $U = \{(y, y^{-1}) \mid y \in U'_1 \cap U'_2\}$ und $\iota^{-1}(U) = U'_1 \cap U'_2 = \prod_{v \in S_1 \setminus S_2} U_{1v}^* \times \prod_{v \in S_1 \cap S_2} (U_{1v}^* \cap U_{2v}^*) \times \prod_{v \in S_2 \setminus S_1} U_{2v}^* \times \prod_{v \notin S_1 \cup S_2} Y_v^*$ eine Umgebung von x in $\mathbf{I}_X$. $\square$

Wir betrachten die Abbildung:

$$\| \cdot \|_{\mathbf{A}_X} \longrightarrow \mathbb{R}_{\geq 0}, \quad \|x\|_{\mathbf{A}_X} := \prod_{v \in \Omega} \|x\|_{X_v}.$$

Nach 2.1.11 ist die Abbildung $\| \cdot \|_{\mathbf{A}_X} \longrightarrow \mathbb{R}_+^*$ die Modulabbildung der lokalkompakten Gruppe $\mathbf{A}_X$. Wir setzen

$$\mathbf{I}_X^1 := \ker(\| \cdot \|_{\mathbf{A}_X})$$

und in 2.3.3 werden wir sehen, dass X sich kokompakt in $\mathbf{I}_X^1$ einbetten lässt.

Bemerkung 2.3.2. Wir hätten $\mathbf{I}_X^1$ auch definieren können, ohne zu wissen, dass $\| \cdot \|_{\mathbf{A}_X}$ das Produkt der lokalen Modulabbildungen ist.

Theorem 2.3.3. *Es sei A eine Quaternionenalgebra, die eine Divisionsalgebra über einem algebraischen Zahlkörper K ist. Dann gilt*

1. *Es ist K^* kokompakt in $\mathbf{I}_K^1$.*
2. *Es ist A^* kokompakt in $\mathbf{I}_A^1$.*

Beweis. Es sei X ein algebraischer Zahlkörper oder eine quaternionische Divisionsalgebra über einem solchen. Nach der Artin'schen Produktformel, siehe etwa [10, Theorem 5.12], und nach 2.1.9 (2) ist $X^* \subseteq \mathbf{I}_X^1$.

Nun seien $m, M \in \mathbb{R}^+$ und es sei

$$Y := \{y \in \mathbf{I}_X \mid 0 < m \leq \|y\|_{\mathbf{A}_X} \leq M\}.$$

Wir zeigen, dass das Bild von Y unter der natürlichen Projektion in $\mathbf{I}_X/X^*$ kompakt ist. Mit $m = M = 1$ folgt dann die Behauptung.

Nach 2.3.1 hat eine kompakte Menge in $\mathbf{I}_X$ die Form $\{x \in \mathbf{I}_X \mid (x, x^{-1}) \in C \times C'\}$, wobei C und C' kompakte Mengen in $\mathbf{A}_X$ sind. Wir müssen also kompakte Mengen C und C' in $\mathbf{A}_X$ finden, sodass für jedes $y \in Y$ ein $a \in X^*$ existiert mit $ay \in C$ und $y^{-1}a^{-1} \in C'$.

Nach 2.2.1 ist $\mathbf{A}_X/X$ kompakt (und lokalkompakt). Es sei μ ein Haar Maß auf $\mathbf{A}_X/X$. Dann ist $\mu(\mathbf{A}_X/X)$ endlich. Es sei $C'' \subseteq \mathbf{A}_X$ mit $\text{Vol}(C'') \geq \text{Vol}(\mathbf{A}_X/X) \max\{m^{-1}, M\}$ und $C := \{x \in \mathbf{A}_X \mid x = c_1 - c_2 \text{ mit } c_1, c_2 \in C''\}$. Für $y \in Y$ ist $\text{Vol}(C''y^{-1}) > \text{Vol}(\mathbf{A}_X/X)$. Also existieren $c_1, c_2 \in \mathbf{A}_X$ mit $c_2y^{-1} = c_1y^{-1} + a$ für ein $a \in X \setminus \{0\}$: Wäre $a = 0$, dann wäre $c_1 = c_2$. Somit ist $ay \in C$. Wenn wir yC'' statt $C''y^{-1}$ betrachten, erhalten wir $y^{-1}b \in C$, für ein $b \in X$. Weil X eine Divisionsalgebra ist, gilt $a, b \in X \setminus \{0\} = X^*$.

Mit C ist auch C^2 kompakt. Deshalb und weil X diskret ist, ist $C^2 \cap X$ endlich. Aus obigem wissen wir $ab \in C^2 \cap X = \{d_1, \dots, d_n\}$. Als endliche Vereinigung kompakter Mengen ist auch $C' := \bigcup_{i=1}^n Cd_i^{-1}$ kompakt. Somit erhalten wir $ay \in C$ und $y^{-1}a^{-1} \in C'$. $\square$

Es sei S eine endliche Menge mit $\Omega_\infty \subseteq S \subseteq \Omega$. Wir setzten $\mathbf{I}_{K,S}^1 := \mathbf{I}_K^1 \cap \mathbf{I}_{K,S}$, und erhalten:

Korollar 2.3.4. *Es bezeichne A eine quaternionische Divisionsalgebra über einem algebraischen Zahlkörper K . Dann gilt*

1. *Es ist $K^* \cap \mathbf{I}_{K,S}^1$ diskret und kokompakt in $\mathbf{I}_{K,S}^1$.*
2. *Es ist $A^* \cap \mathbf{I}_{A,S}^1$ diskret und kokompakt in $\mathbf{I}_{A,S}^1$.*

Beweis. Es sei $X = K$ oder $X = A$. Aus 2.3.1 und 2.2.1 folgt, dass X^* diskret in $\mathbf{I}_X$ ist. Da $\mathbf{I}_{X,S}$ eine offene Untergruppe von $\mathbf{I}_X$ ist, ist $X^* \cap \mathbf{I}_{X,S}$ auch diskret in $\mathbf{I}_{X,S}$. Wegen $X^* \subseteq \mathbf{I}_X^1$ folgt $X^* \cap \mathbf{I}_{X,S} = X^* \cap \mathbf{I}_{X,S}^1$ und somit ist $X^* \cap \mathbf{I}_{X,S}^1$ diskret in $\mathbf{I}_{X,S}^1$. Aus dem selben Grund ist $\mathbf{I}_{X,S}^1/(X^* \cap \mathbf{I}_{X,S}^1)$ eine offene (und abgeschlossene) Untergruppe von $\mathbf{I}_X^1/X^*$. Aus 2.3.3 folgt die Behauptung. $\square$

Kapitel 3

Einheiten in total definiten Quaternionenalgebren

In diesem Kapitel sei K ein algebraischer Zahlkörper mit $[K : \mathbb{Q}] = n$ und $R = \mathcal{O}_K$ sein Ganzheitsring. Weiters bezeichne $\Omega = \Omega(K)$ die Menge aller Stellen von K , Ω_∞ die Menge der unendlichen Stellen und Ω_f die Menge der endlichen Stellen. Für eine Stelle $v \in \Omega(K)$ bezeichne K_v die Vervollständigung von K bezüglich einem zu v gehörigen Absolutbetrages. Für eine endliche Stelle $v \in \Omega_f(K)$ bezeichnen wir den zu K_v gehörigen Bewertungsring mit R_v . Weiters sei S eine endliche Menge von Stellen mit $\Omega_\infty \subseteq S \subseteq \Omega$.

3.1 Der Dirichlet'sche Einheitensatz für S -Einheiten

Wir erinnern an die folgenden Bezeichnungen

$$\mathbf{A}_{K,S} = \prod_{v \in S} K_v \times \prod_{v \in \Omega \setminus S} R_v, \quad \mathbf{I}_{K,S} = \prod_{v \in S} K_v^* \times \prod_{v \in \Omega \setminus S} R_v^*,$$

$$\mathbf{I}_K^1 := \ker(\|\cdot\|_{\mathbf{A}_K}) = \{x \in \mathbf{A}_K \mid \prod_{v \in \Omega} \|x_v\|_v = 1\},$$

$$\mathbf{I}_{K,S}^1 = \mathbf{I}_K^1 \cap \mathbf{I}_{K,S}$$

und setzen weiters

$$R_S := K \cap \mathbf{A}_{K,S}.$$

Bemerkung 3.1.1. Es gilt:

1. $R_S = \{x \in K \mid x \in R_v \text{ für alle } v \notin S\}$
2. $R_S^* = K^* \cap \mathbf{I}_{K,S} = K^* \cap \mathbf{I}_{K,S}^1$
3. Wir zeigen $R_{S_\infty} = R$:

$R_{S_\infty} \subseteq R$: Es sei $x \in R_{S_\infty}$, dann ist $x \in R_v$ für $v \in \Omega_f$, weil K diagonal in $\mathbf{A}_{K,S}$ liegt. Wegen $R = \bigcap_{v \in \Omega_f} R_v$, siehe 1.3.16 folgt die Behauptung.

$R_{S_\infty} \supseteq R$: Für $x \in R$ gilt offensichtlich $x \in R_v$ für $v \in \Omega_f$.

In diesem Abschnitt werden wir den Dirichlet'schen Einheitensatz für S -Einheiten beweisen:

Theorem 3.1.2. *Es sei S eine endliche Menge von Stellen des Zahlkörpers K mit $\Omega_\infty \subseteq S \subseteq \Omega$. Dann ist $\mu_K := \{\zeta \in K \mid \zeta^l = 1 \text{ für ein } l \in \mathbb{N}\}$ eine Untergruppe von R_S^* und die Einbettung gibt Anlass zu folgender exakter Sequenz von abelschen topologischen Gruppen:*

$$1 \longrightarrow \mu_K \longrightarrow R_S^* \longrightarrow \mathbb{Z}^{|S|-1} \longrightarrow 1.$$

Da $\mathbb{Z}^{|S|-1}$ als $\mathbb{Z}$ -Modul projektiv ist, spaltet diese Sequenz und insbesondere gilt:

$$R_S^* \cong \mu_K \times \mathbb{Z}^{|S|-1}.$$

Wir beginnen mit den Vorbereitungen des Beweises. Dafür brauchen wir ein wenig Notation und vier Lemmata.

Nach 2.1.9 stimmt für $v \in \Omega_f$ die Modulfunktion mit dem v -adischen Absolutbetrag überein. Falls v eine reelle Stelle (bzw. komplexe Stelle) ist, gilt $\|x\|_v = |x|$ (bzw. $\|x\|_v = |x|^2$). Wir setzen für alle Stellen $v \in \Omega$:

$$C_v := \{y \in K_v \mid \|y\|_v = 1\}, \quad \text{und} \quad C := \prod_{v \in \Omega} C_v.$$

Für $v \in \Omega_\infty$ ist $C_v = [-1, 1]$ oder $C_v = S^1$ und somit kompakt. Für $v \in \Omega_f$ ist nach 1.4.5 $C_v = \{y \in R_v \mid \|y\|_v = 1\} = R_v^*$ kompakt. Somit ist C kompakt in der Produkttopologie. Nach 2.1.3 ist C kompakt in $\mathbf{I}_K$.

Lemma 3.1.3. *Es sei $\mu_K = \{\zeta \in K \mid \zeta^l = 1 \text{ für ein } l \in \mathbb{N}\}$. Dann gilt:*

$$C \cap K^* = \text{Tor}(R_S^*) = \mu_K.$$

Beweis. Offensichtlich ist $\text{Tor}(R_S^*) = \mu_K$. Es bleibt die erste Gleichheit zu zeigen. Wir beginnen mit folgender Behauptung:

$$C \cap K^* = \{x \in R_S \mid \|x\|_v = 1 \text{ für alle } v \in \Omega\}$$

Es ist $x \in C \cap K^* \iff x \in C_v$ für alle $v \in \Omega \iff x \in R_S$ und $\|x\|_v = 1$ für alle $v \in \Omega$. Die letzte Äquivalenz folgt aus $R = \bigcap_{v \in \Omega_f} R_v$, siehe 1.3.16 und 3.1.1.

1. $C \cap K^* \subseteq \text{Tor}(R_S^*)$: Weil C kompakt und K^* diskret in $\mathbf{I}_K$ ist, ist $C \cap K^*$ eine endliche Untergruppe von K^* . Nach obigem liegt diese in R_S^* .
2. $\mu_K \subseteq C \cap K^*$: Es sei $v \in \Omega$ und $x \in \mu_K$, also $x^l = 1$ für ein $l \in \mathbb{N}$. Wegen $\|1\|_v = 1$ ist $\|x\|_v^n = 1$. Und weil $\| \cdot \|_v$ nur positive Werte annimmt, folgt $\|x\|_v = 1$.

□

Lemma 3.1.4. *Es sei*

$$1 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 1$$

eine exakte Sequenz von Gruppen und $U \triangleleft A$ ein Normalteiler. Dann ist auch die folgende Sequenz exakt:

$$1 \longrightarrow A \cap U \xrightarrow{f} B \cap f(U) \xrightarrow{g} C \cap g(f(U)) \longrightarrow 1$$

Beweis. Zunächst ist die Einschränkung einer injektiven Abbildung wieder injektiv. Die Exaktheit an der Stelle $B \cap f(U)$ folgt aus:

$$\text{Im}(f|_U) = \ker(g) \cap f(U) = \ker(g|_{f(U)}).$$

Auch die Surjektivität der Abbildung $g|_{f(U)} : B \cap f(U) \longrightarrow C \cap g(f(U))$ ist offensichtlich. $\square$

Lemma 3.1.5. *Wir betrachten die natürliche Projektion*

$$\mathbf{I}_{K,S} = \prod_{v \in S} K_v^* \times \prod_{v \in \Omega \setminus S} R_v^* \xrightarrow{p} \prod_{v \in S} K_v^*/C_v,$$

und den stetigen Gruppenhomomorphismus:

$$f : \prod_{v \in S} K_v^*/C_v \longrightarrow \mathbb{R}_{\geq 0}, \quad f(x) := \prod_{v \in S} \|x_v\|_v.$$

Dann liegt $L = p(K^ \cap \mathbf{I}_{K,S}^1)$ diskret und kokompakt in $\ker(f)$.*

Beweis. Weil nach Definition der v -adischen Bewertung, für fast alle $v \in \Omega_f$ $\|x\|_v = 1$ gilt, können wir folgende Abbildung betrachten:

$$F : \mathbf{I}_{K,S} \longrightarrow \mathbb{R}_{\geq 0}, \quad F(x) := \prod_{v \in \Omega} \|x_v\|_v.$$

Wegen $F(C) = 1$ faktorisiert F zu einer Abbildung

$$f : \prod_{v \in S} K_v^*/C_v \longrightarrow \mathbb{R}_{\geq 0}$$

.

$$\begin{array}{ccc} \mathbf{I}_{K,S} & \xrightarrow{F} & \mathbb{R}_{\geq 0} \\ \downarrow p & \nearrow \exists! f & \\ \prod_{v \in S} K_v^*/C_v & & \end{array}$$

Es ist $f(p(K^* \cap \mathbf{I}_{K,S}^1)) = F(K^* \cap \mathbf{I}_{K,S}^1) = 1$ also erhalten wir $L \subseteq \ker(f)$. Weil nach 2.3.4 $K^* \cap \mathbf{I}_{K,S}^1$ diskret in $\mathbf{I}_{K,S}^1$ ist und p offen ist, ist auch $L = p(K^* \cap \mathbf{I}_{K,S}^1)$ diskret in $\ker(f)$. In 2.3.4

haben wir gezeigt, dass $\mathbf{I}_{K,S}^1/(K^* \cap \mathbf{I}_{K,S}^1)$ kompakt ist. Wegen $\ker(f) = p(\mathbf{I}_{K,S}^1)$ erhalten wir eine Isomorphie topologischer Gruppen

$$\ker(f)/L = (I_{K,S}^1/C) / ((K^* \cap \mathbf{I}_{K,S}^1)/C) \cong I_{K,S}^1/(K^* \cap I_{K,S}^1),$$

womit das Lemma bewiesen ist. $\square$

Lemma 3.1.6. *Wir notieren mit $r > 0$ die Anzahl der archimedischen Stellen von K und betrachten den stetigen Gruppenhomomorphismus*

$$\lambda : \mathbb{R}^r \times \mathbb{Z}^{|S|-r} \longrightarrow \mathbb{R}, \quad \lambda((x_l)_{1 \leq l \leq |S|}) = \sum_{1 \leq l \leq |S|} x_l.$$

Es sei Γ eine diskrete, kokompakte Untergruppe von $\ker(\lambda)$. Dann gilt $\Gamma \cong \mathbb{Z}^{|S|-1}$.

Beweis. Wir betrachten die Fortsetzung von λ auf $\mathbb{R}^{|S|}$:

$$\lambda' : \mathbb{R}^{|S|} \longrightarrow \mathbb{R}, \quad \lambda'((x_l)_{1 \leq l \leq |S|}) = \sum_{1 \leq l \leq |S|} x_l.$$

Als topologische Gruppe ist $\ker(\lambda')$ zu $\mathbb{R}^{|S|-1}$ isomorph und es gilt $\ker(\lambda) = \ker(\lambda') \cap \mathbb{R}^r \times \mathbb{Z}^{|S|-r} \cong \mathbb{R}^{r-1} \times \mathbb{Z}^{|S|-r}$.

Es liegt Γ diskret in $\ker(\lambda')$. Weil Γ kokompakt in $\ker(\lambda)$ liegt, existiert eine kompakte Menge F mit $\Gamma + F = \mathbb{R}^{r-1} \times \mathbb{Z}^{|S|-r}$. Wir setzen $F' = F + \{0\}^{r-1} \times [0, 1]^{|S|-r}$ und erhalten wegen $\Gamma + F' = \mathbb{R}^{|S|-1}$, dass Γ kokompakt in $\mathbb{R}^{|S|-1}$ liegt. Somit gilt $\Gamma \cong \mathbb{Z}^{|S|-1}$, siehe etwa [2, Seite 44]. $\square$

Beweis von Theorem 3.1.2. Wegen $C_v = R_v^*$ für $v \notin S$, erhalten wir folgende kurze exakte Sequenz topologischer Gruppen:

$$1 \longrightarrow C \xrightarrow{i} \mathbf{I}_{K,S} \xrightarrow{p} \prod_{v \in S} K_v^*/C_v \longrightarrow 1,$$

wobei i die kanonische Inklusion und p die natürliche Projektion bezeichnet.

Wenn wir die Terme in obiger exakter Sequenz mit K^* schneiden, ergibt sich mit $L = p(K^* \cap \mathbf{I}_{K,S}^1)$ und wegen $C \cap K^* \cong \mu_K$ und $R_S^* = K^* \cap \mathbf{I}_{K,S} = K^* \cap \mathbf{I}_{K,S}^1$ die folgende exakte Sequenz:

$$1 \longrightarrow \mu_K \xrightarrow{i} R_S^* \xrightarrow{p} L \longrightarrow 1.$$

Zu zeigen bleibt $L \cong \mathbb{Z}^{|S|-1}$. Für $v \in S$ ist

$$K_v^*/C_v \cong \begin{cases} \mathbb{R}_{\geq 0} \cong \mathbb{R} & \text{falls } v \text{ archimedisch,} \\ \mathbb{Z} & \text{falls } v \text{ nichtarchimedisch.} \end{cases}$$

Nun bezeichne r die Anzahl der archimedischen Stellen und s die Anzahl der nichtarchimedischen Stellen von K in S . Somit erhalten wir einen Isomorphismus topologischer Gruppen

$$(\|\cdot\|_v)_{v \in S} : \prod_{v \in S} K_v^*/C_v \xrightarrow{\sim} \mathbb{R}^r \times \mathbb{Z}^s.$$

Wir betrachten das kommutative Diagramm,

$$\begin{array}{ccc}
\prod_{v \in S} K_v^*/C_v & \xrightarrow{f(x) = \prod_{v \in S} \|x_v\|_v} & (\mathbb{R}_{\geq 0}, *) \\
\downarrow (\|x_v\|_v)_{v \in S} & & \downarrow \log \\
\mathbb{R}^r \times \mathbb{Z}^{|S|-r} & \xrightarrow{\lambda((x_l)_{1 \leq l \leq |S|}) = \sum_{1 \leq l \leq |S|} x_l} & (\mathbb{R}, +)
\end{array}$$

wobei die beiden vertikalen Abbildungen Isomorphismen topologischer Gruppen sind. Aus 3.1.5 und 3.1.6 erhält man $L \cong \mathbb{Z}^{|S|-1}$, und somit die gewünschte exakte Sequenz:

$$1 \longrightarrow \mu_K \longrightarrow R_S^* \longrightarrow \mathbb{Z}^{|S|-1} \longrightarrow 1.$$

□

Bemerkung 3.1.7. In obigem Beweis waren folgende Zwischenschritte entscheidend:

1. Für $v \in \Omega_\infty$ ist $C_v := \{y \in K_v \mid \|y\|_v = 1\}$ kompakt.
2. Für $v \in \Omega_f$ ist $C_v = \{y \in R_v \mid \|y\|_v = 1\} = R_v^*$.
3. Die Abbildung $F : \mathbf{I}_{K,S} \longrightarrow \mathbb{R}_{\geq 0}$, $F(x) = \prod_{v \in \Omega} \|x_v\|_v$ ist wohldefiniert und $F(C) = 1$.
4. Für $v \in S$ ist

$$K_v^*/C_v \cong \begin{cases} \mathbb{R}_{\geq 0} & \text{falls } v \text{ archimedisch,} \\ \mathbb{Z} & \text{falls } v \text{ nichtarchimedisch.} \end{cases}$$

3.2 Eine Verallgemeinerung des Dirichlet'schen Einheitensatzes auf total definite Quaternionenalgebren

Definition 3.2.1. Eine Quaternionenalgebra A über K erfüllt die *Eichlerbedingung*, falls A an zumindest einer archimedischen Stelle spaltet. Quaternionenalgebren, die nicht die Eichlerbedingung erfüllen, also an allen archimedischen Stellen verzweigen, nennen wir auch *total definit*.

Es sei $\text{Ram}(A) \subseteq \Omega$ die Menge aller Stellen von K , an denen A verzweigt. In diesem Abschnitt sei A eine total definite Quaternionenalgebra, d.h.: $\Omega_\infty \subseteq \text{Ram} A$. Weiters sei S eine endliche Menge von Stellen mit folgender Eigenschaft:

$$\Omega_\infty \subseteq S \subseteq \text{Ram}(A) \subseteq \Omega.$$

Wenn der Zahlkörper K komplexe Stellen besitzt, erfüllt nach 1.2.1 jede Quaternionenalgebra A die Eichlerbedingung. Es genügt also Zahlkörper zu betrachten, deren archimedische Stellen reell sind.

Bemerkung 3.2.2. Es sei $\mathcal{O}$ eine R -Ordnung. Dann gilt:

1. Durch komponentenweise Operation ist $\mathcal{O}_S := A \cap \mathbf{A}_{A,S}$ eine R_S -Ordnung.

2. $\mathcal{O}_S = \{x \in A \mid x \in \mathcal{O}_v \text{ für alle } v \notin S\}$

3. $\mathcal{O}_S^* = A^* \cap \mathbf{I}_{A,S} = A^* \cap \mathbf{I}_{A,S}^1$

4. Wir zeigen $\mathcal{O}_{S_\infty} = \mathcal{O}$:

$\mathcal{O}_{S_\infty} \subseteq \mathcal{O}$: Es sei $x \in \mathcal{O}_{S_\infty}$, dann ist $x \in \mathcal{O}_v$ für $v \in \Omega_f$, weil A diagonal in $\mathbf{A}_{A,S}$ liegt.

Wegen $\mathcal{O} = \bigcap_{v \in \Omega_f} \mathcal{O}_v$, siehe 1.3.16 folgt die Behauptung.

$\mathcal{O} \subseteq \mathcal{O}_{S_\infty}$: Für $x \in \mathcal{O}$ gilt offensichtlich $x \in \mathcal{O}_v$ für $v \in \Omega_f$.

Wir wollen folgenden Satz beweisen:

Theorem 3.2.3 (Hauptsatz). *Es sei A eine total definite Quaternionenalgebra und $\mathcal{O}$ eine R -Ordnung in A . Weiters sei S eine endliche Menge von Stellen von K mit $\Omega_\infty \subseteq S \subseteq \text{Ram}(A) \subseteq \Omega$. Dann ist $E = \text{Tor}(\mathcal{O}_S^*)$ eine endliche Untergruppe der reellen hamiltonschen Quaternionen, und gibt Anlass zu einer exakten Sequenz von topologischen Gruppen:*

$$1 \longrightarrow E \longrightarrow \mathcal{O}_S^* \longrightarrow \mathbb{Z}^{|\Omega|-1} \longrightarrow 1.$$

Wir beginnen mit den Vorbereitungen des Beweises. Dieser verläuft im wesentlichen analog zu 3.1.2.

Wir setzen :

$$B_v := \begin{cases} \{y \in A_v \mid \|y\|_{A_v} = 1\} & \text{falls } v \in S, \\ \{y \in \mathcal{O}_v \mid \|y\|_{A_v} = 1\} & \text{falls } v \in \Omega \setminus S. \end{cases}$$

Für $v \in S$ ist A_v eine Divisionsalgebra, und daher B_v nach 1.4.3 und 2.1.9 kompakt. Für $v \in \Omega \setminus S$ zeigen wir $B_v = \mathcal{O}_v^*$:

$\mathcal{O}_v^* \subseteq B_v$: Es sei μ ein Haar-Maß auf der lokalkompakten Gruppe A_v . Weil $\mathcal{O}_v$ kompakt und nicht leer ist, ist $\mu(\mathcal{O}_v) \neq 0$. Da für $x \in \mathcal{O}_v^*$, $x\mathcal{O}_v = \mathcal{O}_v$ gilt, folgt die Behauptung aus $\|x\|\mu(\mathcal{O}_v) = \mu(x\mathcal{O}_v)$.

$B_v \subseteq \mathcal{O}_v^*$: Nach Definition gilt $\|y\|_{A_v} = 0$ für $y \in \mathcal{O}_v \setminus \mathcal{O}_v^*$.

Somit ist auch für $v \in \Omega \setminus S$ nach 1.4.7 B_v kompakt und daher

$$B := \prod_{v \in \Omega} B_v$$

kompakt in der Produkttopologie. Nach 2.1.3 ist B kompakt in $\mathbf{I}_A$.

Lemma 3.2.4. *Es ist $B \cap A^* = \text{Tor}(\mathcal{O}_S^*)$ die Torsionsgruppe von $\mathcal{O}_S^*$. Diese ist isomorph zu einer endlichen Untergruppe der reellen Quaternionen $\mathbb{H}^*$.*

Beweis. Zunächst zeigen wir:

$$B \cap A^* = \{x \in \mathcal{O}_S^* \mid \|x\|_{A_v} = 1 \text{ für alle } v \in \Omega\}.$$

Es ist $x \in B \cap A^* \iff x \in B_v$ für alle $v \in \Omega \iff x \in \mathcal{O}_S^*$ und $\|x\|_{A_v} = 1$ für alle $v \in \Omega$. Die letzte Äquivalenz folgt aus $\mathcal{O}_S = \bigcap_{v \in S} \mathcal{O}_v$, siehe 1.3.16 und 3.2.2.

1. $B \cap A^* \subseteq \text{Tor}(\mathcal{O}_S^*)$: Aus obiger Identität folgt $B \cap A^* \subseteq \mathcal{O}_S^*$. Weil B kompakt und A^* diskret in $\mathbf{I}_A$ ist, ist $B \cap A^*$ eine endliche Untergruppe von $\mathcal{O}_S^*$, womit jedes Element endliche Ordnung hat.
2. $\text{Tor}(\mathcal{O}_S^*) \subseteq B \cap A^*$: Es sei $x \in \mathcal{O}_S^*$ mit $x^l = 1$ für ein $l \in \mathbb{N}$. Wegen $\|1\|_{A_v} = 1$ ist $\|x\|_{A_v}^n = 1$. Nach 2.1.9 ist für $v \in \Omega$ $\| \cdot \|_{A_v} = \|n(\cdot)\|_{K_v}^2$, sodass $\| \cdot \|_{A_v}$ für $v \in \Omega$ nur positive Werte annimmt. Es folgt $\|x\|_{A_v} = 1$.

Weil der Durchschnitt zweier Untergruppen wieder eine Untergruppe ist, ist $B \cap A^*$ eine endliche Untergruppe von $A^* \subseteq A_v^*$ für $v \in \Omega_\infty$. Somit können wir $B \cap A^*$ als Untergruppe von $\mathbb{H}^*$ auffassen. $\square$

Lemma 3.2.5. *Es sei wie in vorherigem Abschnitt $C_v = \{y \in K_v \mid \|y\|_v = 1\}$. Dann ist für $v \in S$ die Abbildung*

$$g : A_v^*/B_v \longrightarrow K_v^*/C_v, \quad g(xB_v) := n(x)C_v$$

ein topologischer Gruppenisomorphismus.

Beweis. Zunächst zeigen wir

$$n(B_v) = C_v.$$

$n(B_v) \subseteq C_v$: Mit $x \in n(B_v)$ ist offensichtlich auch $x \in C_v$

$C_v \subseteq n(B_v)$: Es sei $x \in C_v$. Dann ist auch $\bar{x} = x \in C_v$ und nach 2.1.9 ist $\|x\|_{A_v} = \|n(x)\|_{K_v}^2 = \|\bar{x}\|_{K_v}^2 \|x\|_{K_v}^2 = 1$.

Nun widmen wir uns der Abbildung g : Es seien $x_1, x_2 \in A_v$. Dann ist

$$x_1 B_v = x_2 B_v \iff x_1 x_2^{-1} \in B_v \iff n(x_1 x_2^{-1}) \in n(B_v) = C_v \iff$$

$$n(x_1)C_v = n(x_2)C_v \iff g(x_1) = g(x_2),$$

und g somit wohldefiniert und injektiv. Weil n multiplikativ ist, ist g ein Gruppenhomomorphismus. Nun genügt es zu zeigen, dass $n : A_v^* \longrightarrow K_v^*$ surjektiv ist. Da A total definit ist, ist für $v \in \Omega_\infty \cap S$ $A_v \cong \mathbb{H}$ und die Surjektivität von n folgt aus $\mathbb{R}_{>0} \supseteq n(\mathbb{H}^*) \supseteq n(\mathbb{R}) \supseteq \mathbb{R}_{>0}$. Für $v \in \Omega_f \cap S$ ist der Beweis komplizierter. Man kann ihn unter [8, Seite 219] nachlesen. $\square$

Lemma 3.2.6. *Wir betrachten die natürliche Projektion*

$$\mathbf{I}_{A,S} = \prod_{v \in S} A_v^* \times \prod_{v \in \Omega \setminus S} \mathcal{O}_v^* \xrightarrow{p} \prod_{v \in S} A_v^*/B_v,$$

und den stetigen Gruppenhomomorphismus:

$$f : \prod_{v \in S} A_v^*/B_v \longrightarrow \mathbb{R}_{\geq 0}, \quad f(x) := \prod_{v \in S} \|x_v\|_{A_v}.$$

Dann liegt $L = p(A^ \cap \mathbf{I}_{A,S}^1)$ diskret und kokompakt in $\ker(f)$.*

Beweis. Weil nach Definition der v -adischen Bewertung und 2.1.9, für fast alle $v \in \Omega_f$ $\|x\|_{A_v} = 1$ gilt, können wir folgende Abbildung betrachten:

$$F : \mathbf{I}_{A,S} \longrightarrow \mathbb{R}_{\geq 0}, \quad F(x) := \prod_{v \in \Omega} \|x_v\|_{A_v}.$$

Wegen $F(B) = 1$ faktorisiert F zu einer Abbildung

$$f : \prod_{v \in S} A_v^*/B_v \longrightarrow \mathbb{R}_{\geq 0}$$

$$\begin{array}{ccc} \mathbf{I}_{A,S} & \xrightarrow{F} & \mathbb{R}_{\geq 0} \\ \downarrow p & \searrow \exists! f & \\ \prod_{v \in S} A_v^*/B_v & & \end{array}$$

Es ist $f(p(A^* \cap \mathbf{I}_{A,S}^1)) = F(A^* \cap \mathbf{I}_{A,S}^1) = 1$ also erhalten wir $L \subseteq \ker(f)$. Weil nach 2.3.4 $A^* \cap \mathbf{I}_{A,S}^1$ diskret in $\mathbf{I}_{A,S}^1$ ist, und p offen ist, ist auch $L = p(A^* \cap \mathbf{I}_{A,S}^1)$ diskret in $\ker(f)$.

Nach 1.2.4 ist mit A_v auch A eine Divisionsalgebra und daher ist nach 2.3.4 $\mathbf{I}_{A,S}^1/(A^* \cap \mathbf{I}_{A,S}^1)$ kompakt. Wegen $\ker(f) = p(\mathbf{I}_{A,S}^1)$ erhalten wir eine Isomorphie topologischer Gruppen

$$\ker(f)/L = (\mathbf{I}_{A,S}^1/B) / ((A^* \cap \mathbf{I}_{A,S}^1)/B) \cong \mathbf{I}_{A,S}^1/(A^* \cap \mathbf{I}_{A,S}^1),$$

womit das Lemma bewiesen ist. □

Beweis von Theorem 3.2.3. Wir gehen analog zu 3.1.2 vor: Wegen $B_v = \mathcal{O}_v^*$ für $v \notin S$, erhalten wir folgende kurze exakte Sequenz topologischer Gruppen:

$$1 \longrightarrow B \xrightarrow{i} \mathbf{I}_{A,S} \xrightarrow{p} \prod_{v \in S} A_v^*/B_v \longrightarrow 1,$$

wobei i die kanonische Einbettung und p die natürliche Projektion bezeichnet.

Wenn wir die Terme in obiger exakter Sequenz mit A^* schneiden, ergibt sich mit $L = p(A^* \cap \mathbf{I}_{A,S})$ und $E = B \cap A^*$ und mit $\mathcal{O}_S^* = A^* \cap \mathbf{I}_{A,S} = A^* \cap \mathbf{I}_{A,S}^1$ folgende exakte Sequenz:

$$1 \longrightarrow E \xrightarrow{i} \mathcal{O}_S^* \xrightarrow{p} L \longrightarrow 1.$$

Zu zeigen bleibt $L \cong \mathbb{Z}^{|S|-1}$. Nach 3.2.5 gilt für $v \in S$:

$$A_v^*/B_v \xrightarrow{n} K_v^*/C_v \xrightarrow{\|\cdot\|_v} \begin{cases} \mathbb{R}_{\geq 0} \xrightarrow{\log} \mathbb{R} & \text{falls } v \text{ archimedisch,} \\ \mathbb{Z} & \text{falls } v \text{ nichtarchimedisch.} \end{cases}$$

Es bezeichne nun r die Anzahl der archimedischen Stellen und s die Anzahl der nichtarchimedischen Stellen von K in S . Somit erhalten wir einen Isomorphismus topologischer Gruppen $(\|n(\cdot)\|_v)_{v \in S} : \prod_{v \in S} A_v^*/B_v \xrightarrow{\sim} \mathbb{R}^r \times \mathbb{Z}^s$.

Aus 3.2.6 und 3.1.6 erhält man wie im Beweis von 3.1.2 $L \cong \mathbb{Z}^{|S|-1}$, und somit die gewünschte exakte Sequenz:

$$1 \longrightarrow E \longrightarrow \mathcal{O}_S^* \longrightarrow \mathbb{Z}^{|S|-1} \longrightarrow 1.$$

□

3.3 Interpretation des Hauptsatzes

Wir übernehmen alle Voraussetzungen und die Notation aus Abschnitt 3.2.

Der Hauptsatz in Abschnitt 3.2 verallgemeinert den Dirichlet'schen Einheitensatz auf total definite Quaternionenalgebren. Die Rolle von μ_K wird durch eine endliche Untergruppe der reellen Quaternionen eingenommen. Diese sind bekannt:

Theorem 3.3.1. *Die endlichen Untergruppen von $\mathbb{H}^*$ sind konjugiert zu einer der folgenden Gruppen:*

1. $\mu_m(\mathbb{C}) = \langle s_m := e^{\frac{2\pi i}{m}} \rangle = \{e^{\frac{2\pi i l}{m}} \mid l \in \mathbb{N}\}$ für ein $m \in \mathbb{N}$.
2. $D_{2m} := \langle s_{2m}, j \rangle$ für ein $m \in \mathbb{N}$.
3. $E_{24} := \{\pm 1, \pm i, \pm j, \pm k, \frac{\pm 1 \pm i \pm j \pm k}{2}\}$.
4. $E_{48} := E_{24} \cup \left\{ \frac{x}{\sqrt{2}} \mid x = a \pm b, a, b \in \{1, i, j, k\} \right\}$.
5. $E_{120} := E_{24} \cup \left\{ \frac{x}{2} \mid x = ab, a \in E_{24}, b \in \left\{ \tau := \frac{1+\sqrt{5}}{2}, i + \tau j + \frac{ij}{\tau} \right\} \right\}$.

Beweis. [12, Seite 17] oder [13, Theorem 5].

□

Ohne Beschränkung der Allgemeinheit werden wir im restlichen Text die endlichen Untergruppen von $\mathbb{H}^*$ mit einer der obigen fünf Gruppen identifizieren.

In 3.1.2 haben wir eine spaltende, kurze exakte Sequenz abelscher Gruppen erhalten. Weil diese Gruppen kommutativ waren, ist dann R_S^* isomorph zu $\mu_K \times \mathbb{Z}^{|S|-1}$, also ein direktes Produkt seiner Torsionsgruppe mit einer freien Gruppe vom Rang $|S| - 1$. Im folgenden werden wir uns überlegen, dass dies für die Sequenz aus 3.2.3 im allgemeinen nicht mehr gilt.

Bemerkung 3.3.2. Es bezeichne $\cdot$ die Multiplikation in der Algebra A . Das Produkt zweier Untergruppen H_1, H_2 von $(A^*, \cdot)$ heißt direkt, falls der kanonische Epimorphismus $H_1 \times H_2 \longrightarrow H_1 \cdot H_2$, $(a, b) \mapsto a \cdot b$, ein Gruppenisomorphismus ist. Falls H_1, H_2 Normalteiler sind, ist das Produkt $H_1 \cdot H_2$ genau dann direkt, wenn $H_1 \cap H_2 = \{1\}$ ist.

Bemerkung 3.3.3. Aus 3.2.3 folgt, dass $[\mathcal{O}_S^* : \text{Tor}(\mathcal{O}_S^*) \cdot R_S^*] < \infty$ gilt.

Beweis. Zunächst existieren nach 3.2.3 $d_1, \dots, d_{|S|-1} \in \mathcal{O}_S^*$ und $e_1, \dots, e_{|S|-1} \in R_S^*$ mit

$$\mathcal{O}_S^* = \text{Tor}(\mathcal{O}_S^*) \cdot \langle d_1, \dots, d_{|S|-1} \rangle_{\mathbb{Z}} \quad \text{und} \quad R_S^* = \text{Tor}(R_S^*) \cdot \langle e_1, \dots, e_{|S|-1} \rangle_{\mathbb{Z}}.$$

Die kanonische Abbildung:

$$\varphi : \langle d_1, \dots, d_{|S|-1} \rangle_{\mathbb{Z}} \longrightarrow \text{Tor}(\mathcal{O}_S^*) \cdot \langle d_1, \dots, d_{|S|-1} \rangle_{\mathbb{Z}} / \text{Tor}(\mathcal{O}_S^*) \cdot \langle e_1, \dots, e_{|S|-1} \rangle_{\mathbb{Z}}$$

ist ein Epimorphismus mit $\langle e_1, \dots, e_{|S|-1} \rangle_{\mathbb{Z}} \subseteq \ker(\varphi)$. Also ist $\text{rg}(\ker(\varphi)) = |S| - 1$ und $[\mathcal{O}_S^* : \text{Tor}(\mathcal{O}_S^*) \cdot R_S^*] = |\langle d_1, \dots, d_{|S|-1} \rangle_{\mathbb{Z}} / \ker(\varphi)| < \infty$. $\square$

Genauer kann man mit gruppentheoretischen Methoden folgendes Theorem zeigen:

Theorem 3.3.4. *Wir verwenden die Notation aus 3.3.1. Dann ist*

$$l = [\mathcal{O}_S^* : \text{Tor}(\mathcal{O}_S^*) \cdot R_S^*] \in \{1, 2, 4\}.$$

Es ist $l = 4$, falls $\text{Tor}(\mathcal{O}_S^*) = \langle s_{2m} \rangle$ und zwei Einheiten $e_1, e_2 \in \mathcal{O}_S^*$ mit folgenden Eigenschaften existieren:

1. $n(e_1), n(e_2) \notin K^{*^2}$
2. falls $m = 1$: $e_1 e_2 = -e_2 e_1$
3. falls $m \neq 1$: $e_1 \in K(s_{2m})$ und $e_2 s_{2m} = s_{2m}^{-1} e_2$

Es ist $l = 2$, falls $l \neq 4$ und eine Einheit $e_1 \in \mathcal{O}_S^*$ mit folgenden Eigenschaften existiert:

1. $n(e_1) \notin K^{*^2}$
2. falls $\text{Tor}(\mathcal{O}_S^*) = \langle s_{2m} \rangle$ für ein $m \in \mathbb{N}$: $e_1 \in K(s_{2m})$ oder $e_1 s_{2m} = s_{2m}^{-1} e_1$
3. falls $\text{Tor}(\mathcal{O}_S^*) = D_{2m}$ für ein $m \in \mathbb{N}$: $e_1 \in (1 + s_{2m})K^*$
4. falls $\text{Tor}(\mathcal{O}_S^*) = E_{24}$: $e_1 \in (1 + i)K^*$

Es ist $l = 1$, in allen anderen Fällen.

Beweis. Wir geben lediglich eine Skizze. Wir lassen A^* wie folgt auf A operieren.

$$A^* \times A \longrightarrow A, \quad (a, x) \mapsto axa^{-1}.$$

Nun bezeichne W eine der Gruppen aus 3.3.1. Dann ergibt sich:

$$\mathcal{O}_S^* \subseteq \{a \in A^* \mid aWa^{-1} = W\} := \mathcal{Z}.$$

Die Menge $\mathcal{Z}$ lässt sich (in Abhängigkeit von W) berechnen, vgl. [13, proposition 6]. Weiters lässt sich der Index $[\mathcal{Z} : W \cdot R_S^*]$ berechnen und man kann auf $[\mathcal{O}_S^* : \text{Tor}(\mathcal{O}_S^*) \cdot R_S^*]$ schließen vgl. [13, Theorem 6]. $\square$

Proposition 3.3.5. *Es gilt:*

1. $[\mathcal{O}_S^* : \text{Tor}(\mathcal{O}_S^*) \cdot R_S^*] = 1 \implies \mathcal{O}_S^* \cong \text{Tor}(\mathcal{O}_S^*) \times \mathbb{Z}^{|S|-1}$
2. $[\mathcal{O}_S^* : \text{Tor}(\mathcal{O}_S^*) \cdot R_S^*] = 4 \implies \mathcal{O}_S^* \not\cong \text{Tor}(\mathcal{O}_S^*) \times \mathbb{Z}^{|S|-1}$

Also ist $\mathcal{O}_S^*$ im allgemeinen kein direktes Produkt seiner Torsionsgruppe mit einer freien Gruppe vom Grad $|S| - 1$.

Beweis. 1. Es existieren nach 3.2.3 $e_1, \dots, e_{|S|-1} \in R_S^*$ mit $R_S^* = \text{Tor}(R_S^*) \cdot \langle e_1, \dots, e_{|S|-1} \rangle_{\mathbb{Z}}$. Als Kern der natürlichen Projektion ist $\text{Tor}(\mathcal{O}_S^*)$ ein Normalteiler in $\mathcal{O}_S^*$.

Weil $\langle e_1, \dots, e_{|S|-1} \rangle_{\mathbb{Z}} \subseteq K$ nach 1.1.3 mit allen Elementen aus A kommutiert, ist auch $\langle e_1, \dots, e_{|S|-1} \rangle_{\mathbb{Z}}$ ein Normalteiler in $\mathcal{O}_S^*$. Aus $\text{Tor}(\mathcal{O}_S^*) \cap \langle e_1, \dots, e_{|S|-1} \rangle_{\mathbb{Z}} = \{1\}$ und aus

$$\text{Tor}(\mathcal{O}_S^*) \cdot R_S^* = \text{Tor}(\mathcal{O}_S^*) \cdot (\text{Tor}(R_S^*) \cdot \langle e_1, \dots, e_{|S|-1} \rangle_{\mathbb{Z}}) = \text{Tor}(\mathcal{O}_S^*) \cdot \langle e_1, \dots, e_{|S|-1} \rangle_{\mathbb{Z}},$$

erhalten wir mit 3.3.2 einen topologischen Gruppenisomorphismus:

$$\mathcal{O}_S^* = \text{Tor}(\mathcal{O}_S^*) \cdot R_S^* \cong \text{Tor}(\mathcal{O}_S^*) \times \mathbb{Z}^{|S|-1}.$$

2. Indirekt angenommen $\mathcal{O}_S^* \cong \text{Tor}(\mathcal{O}_S^*) \times \mathbb{Z}^{|S|-1}$. Dann ist nach 3.3.4 $\text{Tor}(\mathcal{O}_S^*) = \langle s_{2m} \rangle$ zyklisch und daher $\mathcal{O}_S^*$ abelsch. Das ergibt einen Widerspruch zu (2) und (3) in 3.3.4. $\square$

Beispiel 3.3.6. Es sei $K = \mathbb{Q}(\sqrt{d})$ für eine positive ganze quadratfreie Zahl d . In 1.2.7 haben wir gesehen, dass $A := (-1, -1|K)$ total definit ist.

1. Es sei $d = 2$, $S = \Omega_{\infty}$ und somit $\mathcal{O}_S^* = \mathcal{O}^*$. Nach 1.3.13 ist folgende Menge eine Ordnung in A :

$$\mathcal{O} := \mathbb{Z}[\sqrt{2}][1, \frac{1+i}{\sqrt{2}}, \frac{1+j}{\sqrt{2}}, \frac{1+i+j+k}{2}]$$

Man kann zeigen, dass $\mathcal{O}$ eine maximale Ordnung ist.

Aus 3.3.1 erhält man leicht $E_{48} = \text{Tor}(\mathcal{O}^*)$ und aus 3.3.4 und 3.3.2 erhalten wir einen Isomorphismus topologischer Gruppen:

$$\mathcal{O}^* = E_{48} \cdot \mathbb{Z}[\sqrt{2}]^* \cong E_{48} \times \mathbb{Z}.$$

2. Es sei $d = 5$, $S = \Omega_{\infty}$ und somit $\mathcal{O}_S^* = \mathcal{O}^*$. Wir setzen $\tau := (1 + \sqrt{5}/2)$ und

$$\begin{aligned} e_1 &= \frac{1}{2}(1 + \tau^{-1}i + \tau j), & e_2 &= \frac{1}{2}(\tau^{-1}i + j + \tau ij), \\ e_3 &= \frac{1}{2}(\tau i + \tau^{-1}j + ij), & e_4 &= \frac{1}{2}(i + \tau j + \tau^{-1}ij). \end{aligned}$$

Es ist $\{e_1, e_2, e_3, e_4\}$ eine K -Basis von A . Somit ist nach 1.3.13

$$\mathcal{O} := \mathbb{Z}[\tau][e_1, e_2, e_3, e_4]$$

eine Ordnung in A . Man kann zeigen, dass $\mathcal{O}$ eine maximale Ordnung ist.

Aus 3.3.1 erhält man leicht $E_{120} = \text{Tor}(\mathcal{O}^*)$ und aus 3.3.4 und 3.3.2 erhalten wir einen Isomorphismus topologischer Gruppen:

$$\mathcal{O}^* = E_{120} \cdot \mathbb{Z}[\tau]^* \cong E_{120} \times \mathbb{Z}.$$

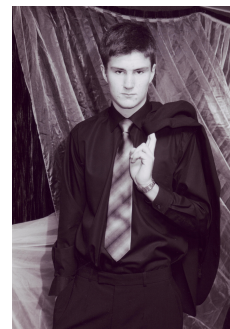
Literaturverzeichnis

- [1] N. Bourbaki, *Commutative Algebra Chapters 1-7*, Springer Verlag, 1989
- [2] L. Goldstein, *Analytic Number Theory*, Prentice Hall, 1971
- [3] Edwin Hewitt, Keneth A. Ross, *Abstract Harmonic Analysis I*, Springer, 1963
- [4] Jens Carsten Jantzen, Joachim Schwermer, *Algebra*, Springer, 2006
- [5] Ina Kersten, *Brauergruppen*, Universitätsverlag Göttingen, 2007
- [6] Markus Kirschmer, *Ideale in Quaternionenalgebren*, Diplomarbeit, Ulm, 2005
- [7] Ernst Kleinert, *Units of Classical Orders: A survey*, L'Enseignement Mathématique, t.40 p.205-248, 1994
- [8] Colin Maclachlan, Alan W. Reid, *Arithmetic of Hyperbolic 3-Manifolds*, Springer, 2003
- [9] Jürgen Neukirch, *Algebraische Zahlentheorie*, Springer, 1992
- [10] Dinakar Ramakrishnan, Robert J. Valenza, *Fourier Analysis on Number Fields*, Springer, 1999
- [11] Irving Reiner, *Maximal Orders*, Academic Press, 1975
- [12] Marie-France Vigneras, *Arithmetique des Algebres de Quaternions*, Springer, Lecture Notes in Mathematics 800, 1980
- [13] Marie-France Vigneras, *Simplification pour les ordres des corps de quaternions totalement définis*, Journal für die Reine und Angewandte Mathematik, Band 286,287 p.257-277, 1976

Lebenslauf

Persönliche Daten

Name: Ludwig Geroldinger
Wohnort: Würthgasse 1/12, 1190 Wien
Geboren am: 27.9.1987 in Ried im Innkreis, OÖ
e-mail: ludwig.geroldinger@gmx.at



Ausbildung

1993–1997: Volkshule Prohaskagasse, Graz
1997–2005: BRG Carnerigasse, Graz
23. Juni 2005: Absolvierung der Reifeprüfung mit ausgezeichnetem Erfolg
Oktober 2005: Beginn der Studien Mathematik und Physik (Diplom) an der Uni Wien
1.2.2007: Abschluss des 1. Abschnitts Physik mit Auszeichnung
4.10.2007: Abschluss des 1. Abschnittes Mathematik mit Auszeichnung
20.11.2009: Abschluss des 2. Abschnittes Mathematik mit Auszeichnung

Sonstige Kenntnisse

Teilnahme am Bundeswettbewerb der 24. österreichischen Physikolympiade
Erwerb des Level 1 Cambridge Zertifikates in Englisch

Wien, 2. Dezember 2009