Quaternionenalgebren – ein Vorlesungsskript

Dr. Stefan Kühnlein, Karlsruhe, Sommer 2003

Kap. I Algebraische Grundlagen

In diesem Kapitel wird erst einmal gesagt, was Quaternionenalgebren sind. Einige Beispiele werden vorgestellt, und es wird grundsätzlich beschrieben, wie man Quaternionenalgebren konstruieren kann. Für manche Grundkörper reicht dies schon aus, um Quaternionenalgebren vollständig zu klassifizieren.

Im dritten Abschnitt lernen wir einiges über die Einheitengruppen von Quaternionenalgebren, und wie sie mit Automorphismen der Algebren und mit Isometrien von einigen dreidimensionalen Räumen zusammenhängen. Im vierten Abschnitt wird eine allgemeinere Konstruktion für zentral einfache Algebren beschrieben, die im Spezialfall der Quaternionenalgebren die bereits erreichten Resultate in ein neues Licht stellt.

§I.1 Definitionen und erste Eigenschaften

In diesem Skript sei stets F ein Körper, von dem wir sicherheitshalber voraussetzen, dass seine Charakteristik nicht 2 ist.

Definition 1.1 Eine *Quaternionenalgebra* über F ist eine vierdimensionale F-Algebra A mit Eins, die außer $\{0\}$ und A keine zweiseitigen Ideale besitzt, und deren Zentrum $Z(A)$ gleich $F = F \cdot 1_A$ ist.

Wir werden stets F mit $F \cdot 1_A$ identifizieren. Man sagt auch kürzer, dass eine Quaternionenalgebra *zentral einfach* ist. Dabei ist „zentral“ die Bedingung ans Zentrum, und „einfach“ die Bedingung an die Ideale.

Beispiele: a) Das erste Beispiel ist der Ring $M_2(F)$ der 2×2-Matrizen mit Koeffizienten in F.

b) Das zweite Beispiel ist die (namensgebende) Algebra $\mathbb{H}$ der Hamilton-Quaternionen. Das ist die vierdimensionale $\mathbb{R}$-Algebra mit Basis $1, I, J, K$, wo die $\mathbb{R}$-bilineare Multiplikation durch

$$I^2 = J^2 = -1,\ IJ = -JI = K$$

festgelegt ist. Dadurch wird zum Beispiel

$$K^2 = (IJ)^2 = I(-IJ)J = -I^2J^2 = -1$$

erzwungen (usw.). Den Nachweis, dass $\mathbb{H}$ eine Quaternionenalgebra über $\mathbb{R}$ ist, führen wir noch nicht hier, sondern erst weiter unten etwas allgemeiner. Letztlich lässt sich nämlich jede Quaternionenalgebra in einer ähnlich Form wie $\mathbb{H}$ angeben.

c) Wenn A eine Quaternionenalgebra über dem Körper F ist und E ein Erweiterungskörper von F, dann ist

$$A_E := A \otimes_F E$$

eine Quaternionenalgebra über E. Dabei sollte man sich vorstellen, dass das Tensorprodukt $A \otimes_F E$ der Vektorraum der E-Linearkombinationen der Elemente aus A ist, konkreter darf man sich eine beliebige Basis von A nehmen und anstelle der Koeffizienten aus F eben Koeffizienten aus E daranschreiben. Die Multiplikation der Basisvektoren geht genauso wie vorher und wird E-bilinear nach $A \otimes_F E$ fortgesetzt.

Zum Beispiel ist $M_2(F) \otimes_F E = M_2(E)$. Diese Interpretation des Tensorproduktes von F-Vektorräumen ist natürlich nur legitim, wenn einer der Faktoren ein Erweiterungskörper von F ist.

Beweis, dass A_E eine Quaternionenalgebra ist: Dies folgt aus den nachstehenden Hilfssätzen 1.2 und 1.4, denn jede Quaternionenalgebra über F ist von der Gestalt $\left(\frac{a,b}{F}\right)$, und nach Tensorieren wird daraus offensichtlich $\left(\frac{a,b}{E}\right)$, also wieder eine Quaternionenalgebra.

$\bigcirc$

Hilfssatz 1.2 *Es seien $a, b \in F^\times$ Einheiten im Körper F, und A sei der vierdimensionale F-Vektorraum mit Basis $1, I, J, K$. Dann wird A zu einer Quaternionenalgebra vermöge der Multiplikationsvorschrift*

$$I^2 := a, J^2 := b, \ IJ := -JI := K,$$

die F-bilinear und unter Wahrung der Assoziativ- und Distributivgesetze nach A fortgesetzt wird.

Bemerkung: Im Falle $F = \mathbb{R}$ und $a = b = -1$ erhalten wir die Hamilton-Quaternionen. Die Algebra, die in Hilfssatz 1.2 beschrieben wird, bezeichnet man mit $\left(\frac{a,b}{F}\right)$. Überlegen Sie sich zum Beispiel, dass $K^2 = -ab$ gilt, oder $IK = aJ \ldots$

Beweis von Hilfssatz 1.2: Es sei $q := w + xI + yJ + zK \in A$ ein beliebiges Element.

Wenn q im Zentrum von A liegt, dann gilt zum Beispiel $Iq = qI$. Aber das heißt, dass

$$Iq = Iw + IxI + IyJ + IzK = ax + wI + azJ + yK$$

und

$$qI = wI + xI^2 + yJI + zKI = ax + wI - azJ - yK$$

übereinstimmen. Also gilt, da die Charakteristik von F nicht 2 ist, $y = z = 0$. Die Gleichheit $qJ = Jq$ führt auch noch zu $x = 0$, also $q = w \in F$.

Das Zentrum von A ist also gleich F.

Jetzt müssen wir noch zeigen, dass für $q \neq 0$ das kleinste zweiseitige Ideal von A, das q enthält, gleich A ist. Ohne Einschränkung sei $w \neq 0$, das lässt sich notfalls durch Multiplikation von q mit einem der Elemente I, J, K erreichen.

Dann ist aber auch $Iq + qI = 2(ax + wI)$ in dem zweiseitigen Ideal, also auch $\tilde{q} := I(Iq + qI) = 2a(w + xI)$, und damit auch $J\tilde{q} + \tilde{q}J = 4awJ$. Dieses wiederum ergibt nach Multiplikation mit J $4abw$, was in F und damit auch in A invertierbar ist. Also liegt in dem kleinsten zweiseitigen Ideal von A, das q enthält, auch eine Einheit, und damit stimmt es mit A überein.

$\bigcirc$

Bevor wir einsehen, dass jede Quaternionenalgebra über F von der Gestalt $\left(\frac{a,b}{F}\right)$ ist (für geeignete $a, b \in F^\times$), wollen wir noch eine Aussage überlegen, die im Fall der Hamilton-Quaternionen auf folgende Weise klar wird. Wenn $w + xI + yJ + zK \in \left(\frac{-1,-1}{\mathbb{R}}\right)$ von 0 verschieden ist, dann gilt:

$$(w + xI + yJ + zK)(w - xI - yJ - zK) = w^2 + x^2 + y^2 + z^2 \in \mathbb{R}^\times.$$

Also ist jedes von Null verschiedene Element invertierbar, $\mathbb{H}$ ist ein Schiefkörper. Dies ist kein Zufall, wie der folgende Hilfssatz lehrt.

Hilfssatz 1.3 *Es sei A eine Quaternionenalgebra über F. Dann ist A entweder ein Schiefkörper oder A ist (als F-Algebra) zum Matrizenring $M_2(F)$ isomorph.*

Beweis. Wir nehmen an, A sei kein Schiefkörper. Also gibt es ein Element $x \in A,\ x \neq 0$, das in A nicht invertierbar ist. (Da A eine endlichdimensionale F-Algebra ist, gibt es keinen Unterschied zwischen links- und rechtsinvertierbar.) Dann ist Ax aber ein F-Vektorraum einer Dimension zwischen 1 und 3, denn $x \in Ax$ und $1 \notin Ax$. Außerdem ist Ax ein A-Untermodul von A, und man erhält F-Algebren-Homomorphismen von A in die F-Endomorphismen der F-Vektorräume Ax und A/Ax. Da diese das Einselement von A auf die Identität schicken, sind sie nichttrivial, und da A einfach ist, sind sie injektiv. Also kann weder Ax noch A/Ax eindimensional sein, da sonst der Endomorphismenring ja eindimensional wäre und keine zu A isomorphe Unteralgebra enthalten könnte.

Demnach ist Ax zweidimensional, und A ist isomorph zu $\mathrm{End}_F(Ax) \cong M_2(F)$.

◯

Folgerung Wenn $a \in F^\times$ das Quadrat eines Elements $\alpha \in F$ ist, dann ist $\left(\frac{a,b}{F}\right)$ isomorph zum Matrizenring, denn es gilt $(\alpha + I)(\alpha - I) = 0$, also ist die Algebra nicht nullteilerfrei.

Zum Beispiel könnten Sie jetzt versuchen, einen expliziten Isomorphismus von $\left(\frac{1,b}{F}\right)$ zum Matrizenring hinzuschreiben, vielleicht auch nur für $b = 1$.

Hilfssatz 1.4 *Es sei A eine Quaternionenalgebra über F. Dann gibt es Elemente $a, b \in F^\times$, sodass*

$$A \cong \left(\frac{a,b}{F}\right).$$

Beweis: Wir wollen von vorneherein annehmen, dass A ein Schiefkörper ist, denn den Matrizenring können wird schon als $\left(\frac{1,1}{F}\right)$ schreiben.

Es sei $q \in A \setminus F$ ein beliebiges Element. Die Unteralgebra $E := F[q]$ von A ist dann eine endlichdimensionale, kommutative, nullteilerfreie Algebra, also eine Körpererweiterung von F. Linksmultiplikation mit Elementen aus E macht aus A einen E-Vektorraum. Da die F-Dimension von A gleich dem Produkt der F-Dimension von E mit der E-Dimension von A ist, muss (A ist ja nicht kommutativ!) E eine quadratische Erweiterung von F sein. Diese ist, da $\mathrm{char}(F) \neq 2$, isomorph zu $F(\sqrt{a})$ für ein $a \in F^\times$, und wir nennen das Element in E, das der gewählten Wurzel von a entspricht, I.

I ist in A invertierbar: $I^{-1} = a^{-1}I$. Die Konjugation mit I liefert einen Isomorphismus von A sowohl als F-Algebra als auch als E-Vektorraum:

$$\Phi : A \longrightarrow A,\ \Phi(X) := IXI^{-1}.$$

Wegen $I^2 = a \in F = Z(A)$ gilt $\Phi^2 = \mathrm{Id}$, und Φ hat die Eigenwerte 1 und -1 (die auch beide vorkommen). Die E-Dimension der Eigenräume ist jeweils 1. Wenn nun $J \neq 0$ ein beliebiges Element im Eigenraum zum Eigenwert -1 ist, so gilt $\Phi(J^2) = \Phi(J)^2 = J^2$, und J^2 ist Eigenvektor zum Eigenwert 1. Also liegt J^2 in E. Folglich kommutiert J^2 mit allen Elementen des Teilrings, der von E und J erzeugt wird, das ist aber die ganze Algebra A. Also liegt J^2 in $Z(A) = F$, und wenn wir $J^2 = b$ nennen, so ist $b \in F^\times$, da J invertierbar ist.

Schließlich setzen wir $K := IJ$. Es ist klar, dass dann $1, I, J, K$ eine F-Basis von A sind. Damit ist der Beweis am Ende.

$\bigcirc$

Nun kennen wir alle Quaternionenalgebren über K, und damit kann die Vorlesung endlich anfangen. Wann ist $\left(\frac{a,b}{F}\right)$ der Matrizenring? Wann sind zwei so gegebene Quaternionenalgebren isomorph?

Bezeichnung: Man sagt, dass eine Quaternionenalgebra A über der Erweiterung E von F (die auch trivial sein darf...) *zerfällt*, wenn $A_E \cong M_2(E)$. Dies ist also genau dann der Fall, wenn A_E kein Schiefkörper ist. Ein Körper E, über dem A zerfällt, heißt ein Zerfällungskörper.

Da jedes Element eines algebraisch abgeschlossenen Körpers F in F ein Quadrat ist, zerfällt jede Quaternionenalgebra über einem algebraisch abgeschlossenen Körper. Zum Beispiel könnte man sich ein Modell der Hamilton-Quaternionen als 4-dimensionale $\mathbb{R}$-Teilalgebra von $M_2(\mathbb{C})$ überlegen und einsehen, dass nach Tensorieren mit $\mathbb{C}$ der ganze Matrizenring herauskommt...

§I.2 Die Spur, die Hauptinvolution und die (reduzierte) Normenform

Bevor wir uns wieder der Frage nach der Klassifikation von Quaternionenalgebren zuwenden, wollen wir noch einmal ein bisschen die Struktur derselben untersuchen. Als erstes taucht die Frage auf, ob der in $\left(\frac{a,b}{F}\right)$ von I, J und K erzeugte Untervektorraum eine basisfreie Definition erlaubt. Dies ist der Fall und geht wie folgt.

Die Linksmultiplikation mit einem Element $q \in A$ liefert einen $F-$Endomorphismus von A. Dieser Endomorphismus hat eine Spur die wir mit $\mathrm{Sp}(q)$ notieren. Sp ist eine Linearform auf A, genannt die Spurform. Wenn $q = w + xI + yJ + zK$ ist, so rechnet man leicht nach, dass

$$\mathrm{Sp}(q) = 4w.$$

Also ist die lineare Hülle von I, J und K der Kern der Spurform. Wir notieren das mit $F^\perp$, was später noch gerechtfertigt wird.

Nun haben wir die Zerlegung

$$A = F \oplus F^\perp,$$

die basisfrei definiert ist. Diese benutzen wir, um auf A einen Antiautomorphimus zu definieren. Für $q = w + q^\perp,\ w \in F, q^\perp \in F^\perp$, setzen wir

$$\iota(q) := w - q^\perp.$$

Nachrechnen in der Basis $1, I, J, K$ zeigt, dass ι ein Antiautomorphismus von A ist:

$$\forall q, r \in A : \iota(qr) = \iota(r)\iota(q), \quad \iota(q + r) = \iota(q) + \iota(r).$$

Außerdem ist ι involutiv: $\iota^2 = \mathrm{Id}$. Interessant ist ι aus dem folgenden Grund.

Die Zahl $N(q) := q \cdot \iota(q) \in F$ heißt die reduzierte Norm von q, und q ist invertierbar genau dann, wenn $N(q) \neq 0$.

Wenn nämlich $N(q) \neq 0$, dann ist $\iota(q)/N(q)$ zu q invers. Und wenn die Norm 0 ist, dann ist q ein Nullteiler, also nicht invertierbar.

Merkregel: Die Quaternionenalgebra A ist genau dann der Matrizenring, wenn es ein $q \in A,\ q \neq 0$ gibt mit $N(q) = 0$. Man sagt dann auch, dass die Normenform isotrop ist.

Als Formel kann man sich merken:

$$N(w+xI+yJ+zK) = (w+xI+yJ+zK)\cdot\iota(w+xI+yJ+zK) = w^2 - ax^2 - by^2 + abz^2.$$

Es gilt $N(qr) = qr\iota(qr) = qr\iota(r)\iota(q) = N(q)N(r)$.

Aufgabe: Für welche Quaternionenalgebra folgt daraus, dass das Produkt zweier Summen von vier Quadraten wieder die Summe von vier Quadraten ist?

Die Linksmultiplikation mit q hat auch eine Determinante die üblicherweise als die Norm von q bezeichnet wird. Bei Quaternionenalgebren ist es aber so, dass diese Determinante das Quadrat der reduzierten Norm $N(q)$ ist. In der nun schon vertrauten Basis $1, I, J, K$ ist die Multiplikation mit $q := w + xI + yJ + zK$ gegeben durch die Matrix

$$\begin{pmatrix} w & ax & by & -abz \\ x & w & bz & -by \\ y & -az & w & ax \\ z & -y & x & w \end{pmatrix},$$

deren Determinante sich eben als $N(q)^2$ ergibt. Es ist aber bequemer, mit der quadratischen Form $q \mapsto N(q)$ zu hantieren, als mit der eigentlichen Normenform. Letztlich ist es dieser Zusammenhang mit quadratischen Formen, der dafür verantwortlich ist, dass wir den Fall $\mathrm{char}\,(F) = 2$ ausschließen.

Der Zusammenhang mit quadratischen Formen ist nämlich viel tiefer, als dies zunächst aussieht. Eine quadratische Form $Q : V \longrightarrow F$ auf einem F-Vektorraum V von endlicher Dimension kann nach Basiswahl immer durch eine Fundamentalmatrix G gegeben werden, deren Eintrag an der i,j-ten Stelle gleich $\frac{1}{2}(Q(b_i + b_j) - Q(b_i) - Q(b_j))$ ist. G ist eine symmetrische Matrix, und Q heißt nicht ausgeartet, wenn G vollen Rang hat. Q ist gegeben durch die Vorschrift

$$v \mapsto q(v) = \kappa^\top G\kappa,$$

wobei κ der Koeffizientenvektor von v bezüglich der Basis $b_1, \ldots, b_n$ von V ist.

Bezüglich unserer Lieblingsbasis $1, I, J, K$ ist die Normenform gegeben durch die Matrix

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

NB: Bezüglich der Normenform stehen F und $F^\perp$ aufeinander senkrecht, was die Notation rechtfertigt.

Zwei quadratische Formen Q_1, Q_2 auf V heißen äquivalent, wenn sie durch Basiswechsel ineinander überführt werden können. Mit anderen Worten: die zugehörigen Fundamentalmatrizen G_1, G_2 sind äquivalent, das heißt es gibt eine invertierbare Matrix S, sodass

$$G_2 = S^\top G_1 S.$$

Satz 1.5 *Es seien A_1 und A_2 zwei Quaternionenalgebren über F. Dann sind äquivalent:*

a) A_1 und A_2 sind als Algebren isomorph.

b) Die Einschränkungen der Normenformen auf $F^{\perp_1}$ und $F^{\perp_2}$ sind äquivalent.

c) Die Normenformen auf A_1 und A_2 sind äquivalent.

Beweis: $a) \Rightarrow b)$: Ein Isomorphismus $\Phi : A_1 \longrightarrow A_2$ von F-Algebren bildet $F^{\perp_1}$ auf $F^{\perp_2}$ ab, da beide Räume durch das Verschwinden der Spur charakterisiert sind. Auch die Norm bleibt erhalten unter Φ, das zeigt bereits alles.

$b) \Rightarrow c)$: Das ist klar, da in beiden Algebren die orthogonalen Komplemente zu den Spur-0-Teilen gleich F sind, und die Normenform darauf in beiden Fällen durch $f \mapsto f^2$ gegeben ist.

$c) \Rightarrow a)$: Wenn die Normenformen beide isotrop sind, so sind die Quaternionenalgebren beide isomorph zum Matrizenring, also auch zueinander. Betrachten wir also nur noch den Fall, dass die Normenformen anisotrop sind.

Es sei $\Phi : A_1 \longrightarrow A_2$ eine F-lineare Abbildung, die die Norm erhält:

$$\forall q \in A_1 : N(\Phi(q)) = N(q).$$

Insbesondere hat also $\Phi(1)$ die Norm 1. Wenn $\Phi(1) \neq 1$, so betrachte $q := \Phi(1) - 1$. Es gilt $N(q) \neq 0$, da die Normenform ja anisotrop ist. Die Abbildung

$$\sigma_q : A_2 \longrightarrow A_2, \quad X \mapsto X - \frac{N(X+q) - N(X) - N(q)}{N(q)} q,$$

erhält die Norm (es ist nämlich eine Spiegelung an der zu q orthogonalen Hyperebene bezüglich der zu N gehörigen Bilinearform) und bildet $\Phi(1)$ auf 1 ab. Wir können also Φ durch $\sigma_q \circ \Phi$ ersetzen und von vorneherein annehmen, dass die Äquivalenz der Normenformen das Einselement von A_1 auf das von A_2 abbildet. Dann werden aber auch die orthogonalen Komplemente von F durch Φ miteinander identifiziert, also erhält Φ die Norm und die Spur. Nun wählen wir eine Basis $1, I, J, K$ von A_1 wie üblich. Die Normerhaltung von Φ schenkt uns dann die Identitäten

$$\Phi(X^2) = \Phi(-N(X)) = -N(\Phi(X)) = \Phi(X)^2$$

für alle X in $F^{\perp_1}$, also insbesondere $X = I, J, K$. Wenn wir nun noch $\Phi(IJ) = \Phi(I)\Phi(J)$ zeigen können, dann sind wir fertig. Aber $\Phi(IJ) = \Phi(K)$ steht natürlich auf $1, \Phi(I), \Phi(J)$ senkrecht, ist also ein Vielfaches von $\Phi(I)\Phi(J)$, denn $1, \Phi(I), \Phi(J), \Phi(I)\Phi(J)$ ist offensichtlich eine Basis von A_2, wie wir sie wollen.

Spätestens wenn wir hinter Φ noch die Spiegelung an der Hyperebene durch $1, \Phi(I), \Phi(J)$ schalten, erhalten wir einen Isomorphismus von F-Algebren.

◯

Beispiele:

- Im Fall $F = \mathbb{R}$ gibt es genau zwei Quaternionenalgebren. Damit nämlich die Normenform anisotrop ist, muss sie positiv definit sein (da die Norm von 1 positiv ist, entfällt die Möglichkeit einer negativ definiten Normenform). Also sind I^2 und J^2 negativ zu wählen, und durch Ersetzen von I und J durch geeignete Vielfache erhalten wir $\left(\frac{-1,-1}{\mathbb{R}}\right)$.

- Wenn F ein endlicher Körper ist, dann zerfällt jede Quaternionenalgebra über F. Zwar ist es bekanntlich so, dass nicht jedes Element aus F ein Quadrat ist, es gibt aber, wenn der Körper q Elemente hat, jeweils genau $\frac{q-1}{2}$ Quadrate und Nichtquadrate in $F^\times$. Damit kann man sich durch ein leichtes Abzählargument überzeugen, dass jede vierdimensionale quadratische Form über F isotrop ist (sogar schon jede dreidimensionale!). **NB:** Ein Satz von Wedderburn sagt, dass jede endliche Divisionsalgebra kommutativ ist. Das ist schwieriger zu zeigen als die Nichtexistenz endlicher Quaternionen-Schiefkörper.

- Im Falle $F = \mathbb{Q}$ gibt es unendlich viele (Isomorphieklassen von) Quaternionenalgebren. Man unterscheidet zwischen den definiten und den indefiniten Quaternionenalgebren, je nachdem ob nach Tensorieren mit $\mathbb{R}$ die Hamilton-Quaternionen herauskommen oder der Ring $M_2(\mathbb{R})$. Zum Beispiel sind die Quaternionenalgebren $\left(\frac{-1,-1}{\mathbb{Q}}\right)$ und $\left(\frac{-2,-5}{\mathbb{Q}}\right)$ beide positiv definit, aber nicht zueinander isomorph. Sonst gäbe es ja in der zweiten ein Element mit Spur 0 und Norm 1, das heißt es gäbe ganze Zahlen a, b, c, d mit

  $$2a^2 + 5b^2 + 10c^2 = d^2.$$

  Reduktion modulo 5 zeigt, dass 5 ein Teiler von a und von d sein muss, da sonst 2 ein Quadrat in $\mathbb{F}_5$ wäre. Division der Gleichung durch 5 liefert dann eine neue Gleichung mit denselben b, c und $\alpha = a/5,\ \delta = d/5$:

  $$10\alpha^2 + b^2 + 2c^2 = 5\delta^2,$$

  und Reduktion modulo 5 zeigt, dass 5 auch ein Teiler von b und c ist, da sonst -2 ein Quadrat in $\mathbb{F}_5$ wäre. Demnach ist 5 ein gemeinsamer Teiler von a, b, c, d, und wenn alle vier durch 5 geteilt wurden, erhält man wieder vier ganze Zahlen, die dieselbe Gleichung erfüllen, also auch alle durch 5 teilbar sind... Das ist der Anfang eines „unendlichen Abstiegs“ und zeigt die Unmöglichkeit eines Isomorphismus.

Bemerkung: Der vorangehende Satz sorgt dafür, dass in Büchern über quadratische Formen meistens etwas über Quaternionenalgebren steht. Dort steht aber nocht viel mehr, zum Beispiel dass zu quadratischen Formen gehörige orthogonale Gruppen von Spiegelungen erzeugt werden, oder dass der Witt'sche Fortsetzungssatz gilt. Maßgeschneidert für unsere Überlegungen sind Spezialfälle dieser Aussagen in den Beweis eingegangen.

Was der Beweis eigentlich sogar zeigt ist, dass die Algebrenautomorphismen der Quaternionenalgebra eine Untergruppe vom Index 2 in der orthogonalen Gruppe von $F^\perp$ bilden. Nun wollen wir doch einmal sehen, welche Algebrenautomorphismen es eigentlich gibt!

§I.3 Die Einheitengruppe und Automorphismen von A

Wir haben gesehen, dass die Gruppe $A^\times$ der invertierbaren Elemente in einer Quaternionenalgebra durch das Nichtverschwinden der Norm gegeben ist. Das lässt sich etwas anders formulieren, indem wir zur fünfdimensionalen F-Algebra $A \oplus F$ übergehen. Die Einheitengruppe von A ist dann offensichtlich isomorph zur Menge $\{(q, f) \in A \oplus F \mid N(q) \cdot f = 1\}$. Auf diese Weise wird die Ungleichung ($N(q) \neq 0$) zu einer Gleichung, und $A^\times$ lässt sich als Nullstellenmenge eines Polynoms auffassen. So etwas nennen wir eine affine algebraische Varietät.

Die Multiplikation in $A^\times$ wird durch Polynome gegeben, und das gilt auch für das Invertieren: $(q,f)^{-1} = (f \cdot \iota(q), N(q))$. Damit ist $A^\times$ ein Beispiel für eine affine algebraische Gruppe.

Es gilt nun für den algebraischen Abschluss $\overline{F}$ von F, dass $A_{\overline{F}} \cong M_2(\overline{F})$, und die Einheitengruppe hiervon ist $\mathrm{GL}(2,\overline{F})$. Daher sagt man auch, $A^\times$ sei eine F-Form von $\mathrm{GL}(2)$. Diese Tatsache spielt in der Theorie der automorphen Formen eine wichtige Rolle, ein Stichwort dazu ist der sogenannte Basiswechsel.

Für eine Einheit e von A betrachten wir nun die Abbildung

$$\kappa_e : A \longrightarrow A, X \mapsto eXe^{-1}.$$

Diese ist ein Automorphismus von A. Insbesondere ist sie auch normerhaltend und damit in der orthogonalen Gruppe bezüglich der Normenform.

Da das Zentrum F von A von κ_e (punktweise) festgelassen wird, ist auch $F^\perp$ ein κ_e-invarianter Teilraum von A. (Alternativ hätte man argumentieren können, dass κ_e auch die Spur erhält, und daher den Kern der Spurabbildung.) Nach Einschränkung erhält man also einen Homomorphismus von $A^\times$ nach $\mathrm{O}(N^\perp)$, die orthogonale Gruppe der Normenform auf $F^\perp$.

Der Kern von diesem Homomorphismus ist genau das Zentrum von $A^\times$, also $F^\times$. Wir erhalten also einen injektiven Homomorphismus

$$A^\times/F^\times \longrightarrow \mathrm{O}(N^\perp).$$

Dieser Homomorphismus ist der Grund dafür, dass Quaternionen manchmal in der physikalischen Literatur auftauchen. Eigentlich aber nur in etwas anderer Form. Es gilt nämlich für die Hamilton-Quaternionen, dass

$$\mathbb{H}^\times = \mathbb{R}^\times \cdot \mathbb{H}_1^\times,$$

wobei $\mathbb{H}_1^\times$ die Untergruppe der Quaternionen von Norm eins ist. Diese Untergruppe ist die 3-Sphäre, wenn man $\mathbb{H}$ als euklidischen Standardraum auffasst. Und dann schaut man sich nur noch den Homomorphismus

$$\mathbb{H}_1^\times \longrightarrow \mathrm{O}(3)$$

an, denn $\mathbb{R}^\perp$ ist ja der euklidische Standardraum von Dimension drei. Dieser letzte Homomorphismus hat Kern ± 1, also die Norm-1-Elemente im Zentrum, und das Bild ist $\mathrm{SO}(3)$, was man nachrechnen kann. Zum Beispiel ist die Isometrie, die durch Konjugation mit $\cos\phi + \sin\phi I$ gegeben wird, die Drehung um die I-Achse um den Winkel 2ϕ, ähnlich auch mit J, und dann kann man Euler-Winkel benützen, um jede Drehung in $\mathrm{SO}(3)$ mithilfe einer Quaternion zu beschreiben.

Ähnlich erhält man auch einen Homomorphismus von $\mathrm{GL}(2,F)/F^\times$ nach $\mathrm{SO}(1,2)$, das ist die spezielle orthogonale Gruppe der quadratischen Form zur Diagonalmatrix $\mathrm{diag}(1,-1,-1)$, die die Determinantenform auf den Spur-0-Matrizen in $M_2(F)$ beschreibt. Dieser Homomorphismus ist eine Isogenie, das heißt, der Kern ist endlich (hier sogar trivial) und das Bild hat endlichen Index (hier sogar Index 1).

Hier ist dieser Homomorphismus also sogar ein Isomorphismus, einer der sogenannten Ausnahmeisomorphismen zwischen einfachen Liegruppen.

Nun kommen wir zu einem Spezialfall des Satzes von Skolem und Noether, der sagt, dass jeder Automorphismus einer endlichdimensionalen, zentral einfachen F-Algebra ein innerer Automorphismus ist. Genauer gilt:

Satz 1.6 *Es sei Φ ein F-Algebren Automorphismus der Quaternionenalgebra A. Dann gibt es eine Einheit $e \in A^\times$, sodass*

$$\forall X \in A : \Phi(X) = eXe^{-1}.$$

Bemerkung: Das zeigt, dass die Automorphismengruppe von A gleich $A^\times/F^\times$ ist. Denn Konjugation mit e ist genau dann die Identität, wenn e im Zentrum, also in F, liegt. Das hängt eng mit den eben beschriebenen Isogenien zusammen, denn eine Isometrie, die die 1 festlässt, ist fast so gut wie ein Algebren-Automorphismus – das haben wir im Beweis von Satz 1.5 implizit gesehen und schon am Ende von §I.2 als Bemerkung formuliert.

Beweis von Satz 1.6 Der Endomorphismenring $\mathrm{End}_F(A)$ des F-Vektorraums A ist (nach Basiswahl) der Matrizenring $M_4(F)$. Darin liegen die Endomorphismen

$$\alpha_{a,b} : X \mapsto aXb$$

für $a, b \in A$, und weil A eine Quaternionenalgebra ist, erzeugen diese das ganze $\mathrm{End}_F(A)$. Die Vorschrift $\alpha_{a,b} \mapsto \alpha_{\Phi(a),b}$ definiert eine neue $M_4(F)$-Modulstruktur auf F^4. Aber $M_4(F)$ hat nur einen Isomorphietyp von Moduln, die vierdimensionale F-Vektorräume sind. Also gibt es eine bijektive Abbildung $\Psi : A \longrightarrow A$, sodass

$$\forall a, X, b \in A : \Psi(aXb) = \Phi(a)\Psi(X)b.$$

Für $a = 1$ folgt $\Psi(Xb) = \Psi(X)b$, also $\Psi(b) = \Psi(1) \cdot b$. Das Element $\Psi(1)$ muss natürlich invertierbar sein. Einsetzen in die Gleichung vorher sowie Kürzen von b und X rechts liefert

$$\forall a \in A : \Phi(a) = \Psi(1)a\Psi(1)^{-1}.$$

◯

§I.4 Galoiskohomologie – naja, ein bisschen jedenfalls

Wenn E eine quadratische Erweiterung von F ist, die sich als Teilalgebra in A einbetten lässt, dann ist E offensichtlich ein Zerfällungskörper von A, denn $E = F(\sqrt{a})$ für ein $a \in F^\times$, und dieses a hat dann auch in $F^\perp \subseteq A$ eine Quadratwurzel I usw. (s.o.).

Nun kann man die Frage umkehren und versuchen, alle Quaternionenalgebren zu verstehen, die eine gegebene quadratische Erweiterung E von F als Teilkörper enthält.

In diesem Fall ist A ein zweidimensionaler E-Vektorraum durch Linksmultiplikation. Wir wählen wie im Beweis von Hilfssatz 1.4 eine Basis $1, I, J, K$, wobei $E = F(I)$ gelte. Dass dies möglich ist haben wir dort gesehen. Nun schreiben wir die Elemente von A als

$$q = e_1 + e_J J, \quad e_1, e_J \in E = F(I).$$

Es gilt $Je = \sigma(e)J$, wobei σ der nichttriviale Automorphismus von E über F ist: $G := \mathrm{Gal}(E/F) = \{1, \sigma\}$.

Zwei Elemente aus A multiplizieren sich dann mittels der folgenden Regel:

$$(e_1 + e_J J)(f_1 + f_J J) = e_1 f_1 + e_J \sigma(f_J) b + (e_J \sigma(f_1) + e_1 f_J) J.$$

Dabei ist $b = J^2$.

Dies versuchen wir nun künstlich etwas allgemeiner nachzubauen. Damit der allgemeine Charakter der Konstruktion klarer wird, nehmen wir zunächst an, E sei eine beliebige (endliche) Galois-Erweiterung von F mit Galoisgruppe G. Der Ansatz ist, dass wir eine F-Algebra A bauen, die E enthält, indem wir zunächst den E-Vektorraum mit Basis $\{u_g | g \in G\}$ nehmen. Für die Multiplikation verlangen wir, dass zum Einen

$$\forall g \in G,\ e \in E : u_g \cdot e = g(e) u_g$$

gilt und zum Anderen

$$\forall g, h \in G : \exists \kappa(g,h) \in E^\times : u_g \cdot u_h = \kappa(g,h) u_{gh}.$$

Diese Forderungen und die erwünschten Ditributivgesetze legen die Multiplikation vollkommen fest:

$$(\sum e_g u_g) \cdot (\sum f_h u_h) := \sum_{g,h \in G} e_g g(f_h) \kappa(g,h) u_{gh}.$$

Damit diese Multiplikation assoziativ ist, muss gelten: $u_g \cdot (u_h u_k) = (u_g u_h) \cdot u_k$. Dies ist gleichbedeutend mit der sogenannten 2-Kozykelbedingung

$$\forall g, h, k \in G : \kappa(g,h)\kappa(gh,k) = \kappa(g,hk) \cdot g(\kappa(h,k)).$$

Die Menge aller Abbildungen $\kappa : G \times G \longrightarrow E^\times$, die dieser Bedingung genügen, nennen wir 2-Kozykel: $Z^2(G, E^\times)$. Dies ist eine Gruppe unter Multiplikation der Funktionswerte. Den mittels $\kappa \in Z^2(G, E^\times)$ konstruierten Ring nennen wir (E, κ).

Speziell für $g = h = 1$ zeigt die Kozykelrelation, dass $\kappa(1,k) = \kappa(1,1)$. Analog auch $\kappa(k,1) = \kappa(1,1)$. Dies sorgt dafür, dass $\kappa(1,1)^{-1} u_1$ das neutrale Element der konstruierten Algebra ist.

Um uns das Leben etwas zu vereinfachen erlauben wir nun einen Basiswechsel. Statt der ursprünglichen u_g nehmen wir Vektoren $v_g := f(g) u_g$ für eine Abbildung $f : G \longrightarrow E^\times$. Wir erhalten

$$v_g v_h = f(g) u_g f(h) u_h = f(g) g(f(h)) \kappa(g,h) u_{gh} = f(g) g f(h) f(gh)^{-1} \kappa(g,h) v_{gh}.$$

Das definiert den neuen 2-Kozyklus

$$\tilde{\kappa}(g,h) := f(g) g(f(h)) f(gh)^{-1} \kappa(g,h).$$

Durch die Wahl von $f(1) := \kappa(1,1)^{-1}$ wird $\tilde{\kappa}$ ein normalisierter 2-Kozykel, d.h. $\tilde{\kappa}(1,1) = 1$, und damit auch – wie eben gesehen $\tilde{\kappa}(1,k) = \tilde{\kappa}(k,1) = 1$.

Nun ist v_1 das Einselement von $(E, \tilde{\kappa})$, und man sieht leichter, dass $(E, \tilde{\kappa})$ eine F-Algebra ist. Ab jetzt heißt der 2-Kozykel wieder κ und wird als normiert vorausgesetzt. Die Menge aller normierten 2-Kozykel heißt $Z_0^2(G, E^\times)$.

Hilfssatz *Es sei $\kappa \in H^2(G, E^\times)$ ein Kozykel und A die Algebra (E, κ). Dann ist A eine zentral einfache F-Algebra der Dimension $(E : F)^2$.*

Beweis. Ohne Einschränkung dürfen wir annehmen, κ sei normalisiert, also $\kappa(1,1)=1$, sodass u_1 das neutrale Element von A ist. Dann ist Fu_1 offensichtlich im Zentrum enthalten.

Es sei $z=\sum_{g\in G} a_g u_g$ mit $a_g \in E$. Wenn z im Zentrum von A enthalten ist, so gilt

$$\forall x \in E : xz = zx, \text{ also } \forall g \in G : xa_g = a_g g(x),$$

und damit ist $z \in E$. Da z auch noch mit allen u_g vertauschen soll, folgt $z \in F$. Also ist F das Zentrum von A.

Nun sei $z \neq 0$. Was ist das kleinste zweiseitige Ideal I, das z enthält? Durch Multiplikation mit einem geeigneten u_g können wir erreichen, dass $a_1 \neq 0$, was wir von jetzt ab annehmen. Wenn nun noch mindestens ein weiteres $a_g \neq$ ist, so kann die Anzahl der von 0 verschiedenen Koeffizienten verkleinert werden. Für das fragliche $g \neq 1$ gibt es nämlich ein $x \in E$ mit $g(x) \neq x$. Dann ist der Koeffizient bei u_g in $g(x)z - zx$ gleich Null, aber der bei u_1 ist nach wie vor nicht Null, und wenn ein Koeffizient vorher Null war, so auch hinterher. Also ist die Anzahl der von Null verschiedenen Koeffizienten echt kleiner geworden. Damit liegt letztlich ein von Null verschiedenes Element aus Eu_1 in I, also eine Einheit, und $I = A$: A ist einfach. ◯

Beispiel: Wenn $E = F(\sqrt{a})$ ist und $\kappa \equiv 1$, dann ist $(E,\kappa) \cong M_2(F)$. Ein Isomorphismus wird zum Beispiel gegeben durch

$$(w + x\sqrt{a})u_1 + (y + z\sqrt{a})u_\sigma \mapsto \begin{pmatrix} w+y & x-z \\ a(x+z) & w-y \end{pmatrix}.$$

Ähnliches gilt auch allgemein: Wenn κ konstant gleich 1 ist, dann erhält man einen Homomorphismus von (E,κ) in die F-Vektorraum-Endomorphismen von E via

$$\forall x \in E : (\sum_{g\in G} a_g u_g)(x) := \sum_{g\in G} a_g u_g(x).$$

Dieser Homomorphismus ist dann aus Dimensionsgründen ein Isomorphismus (injektiv ist er, da (E,κ) einfach ist). Insbesondere sieht man an dieser Tatsache, dass die Elemente der Galoisgruppe von E über F sogar E-linear unabhängig sind.

Anstelle der 2-Kozykel betrachten wir nun nur die Äquivalenzklassen von 2-Kozykeln vermöge der Äquivalenzrelation, die weiter oben durch den Basiswechsel motiviert wurde. In Wirklichkeit gehört die zentral einfache Algebra nämlich zu einer solchen Äquivalenzklasse. Die Menge aller dieser Äquivalenzklassen nennen wir die zweite Kohomologiegruppe $H^2(G,E^\times)$. Es gibt eine Bijektion zwischen der Menge aller Isomorphieklassen von zentral-einfachen F-Algebren der Dimension $(E:F)^2$, die E als Zerfällungskörper haben, und der Gruppe $H^2(G,E^\times)$.

Nun kehren wir zurück zum Fall, dass E über F quadratisch ist. Dann sagt das eben Gesehene, dass es eine Bijektion zwischen der Menge der Isomorphieklassen von Quaternionenalgebren über F mit Zerfällungskörper E und der Gruppe $H^2(G,E^\times)$ gibt. Also berechnen wir nun $H^2(G,E^\times)$. Jede Äquivalenzklasse hierin wird durch einen normalisierten 2-Kozykel repräsentiert. Dieser hat höchstens einen von 1 verschiedenen Funktionswert hat, nämlich $\kappa(\sigma,\sigma)$, und wir erhalten eine injektive Abbildung

$$Z_0^2(G,E^\times) \longrightarrow E^\times, \kappa \mapsto \kappa(\sigma,\sigma).$$

Was ist das Bild von Φ? Die Kozykelbedingung (für $g = h = k = \sigma$) verlangt $\kappa(\sigma,\sigma) \cdot \kappa(1,\sigma) = \kappa(\sigma,1) \cdot \sigma(\kappa(\sigma,\sigma))$. Also ist $\kappa(\sigma,\sigma)$ invariant unter σ, und damit in $F^\times$. Umgekehrt rechnet man nach, dass jeder Wert aus $F^\times$ als Funktionswert eines normalisierten 2-Kozykels vorgeschrieben werden kann. Wie steht es um die Äquivalenz zweier normalisierter 2-Kozykel? Hier darf ich nur noch Funktionen $f : G \longrightarrow E^\times$ verwenden, die die Normierung nicht kaputt machen, also $f(1) = 1$ erfüllen. Dann wird aber

$$\tilde{\kappa}(\sigma,\sigma) = f(\sigma)\sigma(f(\sigma))f(\sigma^2)^{-1}\kappa(\sigma,\sigma).$$

Da $f(\sigma^2) = 1$ gilt, folgt $\tilde{\kappa}(\sigma,\sigma) = N_{E/F}(f(\sigma))\kappa(\sigma\sigma)$, und damit

$$H^2(G, E^\times) \cong F^\times / N_{E/F}(E^\times).$$

Rechts steht die sogenannte Normenrestklassengruppe.

Wenn $b \in F^\times$ gewählt ist, so definiert b einen 2-Kozykel, und die zugehörige Quaternionenalgebra lässt sich realisieren als

$$A = \{ \begin{pmatrix} x & y \\ b\sigma(y) & \sigma(x) \end{pmatrix} \mid x, y \in E \} \subseteq M_2(E).$$

Nun fassen wir endlich die Hauptaussage des Abschnittes in zwei Sätzen zusammen.

Satz *Es sei E eine quadratische Körpererweiterung von F. Dann gibt es eine natürliche Bijektion zwischen der Menge aller Isomorphieklassen von F-Quaternionenalgebren, die über E zerfallen, und der Gruppe*

$$F^\times / N_{E/F}(E^\times).$$

Satz *Die Quaternionenalgebra $\left(\frac{a,b}{F}\right)$ zerfällt genau dann schon über F, wenn b eine Norm der Körpererweiterung $F(\sqrt{a})/F$ ist, also genau dann, wenn die Gleichung*

$$w^2 - ax^2 = by^2$$

in F^3 nichttrivial gelöst werden kann.

Beispiele 1. Für $F = \mathbb{R}$ und $E = \mathbb{C}$ ist die Normengruppe die Gruppe der positiven Zahlen, und die Normenrestklassengruppe ist $\{\pm 1\}$. Also finden wir wieder die zwei alten Quaternionenalgebren, die es eben über den reellen Zahlen gibt – $\mathbb{C}$ muss ja jede reelle Quaternionenalgebra zerfällen.

2. Wenn F ein endlicher Körper ist und E die quadratische Erweiterung von F, dann ist die Normengruppe ganz $F^\times$. Also gibt es keine nichttriviale Quaternionenalgebra über F, was wir ja schon lange wissen.

3. Wenn $F = \mathbb{Q}$ gilt und $E = \mathbb{Q}(\sqrt{-2})$, dann ist die Normenrestklassengruppe unendlich. Zum Beipiel ist -5 keine Normenrest, da die Normen nur positive Zahlen sind, und wir finden wieder die Quaternionenalgebra $\left(\frac{-2,-5}{\mathbb{Q}}\right)$. Wir wissen schon, dass diese nicht zu $\left(\frac{-1,-1}{\mathbb{Q}}\right)$ isomorph ist, aber jetzt sehen wir es mit anderen Augen. Dazu zeigen wir, dass $\mathbb{Q}(\mathrm{i})$ kein Zerfällungskörper von $\left(\frac{-2,-5}{\mathbb{Q}}\right)$ ist. Dann würde ja $\left(\frac{-2,-5}{\mathbb{Q}(\mathrm{i})}\right)$ zerfallen, und das hieße, dass -5 eine Norm der Erweiterung $\mathbb{Q}(\mathrm{i}, \sqrt{-2})/\mathbb{Q}(\mathrm{i})$ ist. Dann wäre

$$x^2 + 2y^2 = -5z^2$$

für geeignete $x, y, z \in \mathbb{Z}[\mathrm{i}]$, und Reduktion modulo $1 \pm 2\mathrm{i}$ würde zeigen, dass 5 ein Teiler von x und y ist und damit auch von z, womit wir wieder beim unendlichen Abstieg angelangt wären. Ist das nicht toll?

Kap. II Arithmetische Aspekte

In diesem Kapitel wollen wir spezieller auf Quaternionenalgebren über dem Körper $\mathbb{Q}$ eingehen. Ein wichtiger Aspekt hierbei ist es, Quaternionenalgebren über sogenannten lokalen Körpern zu betrachten. Ähnlich wie der Begriff der Definitheit oder Indefinitheit einer rationalen Quaternionenalgebra wiederspiegelt, welche Quaternionenalgebra nach Eweiterung des Grundkörpers von $\mathbb{Q}$ nach $\mathbb{R}$ herauskommt, erhält man für jede Primzahl p die Information, ob die Quaternionenalgebra bei dem zu p gehörigen lokalen Körper zerfällt oder nicht. Daher zunächst ein Abschnitt über lokale Körper.

§II.1 Lokale Körper

Eine diskrete Bewertung v auf einem Körper F ist eine Abbildung von $F^\times$ in die Gruppe $\mathbb{Z}$ der ganzen Zahlen, für die die folgenden Regeln gelten:

$$\mathrm{v}(xy) = \mathrm{v}(x) + \mathrm{v}(y), \quad \mathrm{v}(x+y) \geq \min(\mathrm{v}(x), \mathrm{v}(y)).$$

Wir nehmen stets an, dass v nichttrivial ist, also nicht konstant gleich 0. Durch Wahl einer reellen Zahl $2 > 1$ kann man mittels einer Bewertung v eine Metrik auf F definieren. Für $x \neq y$ setzt man einfach

$$d_{\mathrm{v}}(x,y) := 2^{-\mathrm{v}(x-y)},$$

und $d_{\mathrm{v}}(x,x)$ ist natürlich 0.

Wenn man nun schon eine Metrik auf dem Körper hat, so betrachtet man sich natürlich umgehend auch Cauchy-Folgen in F. Wenn jede Cauchy-Folge in F gegen einen Grenzwert in F konvergiert, so sagt man, der Körper sei vollständig bewertet. Ist dies nicht der Fall, so bildet man den Ring aller Cauchy-Folgen in F und faktorisiert aus diesem das Ideal aller Nullfolgen heraus. Dieses ist ein maximales Ideal, und der Quotientenkörper ist ein Erweiterungskörper F_{v} von F. Die Bewertung v lässt sich auf diesen fortsetzen, und man kann nachrechnen, dass F_{v} vollständig ist. Dieser Körper heißt die Komplettierung von F (bezüglich der betrachteten Bewertung).

Im Prinzip ist das auch eine Möglichkeit, $\mathbb{R}$ aus $\mathbb{Q}$ zu konstruieren, nur dass man nicht von einer diskreten Bewertung ausgeht. Eine Dezimalzahl ist als Repräsentant einer Äquivalenzklasse von Cauchy-Folgen in $\mathbb{Q}$ zu verstehen, indem man sich die Partialsummen ansieht.

Beispiel: Auf dem Körper $k(X)$ der rationalen Funktionen über dem Körper k gibt es als Bewertung die negative Gradbewertung:

$$\mathrm{v}(f/g) := \mathrm{grad}(g) - \mathrm{grad}(f),$$

und die zugehörige Komplettierung von $k(X)$ ist der Ring der Laurent-Reihen in $1/X$ mit Koeffizienten in k.

Definition: Es sei F ein Körper mit Bewertung v.

a) Die Menge

$$\mathcal{O} := \{x \in F \mid \mathrm{v}(x) \geq 0\} \cap \{0\}$$

ist der *Bewertungsring* von F, und

$$\mathcal{M} := \{x \in F \mid \mathrm{v}(x) > 0\} \cap \{0\}$$

sein maximales Ideal. $\mathcal{O}/\mathcal{M}$ ist der *Restklassenkörper* von F.

b) F heißt ein *lokaler Körper*, wenn er vollständig und der Restklassenkörper endlich ist.

Konstruktion von $\mathbb{Q}_p$. Für eine Primzahl p ist die p-adische Bewertung auf $\mathbb{Q}$ gegeben durch

$$\mathrm{v}_p(a/b) := e - f, \text{ wobei } p^e||a,\ p^f||b,\ a, b \in \mathbb{Z}.$$

Der Bewertungsring ist

$$\mathbb{Z}_{(p)} := \{a/b \mid p \not| b\},$$

das maximale Ideal ist

$$p\mathbb{Z}_{(p)} := \{a/b \mid p|a,\ p \not| b\}.$$

Der Restklassenkörper ist einfach der Körper $\mathbb{F}_p$ mit p Elementen. Der Abschluss von $\mathbb{Z}$ in der Komplettierung $\mathbb{Q}_p$ ist der Ring $\mathbb{Z}_p$ der ganzen p-adischen Zahlen.

Als Übung könnten wir uns überlegen, dass $\mathbb{Z}_{(p)} \subseteq \mathbb{Z}_p$. Da $\mathbb{Z}_{(p)}$ von 1 und den Zahlen $1/\ell$ (wobei ℓ die von p verschiedenen Primzahlen durchläuft) erzeugt wird, genügt es, von diesen zu zeigen, dass sie p-adisch ganz sind. Für 1 ist das klar. Für die Zahlen $1/\ell$ lässt sich so argumentieren: ℓ ist in $\mathbb{Z}/p^m\mathbb{Z}$ für jedes $m \geq 0$ invertierbar, also gibt es ganze Zahlen a_m, sodass $1/\ell \equiv a_m \bmod (p^m)$, und diese Zahlen a_m bilden eine Cauchy-Folge in $\mathbb{Z}$, die gegen $1/\ell$ konvergiert, das folglich in $\mathbb{Z}_p$ liegt.

Das war schon eine ziemlich gute Übung für das folgende Lemma. Sie zeigt aber auch, dass $\mathbb{Q}_p^\times = p^{\mathbb{Z}} \cdot \mathbb{Z}_p^\times$.

Lemma von Hensel *Es sei $f \in \mathbb{Z}[X]$ ein Polynom, das modulo der Primzahl p eine einfache Nullstelle a hat, das heißt*

$$f(a) \equiv 0 \pmod p,\ f'(a) \not\equiv 0 \pmod p.$$

Dann hat f eine Nullstelle in $\mathbb{Z}_p$, die modulo p zu a kongruent ist.

Beweis: Zum Beweis zeigen wir, dass es in $\mathbb{Z}$ eine Cauchyfolge (a_m) gibt, sodass die Funktionswerte $f(a_m)$ gegen 0 konvergieren. Dies ist eine Variante des Newton-Verfahrens (mit dem kleinen aber feinen Unterschied, dass es hier richtig schön funktioniert...).

Hierzu setzen wir $a_1 := a$. Wir nehmen nun an, dass wir bereits $a_1, \ldots, a_k$ konstruiert hätten, sodass gilt:

$$\begin{array}{rcll} a_{i+1} & \equiv & a_i \pmod{p^i}, & 1 \leq i \leq k-1, \\ f(a_i) & \equiv & 0 \pmod{p^i}, & 1 \leq i \leq k, \\ f'(a_i) & \not\equiv & 0 \pmod p, & 1 \leq i \leq k. \end{array}$$

Nun konstruieren wir ein dazu passendes a_{k+1}. Dazu setzen wir $a_{k+1} := a_k - tf(a_k)$, wobei t modulo p^{k+1} zu $f'(a_k)$ invers sei. Dann gilt $a_{k+1} \equiv a_k \pmod{p^k}$, da p^k ein Teiler von $f(a_k)$ ist. Außerdem ist $f'(a_{k+1}) \equiv f'(a_k) \not\equiv 0 \pmod p$. Schließlich gilt wegen der binomischen Formel

$$f(a_{k+1}) = f(a_k) - f'(a_k)tf(a_k) + \ldots \equiv 0 \pmod{p^{k+1}},$$

da ... modulo p^{k+1} Null ist – es wird ja von $f(a_k)^2$ geteilt. So, das wars.

○

Beispiele:

a) In $\mathbb{F}_p$ gibt es ein Element mit multiplikativer Ordnung $p-1$, eine sogenannte primitive $(p-1)$-te Einheitswurzel. Dies ist eine Nullstelle des $(p-1)$-ten Kreisteilungspolynoms $(X^p-1)/(X-1) = X^{p-1} + X^{p-2} + \ldots + X + 1$. Hensels Lemma sagt nun, dass dieses Polynom auch in $\mathbb{Z}_p$ eine Nullstelle hat, denn $X^p - 1$ hat nur einfache Nullstellen. Mithin gibt es auch in $\mathbb{Z}_p$ eine primitive $(p-1)$-te Einheitswurzel.

b) Die Quadrate in $\mathbb{F}_p^\times$ bilden eine Untergruppe vom Index 2, denn sie sind das Bild des Gruppenendomorphismus $x \mapsto x^2$ mit Kern $\{\pm 1\}$. Wenn $a \in \mathbb{Z}_p^\times$ modulo p ein Quadrat ist, so sagt Hensels Lemma, dass $x^2 - a$ auch eine Nullstelle in $\mathbb{Z}_p^\times$ hat, sofern $p \neq 2$. Das heißt, dass die Quadrate auch in $\mathbb{Z}_p^\times$ eine Untergruppe vom Index 2 bilden. In $\mathbb{Q}_p^\times$ haben die Quadrate Index 4, da ein Element $p^n u$ mit $n \in \mathbb{Z}$, $u \in \mathbb{Z}_p^\times$ genau dann ein Quadrat ist, wenn n gerade und u selbst ein Quadrat ist.

Achtung: In $\mathbb{Q}_2^\times$ gibt es 8 Quadrateklassen. Sie werden von den Zahlen $1, 3, 5, 7, 2, 6, 10, 14$ repräsentiert. Für einen Beweis hiervon müsste man erst einmal das Lemma von Hensel etwas verfeinern. Alternativ darf man die Taylor-Reihe für $\sqrt{1+x}$ verwenden und sich überlegen, dass

$$\sqrt{1+x} = 1 + \frac{1}{2}x - \frac{1\cdot 1}{2\cdot 4}x^2 + \frac{1\cdot 1\cdot 3}{2\cdot 4\cdot 6}x^3 - \frac{1\cdot 1\cdot 3\cdot 5}{2\cdot 4\cdot 6\cdot 8}x^4 \ldots$$

in $\mathbb{Z}_2$ konvergiert, wenn $x \in 8\mathbb{Z}_2$. Die obigen Zahlen sind offensichtlich keine Quadrate, und sie repräsentieren die Restklassen von

$$\mathbb{Q}_2^\times / (\langle 2^2 \rangle \cdot (1 + 8\mathbb{Z}_2)).$$

Quaternionenalgebren über $\mathbb{Q}_p$

Wir bezeichnen mit $1, e, p, ep$ Repräsentanten der vier Quadrateklassen in $\mathbb{Q}_p$, wobei wir $p \neq 2$ voraussetzen. Das Element e liege dabei in $\mathbb{Z}_p^\times$, wir könnten auch eine geeignete ganzrationale Zahl zwischen 2 und $p-1$ veranschlagen.

Nun sei $\left(\frac{a,b}{\mathbb{Q}_p}\right)$ eine nicht zerfallende Quaternionenalgebra. Die Elemente $a, b \in \mathbb{Q}_p$ können wir um beliebige von Null verschiedene Quadrate abändern und dürfen also annehmen, dass sie alle in $\{e, p, ep\}$ liegen. $a = 1$ oder $b = 1$ sind ausgeschlossen, da die Algebra ja nicht zerfallen soll. Außerdem dürfen a und $-b$ nicht in der selben Quadrateklasse liegen, da sonst $K^2 = -ab$ ein Quadrat in $\mathbb{Q}_p$ wäre, und die Algebra wieder zerfiele. Wären a und b beide gleich e, so wäre die Normenform auch modulo p regulär und durch die Diagonalmatrix $\operatorname{diag}(1, e, e, -e^2)$ gegeben, aber das ist eine isotrope Form, und das Lemma von Hensel zeigt, dass dann die Normenform auch über $\mathbb{Q}_p$ isotrop ist, was wir ausgeschlossen haben.

Wenn man so weiter macht, sieht man schließlich ein, dass die einzige nicht zerfallende Quaternionenalgebra über $\mathbb{Q}_p$ die Algebra

$$\left(\frac{e, p}{\mathbb{Q}_p}\right)$$

ist.

Übrigens ist die einzige nicht zerfallende Quaternionenalgebra über $\mathbb{Q}_2$ die Algebra

$$\left(\frac{-1, -1}{\mathbb{Q}_2}\right).$$

Normen Die Liste der Quaternionenalgebren über $\mathbb{Q}_p$ zeigt, dass jede quadratische Erweiterung von $\mathbb{Q}_p$ Zerfällungskörper der nicht zerfallenden Algebra ist. Aus dem Abschnitt über Galoiskohomologie lernen wir, dass die Normengruppe der Erweiterung daher Index 2 in der Einheitengruppe $\mathbb{Q}_p^\times$ hat. Dies könnte man natürlich auch Fall für Fall nachrechnen. Das Ergebnis im Fall $p \neq 2$ ist dabei (wenn $e \in \mathbb{Z}_p^\times$ ein Nichtquadrat ist)

$$\begin{array}{rcl} N(\mathbb{Q}_p(\sqrt{p})) & = & \langle \text{Quadrate}, -p\rangle \\ N(\mathbb{Q}_p(\sqrt{e})) & = & \langle \mathbb{Z}_p^\times, p^2\rangle, \\ N(\mathbb{Q}_p(\sqrt{pe})) & = & \langle \text{Quadrate}, -p\epsilon\rangle. \end{array}$$

Eine analoge Liste für $\mathbb{Q}_2$ würde über die 7 quadratischen Erweiterungen Aufschluss geben. Zum Beispiel ist die Normengruppe von $\mathbb{Q}_2(\sqrt{2})$ gleich der Gruppe, die von Quadraten in $\mathbb{Z}_2$, von 2 und 7 erzeugt wird– siehe unten im Beweis von Hilberts Reziprozitätsgesetz!

Das Hilbertsymbol

Für zwei Einheiten $a, b \in \mathbb{Q}_p^\times$ definiert man nun (die Notation etwas strapazierend) das Hilbertsymbol

$$(a,b)_p := \begin{cases} 1, & \text{Quaternionenalgebra zerfällt,} \\ -1, & \text{Quaternionenalgebra zerfällt nicht.} \end{cases}$$

In den reellen Zahlen kann man genauso das Hilbertsymbol $(a,b)_\infty$ definieren.

Aus der Charakterisierung der Quaternionenalgebren durch ihre Normenform folgt sofort, dass

$$(a,b)_v = 1 \iff \exists (x,y,z) \neq (0,0,0) \in \mathbb{Q}_v^3 \text{ mit } x^2 - ay^2 - bz^2 = 0 \iff b \in N_{\mathbb{Q}_v(\sqrt{a})/\mathbb{Q}_v}(\mathbb{Q}_v(\sqrt{a})^\times).$$

Hilfssatz *Das Hilbertsymbol erfüllt die folgenden Bedingungen.*

a) Für festes $a \in F = \mathbb{Q}_v^\times$ *gilt* $(a, b_1 b_2)_v = (a,b_1)_v (a,b_2)_v$.

a') Für festes $b \in F = \mathbb{Q}_v^\times$ *gilt* $(a_1 a_2, b)_v = (a_1,b)_v (a_2,b)_v$.

b) $(a,-a)_v = 1$.

c) $(a, 1-a)_v = 1$

Beweis. a) Wenn a ein Quadrat ist, so ist das Hilbertsymbol mit festem a konstant gleich 1, also die Behauptung wahr.

Wenn a kein Quadrat ist, so hat die Normengruppe von $\mathbb{Q}_v(\sqrt{a})$ Index 2 in $\mathbb{Q}_v^\times$. Aber diese Normengruppe ist genau die Menge der Werte für b, wo das Hilbertsymbol 1 wird. Das zeigt die Behauptung.

a') geht genauso. Überhaupt gilt ja auch $(a,b)_v = (b,a)_v$.

b) Wenn a ein Quadrat ist, so ist $(a,-a) = 1$ klar. Wenn es kein Quadrat ist, so ist $-a$ die Norm von $\sqrt{a}$.

c) $1^2 - a \cdot 1^2 - (1-a) \cdot 1^2 = 0$. ◯

§II.?? Einschub: Minkowskis Gitterpunktsatz

Vorbereitend dürfen wir den Gitterpunktsatz von Minkowski beweisen. Sie werden sehen, das macht Spaß.

Dazu sei $\Gamma \subset \mathbb{R}^d =: V$ die Untergruppe, die von einer Basis $\{b_1, \ldots, b_d\}$ von V erzeugt wird, zum Beispiel die Ordnung $\mathcal{O}$ im Matrizenring. Solch eine Untergruppe heißt ein *Gitter* in V. Zu der Basis gehört das *Fundamentalepiped*

$$\mathcal{F} := \{\sum a_i b_i | 0 \leq a_i \leq 1\},$$

und es gilt

$$V = \cup_{\gamma \in \Gamma} \gamma + \mathcal{F}.$$

Jetzt betrachten wir V als den euklidischen Standardraum, und hier hat $\mathcal{F}$ ein Volumen, nämlich $|\det(b_1 \ldots b_d)|$. Wenn $M \subseteq V$ eine beliebige messbare Menge ist, dann gilt

$$\mathrm{vol}(M) = \sum_{\gamma \in \Gamma} \mathrm{vol}(M \cap (\gamma + \mathcal{F})),$$

denn der Rand $R(\mathcal{F})$ von $\mathcal{F}$ ist eine Nullmenge, damit auch die abzählbare Vereinigung

$$\cup_{\gamma \in \Gamma} \gamma + R(\mathcal{F}),$$

und auf dem Komplement dieser Menge ist die Zerlegung von $v \in V$ in $v = \gamma + f, \gamma \in \Gamma,\ f \in \mathcal{F}$, eindeutig.

Nun beweisen wir einen der schönsten und einfachsten Sätze der Mathematik.

Satz (Gitterpunktsatz von Minkowski) *Es seien V der reelle d-dimensionale Standardraum, Γ die von der Basis $b_1, \ldots, b_d$ erzeugte Untergruppe, $\mathrm{cov}(\Gamma)$ das Volumen von $\mathcal{F}$ und M eine abgeschlossene, konvexe Teilmenge von V, die mit jedem Element x auch $-x$ enthält und Volumen $> 2^d \mathrm{cov}(\Gamma)$ hat. Dann enhält M ein von Null verschiedenes Element aus Γ.*

Beweis. Zunächst enthält M zwei verschiedene Elemente x und y, deren Differenz in 2Γ liegt. Denn ansonsten wäre

$$\mathrm{vol}(M) = \sum_{\gamma \in \Gamma} \mathrm{vol}((2\gamma + 2\mathcal{F}) \cap M) = \sum_{\gamma \in \Gamma} \mathrm{vol}(2\mathcal{F} \cap (2\gamma + M)) \leq \mathrm{vol}(2\mathcal{F}) = 2^d \mathrm{cov}(\Gamma).$$

Ätsch.

Dann ist aber $-y \in M$ wegen der Zentralsymmetrie, und auch die Konvexkombination $\frac{1}{2}(x - y)$ liegt in M. Diese liegt ebenso in Γ. ◯

Bemerkungen: a) Dieser Satz hat verschiedenste Anwendungen in der Zahlentheorie. Zum Beispiel kann man mit ihm zeigen, dass sich jede ungerade Primzahl p als Summe von 4 Quadraten schreiben lässt (hierzu muss man das Gitter geschickt wählen und ausnützen, dass $\left(\frac{-1,-1}{\mathbb{F}_p}\right)$ zerfällt...).

b) Wenn Γ eine Untergruppe von $\mathbb{Z}^d$ ist, so hat Λ endlichen Index, und dieser stimmt mit dem Kovolumen überein.

c) Wenn Λ ein Gitter vom Kovolumen v in $\mathbb{R}^d$ ist und $g \in \mathrm{GL}(d, \mathbb{R})$, so ist $g\Gamma$ ein Gitter vom Kovolumen $|\det(g)v|$ (Determinantenmultiplikationssatz...).

§II.2 Quaternionenalgebren über $\mathbb{Q}$

Über dem Körper der rationalen Zahlen wird das Verhalten der Quaternionenalgebra $\left(\frac{a,b}{\mathbb{Q}}\right)$ dominiert davon, wie die Quaternionenalgebren $\left(\frac{a,b}{F}\right)$ aussieht, wenn F die lokalen

Körper aus dem vorherigen Abschnitt durchläuft, wozu auch die reellen Zahlen gezählt werden.

Insbesondere kann man für rationale Zahlen $a, b \in \mathbb{Q}^\times$ die Hilbertsymbole auswerten. Dazu sei $\Sigma := \mathbb{P} \cup \{\infty\}$. Dann ist klar, dass es nur endlich viele Primzahlen p gibt, bei denen das Hilbertsymbol $(a,b)_p$ gleich -1 ist. Wir können ja a und b durch quadratfreie ganze Zahlen ersetzen, ohne das Hilbertsymbol zu ändern, und dann ist für $p \neq 2$ das Hilbertsymbol sicher 1, wenn p kein Teiler von ab ist. Also gibt es nur endlich viele $v \in \Sigma$ mit $(a,b)_v = -1$.

Es folgen zwei Sätze, die das Wechselspiel zwischen dem globalen Körper der rationalen Zahlen und seinen Komplettierungen $\mathbb{Q}_v,\ v \in \Sigma$ beleuchten.

Satz (Hilbert-Reziprozität) *a) Es seien $a, b \in \mathbb{Q}^\times$ gegeben. Dann gilt:*

$$\prod_{v \in \Sigma} (a,b)_v = 1.$$

Insbesondere ist die Anzahl der Stellen, bei denen die Quaternionenalgebra unzerlegt ist, gerade.

b) Ist $I \subseteq \Sigma$ eine endliche Teilmenge gerader Kardinalität, so gibt es Zahlen $a, b \in \mathbb{Q}^\times$, so dass

$$\forall v \in \Sigma : (a,b)_v = -1 \iff v \in I.$$

Es lässt sich also recht präzise vorschreiben, wie ein Quaternionenalgebra lokal auszusehen hat. Dieses Faktum ist bisweilen in der Theorie der automorphen Formen von Wichtigkeit (base change formalism...). Teil b) ist sehr aufwändig zu beweisen; wir wollen uns mit Teil a) begnügen. Er sollte als Analogon zur Produktformel

$$\forall a \in \mathbb{Q}^\times : \prod_{v \in \Sigma} |a|_v = 1$$

betrachtet werden. Dabei ist $|a|_p := p^{-\mathrm{v}_p(a)}$ der normierte p-adische Betrag von a, und $|a|_\infty$ ist der übliche reelle Absolutbetrag von a.

Beweis von Aussage a) Wir müssen zeigen, dass

$$\prod_{v \in \Sigma} (a,b)_v = 1.$$

Die linke und die rechte Seite dieser Gleichung sind multiplikativ in a und b, also langt es, wenn wir die Gleichung für Erzeuger der Gruppe $\mathbb{Q}^\times$ zeigen. Hierfür wählen wir natürlich die Primzahlen und die Zahl -1.

Fall 1: $a = p$ und $b = q$ sind verschiedene ungerade Primzahlen. Für $v = \infty$ ist dann

$$(p,q)_v = 1,$$

genauso auch für Primzahlen $v \notin \{2, p, q\}$. Bleiben die Fälle $v = 2, p, q$. Zunächst gilt

$$(p,q)_p = \left(\frac{q}{p}\right) \text{ und } (p,q)_q = \left(\frac{p}{q}\right),$$

wobei links jeweils das Legendre-Symbol steht. Denn die Normengruppe von $\mathbb{Q}_p(\sqrt{p})$ wird von den Quadraten in $\mathbb{Q}_p$ und von $-p$ erzeugt, und q ist darin genau dann, wenn q ein Quadrat in $\mathbb{Q}_p$ ist, also genau dann, wenn q ein Quadrat in $\mathbb{Z}_p$ ist, also genau dann, wenn q ein Quadrat in $\mathbb{F}_p$ ist. Nun muss man noch nachrechnen, dass

$$(p,q)_2 = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

gilt, um mit dem quadratischen Reziprozitätsgesetz zu sehen, dass die Formel in a) stimmt. Diese Gleichung aber folgt, wenn man beachtet, dass

$$(p,q)_2 = 1 \iff p \text{ ist Quadrat oder } q = x^2 - py^2, x, y, \in \mathbb{Q}_2.$$

Der erste Fall ist gleichbedeutend mit $p \equiv 1 \pmod 8$, und hier wird die rechte Seite auch 1. Im zweiten Fall gibt es sogar $x, y \in \mathbb{Z}_2$ mit $q = x^2 - py^2$, und Reduktion modulo 4 zeigt, dass q zu 1 oder $-p$ kongruent ist. Dann ist aber p oder q kongruent zu 1 (modulo 4) und damit der Exponent auf der rechten Seite gerade. Hensels Lemma zeigt umgekehrt, dass im Fall $p \equiv 1 \pmod 4$ tatsächlich jedes ungerade q als Norm von $\mathbb{Q}_2(\sqrt{p})$ auftaucht. Wenn umgekehrt beide Primzahlen 3 modulo 4 sind, so ist $(p,q)_2 = -1 = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Fall 2: $a = 2$ und $b = p$ eine ungerade Primzahl. Für $v = \infty$ sowie für Primzahlen $v \neq 2, p$ gilt wieder $(2,p)_v = 1$. $(2,p)_p = \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ gilt wie eben, und $(2,p)_2 = 1$ genau dann, wenn p eine Norm von $\mathbb{Q}_2(\sqrt{2})$ ist, aber diese Normengruppe wird erzeugt von den Quadraten in $\mathbb{Z}_2^\times$ und von $-1 = 1^2 - 2 \cdot 1^2$ und $-2 = 0^2 - 2 \cdot 1^2$. Also ist p eine Norm genau dann, wenn $p \equiv \pm 1 \pmod 8$, so wie wir es brauchen.

Die übrigen Fälle können analog behandelt werden. ◯

Satz (Hasse-Minkowski) *Es seien $a, b \in \mathbb{Q}^\times$ gegeben. Dann zerfällt die Quaternionenalgebra $\left(\frac{a,b}{\mathbb{Q}}\right)$ genau dann, wenn für alle $v \in \Sigma$ das Hilbertsymbol $(a,b)_v$ gleich 1 ist.*

Der Satz von Hasse und Minkowski ist eigentlich ein Satz über quadratische Formen, den wir hier aber direkt für Quaternionenalgebren hingeschrieben haben, da eine Quaternionenalgebra ja genau dann zerfällt, wenn ihre Normenform isotrop ist.

Eigentlich sagt der Satz von Hasse und Minkowski, dass eine reguläre rationale quadratische Form genau dann über $\mathbb{Q}$ isotrop ist, wenn sie über allen Komplettierungen $\mathbb{Q}_v$, $v \in \Sigma$, isotrop ist. Der Beweis verläuft in der Regel induktiv nach der Dimension, wobei die Dimensionen ≤ 4 einzeln abgehandelt werden müssen, auch wenn die Induktionsvoraussetzung jeweils von Belang ist. Schließlich wird in vielen Beweisen der Satz von Dirichlet benutzt, dass sich unter den natürlichen Zahlen, die modulo b zu a kongruent sind, immer mindestens eine Primzahl befindet, wenn a und b teilerfremd sind.

Ein leichter Vorgeschmack auf die Qualität der Aussage des Satzes findet sich wieder in der Tatsache, dass eine von 0 verschiedene rationale Zahl a genau dann in $\mathbb{Q}$ ein Quadrat ist, wenn sie in allen $\mathbb{Q}_v$, $v \in \Sigma$, ein Quadrat ist. Denn dann ist sie positiv (Quadrat in $\mathbb{R}$) und wird von jeder Primzahl p in einer geraden Potenz geteilt (Quadrat in $\mathbb{Q}_p$).

Nun folgt der Beweis der uns interessierenden Aussage des Satzes.

(länglicher) Beweis. Offensichtlich haben wir zu zeigen, dass die rationale quadratische Form $x^2 - ay^2 - bz^2$ genau dann eine nichttriviale rationale Nullstelle hat, wenn sie in jeder Komplettierung eine nichttriviale Nullstelle hat. Dabei dürfen wir die Zahlen a und

b als quadratfrei und ganz annehmen. Falls a und b den gemeinsamen Teiler d haben, so können wir diesen durch Variablentransformation $x \mapsto x/d$ und Division der Form durch d in den ersten Eintrag schieben (wir interessieren uns ja nur für die Isotropie...). Also haben wir das folgende Problem:

Es seien ab jetzt $a_1, a_2, a_3 \in \mathbb{Z}$ paarweise teilerfremd und quadratfrei. Die quadratische Form $Q(x_1, x_2, x_3) := \sum a_i x_i^2$ sei über jedem Körper $\mathbb{Q}_v$ isotrop. Dann ist sie auch über $\mathbb{Q}$ isotrop.

Dies zeigen wir mittels des Gitterpunktsatzes von Minkowski (siehe später), indem wir eine Untergruppe Λ von $\mathbb{Z}^3$ durch Kongruenzbedingungen definieren, die von den Primteilern von $2a_1a_2a_3$ herkommen.

Fall 1: Die ungerade Primzahl p teilt a_i. Seien $j < k$ die beiden übrigen Indizes: $\{i, j, k\} = \{1, 2, 3\}$. Da Q über $\mathbb{Q}_p$ isotrop ist, gibt es sogar eine Nullstelle in $\mathbb{Z}_p^3$, und es muss $a_j x_j^2 + a_k x_k^2 \equiv 0 \pmod{p}$ gelten. Wenn x_j durch p teilbar ist, so auch x_k und dann auch x_i (hier benutzen wir, dass $p \mid a_i$ und $p^2 \not| a_1a_2a_3$), also lassen sich alle durch p teilen und wir können ohne Einschränkung annehmen, dass x_j und x_k nicht durch p geteilt werden. Dann lassen sie sich aber in $\mathbb{Z}_p$ invertieren und es gibt eine ganze Zahl $r_p \in \mathbb{Z}$, sodass $a_j r_p^2 + a_k \equiv 0 \pmod{p}$. An das Gitter Λ stellen wir nun die Bedingung, dass seine Elemente (z_1, z_2, z_3) die Kongruenz

$$z_j \equiv r_p z_k \pmod{p}$$

erfüllen, wobei j und k die selbe Bedeutung wie oben haben, und auch r_p das gerade gewählte ist.

Fall 2: 2 teilt a_i. Dann gilt mit j und k wie in Fall 1, dass es ein $s \in \{0, 1\}$ gibt mit $a_i s^2 + a_j + a_k \equiv 0 \pmod{8}$, wie man ähnlich wie in Fall 1 zeigt. Hier fordern wir die Kongruenzen

$$z_j \equiv z_k \pmod{4}, \quad z_i \equiv s z_j \pmod{2}.$$

Fall 3: $a_1a_2a_3$ ist ungerade. Dann gibt es Indizes j und k, sodass $a_j + a_j \equiv 0 \pmod{4}$. Unsere Bedingung an Λ ist dann

$$z_j \equiv z_k \pmod{2}, \quad z_i \equiv 0 \pmod{2}.$$

Damit haben wir eine Untergruppe Λ vom Index $4|a_1a_2a_3|$ in $\mathbb{Z}^3$ definiert. Der Gitterpunktsatz von Minkowski sagt dann, dass diese Untergruppe ein von Null verschiedenes Element der konvexen, zentralsymmetrischen Menge

$$M := \{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid |a_1|x_1^2 + |a_2|x_2^2|a_3|x_3^2 < 4|a_1a_2a_3|\}$$

enthält, denn diese Menge hat Volumen $\frac{\pi}{3} 2^3 |4a_1a_2a_3| > 2^3 \mathrm{cov}(\Lambda)$.

Dieses Element $(z_1, z_2, z_3) \in \Lambda \cap M$ erfüllt dann nach Konstruktion von Λ sicher die Kongruenz $Q(z_1, z_2, z_3) \equiv 0 \pmod{4a_1a_2a_3}$, also gilt wegen der Definition von M sogar Gleichheit, und die Form ist isotrop. ◯

Bemerkung: Der Satz von Hasse und Minkowski sagt uns, das es ganz einfach zu entscheiden ist, ob eine Quaternionenalgebra zerfällt. In Wirklichkeit, wenn wir den Satz für alle quadratischen Formen bewiesen hätten, könnten wir sogar zeigen, dass zwei rationale Quaternionenalgebren genau dann isomorph sind, wenn ihre Hilbertsymbole sämtlich

übereinstimmen. Oder auch nur alle bis auf eins, denn dann sagt uns Hilbert's Reziprozitätsgesetz, dass das letzte jeweils auch übereinstimmt. Das erleichtert manchmal die Arbeit.

§II.3 Ordnung muss sein

Im Körper der rationale Zahlen gibt es den Teilring der ganzen Zahlen, und manche Aussagen über $\mathbb{Q}$ lassen sich geometrisch verstehen, indem man ausnützt, dass $\mathbb{Z}$ diskret in $\mathbb{R}$ liegt. So etwas ähnliches möchte man für Quaternionenalgebren auch können.

Definition Es sei A eine Quaternionenalgebra über $\mathbb{Q}$. Eine *Ordnung* in A ist ein Teilring, dessen additive Gruppe endlich erzeugt ist, und der A über $\mathbb{Q}$ erzeugt.

Eine Ordnung heißt *Maximalordnung*, wenn es keine Ordnung gibt, die sie echt enthält.

Beispiele a) Wenn a und b ganze Zahlen sind, so ist

$$\mathbb{Z} \oplus \mathbb{Z}I \oplus \mathbb{Z}J \oplus \mathbb{Z}K$$

eine Ordnung in $\left(\frac{a,b}{\mathbb{Q}}\right)$.

b) Die Ordnung

$$\mathbb{Z} \oplus \mathbb{Z}I \oplus \mathbb{Z}J \oplus \mathbb{Z}\frac{1+I+J+K}{2}$$

ist eine Maximalordnung in $\left(\frac{-1,-1}{\mathbb{Q}}\right)$, die sogenannte Hurwitzordnung.

An Beispiel a) sieht man, dass es in jeder Quaternionenalgebra Ordnungen gibt. Beispiel b) zeigt, dass man sich auch im 19. Jhdt. schon mit der Arithmetik von Quaternionenalgebren beschäftigt hat.

Lemma *Es sei A eine rationale Quaternionenalgebra.*

a) Die additive Gruppe einer Ordnung von A wird von einer $\mathbb{Q}$-Basis von A erzeugt.

b) Jede Ordnung von A ist in einer Maximalordnung enthalten.

Beweis. a) Da die additive Gruppe der Ordnung endlich erzeugt ist, ist sie frei abelsch, da torsionsfrei. Ein minimales Erzeugendensystem ist damit über den rationalen Zahlen linear unabhängig, muss aber andererseits ein Erzeugendensystem des Vektorraums sein.

b)

◯

Lemma *Es sei $\mathcal{O}$ eine Ordnung in der rationalen Quaternionenalgebra A und $N \in \mathbb{Z} \setminus \{0\}$. Dann gibt es nur endlich viele Assoziiertenklassen von Elementen der Norm N in $\mathcal{O}$, d.h. es gibt Elemente $o_1, \ldots, o_n \in \mathcal{O}$, sodass für jedes Element von Norm N in $\mathcal{O}$ ein $i \in \{1, \ldots n\}$ und eine Einheit $u \in \mathcal{O}^\times$ existieren mit*

$$x = u \cdot o_i.$$

Beweis. Ein Element x von Norm N erzeugt ein einseitiges Hauptideal $\mathcal{O}x$ in $\mathcal{O}$ vom Index N^2. Da es in der Gruppe $\mathbb{Z}^4$ nur endlich viele Untergruppen vom Index N^2 gibt (diese finden sich ja als Urbilder von Untergruppen vom Index N^2 in $(\mathbb{Z}/N^2\mathbb{Z})^4$) gibt es auch nur endlich viele einseitige Hauptideale, die von Elementen von Norm N erzeugt werden. Nenne ihre Anzahl n und wähle Erzeuger $o_1, \ldots, o_n$. ◯

Lemma *Es sei $\mathcal{O}$ eine Ordnung in der rationalen Quaternionenalgebra A. Dann ist $x \in \mathcal{O}$ genau dann eine Einheit, wenn die Norm von x gleich ± 1 ist.*

Beweis. Entweder man glaubt die Aussage über den Index des von x erzeugten einseitigen Hauptideals aus dem vorherigen Lemma oder man überlegt sich, dass $\mathcal{O}$ unter der Hauptinvolution von A invariant ist, da die Spur eines Elements aus $\mathcal{O}$ in $2\mathbb{Z}$ liegt, und somit $\iota(x) = \frac{1}{2}\mathrm{Spur}(x) - x$ auch in $\mathcal{O}$ liegt. Wenn nun x eine Einheit ist, so liegt auch x^{-1} in $\mathcal{O}$, und somit mnuss die Norm eine Eiheit in $\mathbb{Z}$ sein. Wenn umgekehrt x Norm ± 1 hat, so ist auch $x^{-1} = N(x)^{-1}\iota(x) \in \mathcal{O}$ und somit x eine Einheit. ◯

Folgerung *Es sei $\mathcal{O}$ eine Ordnung in der definiten rationalen Quaternionenalgebra A. Dann ist die Einheitengruppe $\mathcal{O}^\times$ endlich.*

Beweis. Die zugehörige reelle Quaternionenalgebra $A_\mathbb{R}$ ist die Algebra der Hamilton-Quaternionen. Darin bilden die Elemente von Norm 1 eine kompakte Teilmenge, es ist ja die dreidimensionale Sphäre. Andererseits ist $\mathcal{O}$ in $A_\mathbb{R}$ diskret, da es von einer Basis erzeugt wird. Das heißt aber auch, dass $\mathcal{O}^\times$ eine diskrete Teilmenge der kompakten Dreisphäre ist, also endlich sein muss. ◯

§II.4 Die Einheitengruppen von indefiniten Quaternionenalgebren

Ab jetzt wollen wir annehmen, dass die rationale Quaternionenalgebra A indefinit ist, d.h. $A_\mathbb{R}$ ist isomorph zu $M_2(\mathbb{R})$, und wir wählen einen solchen Isomorphismus, der insbesondere auch A nach $M_2(\mathbb{R})$ einbettet und damit auch jede Ordnung $\mathcal{O}$ von A. Wie im letzten Abschnitt ist dann $\mathcal{O}$ eine diskrete Untergruppe von $M_2(\mathbb{R}) \simeq \mathbb{R}^4$, und die Gruppe $\mathcal{O}_1^\times$ der Einheiten in $\mathcal{O}$ mit Norm 1 ist eine diskrete Untergruppe von $\mathrm{SL}_2(\mathbb{R})$. Diese geometrische Situation soll nun benutzt werden, um zu zeigen, dass $\mathcal{O}_1^\times$ unendlich ist, ja sogar mehr, dass es so groß ist, dass $\mathrm{SL}_2(\mathbb{R}) = \mathcal{O}_1^\times \cdot C$ für eine geeignete kompakte Teilmenge $C \subset \mathrm{SL}_2(\mathbb{R})$ gilt – vorausgesetzt, die Quaternionenalgebra ist über $\mathbb{Q}$ ein Schiefkörper.

Satz *Es sei $A \subseteq M_2(\mathbb{R})$ eine indefinite nicht zerfallenden rationale Quaternionenalgebra und $\mathcal{O}$ eine Ordnung in A. Dann gibt es eine kompakte Teilmenge C von $SL(2,\mathbb{R})$, sodass*

$$\mathrm{SL}(2,\mathbb{R}) = \mathcal{O}_1^\times \cdot C.$$

Da $SL(2,\mathbb{R})$ nicht kompakt ist, muss also $\mathcal{O}_1^\times$ unendlich sein.

Beweis. Wir fassen $M_2(\mathbb{R})$ als vierdimensionalen euklidischen Vektorraum auf und wählen darin eine Kugel B um den Nullpunkt so groß, dass ihr Volumen größer ist als $2^4\mathrm{cov}(\mathcal{O})$. Nun sei $g \in \mathrm{SL}(2,\mathbb{R})$ beliebig.

Dann ist $g\mathcal{O}$ ein Gitter in $M_2(\mathbb{R})$ vom selben Kovolumen wie $\mathcal{O}$. Also gibt es ein von Null verschiedenes Element $o_g \in \mathcal{O}$, sodass

$$o_g g \in B.$$

Da A nicht zerfällt, hat o_g eine von Null verschiedene Norm, die in $\mathbb{Z}$ liegt, da o_g in einer Ordnung liegt, also ganz über $\mathbb{Z}$ ist. Das Element $o_g g$ liegt in B, und da B kompakt ist, werden auf B nur endlich viele ganze Normen angenommen ($N(B)$ ist kompakt...).

Nach dem Lemma über die Endlichkeit der Menge der Assoziiertenklassen von Elementen aus $\mathcal{O}$ mit gegebener Norm gibt es also endlich viele ELemente $g_1, \ldots, g_k \in \mathrm{SL}(2,\mathbb{R})$, sodass alle o_g zu mindestens einem der o_{g_i} assoziiert sind. Bei Übergang zu den Einheiten

von Norm 1 ändert sich daran nichts:

$$\forall g \in \mathrm{SL}(2,\mathbb{R}) : \exists i \in \{1,\ldots,k\}, u_g \in \mathcal{O}_1^\times : o_g = o_{g_i} u_g.$$

Dann ist aber

$$g \in o_g^{-1} B = u_g^{-1} o_{g_i}^{-1} B \subseteq \mathcal{O}_1^\times \cup_{j=1}^k o_{g_j}^{-1} B,$$

und die endliche Vereinigung $\cup_{j=1}^k o_{g_j}^{-1} B$ ist kompakt. Wenn man sie mit $\mathrm{SL}(2,\mathbb{R})$ schneidet, erhält man die gewünschte Menge C. ◯

Ausblicke

Nun betrachten wir die Iwasawa-Zerlegung von $\mathrm{SL}(2,\mathbb{R})$, wir schreiben also

$$\mathrm{SL}(2,\mathbb{R}) = N \cdot T \cdot K,$$

wobei $N, T,$ und K die folgenden Untergruppen sind:

$$\begin{aligned} N &= \{\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \mid y \in \mathbb{R}\}, \\ T &= \{\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \mid 0 < x \in \mathbb{R}\}, \\ K &= \{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{R},\ a^2 + b^2 = 1\} = \mathrm{SO}(2). \end{aligned}$$

Diese Zerlegung stimmt wegen des Gram-Schmidt-Verfahrens. Dabei ist K eine maximale kompakte Untergruppe. $\Gamma := \mathcal{O}_1^\times$ operiert nun auf dem Raum der Nebenklassen $\mathcal{H} := \mathrm{SL}(2,\mathbb{R})/K$, der als Repräsentantenmenge die Menge NT hat. Diese wiederum kann man via Möbiustransformationen topologisch mit der oberen Halbebene $\{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ identifizieren. Eine kompakte Teilmenge M von $\mathcal{H}$ wird von einem Element $\gamma \in \Gamma$ genau dann mit sich zum Schnitt gebracht, wenn γ in der kompakten Menge $\{m\tilde{m}^{-1} \mid mK \in M\}$ von $\mathrm{SL}(2,\mathbb{R})$ liegt. Da Γ eine diskrete Untergruppe von $\mathrm{SL}(2,\mathbb{R})$ ist, kann dies nur für endlich viele Elemente von Γ zutreffen. Man sagt in diesem Fall, dass Γ eigentlich diskontinuierlich auf $\mathcal{H}$ operiert.

NB Wir haben gezeigt, dass $\Gamma \subseteq \mathrm{SL}(2,\mathbb{R})$ sicher dann eigentlich diskontinuierlich auf $\mathcal{H}$ operiert, wenn es diskret ist. Die Umkehrung hiervon gilt auch.

Aufgrund des vorherigen Satzes gibt es eine kompakte Teilmenge von $\mathcal{H}$, die von jeder Γ–Bahn ein Element enthält. Dies zeigt, dass es auch einen kompakten Fundamentalberecih von Γ geben muss. Der Quotient $\Gamma\backslash\mathcal{H}$ ist eine kompakte Riemannsche Fläche. Nach einem Satz von Poincaré lässt sich ein Fundamentalbereich finden, der nur endlich viele „Randstücke“ hat. Dies zeigt dann sogar, dass die Gruppe Γ endlich erzeugt ist. Ein Lemma von Selberg sagt dann, dass es in Γ eine Untergruppe Δ von endlichem Index gibt, die torsionsfrei ist, also keine Elemente von endlicher Ordnung enthält. Diese Untergruppe ist dann die Fundamentalgruppe von $\Delta\backslash\mathcal{H}$. In aller Regel ist es nicht sehr einfach, einen Fundamentalbereich zu bestimmen, zumal die Einheitengruppe nicht sehr leicht anzugeben ist.

Dies lässt sich verallgemeinern, indem man Quaternionenalgebren A über total reellen Zahlkörpern F verwendet, die an genau einer unendlichen Stelle zerfallen und sonst die Hamilton-Quaternionen sind. Dann ist immer noch die Einheitengruppe einer Ordnung (die man hier ausgehend von einer Ordnung in F definiert) kokompakt in $(A \otimes_{\mathbb{Q}} \mathbb{R})_1^\times$,

und operiert eigentlich diskontinuierlich auf dem einzigen nichtkompakten Faktor dieser Gruppe, der wieder $\mathrm{SL}(2,\mathbb{R})$ ist.

Beispiel: $F = \mathbb{Q}(\sqrt{2})$, $R = \mathbb{Z}[\sqrt{2}], A = \left(\frac{1-\sqrt{2},1-\sqrt{2}}{F}\right), \mathcal{O} = R[I,J]$. Dabei ist $A \otimes_{\mathbb{Q}} \mathbb{R} = M_2(\mathbb{R}) \oplus \mathbb{H}$, und $\mathcal{O}_1^\times \subseteq \mathrm{SL}(2,\mathbb{R}) \times \mathbb{H}_1^\times \longrightarrow \mathrm{SL}(2,\mathbb{R})$ ist eine diskrete Untergruppe.

Mithilfe von solchen arithmetischen Gruppen hat Marie-France Vigneras eine Frage von Milnor (1964) beantwortet, (das war 1978) nämlich ob es zwei Riemannsche Flächen gibt, deren geodätischen dieselben Längen haben, die aber nicht durch eine Isometrie ineinander abgebildet werden können. Die Antwort ist JA, und Beispiele lassen sich eben durch Einheitengruppen in Ordnungen von Quaternionenalgebren „konstruieren“, wobei die Arithmetik der Quaternionengruppen überhaupt dafür sorgt, dass man die Übersicht über die Längen der Geodätischen behält. Mittlerweile gibt es eine ganze Industrie, die solche Beispiele konstruiert, auch auf andere Weise, siehe zum Beispiel Arbeiten von Sunada oder Schüth.

Im Fall der zerfallenden Quaternionenalgebra über $\mathbb{Q}$ ist der entsprechende Quotient $\mathrm{SL}(2,\mathbb{Z})\backslash\mathcal{H}$ nicht kompakt, hat aber immerhin endliches (hyperbolisches) Volumen. Auf ihm wird die Analysis erleichtert durch die Möglichkeit, Fouriertransformationen zu betrachten. Diese Möglichkeit hat man für die kompakten Quotienten $\Gamma\backslash\mathcal{H}$ nicht, dafür gelten hier eben Sätze, für deren Beweis man die Kompaktheit benützt (Spektrum des Laplace-Operators, Hodge-Zerlegung...). Diese Sätze in dem anderen arithmetischen Fall $\mathrm{SL}(2,\mathbb{Z})\backslash\mathcal{H}$ anzunähern ist in mancherlei Hinsicht mithilfe zahlentheoretischer Argumente möglich, aber nicht einfach. Es ist hier ein sehr interessantes Gebiet entstanden, in dem sich Differentialgeometrie, Zahlentheorie, algebraische Geometrie, Topologie, Funktionalanalysis usw. gegenseitig befruchten. Aber das wäre ein Thema für (mindestens!) eine andere Vorlesung.