

Lösung 6

Aufgabe 1.

Sei $I \in \mathbf{C}$ die imaginäre Einheit in $\mathbf{C}$, $I^2 = -1$ (um Verwechslungen mit $i \in \mathbf{H}$, $i \in \Omega$ zu vermeiden.)

(1+2) **H** : Wir haben einen $\mathbf{C}$ -Algebren-Morphismus

$$\begin{aligned} \mathbf{H}_{\mathbf{C}} &\xrightarrow{\varphi} \mathbf{C}^{2 \times 2} \\ i &\longmapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ j &\longmapsto \begin{pmatrix} I & 0 \\ 0 & -I \end{pmatrix}, \end{aligned}$$

wie man durch Nachrechnen der Relationen $i^2 = -1$, $j^2 = -1$ und $ij = -ji$ auf den Bildern bestätigt. Da $1 \longmapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ und $ij \longmapsto \begin{pmatrix} 0 & -I \\ -I & 0 \end{pmatrix}$, da also ein $\mathbf{C}$ -lineares Erzeugendensystem von $\mathbf{C}^{2 \times 2}$ im Bild von φ liegt, ist φ surjektiv.

Für die Injektivität wollen wir zeigen, daß $\dim_{\mathbf{C}} \mathbf{H}_{\mathbf{C}} \leq 4$. Dazu genügt es, jedes Element von $\mathbf{H}_{\mathbf{C}}$ als in $\mathbf{C}\langle 1, i, j, ij \rangle$ liegend nachzuweisen. Vermittels $ij = -ji$ dürfen wir annehmen, daß das Element von der Form $i^{\alpha}j^{\beta}$ ist, $\alpha, \beta \geq 0$. Die Relationen $i^2 = -1$ und $j^2 = -1$ erlauben dann, anzunehmen, daß $\alpha, \beta \leq 1$.

Damit ist sowohl gezeigt, daß φ ein Isomorphismus ist, als auch, daß $(1, i, j, ij)$ eine Basis von $\mathbf{H}_{\mathbf{C}}$ darstellt.

Insbesondere ist φ surjektiv, die durch φ auf $\mathbf{C}^2$ definierte Moduloperation, $\begin{pmatrix} x \\ y \end{pmatrix} \cdot \xi := \begin{pmatrix} x \\ y \end{pmatrix} (\xi\varphi)$ für $x, y \in \mathbf{C}$, $\xi \in \mathbf{H}_{\mathbf{C}}$, liefert mithin einen einfachen Modul. Um nun zu zeigen, daß $(1, i, j, ij)$ auch eine Basis von $\mathbf{H} := \mathbf{H}_{\mathbf{Q}}$ darstellt, verwendet man dasselbe Argument wie eben, um zu zeigen, daß es ein Erzeugendensystem ist. Eine $\mathbf{Q}$ -Linearkombination von $(1, i, j, ij)$ wäre insbesondere eine $\mathbf{C}$ -Linearkombination, ist also trivial.

Nun ist $\mathbf{H}_K \simeq \mathbf{H} \otimes_{\mathbf{Q}} K$, und eine $\mathbf{Q}$ -lineare Basis von $\mathbf{H}$ gibt eine K -lineare Basis von $\mathbf{H}_K$.

Ω : Wir haben einen $\mathbf{C}$ -Algebren-Morphismus

$$\begin{aligned} \Omega_{\mathbf{C}} &\xrightarrow{\psi} \mathbf{C}^{2 \times 2} \\ i &\longmapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ \omega &\longmapsto \begin{pmatrix} 0 & I \\ I & -1 \end{pmatrix}, \end{aligned}$$

wie man durch Nachrechnen der Relationen $i^2 = -1$, $\omega^2 = -1 - \omega$ und $\omega i = -i\omega - i$ auf den Bildern bestätigt. Da $1 \longmapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ und $i\omega \longmapsto \begin{pmatrix} I & -1 \\ 0 & -I \end{pmatrix}$, da also ein $\mathbf{C}$ -lineares Erzeugendensystem von $\mathbf{C}^{2 \times 2}$ im Bild von ψ liegt, ist ψ surjektiv.

Für die Injektivität wollen wir zeigen, daß $\dim_{\mathbf{C}} \Omega_{\mathbf{C}} \leq 4$. Dazu genügt es, jedes Element von $\Omega_{\mathbf{C}}$ als in $\mathbf{C}\langle 1, \omega, i, i\omega \rangle$ liegend nachzuweisen. Vermittels $\omega i = -i\omega - i$ dürfen wir annehmen, daß das Element von der Form $i^{\alpha}\omega^{\beta}$ ist, $\alpha, \beta \geq 0$. Die Relationen $i^2 = -1$ und $\omega^2 = -1 - \omega$ erlauben dann, anzunehmen, daß $\alpha, \beta \leq 1$.

Damit ist sowohl gezeigt, daß ψ ein Isomorphismus ist, als auch, daß $(1, \omega, i, i\omega)$ eine Basis von $\Omega_{\mathbf{C}}$ darstellt.

Insbesondere ist ψ surjektiv, die durch ψ auf $\mathbf{C}^2$ definierte Moduloperation liefert mithin einen einfachen Modul.

Genauso wie für Ω folgert man nun, daß $(1, \omega, i, i\omega)$ eine K -lineare Basis von Ω_K darstellt.

Um nun zu zeigen, daß $(1, \omega, i, i\omega)$ auch eine Basis von $\Omega := \Omega_{\mathbf{Q}}$ darstellt, verwendet man dasselbe Argument wie eben, um zu zeigen, daß es ein Erzeugendensystem ist. Eine $\mathbf{Q}$ -Linearkombination von $(1, \omega, i, i\omega)$ wäre insbesondere eine $\mathbf{C}$ -Linearkombination, ist also trivial.

Nun ist $\Omega_K \simeq \Omega \otimes_{\mathbf{Q}} K$, und eine $\mathbf{Q}$ -lineare Basis von Ω gibt eine K -lineare Basis von Ω_K .

- (3) **H** : Wir berechnen die $\mathbf{Q}$ -lineare Norm eines Elementes in **H** als $\mathbf{C}$ -lineare Norm des Elementes in $\mathbf{H}_{\mathbf{C}}$. Diese können wir unter Zuhilfenahme des Isomorphismus φ ausrechnen. Beachte, daß $N(\xi) = \det(\xi\varphi)^2$, da die Rechtsoperation von $\xi \in \mathbf{H}_{\mathbf{C}}$ auf $\mathbf{C}^{2 \times 2}$ als Blockdiagonalmatrix $\begin{pmatrix} \xi\varphi & \\ & \xi\varphi \end{pmatrix}$ geschrieben werden kann. (Die Determinante $\det(\xi\varphi)$ heißt auch die *reduzierte Norm* von ξ .) Das allgemeine Element $a + bi + cj + dij$, $a, b, c, d \in \mathbf{C}$, kommt unter φ auf $\begin{pmatrix} a+bI & c+dI \\ -c+dI & a-bI \end{pmatrix}$, und diese Bildmatrix hat Determinante $a^2 + b^2 + c^2 + d^2$.

Die Norm von $\mathbf{H}_K$ über K ist übrigens von derselben Formel gegeben. Denn hält man $a, b, c \in \mathbf{Q} \subseteq K$ fest, so ist diese Formel für alle $d \in \mathbf{Q}$ korrekt. Da die Norm ein Polynom (homogen von Grad 4) in a, b, c, d ist, folgt wegen $\#\mathbf{Q} = \infty$, daß die Formel für alle $a, b, c \in \mathbf{Q}$ und alle $d \in K$ gilt. Nun hält man $a, b \in \mathbf{Q}$ und $d \in K$ fest, läßt c durch $\mathbf{Q}$ laufen, und findet genauso, daß die Formel $a, b \in \mathbf{Q}$ und alle $c, d \in K$ gilt. So fährt man fort, bis nachgewiesen ist, daß die Formel für alle $a, b, c, d \in K$ gilt.

Ω : Das allgemeine Element $a + b\omega + ci + di\omega$, $a, b, c, d \in \mathbf{C}$, kommt unter φ auf $\begin{pmatrix} a+dI & c-d+bI \\ -c+bI & a-b-dI \end{pmatrix}$, und diese Bildmatrix hat Determinante $a^2 - ab + b^2 + c^2 - cd + d^2$.

- (4) **H** : Es ist **H** ein Schiefkörper, da alle $\xi \in \mathbf{H} \setminus \{0\}$ positive Norm haben. Ein maximaler Teilkörper in **H** ist durch $\mathbf{Q}(i) \simeq \mathbf{Q}[X]/(X^2 + 1)$ gegeben, ein anderer durch $\mathbf{Q}(i + j) \simeq \mathbf{Q}[X]/(X^2 + 2)$. In zweiterem ist -1 kein Quadrat.

Ω : Es ist Ω ein Schiefkörper, da alle $\xi \in \mathbf{H} \setminus \{0\}$ positive Norm haben. In der Tat ist die Norm von $\tilde{a} + \tilde{b}(1 + 2\omega) + \tilde{c}i + \tilde{d}(1 + 2\omega)i$ gleich $\tilde{a}^2 + 3\tilde{b}^2 + \tilde{c}^2 + 3\tilde{d}^2$. Ein maximaler Teilkörper in Ω ist durch $\mathbf{Q}(i) \simeq \mathbf{Q}[X]/(X^2 + 1)$ gegeben, ein anderer durch $\mathbf{Q}(\omega) \simeq \mathbf{Q}[X]/(X^2 + X + 1)$. In zweiterem ist -1 kein Quadrat.

- (5) **H** : Wir müssen untersuchen, wann die quadratische Form $a^2 + b^2 + c^2 + d^2$ für ein $(a, b, c, d) \neq (0, 0, 0, 0)$ die Null als Wert annehmen kann, kurz, wann die Normform die Null darstellt.

Für $v = \infty$ stellt die Normform die Null nicht dar.

Für $v \in V \setminus \{2, \infty\}$ behaupten wir, daß die Normform die Null darstellt. Wegen $\#\mathbf{F}_v^2 = (v+1)/2$ ist $-\mathbf{F}_v^2 \cap (1 + \mathbf{F}_v^2) \neq \emptyset$. Seien also $s, t \in \mathbf{Z}$ gegeben mit $1 + s^2 + t^2 = 0$. Es genügt, eine Nullstelle des Polynoms $f(X) = X^2 + s^2 + t^2$ in $\mathbf{Q}_v$ zu finden. Das geht mit Hensel, da $f(1) \equiv_v 0$, aber $f'(1) = 2 \not\equiv_v 0$.

Wir behaupten, daß für $v = 2$ die Normform die Null nicht darstellt. Wir können o.E. nach einer Lösung $(a, b, c, d) \in \mathbf{Z}_2^4$ mit $(a, b, c, d) \not\equiv_2 (0, 0, 0, 0)$

suchen. Modulo 8 haben wir die Quadrate $\{0, 1, 4\}$. Da die 1 als Summand vorkommen muß, ist unter den gemachten Voraussetzungen $a^2 + b^2 + c^2 + d^2 \not\equiv_8 0$. Es bleibt, in $\mathbf{H}_2$ die Maximalordnung $\Delta_{\mathbf{H},2}$ zu betrachten. Wir haben Elemente in $\mathbf{H}_2$ mit Norm in $\mathbf{Z}_2$ zu finden. Angenommen, es hätte ein Element $a + bi + cj + dij$ mit $(a, b, c, d) \notin \frac{1}{2}\mathbf{Z}_2^4$ Norm in $\mathbf{Z}_2$. Nach Multiplikation mit 2^{-s} , wobei s die minimale Bewertung bei 2 der nichtverwindenden Elemente in $\{a, b, c, d\}$ bezeichnet, erhalten wir ein primitives Tupel (eine Koeffizientenbewertung ist gleich 0) mit $a^2 + b^2 + c^2 + d^2 \in 2^{2s}\mathbf{Z}_2$. Da nun nach Voraussetzung $s \geq 2$, ist dies nach dem eben gesehenen nicht möglich.

Also hat jedes Element in der Maximalordnung Koeffizienten in $\frac{1}{2}\mathbf{Z}_2^4$. Da die Elemente mit Koeffizienten in $\mathbf{Z}_2$ ohnehin Norm in $\mathbf{Z}_2$ haben, genügt es, die endlich vielen Elemente in $\frac{1}{2}\mathbf{Z}_2^4/\mathbf{Z}_2^4$ zu testen. Und in der Tat hat ein solches Element $a + bi + cj + dij$, mit $(a, b, c, d) \in \frac{1}{2}\mathbf{Z}_2$, eine ganzzahlige Norm genau dann, wenn (a, b, c, d) kongruent modulo $\mathbf{Z}_2^4$ zu $(0, 0, 0, 0)$ oder zu $\frac{1}{2}(1, 1, 1, 1)$ ist. Damit ist die Maximalordnung mit $\rho := (1 + i + j + ij)/2$ gegeben durch

$$\Delta_{\mathbf{H},2} = \mathbf{Z}_2\langle 1, i, j, \rho \rangle.$$

Wir haben $ef = 4$. Zur Bestimmung des Verzweigungsindex e haben wir das Bild der Abbildung $\Delta_{\mathbf{H},2} \xrightarrow{w} \mathbf{Q}, \xi \mapsto v_2(N(\xi))/4$ zu betrachten. Die Norm von $\xi = a + bi + cj + d'\rho = (a + d'/2) + (b + d'/2)i + (c + d'/2)j + (d'/2)ij$ ist gegeben durch

$$(a^2 + b^2 + c^2 + d'^2 + ad' + bd' + cd')^2.$$

und somit ist $w(\xi) \in \frac{1}{2}\mathbf{Z}$. Es folgt $w(\Delta_{\mathbf{H},2}) = \frac{1}{2}\mathbf{Z}$. Es wird $e = 2$, und folglich der Trägheitsindex $f = 2$, sowie e.g. $\pi = 1 + i$.

Es ist übrigens $\Delta_{\mathbf{H},2}/\pi\Delta_{\mathbf{H},2} \simeq \mathbf{F}_2(\rho) \simeq \mathbf{F}_4$, mit $\mu_{\rho,\mathbf{F}_2}(X) = X^2 + X + 1 \in \mathbf{F}_2[X]$. In der Tat ist $\rho \not\equiv_{\pi} 1$, da $\rho - 1$ eine Einheit in $\Delta_{\mathbf{H},2}$ ist; und ferner gilt $\rho^2 - \rho + 1 = 0$ bereits in $\Delta_{\mathbf{H},2}$.

Ω : Wir müssen untersuchen, wann die quadratische Form $\tilde{a}^2 + 3\tilde{b}^2 + \tilde{c}^2 + 3\tilde{d}^2$ für ein $(a, b, c, d) \neq (0, 0, 0, 0)$ die Null darstellt (cf. (4)).

Für $v = \infty$ stellt die Normform die Null nicht dar.

Für $v \in V \setminus \{2, 3, \infty\}$ behaupten wir, daß die Normform die Null darstellt. Wegen $\#\mathbf{F}_v^2 = (v+1)/2$ ist $-\mathbf{F}_v^2 \cap (3 + \mathbf{F}_v^2) \neq \emptyset$. Seien also $s, t \in \mathbf{Z}$ gegeben mit $3 + s^2 + t^2 = 0$. Es genügt, eine Nullstelle des Polynoms $f(X) = X^2 + s^2 + t^2$ in $\mathbf{Q}_v$ zu finden. Das geht mit Hensel, da $f(3) \equiv_v 0$, aber $f'(3) = 6 \not\equiv_v 0$.

Wir behaupten, daß für $v = 2$ die Normform die Null darstellt. Setzt man $b = c = d = 1$, so sieht man, daß es genügt, eine Nullstelle des Polynoms $X^2 + 7 = 0$ zu finden. Das geht mit Hensel, da $v_2(f(1)) = 3 > 2 = 2v_2(f'(1))$.

Wir behaupten, daß für $v = 3$ die Normform die Null nicht darstellt. Wir können o.E. nach einer Lösung $(\tilde{a}, \tilde{b}, \tilde{c}, \tilde{d}) \in \mathbf{Z}_3^4$ mit $(\tilde{a}, \tilde{b}, \tilde{c}, \tilde{d}) \not\equiv_3 (0, 0, 0, 0)$ suchen. Modulo 9 haben wir $\tilde{a}^2, \tilde{c}^2 \in \{0, 1, 4, 7, 9\}$ und $3\tilde{b}^2, 3\tilde{d}^2 \in \{0, 3\}$. Es folgt zunächst, daß $\tilde{a}^2 \equiv_9 0$ und $\tilde{c}^2 \equiv_9 0$, und dann, daß für $\tilde{b}^2$ und $\tilde{d}^2$ keine Möglichkeit mehr bleibt, um modulo 9 nichttrivial eine Null hervorzubringen.

Es bleibt, in Ω_3 die Maximalordnung $\Delta_{\Omega,3}$ zu betrachten. Wir haben Elemente in Ω_3 mit Norm in $\mathbf{Z}_3$ zu finden. Angenommen, es hätte ein Element $\tilde{a} + \tilde{b}(2\omega + 1) + \tilde{c}i + \tilde{d}i(2\omega + 1)$ mit $(\tilde{a}, \tilde{b}, \tilde{c}, \tilde{d}) \notin \mathbf{Z}_3^4$ Norm in $\mathbf{Z}_3$. Nach Multiplikation mit 3^{-s} , wobei s die minimale Bewertung bei 3 der nichtverwindenden

Elemente in $\{\tilde{a}, \tilde{b}, \tilde{c}, \tilde{d}\}$ bezeichnet, erhalten wir ein primitives Tupel (eine Koeffizientenbewertung ist gleich 0) mit $\tilde{a}^2 + 3\tilde{b}^2 + \tilde{c}^2 + 3\tilde{d}^2 \in 3^{2s}\mathbf{Z}_2$. Da nun nach Voraussetzung $s \geq 1$, ist dies nach dem eben gesehenen nicht möglich.

Damit sind alle Elemente mit Norm in $\mathbf{Z}_3$ im $\mathbf{Z}_3$ -linearen Erzeugnis von $(1, \omega, i, i\omega)$, und mithin

$$\Delta_{\Omega,3} = \mathbf{Z}_3\langle 1, \omega, i, i\omega \rangle$$

die Maximalordnung.

Wir haben $ef = 4$. Zur Bestimmung e haben wir das Bild der Abbildung $\Delta_{\Omega,3} \xrightarrow{w} \mathbf{Q}$, $\xi \mapsto v_3(N(\xi))/4$ zu betrachten. Die Norm von $\xi = \tilde{a} + \tilde{b}(1 + 2\omega) + \tilde{c}i + \tilde{d}i(1 + 2\omega)$ ist gegeben durch $(\tilde{a}^2 + 3\tilde{b}^2 + \tilde{c}^2 + 3\tilde{d}^2)^2$, und somit ist $w(\xi) \in \frac{1}{2}\mathbf{Z}$. Ferner ist $w(1 + 2\omega) = 1/2$, und also $w(\Delta_{\Omega,3}) = \frac{1}{2}\mathbf{Z}$. Also $e = 2$, und folglich $f = 2$, sowie e.g. $\pi = 1 + 2\omega$.

Es ist übrigens $\Delta_{\Omega,3}/\pi\Delta_{\Omega,3} \simeq \mathbf{F}_3(i) \simeq \mathbf{F}_9$, mit $\mu_{\rho, \mathbf{F}_9}(X) = X^2 + 1 \in \mathbf{F}_3[X]$. In der Tat ist $i \not\equiv_{\pi} 1$, da $i - 1$ eine Einheit in $\Delta_{\Omega,3}$ ist.

- (6) Wären $\mathbf{H}$ und Ω als $\mathbf{Q}$ -Algebren isomorph, so würde aus $\mathbf{H}_2$ Schiefkörper folgen, daß auch Ω_2 Schiefkörper ist. Das ist aber nicht der Fall.
- (7) Zunächst nehmen wir mit (6) den Fall $d = 1$ aus, in welchem die Algebren nicht isomorph sind.

Wir müssen ermitteln, für welches $d \neq 1$ quadratfrei Elemente $\tilde{a}, \tilde{b}, \tilde{c}, \tilde{d} \in \mathbf{Q}(\sqrt{d})$ existieren mit

$$\begin{array}{ccc} \mathbf{H}_{\mathbf{Q}(\sqrt{d})} & \longrightarrow & \Omega_{\mathbf{Q}(\sqrt{d})} \\ i & \longmapsto & i \\ j & \longmapsto & \tilde{a} + \tilde{b}(2\omega + 1) + \tilde{c}i + \tilde{d}i(2\omega + 1) \end{array}$$

wohldefiniert. Wenn die Existenz eines solchen Tupels $(\tilde{a}, \tilde{b}, \tilde{c}, \tilde{d})$ bekannt ist, genügt es für die Surjektivität dieser Abbildung $\tilde{b} \neq 0$ oder $\tilde{d} \neq 0$ zu wissen.

Für die Wohldefiniertheit müssen wir sehen, daß j^2 auf -1 und $ij + ji$ auf 0 kommt. Letztere Bedingung liefert wegen $i(1 + 2\omega) = (1 + 2\omega)i$, daß $\tilde{a} = 0$ und daß $\tilde{c} = 0$. Da das Bild von j wegen $j^2 = -1$ nicht verschwinden darf, ist die Abbildung mit voriger Bemerkung automatisch ein Isomorphismus, falls nur wohldefiniert.

Die Bedingung $j^2 = -1$ wird nun zur Forderung, daß

$$-1 \stackrel{!}{=} ((\tilde{b} + \tilde{d}i)(1 + 2\omega))^2 = (\tilde{b} + \tilde{d}i)(\tilde{b} - \tilde{d}i)(1 + 2\omega)^2 = -3(\tilde{b}^2 + \tilde{d}^2) .$$

Setzen wir nun

$$\begin{aligned} \tilde{b} &=: \alpha + \beta\sqrt{d} \\ \tilde{d} &=: \gamma + \delta\sqrt{d} \end{aligned}$$

mit $\alpha, \beta, \gamma, \delta \in \mathbf{Q}$ an. Einsetzen liefert die Bedingungen

$$\begin{aligned} \alpha\beta + \gamma\delta &= 0 \\ \alpha^2 + \gamma^2 + d\beta^2 + d\delta^2 &= \frac{1}{3} . \end{aligned}$$

Die erste Bedingung übersetzt sich via Determinante in die Existenz von $\lambda, \mu \in \mathbf{Q}$, nicht beide 0, mit $\lambda \begin{pmatrix} \alpha \\ \gamma \end{pmatrix} + \mu \begin{pmatrix} -\delta \\ \beta \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$.

Fall $\mu = 0$. Nun ist $\lambda \neq 0$ und folglich $\alpha = \gamma = 0$, und damit hat zu sein

$$d\beta^2 + d\delta^2 = \frac{1}{3}.$$

Fall $\mu \neq 0$. Wir dürfen $\mu = 1$ setzen und haben

$$(\alpha^2 + \gamma^2)(d + d\lambda^2) = \frac{1}{3}.$$

zu lösen. Eine Zahl ξ in $\mathbf{Q}^*$ ist genau dann Norm einer Zahl in $\mathbf{Q}(i)^*$, wenn dasselbe für $1/\xi$ zutrifft. Wir haben, mit veränderten α und γ , also

$$3 + 3d\lambda^2 = \alpha^2 + \gamma^2$$

zu lösen.

Beide Fälle laufen darauf hinaus, sich von der quadratischen Form

$$\alpha^2 + \gamma^2 - 3\mu^2 - 3d\lambda^2$$

über $\mathbf{Q}$ die Null darstellen zu lassen. Denn ist $\mu \neq 0$, so gibt das eine Lösung im zweiten Fall, und ist $\mu = 0$, so gibt das eine Lösung im ersten Fall.

Eine Betrachtung modulo 9 einer primitiven Lösung zeigt, daß $d \equiv_3 1$ nicht sein darf. Diesenfalls schließt man nämlich zunächst auf $\alpha \equiv_3 0$ und $\beta \equiv_3 0$, und dann auch $\mu \equiv_3 0$ und $\lambda \equiv_3 0$.

Eine Betrachtung modulo 8 einer primitiven Lösung zeigt, daß $d \equiv_8 1$ nicht sein darf. Diesenfalls ist modulo 8 nämlich $\alpha^2 + \gamma^2 \in \{0, 1, 2, 4, 5\}$, während $3\mu^2 - 3d\lambda^2 \in \{0, 3, 6, 4, 7\}$, und die Schnittmenge $\{0, 4\}$ kann mit einer primitiven Lösung nicht erreicht werden.

Wir werden unter Zuhilfenahme von SERRE, *A course in arithmetic*, 1970, abgekürzt [S], zeigen, daß dies die einzigen Bedingungen an d sind. Nach dem Hasse-Minkowski-Prinzip [S, p. 41, th. 8] müssen wir entscheiden, für welches d die quadratische Form die Null über allen Körpern $\mathbf{Q}_v$ darstellt. Für $v = \infty$ ist das der Fall. Sei v eine Primzahl. Wir multiplizieren die Form mit (-3) durch und fragen uns, wann

$$-3\alpha^2 - 3\gamma^2 + \mu^2 + d\lambda^2$$

die Null *nicht* darstellt über $\mathbf{Q}_v$. Nach [S, p. 36-37, th. 6] ist dies genau dann der Fall, wenn d ein Quadrat in $\mathbf{Q}_v$ ist und $(-3, -3)_v \neq (-1, -1)_v$. Letztere Bedingung ist genau dann erfüllt, wenn $v \in \{2, 3\}$, cf. [S, p. 20, th. 1]. Nun ist d genau dann ein Quadrat in $\mathbf{Q}_2$, wenn $d \equiv_8 1$ ([S, p. 18, th. 4] oder Hensel direkt) und genau dann ein Quadrat in $\mathbf{Q}_3$, wenn $d \equiv_3 1$ ([S, p. 17, th. 3], oder Hensel direkt).

Resultat. Es sind $\mathbf{H}_{\mathbf{Q}(\sqrt{d})}$ und $\Omega_{\mathbf{Q}(\sqrt{d})}$ isomorph genau dann, wenn $d \not\equiv_3 1$ und $d \not\equiv_8 1$.

Zum Beispiel also für $d \in \{\dots, -3, -1, 2, 3, 5, 6, 11, \dots\}$.

- (8) Eine $\mathbf{Z}$ -Ordnung Λ in einer $\mathbf{Q}$ -Algebra A ist genau dann eine Maximalordnung, wenn $\Lambda_p := \Lambda \otimes_{\mathbf{Z}} \mathbf{Z}_p$ eine Maximalordnung in $A_p := A \otimes_{\mathbf{Q}} \mathbf{Q}_p$ ist für alle p prim. Denn der Index von Λ in einer Maximalordnung hätte sonst einen Primteiler p , und über $\mathbf{Z}_p$ wäre so die Ordnung nicht maximal.

H : Zunächst ist $\mathbf{Z}\langle 1, i, j, ij \rangle$ keine Maximalordnung in **H**, wie man bei 2 sieht, cf. (5).

Wir behaupten, daß $\Delta_{\mathbf{H}} := \mathbf{Z}\langle 1, i, j, \rho \rangle$ eine Maximalordnung in **H** darstellt, wobei $\rho = (1 + i + j + ij)/2$.

Über $\mathbf{Z}_2$ ist $\Delta_{\mathbf{H},2}$ bereits maximal, siehe (5).

Sei $p \neq 2$. Bezüglich der $\mathbf{Z}_p$ -linearen Basis $(1, i, j, ij)$ von $\Delta_{\mathbf{H},p}$ hat die Spurbilinearform die Grammatrix $\text{diag}(4, -4, -4, -4)$, und somit invertierbare Diskriminante in $\mathbf{Z}_p$. Wäre $\Delta_{\mathbf{H},p}$ in einer Oberordnung enthalten, so müßte deren Diskriminante diese Diskriminante in $\mathbf{Z}_p$ echt teilen, was nicht geht.

Eine zweite Maximalordnung ist e.g. durch $(1 + 2i)\Delta_{\mathbf{H}}(1 + 2i)^{-1}$ gegeben. In der Tat enthält diese das Element $(1 + 2i)j(1 + 2i)^{-1} = \frac{1}{5}(4ij - 3j)$, welches nicht in Δ enthalten ist. (Die Maximalordnung in **H**₅ ist *nicht* eindeutig, da kein Schiefkörper vorliegt.)

Ω : Wir behaupten, daß $\Delta_{\Omega} := \mathbf{Z}\langle 1, \omega, i, i\omega \rangle$ eine Maximalordnung in **Ω** darstellt.

Über $\mathbf{Z}_3$ ist $\Delta_{\Omega,3}$ bereits maximal, siehe (5).

Sei $p \notin \{2, 3\}$. Bezüglich der $\mathbf{Z}_p$ -linearen Basis $(1, \omega, i, i\omega)$ von $\Delta_{\Omega,p}$ hat die Spurbilinearform die Grammatrix

$$\begin{bmatrix} 4 & -2 & 0 & 0 \\ -2 & -2 & 0 & 0 \\ 0 & 0 & -4 & 2 \\ 0 & 0 & 2 & -4 \end{bmatrix},$$

und somit eine in $\mathbf{Z}_p$ invertierbare Diskriminante -144 . Damit ist $\Delta_{\Omega,p}$ maximal.

Sei $p = 2$. Wir müssen zeigen, daß $\Delta_{\Omega,2}$ eine Maximalordnung in **Ω**₂ darstellt. Hierzu verwenden wir den Trick der *reduzierten Spur*. Wir behaupten, daß für ξ Element einer $\mathbf{Z}_2$ -Ordnung in **Ω**₂ auch $\text{tr}(\xi) := \text{Tr}(\xi)/2$ noch in $\mathbf{Z}_2$ liegt. In der Tat können wir den Isomorphismus aus (1) ebenso über $\mathbf{Q}_2(I) \simeq \mathbf{Q}_2[X]/(X^2 + 1)$ durchführen statt über **C**, und erhalten nach Tensorieren mit $\mathbf{Z}_2[I]$ eine $\mathbf{Z}_2[I]$ -Ordnung in $\mathbf{Q}_2(I)^{2 \times 2}$. Jedes Element dieser Ordnung hat ein Minimalpolynom mit Koeffizienten in $\mathbf{Z}_2[I]$ (ganzabgeschlossen), und somit eine Spur $\text{tr}(\xi)$ (als Element von $\mathbf{Q}_2(I)^{2 \times 2}$) in $\mathbf{Z}_2[I]$. Damit ist $\text{tr}(\xi) \in \mathbf{Q}_2 \cap \mathbf{Z}_2[I] = \mathbf{Z}_2$. Bezüglich tr erhalten wir die Grammatrix

$$\begin{bmatrix} 2 & -1 & 0 & 0 \\ -1 & -1 & 0 & 0 \\ 0 & 0 & -2 & 1 \\ 0 & 0 & 1 & -2 \end{bmatrix},$$

und somit eine in $\mathbf{Z}_2$ invertierbare Diskriminante -9 . Damit ist $\Delta_{\Omega,2}$ maximal.

Eine alternative Maximalordnung erhalten wir e.g. mit $(1 + i)\Delta_{\Omega}(1 + i)^{-1}$, die das Element $(1 + i)\omega(1 + i)^{-1} = \frac{1}{2}(2i\omega + i - 1)$ enthält, welches in Δ_{Ω} nicht enthalten ist.

Aufgabe 2.

(1) Schreibe $n := [L : K]$. Wir behaupten, daß der Morphismus

$$\begin{array}{ccc} L \otimes_K L & \xrightarrow{\delta} & \prod_{\sigma \in G} L \\ x \otimes y & \mapsto & ((x\sigma)y)_{\sigma \in G} \end{array}$$

von L -Algebren (mit der L -Operation auf dem rechten Tensorfaktor) ein Isomorphismus ist.

Sei hierzu $(x_i)_{i \in [1, n]}$ eine K -lineare Basis von L . Die L -lineare Matrix von δ ist diesbezüglich gegeben durch $(x_i \sigma)_{i, \sigma} \in L^{n \times n}$. Wir behaupten, daß diese Matrix linear unabhängige Spalten hat. In der Tat folgt aus $\sum_{\sigma \in G} (x_i \sigma) \lambda_\sigma = 0$ für alle $i \in [1, n]$, wobei $\lambda_i \in L$, daß $\sum_{\sigma \in G} (x \sigma) \lambda_\sigma = 0$ für alle $x \in L$. Dedekinds Lemma impliziert nun, daß $\lambda_\sigma = 0$ für alle $\sigma \in G$.

Alternativ: Es ist $L = K[X]/(f(X))$, $f(X)$ zerfällt in $L[X]$ in Linearfaktoren, und $L \otimes_K L \simeq L[X]/(f(X)) \dots$

(2) Es werden

$$\begin{aligned} N_{L|K}(x) &= N_{L \otimes_K L|L}(x \otimes 1) \stackrel{\text{Iso}}{=} N_{(\prod_{\sigma} L)|L}((x \sigma)_{\sigma}) = \prod_{\sigma \in G} x \sigma \\ \text{Tr}_{L|K}(x) &= \text{Tr}_{L \otimes_K L|L}(x \otimes 1) \stackrel{\text{Iso}}{=} \text{Tr}_{(\prod_{\sigma} L)|L}((x \sigma)_{\sigma}) = \sum_{\sigma \in G} x \sigma . \end{aligned}$$

(3) Wir müssen ein Element $e \in \mathbf{Q}(\sqrt{d}) \otimes_{\mathbf{Q}} \mathbf{Q}(\sqrt{d})$ finden, welches unter δ auf $(1, 0)$ abgebildet wird. Setzen wir $e = s(1 \otimes 1) + t(1 \otimes \sqrt{d}) + u(\sqrt{d} \otimes 1) + v(\sqrt{d} \otimes \sqrt{d})$ mit $s, t, u, v \in \mathbf{Q}$ an, so wird

$$e\delta = (s, s) + (t\sqrt{d}, t\sqrt{d}) + (u\sqrt{d}, -u\sqrt{d}) + (dv, -dv) = (s+dv+(t+u)\sqrt{d}, s-dv+(t-u)\sqrt{d}) .$$

Daraus erhalten wir $t = u = 0$, $s = 1/2$ und $v = 1/2d$, d.h. die orthogonale Zerlegung

$$1 \otimes 1 = \frac{1}{2d}(d \otimes 1 + \sqrt{d} \otimes \sqrt{d}) + \frac{1}{2d}(d \otimes 1 - \sqrt{d} \otimes \sqrt{d}) .$$

in primitive Idempotente.

Betrachten wir die eingeschränkte Abbildung $\mathbf{Z}_L \otimes_{\mathbf{Z}} \mathbf{Z}_L \xrightarrow{\delta} \mathbf{Z}_L \times \mathbf{Z}_L$.

Fall $d \equiv_4 1$, i.e. $\mathbf{Z}_L = \mathbf{Z}[(1 + \sqrt{d})/2]$. Schreibe $\rho := (1 + \sqrt{d})/2$ und $m := (d - 1)/4$. Es ist $\rho^2 = \rho + m$, und der nichttriviale Galoisautomorphismus schickt ρ auf $1 - \rho$.

Bezüglich der $\mathbf{Z}$ -linearen Basis $(1, \rho)$ wird also

$$\begin{aligned} 1 \otimes 1 &\mapsto (1, 1) \\ 1 \otimes \rho &\mapsto (\rho, \rho) \\ \rho \otimes 1 &\mapsto (\rho, 1 - \rho) \\ \rho \otimes \rho &\mapsto (\rho + m, -m) . \end{aligned}$$

Die $\mathbf{Z}$ -lineare Determinante von δ ist mithin $-d$, der Index von $(\mathbf{Z}[\rho] \otimes_{\mathbf{Z}} \mathbf{Z}[\rho])\delta$ in $\mathbf{Z}[\rho] \times \mathbf{Z}[\rho]$ also gleich d .

Ferner liegt das Bild in

$$\Lambda := \{(u, v) \in \mathbf{Z}[\rho] \times \mathbf{Z}[\rho] : u \equiv_{\sqrt{d}} v\} .$$

Da Λ ebenfalls Index d in $\mathbf{Z}[\rho] \times \mathbf{Z}[\rho]$ hat, ist $(\mathbf{Z}[\rho] \otimes_{\mathbf{Z}} \mathbf{Z}[\rho])\delta = \Lambda$.

Fall $d \not\equiv_4 1$, i.e. $\mathbf{Z}_L = \mathbf{Z}[\sqrt{d}]$. Bezüglich der $\mathbf{Z}$ -linearen Basis $(1, \rho)$ wird also

$$\begin{aligned} 1 \otimes 1 &\mapsto (1, 1) \\ 1 \otimes \sqrt{d} &\mapsto (\sqrt{d}, \sqrt{d}) \\ \sqrt{d} \otimes 1 &\mapsto (\sqrt{d}, -\sqrt{d}) \\ \sqrt{d} \otimes \sqrt{d} &\mapsto (d, -d) . \end{aligned}$$

Die $\mathbf{Z}$ -lineare Determinante von δ ist mithin $-4d$, der Index von $(\mathbf{Z}[\rho] \otimes_{\mathbf{Z}} \mathbf{Z}[\rho])\delta$ in $\mathbf{Z}[\rho] \times \mathbf{Z}[\rho]$ also gleich $4d$.

Ferner liegt das Bild in

$$\Lambda := \{(u, v) \in \mathbf{Z}[\rho] \times \mathbf{Z}[\rho] : u \equiv_{2\sqrt{d}} v\}.$$

Da Λ ebenfalls Index $4d$ in $\mathbf{Z}[\rho] \times \mathbf{Z}[\rho]$ hat, ist $(\mathbf{Z}[\rho] \otimes_{\mathbf{Z}} \mathbf{Z}[\rho])\delta = \Lambda$.

- (4) Sei ${}_A M_B$ ein A - B -Bimodul über R . Setzen wir

$$m \cdot (a \otimes b) := amb$$

für $m \in M$, $a \in A$ und $b \in B$, so wird M zu einem $A^\circ \otimes_R B$ -Rechtsmodul. Die R -Balanciertheit dieser Multiplikationsabbildung ergibt sich aus der Voraussetzung an M , ein Bimodul über R zu sein.

Ist umgekehrt ein $A^\circ \otimes_R B$ -Rechtsmodul M gegeben, so erhalten wir eine A - B -Bimodulstruktur auf M , indem wir die obige Operationsdefinition von rechts nach links lesen.

- (5) Ein L - L -Bimodul über K ist nach (4) ein $L \otimes L$ -Rechtsmodul. Da nach (1) der Ring $L \otimes_K L$ in ein Produkt von Kopien von L zerfällt, gilt dies auch, via Multiplikation mit primitiven Idempotenten, für einen $L \otimes_K L$ -Modul, er zerfällt so in eine direkte Summe von L -Moduln, mit $L \otimes_K L$ -Operationen gegeben durch $\delta\pi_\sigma$, $\sigma \in G$, wobei π_σ die Projektion $\prod_{\sigma} L \longrightarrow L$ auf den mit σ indizierten Faktor bezeichne. Ausgeschrieben schickt $\delta\pi_\sigma$ das Element $x \otimes y$ auf $(x\sigma)y$.

Ein als K -Vektorraum endlichdimensionaler L -Modul ist nun endliche direkte Summe von eindimensionalen L -Moduln, isomorph zu L .

Auf L operiert nun $x \otimes y \in L \otimes_K L$ durch $l \cdot (x \otimes y) = l(x\sigma)y = (x\sigma)ly$, für $l \in L$. Via (4) entspricht dies der Bimoduloperation $x \cdot l \cdot y := (x\sigma)ly$. Wir bezeichnen L , ausgestattet mit dieser Bimoduloperation, provisorisch als $L_{(\sigma)}$.

Schließlich haben wir einen Isomorphismus von L - L -Bimoduln

$$\begin{array}{ccc} L_{(\sigma)} & \xrightarrow{\sim} & L_{\sigma^{-1}} \\ l & \longmapsto & l\sigma^{-1} \end{array}$$

- (6) Wir haben einen Isomorphismus von L - L -Bimoduln

$$\begin{array}{ccccc} L_\rho & \otimes_L & L_\sigma & \xrightarrow{\sim} & L_{\rho\sigma} \\ l & \otimes & l' & \longmapsto & (l\sigma)l' \end{array}.$$

In der Tat kommt $x \cdot (l \otimes l') \cdot y = (x\rho)l \otimes l'y$ für $x, y \in L$ auf $(x\rho\sigma)(l\sigma)l'y$, was mit $x \cdot ((l\sigma)l') \cdot y$ übereinstimmt.