G. Nebe, M. Künzer

Übungen Algebra II, Sommersemester 03

Lösung 10

Aufgabe 1.

(a)

(a, i) Die Norm eines Elements $a + bi + cj + dij \in \mathbf{H}$ mit $a, b, c, d \in \mathbf{Q}$ ist gegeben durch $(a^2 + b^2 + c^2 + d^2)^2$. Nach [Serre, *A Course in Arithmetic,* IV, §2, th. 6] ist also $\mathbf{H}_p$ für p prim genau dann ein Schiefkörper, wenn $(-1, -1)_p = -1$. Dies trifft mit [loc. cit., III, §1, th. 1] genau für $p = 2$ zu, i.e. endlich$(\mathbf{H}) = \{2\}$. (Vgl. Blatt 7, Aufgabe 2 (2).)

(a, ii) Sei $p = 2$. Es ist $m = 2$, wir haben also eine primitive 3-te Einheitswurzel in $\mathbf{H}_2$ zu finden, i.e. eine Lösung $\zeta \in \mathbf{H}_2$ von $\zeta^2+\zeta+1$. Der Ansatz $\zeta = a+bi+cj+dij$ mit $a, b, c, d \in \mathbf{Q}_2$ führt auf

$$\zeta^2 + \zeta + 1 \;=\; (a^2 + a + 1 - b^2 - c^2 - d^2) + i(2ab + b) + j(2ac + c) + ij(2ad + d)\ .$$

Der Fall $a \neq -1/2$ führt auf $b = c = d = 0$, also auf $a^2 + a + 1 = 0$, was nicht eintreten kann. Also bleibt im Fall $a = -1/2$ die Gleichung

$$3/4 - b^2 - c^2 - d^2 \;=\; 0$$

zu lösen, was etwa mit $b = c = d = 1/2$ möglich ist. (So man das nicht sieht, wende man Hensels Lemma an.) Wir wählen $\zeta = (-1 + i + j + ij)/2$.

Nun gilt es, ein $\pi \in \mathbf{H}_2$ zu finden mit $\pi^2 = 2$ und $\pi\zeta = \zeta^{2^r}\pi$ für ein geeignetes r. Da ein Schiefkörper vorliegt, muß $r = 1$ sein. Der Ansatz $\pi = a+bi+cj+dij$ mit $a, b, c, d \in \mathbf{Q}_2$ führt auf

$$\pi^2 - 2 \;=\; (a^2 - b^2 - c^2 - d^2 - 2) + i \cdot 2ab + j \cdot 2ac + ij \cdot 2ad\ .$$

Es ist $a \neq 0$ wegen der Konsequenz $b = c = d = 0$ und $a^2 = 2$ nicht möglich. Also $a = 0$, und wir haben eine Lösung von $b^2 + c^2 + d^2 + 2 = 0$ in $\mathbf{Q}_2$ zu finden derart, daß

$$\pi\zeta - \zeta^2\pi \;=\; -b - c - d \;=\; 0\ .$$

Setzen wir also $d = -b - c$ und lösen $2b^2 + 2c^2 + 2bc + 2 = 0$ in $\mathbf{Q}_2$. Wir nützen unsere Wahlfreiheit, um $c = 1$ zu setzen, und finden die Nullstelle

$$b \;=\; (0, -2, -2/3, 14/3, \ldots)$$

von $b^2 + b + 2 = 0$. Entsprechend wird

$$\pi \;=\; (0, -2, 2, 10, \ldots)i + j + (-1, 1, 5, 5, \ldots)ij\ .$$

Der gesuchte Isomorphismus resultiert nun aus $\zeta \longmapsto \zeta$, $\pi \longmapsto \pi$ (unter Mißbrauch der Elementbezeichnungen), und es ist, wie schon erwähnt, $r = 1$.

(a, iii) Sei $p = 2$. Die Maximalordnung in $\mathbf{H}_2$ ist gegeben durch $\mathbf{Z}_2\langle \pi^i\zeta^j | i,j \in [0,1]\rangle$. Bezüglich der Basis $(1,\zeta,\pi,\pi\zeta)$ ist die Multiplikation mit ζ gegeben durch $\begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & -1 \end{bmatrix}$ und die Multiplikation mit π durch $\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & -1 \\ 2 & 0 & 0 & 0 \\ -2 & -2 & 0 & 0 \end{bmatrix}$. Wir erhalten als Grammatrix der reduzierten Spurbilinearform bezüglich dieser Basis

$$\frac{1}{2}\begin{bmatrix} 4 & -2 & 0 & 0 \\ -2 & -2 & 0 & 0 \\ 0 & 0 & 8 & -4 \\ 0 & 0 & -4 & 8 \end{bmatrix},$$

und es ergeben sich die $\mathbf{Z}_2$-linearen Elementarteiler $(1,1,2,2)$.

(b)(b, i) Die Norm eines Elements $a + bi + cj + dij \in D_{-2,3}$ mit $a,b,c,d \in \mathbf{Q}$ ist gegeben durch $(a^2 - 2b^2 + 3c^2 - 6d^2)^2$. Nach loc. cit. ist $D_{-2,3;\,p}$ genau dann ein Schiefkörper, wenn $(2,-3)_p = -1$; und es wird $(2,-3)_2 = -1$, $(2,-3)_3 = -1$, und $(2,-3)_p = +1$ für $p \notin \{2,3\}$. Wir erhalten $\mathrm{endlich}(D_{-2,3}) = \{2,3\}$.

(b, ii) Sei $p = 2$. Es ist $m = 2$. Als primitive 3-te Einheitswurzel ergibt sich $\zeta = (j-1)/2$. Wir erhalten $\pi = i$ und $\pi\zeta = \zeta^2\pi$, also $r = 1$. Der Isomorphismus ergibt sich zu $\zeta \longmapsto \zeta$, $\pi \longmapsto \pi$. Insbesondere ist $D_{-2,3;\,2} \simeq \mathbf{H}_2$, vgl. (a), vgl. auch Aufgabe 2.

Sei $p = 3$. Es ist $m = 2$. Als primitive 4-te Einheitswurzel diene $i + j$. Wir suchen ein Element ζ mit $\zeta^2 = i + j$. Setzen wir $\zeta = a + bi + cj + dij$ mit $a,b,c,d \in \mathbf{Q}_3$ an, so erhalten wir $d = 0$, $b = c = \frac{1}{2a}$, und müssen $4a^4 = 1$ lösen. Da $2a^2 = 1$ schon modulo 3 unlösbar ist, bleibt $2a^2 = -1$ zu lösen. Wir schreiben im folgenden kurz

$$w \;=\; (1,4,22,22,22,508,\ldots) \;\in\; \mathbf{Q}_3$$

und erhalten $\zeta := w(1-i-j)/2$, mit Minimalpolynom $\mu_{\zeta,\mathbf{Q}_3}(X) = X^2 - wX - 1$. Setzen wir $\pi = a+bi+cj+dij$ an, so erzwingt $\pi\zeta = \zeta^3\pi$, daß $a = 0$ und $2b = 3c$. Wählen wir $b = 3$, so erhalten wir $d = w/2$. Es wird somit $\pi = 3i + 2j + wij/2$.

(b, iii) Wir haben wieder zwei Fälle zu unterscheiden.

Sei $p = 2$. Wegen $D_{-2,3;\,2} \simeq \mathbf{H}_2$ erhalten wir dasselbe Ergebnis wie in (a, iii), d.h. die Elementarteiler $(1,1,2,2)$.

Sei $p = 3$. Bezüglich der Basis $(1,\zeta,\pi,\pi\zeta)$ ist die Multiplikation mit ζ gegeben durch $\begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & w & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & w \end{bmatrix}$ und die Multiplikation mit π durch $\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & w & -1 \\ 3 & 0 & 0 & 0 \\ 3w & -3 & 0 & 0 \end{bmatrix}$. Wir erhalten als Grammatrix der reduzierten Spurbilinearform bezüglich dieser Basis

$$\frac{1}{2}\begin{bmatrix} 4 & 2w & 0 & 0 \\ 2w & 0 & 0 & 0 \\ 0 & 0 & 12 & 6w \\ 0 & 0 & 6w & -12 \end{bmatrix},$$

und es ergeben sich die $\mathbf{Z}_3$-linearen Elementarteiler $(1,1,3,3)$.

(c) Es ist D eine zentraleinfache $\mathbf{Q}$-Algebra von $\mathbf{Q}$-Dimension 16, wie man anhand des Isomorphismus $\mathbf{Q}(\zeta_5)\otimes_{\mathbf{Q}} D \longrightarrow \mathbf{Q}(\zeta_5)^{4\times 4}$, $\xi \longmapsto \begin{bmatrix} \zeta_5 & 0 & 0 & 0 \\ 0 & \zeta_5^2 & 0 & 0 \\ 0 & 0 & \zeta_5^4 & 0 \\ 0 & 0 & 0 & \zeta_5^8 \end{bmatrix}$, $\xi \longmapsto \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 2 & 0 & 0 & 0 \end{bmatrix}$, erkennen kann. Denn wäre das Zentrum von D echt größer als $\mathbf{Q}$, so wäre auch das Zentrum von $\mathbf{Q}(\zeta_5) \otimes_{\mathbf{Q}} D$ echt größer als $\mathbf{Q}(\zeta_5)$. Und hätte D ein Ideal $0 \subset I \subset D$, so hätte auch $\mathbf{Q}(\zeta_5) \otimes_{\mathbf{Q}} D$ ein Ideal $0 \subset \mathbf{Q}(\zeta_5) \otimes_{\mathbf{Q}} I \subset \mathbf{Q}(\zeta_5) \otimes_{\mathbf{Q}} D$. Beides ist nicht der Fall.

Nun berechnen wir die $\mathbf{Z}$-linearen Elementarteiler der Grammatrix der reduzierten Spurbilinearform auf der $\mathbf{Z}$-Ordnung $D_0 = \mathbf{Z}\langle\langle \xi, \pi \rangle\rangle \subseteq D$. Bezüglich der Basis $(\xi^i \pi^j : i, j \in [0,3])$ erhalten wir die Grammatrix

$$\begin{bmatrix}
4 & -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & -1 & -1 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & -1 & 4 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 8 & -2 & -2 & -2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -2 & -2 & 8 & -2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -2 & -2 & -2 & -2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -2 & 8 & -2 & -2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 8 & -2 & -2 & -2 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -2 & 8 & -2 & -2 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -2 & -2 & 8 & -2 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -2 & -2 & -2 & 8 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 8 & -2 & -2 & -2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -2 & -2 & -2 & 8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -2 & 8 & -2 & -2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -2 & -2 & -2 & -2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}$$

mit den $\mathbf{Z}$-linearen Elementarteilern $(1^4, 10^{12})$.

Nun betrachten wir die verschiedenen Primstellen.

$p \notin \{2,5\}$ Die Diskriminante der Ordnung $D_{0;p} := \mathbf{Z}_p \otimes_{\mathbf{Z}} D_0$ ist 1, also liegt eine Maximalordnung vor, da die Diskriminante einer echten Oberordnung die Diskriminante der Ordnung teilte. Wäre D_p ein Schiefkörper, so könnte man ihn auf Standardform bekommen, und seine Diskriminante wäre folglich $p^{m(m-1)} = p^{12}$. Das ist hier aber nicht der Fall. Also ist $p \notin \text{endlich}(D)$.

$p = 2$ Wir wollen zeigen, daß D_2 ein Schiefkörper ist, *indem* wir D_2 auf Standardform bringen. Es ist $[\mathbf{Q}_2(\xi) : \mathbf{Q}_2] = 4$. Wir behaupten, daß $\mathbf{Q}_2(\xi)$ eine primitive 15te Einheitswurzel ζ enthält. Wir suchen also eine Nullstelle von $\Phi_{15}(X) = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1$ in $\mathbf{Z}_2[\xi]$. Modulo 2 finden wir die Lösung $\xi + 1$, welche wir zu einer Lösung

$$\zeta \;:=\; (\xi + 1,\; 2\xi^2 + 3\xi + 3,\; 4\xi^3 + 2\xi^2 + 7\xi + 3,\; 12\xi^3 + 2\xi^2 + 7\xi + 11,\; \ldots\,)$$

hochhenseln können. Die Konjugation mit π induziert einen Automorphismus von $\mathbf{Z}_2[\xi]$. Modulo 2 induziert dieser den Frobeniusautomorphismus $\xi \longmapsto \xi^2$, der also auch $\zeta \longmapsto \zeta^2$ schickt. Dies gilt nun auch in $\mathbf{Z}_2[\xi]$ selbst, i.e. $\pi\zeta = \zeta^2\pi$. Zusammen mit $\pi^4 = 2$ liefert dies die Standardform, i.e. den gesuchten Algebrenisomorphismus, wobei $r = 1$. (Beachte, daß das Minimalpolynom von ζ über $\mathbf{Q}_2$ das Kreisteilungspolynom $\Phi_{15}(X)$ echt teilt, cf. Aufgabe 4.)

Die in (iii) noch gefragten $\mathbf{Z}_2$-linearen Elementarteiler entnimmt man den oben berechneten $\mathbf{Z}$-linearen Elementarteilern zu $(1^4, 2^{12})$.

$p = 5$ Sei $\vartheta := 1 - \xi$. Es ist $\vartheta D_{0;5}$ ein zweiseitiges Ideal in $D_{0;5}$. Ein Element x, das modulo ϑ invertierbar ist, ist invertierbar: Da $(\vartheta D_{0;5})^4 \subseteq 5D_{0;5}$, liegt $\vartheta(D_{0;5}/5D_{0;5}) \subseteq \text{Jac}(D_{0;5}/5D_{0;5})$. Es ist also x zunächst in $D_{0;5}/5D_{0;5}$ invertierbar, nach Nakayama für diesen Ring. Nun ist die Multiplikation $D_{0;5} \longrightarrow D_{0;5}$, $y \longmapsto yx$, modulo 5 ein Isomorphismus, und damit nach Nakayama für den Ring $\mathbf{Z}_5$ ein Isomorphismus.

Durch Betrachtung der π^i-Koeffizienten aus $\mathbf{Q}_5(\vartheta)$ sieht man, daß jedes Element $x \in D_5 \smallsetminus \{0\}$ geschrieben werden kann als $x = \vartheta^m y$ mit $y \in D_{0;\,5} \smallsetminus \vartheta D_{0;\,5}$ und $m \in \mathbf{Z}$. Da

$$D_{0;\,5}/\vartheta D_{0;\,5} \xleftarrow{\sim} \mathbf{Z}_5[\pi]/5\mathbf{Z}_5[\pi] \;\simeq\; \mathbf{F}_{5^4}\ ,$$

induziert von der Inklusion, ist y eine Einheit modulo ϑ, also eine Einheit in $D_{0;\,5}$. Nun ist ϑ^m aber ebenfalls eine Einheit in D_5, so daß insgesamt x als Einheit und D_5 als Schiefkörper nachgewiesen ist.

Da die Grammatrix der reduzierten Spurbilinearform auf $D_{0;\,5}$ die $\mathbf{Z}_5$-linearen Elementarteiler $(1^4, 5^{12})$ hat, da damit die Diskriminante 5^{12} beträgt, und da dies für die Maximalordnung ebenfalls zutrifft, ist $D_{0;\,5}$ in der Tat die Maximalordnung. (Oder: Ein Element der Form $\vartheta^m y$ mit $m \in \mathbf{Z}$ und y Einheit in $D_{0;\,5}$ ist ganz über $\mathbf{Z}_5$ genau dann, wenn $m \geq 0$, wie eine Betrachtung der ϑ-Bewertung seines Minimalpolynoms lehrt.)

Es ist $\mathbf{Q}_5(\pi) \simeq \mathbf{Q}_5(\sqrt[4]{2})$ eine unverzweigte Erweiterung von Grad 4 über $\mathbf{Q}_5$, da $X^4 - 2$ modulo 5 irreduzibel bleibt. Modulo 5 ist $\pi^2 + \pi + 1$ eine primitive $(5^4 - 1)$ste Einheitswurzel, welche zur primitiven $(5^4 - 1)$sten Einheitswurzel

$$\zeta \;=\; (\pi^2 + \pi + 1,\ 5\pi^3 + 16\pi^2 + 11\pi + 1,\ 55\pi^3 + 41\pi^2 + 11\pi + 101,\ \dots)$$

in $\mathbf{Q}_5(\pi)$ liftet.

Wir suchen nun ein Element $\varpi \in D_5$ mit $\varpi^m = p$ und $\varpi\zeta = \zeta^{5^r}\varpi$ für ein $r \in [1, 4]$. Das Problem ist die praktische Durchführung des Satzes von Skolem-Noether. Hier eine Näherung, unbefriedigend, da von Hand zu approximieren ist, und die Konvergenz der angeführten 'Lösung' nicht gezeigt wird.

Wir erinnern uns der Verzweigung des Ideals $(5) = \vartheta^4$ in $\mathbf{Z}_5[\xi]$ und setzen daher einmal $\varpi_1 := \vartheta$. Dies ist ein Erzeuger des maximalen Ideals von $D_{0;\,5}$. Nun ist $\varpi_1\zeta \equiv_{\vartheta^2} \zeta^{5^3}\varpi_1$, und dem Beweis der Eindeutigkeit von r entnimmt man, daß dies bereits

$$r \;=\; 3$$

nach sich zieht.

Vorsicht, wir dürfen aus $\varpi_1\zeta\varpi_1^{-1} \equiv_\vartheta \zeta^{5^3}$ *nicht* auf $\varpi_1\zeta\varpi_1^{-1} = \zeta^{5^3}$ schließen, obwohl $\varpi_1\zeta\varpi_1^{-1}$ eine primitive (5^4-1)ste Einheitswurzel ist. Denn es liegt $\varpi_1\zeta\varpi_1^{-1}$ nicht in $\mathbf{Q}_5(\zeta)$ – in einem Schiefkörper kann ein Polynom wie hier das Kreisteilungspolynom mehr Nullstellen haben, als sein Grad anzeigt.

Arbeiten wir mit obiger Näherung für ζ, so erhalten wir als eine Näherung ein $\varpi_2 \equiv_\vartheta \varpi_1$ mit $\varpi_2\zeta \equiv_{\vartheta^{11}} \zeta^{5^3}\varpi_2$, nämlich

$$\varpi_2 \;:=\; \vartheta - 2\vartheta^2 + 2\vartheta^3 - \vartheta^4 - \vartheta^7 - \vartheta^8 + \vartheta^{10}\ .$$

Es ist nun $\varpi_2^4 \equiv_{5^3} -5$.

Für eine genaue Lösung gälte, daß ihre 4te Potenz in $\mathbf{Z}_5$ läge, da sie mit ζ und sich selbst kommutierte.

Es bleibt uns, den Faktor -1 mittels eines Elements aus $\mathbf{Z}_5[\pi]$ mit Norm -1 zu entfernen.

Das Element π^2 hat Norm -1 modulo 5. Als daran ansetzende Näherung erhalten wir etwa das Element $221\pi^2$, das Norm -1 hat modulo 5^4. Unsere Näherung lautet also insgesamt

$$\varpi \ := \ 221\pi^2\varpi_2 \ .$$

Stellen wir zusammen. Es ist mit unseren Approximationen

$$\varpi^4 \ \equiv_{5^3} \ 5 \ , \qquad \varpi\zeta \equiv_{\vartheta^{11}} \zeta^{5^3}\varpi \ , \qquad \Phi_{(5^4-1)}(\zeta) \ \equiv_{5^3} \ 0 \ ,$$

und es ist als einziges davon $r = 3$ exakt gezeigt.

Beachte auch, daß $\Phi_{(5^4-1)}(X)$ nicht das Minimalpolynom einer primitiven (5^4-1)sten Einheitswurzel über $\mathbf{Q}_5$ ist, denn ein solches hat Grad 4. Vgl. auch die Faktorisierung modulo 5 von $\Phi_{(5^4-1)}(X)$ in 48 irreduzible Faktoren vom Grad 4.

Aufgabe 2.

Es gibt wegen der Hasse-Invarianten bis auf Isomorphie nur einen Schiefkörper der Dimension 4 über $\mathbf{Q}_2$, nämlich $\mathbf{H}_2$. Es muß daher $D_{a,b;\,2}$ isomorph zu $\mathbf{H}_2$ sein, sofern es nur ein Schiefkörper ist. Dies ist der Fall, sobald $(-a,-b)_2 = -1$, vgl. Blatt 7, Aufgabe 2 (2) und [loc. cit., III, §1, th. 1]. Ein konkreter Isomorphismus kann stets mit dem in Aufgabe 1 durchgeführten Standardisierungsverfahren gefunden werden (vgl. $\mathbf{H}_2 \simeq D_{-2,3;\,2}$, wie in Aufgabe 1 (b) erwähnt).

Aufgabe 3.

Zunächst gilt es zu bemerken, daß die Bezeichnung ζ_{12} in (1) und in (2) unzweideutig ein Minimalpolynom festlegt, da eine primitive 12-te Einheitswurzel über $\mathbf{Q}_2$ und über $\mathbf{Q}_3$ das Minimalpolynom $X^4 - X^2 + 1$ über $\mathbf{Q}$ behält. Denn würde $X^4 - X^2 + 1$ über $\mathbf{Q}_2$ in zwei nichttriviale normierte Faktoren zerfallen, so auch über $\mathbf{Z}_2$, und es wären beide Faktoren wegen $X^4 - X^2 + 1 \equiv_2 (X^2 + X + 1)^2$ kongruent zu $X^2 + X + 1$ modulo 2. Man überzeugt sich modulo 4, daß dies nicht möglich ist. Und würde $X^4 - X^2 + 1$ über $\mathbf{Q}_3$ in zwei nichttriviale normierte Faktoren zerfallen, so auch über $\mathbf{Z}_3$, und es wären beide Faktoren wegen $X^4 - X^2 + 1 \equiv_2 (X^2 + 1)^2$ kongruent zu $X^2 + 1$ modulo 3. Man überzeugt sich modulo 9, daß dies nicht möglich ist.

Um die maximale unverzweigte Teilerweiterung zu bestimmen, kann man nun entweder den Fixkörper der Trägheitsgruppe berechnen (vgl. Blatt 4, Aufgabe 2 (d)) oder aber, da wir über vollständig bewerteten Grundkörpern arbeiten, eine primitive $(p^m - 1)$ste Einheitswurzel in L ausfindig machen, wobei p^m die Anzahl der Elemente im Restklassenkörper bezeichnet. Von dieser Einheitswurzel wird dann die maximale unverzweigte Teilerweiterung erzeugt.

(1) Es ist $\mathbf{F}_2[X]/(X^4 - X^2 + 1) = \mathbf{F}_2[X]/(X^2 - X + 1)^2$, also hat der Restklassenkörper des einzigen Primideals $\mathfrak{p} = (2, \zeta_{12}^2 + \zeta_{12} + 1)$ über (2) gerade 4 Elemente. Als maximal unverzweigte Teilerweiterung finden wir $\mathbf{Q}_2(\zeta_3)$, wobei $\zeta_3 := \zeta_{12}^4$. Und in der Tat ist 2 in $\mathbf{Q}_2(\zeta_3) = \mathbf{Q}_2[X]/(X^2 + X + 1)$ unverzweigt, es ist $(X^2 + X + 1)$ prim in $\mathbf{F}_2[X]$.

(2) Es ist $\mathbf{F}_3[X]/(X^4 - X^2 + 1) = \mathbf{F}_3[X]/(X^2 + 1)^2$, also hat der Restklassenkörper des einzigen Primideals $\mathfrak{p} = (3, \zeta_{12}^2 + 1)$ über (3) gerade 9 Elemente. Wir suchen

nun eine primitive 8-te Einheitswurzel in $\mathbf{Q}_3(\zeta_{12})$, d.h. wir wollen eine Nullstelle von $x^2 = i$ in $\mathbf{Q}_3(\zeta_{12})$ bestimmen, wobei $i := \zeta_{12}^3$. Es zerfällt $\Phi_8(X) = X^4 + 1 = (X^2 + wX - 1)(X^2 - wX - 1) \in \mathbf{Q}_3[X]$, mit $w = \sqrt{-2} \in \mathbf{Q}_3$, cf. Aufgabe 1 (b, ii). Also ist wegen $\mathbf{Q}_3(i) \subseteq \mathbf{Q}_3(x)$ aus Gradgründen $\mathbf{Q}_3(i) = \mathbf{Q}_3(x)$, und $\mathbf{Q}_3(i)$ ist die maximale unverzweigte Teilerweiterung.

Nichtsdestotrotz, der Ansatz $x = a + bi$ mit $a, b \in \mathbf{Q}_3$ führt uns auf $a^2 - b^2 = 0$ und $2ab = 1$. Wählen wir $a = -b$, so sehen wir, daß $a = w/2$ und $b = -w/2$ die Gleichungen lösen. Wir erhalten die primitive 8te Einheitswurzel $\zeta_8 := w(1-i)/2 \in \mathbf{Q}_3(i) \subseteq \mathbf{Q}_3(\zeta_{12})$.

(3) Zunächst merken wir an, daß $X^4 - X^2 + (1+t)$ in der Tat irreduzibel ist. Modulo t haben wir die Faktorisierung $X^4 - X^2 + (1+t) \equiv_t (X^2+1)^2$, und modulo t^2 sieht man, daß sich diese nicht heben läßt.

Wir schreiben α für das Bild von X in L, so daß $\alpha^4 - \alpha^2 + 1 + t = 0$, und behaupten, daß $S := \mathbf{F}_3[\![t]\!][\alpha]$ der ganze Abschluß von $R := \mathbf{F}_3[\![t]\!]$ in L ist. Das Diskriminantenideal von S über R berechnet sich zu $\Delta_{S|R} = Rt^2$. Eine Oberordnung von S könnte also nur noch das triviale Diskriminantenideal R haben.

Lemma. *Sei R ein vollständiger diskreter Bewertungsring, sei $S|R$ eine endliche Erweiterung, sei S wiederum ein diskreter Bewertungsring. Ist $\Delta_{S|R} = R$, dann ist $S|R$ unverzweigt, i.e. es gibt r Primelement in R und S.*

Beweis. Sei $R \subseteq U \subseteq S$ die maximale unverzweigte Zwischenerweiterung. Wegen $\Delta_{S|R} = \Delta_{U|R}^{[S:U]} \cdot \mathrm{N}_{U|R}(\Delta_{S|U})$ dürfen wir $U = R$ und $S|R$ total verzweigt annehmen. Insbesondere ist $S = R[s]$, wobei Ss maximal in S. Es ist für $j > 1$ die Spur $\mathrm{Tr}_{S|R}(s^j)$ teilbar durch r, wie unter Betrachtung der Matrix bezüglich $(s^0, \ldots, s^{[S:R]-1})$ zu erkennen. Also ist die Diskriminante, genommen bezüglich dieser Basis, teilbar durch $r^{[S:R]-1}$. Damit kann sie nur dann das Einsideal erzeugen, wenn $[S:R] = 1$, q.e.d.

Bleibt zu zeigen, daß bei uns der ganze Abschluß S' von R in L verzweigt ist, um $S' = S$ gezeigt zu haben. In der Tat ist

$$(S'(t, \alpha^2+1))^2 \; = \; S'(t^2, t(\alpha^2+1), \alpha^4 + 2\alpha + 1) \; = \; S'(t^2, t(\alpha^2+1), -t) \; = \; S't \; ,$$

i.e. das Primideal Rt bleibt nicht prim in S'.

Modulo t wird nun $\mathbf{F}_3[\![t]\!][\alpha]/(t) \simeq \mathbf{F}_3[X]/(X^2+1)^2$, wir erhalten also das einzige Primideal $\mathfrak{p} := (t, X^2+1) \subseteq \mathbf{F}_3[\![t]\!][X]/(X^4 - X^2 + (1+t))$ über (t), mit Restklassenkörper isomorph zu $\mathbf{F}_3[X]/(X^2+1)$, also mit 9 Elementen. Wir haben demnach eine primitive 8-te Einheitswurzel in L zu suchen, i.e. eine Nullstelle von $f(y) := y^4 + 1$. Modulo $\mathfrak{p}$, i.e. in $\mathbf{F}_9$, haben wir die Nullstelle $X+1$, und diese wollen wir zu einer veritablen Nullstelle hochhenseln. Es ist $v_{\mathfrak{p}}(f'(X+1)) = v_{\mathfrak{p}}(X^3+1) = 0$, also ist das möglich.

Als Iterationsschritt erhalten wir $y_{i+1} = y_i - f(y_i)/f'(y_i) = -1/y_i^3$, wobei $y_1 := X+1$, und damit die Cauchyfolge

$$(X+1, -(X^3+1)^{-1}, X^9+1, -(X^{27}+1)^{-1}, \ldots) \, .$$

Vernachlässigen wir jedes zweite Folgenglied (was den Grenzwert nicht ändert), und reduzieren wir modulo $X^4 - X^2 + (1+t))$ (i.e. rechnen wir in L), so erhalten wir die Folge

$$\begin{array}{l} \Big(X+1, X^9+1, X^{81}+1, \dots\Big) \;=\; \\ \Big(\, X+1, \\ (-1+t)X^3+(t+t^2)X+1, \\ (-1+t-t^4-t^6+t^{13}+t^{15}+t^{18}+t^{19})X^3+(t+t^2-t^4-t^5+t^{13}+t^{14}+t^{19}+t^{20})X+1, \\ \dots\Big)\,. \end{array}$$

Diese strebt gegen ein Element $\zeta_8 \in L$, und der angegebene Folgenanfang möge uns als Näherungslösung genügen. Die maximale unverzweigte Teilerweiterung ist dann gegeben durch $K(\zeta_8)$.

Aufgabe 4.

(1) Modulo 2 zerfällt $\Phi_7(X) = X^6+X^5+X^4+X^3+X^2+X+1 \equiv_2 (X^3+X+1)(X^3+X^2+1)$. Diese Zerlegung läßt sich hochheben zu einer Zerlegung über $\mathbf{Q}_2$, da die Faktoren teilerfremd sind. Die Methode der Idempotentliftung (cf. Blatt 5, Aufgabe 2) liefert

$$\Phi_7(X) \;=\; f(X)g(X)$$

mit

$$\begin{array}{rcl} f(X) & := & X^3+(0,2,6,6,\dots)X^2+(1,1,5,5,\dots)X+(-1,-1,-1,-1,\dots) \\ g(X) & := & X^3+(1,3,3,11,\dots)X^2+(0,2,2,10,\dots)X+(-1,-1,-1,-1,\dots) \end{array}$$

irreduzibel in $\mathbf{Q}_2[X]$, und entsprechend

$$\mathbf{Z}_2 \otimes_{\mathbf{Z}} \mathbf{Z}[\zeta_7] \;\simeq\; \mathbf{Z}_2[X]/(f(X)) \times \mathbf{Z}_2[X]/(g(X))\;,$$

und also

$$\mathbf{Q}_2 \otimes_{\mathbf{Q}} \mathbf{Q}[\zeta_7] \;\simeq\; \mathbf{Q}_2[X]/(f(X)) \times \mathbf{Q}_2[X]/(g(X))\;.$$

(2) Wir suchen einen Isomorphismus von $\mathbf{Q}_2(\alpha) := \mathbf{Q}_2[X]/(f(X))$, $\alpha \longleftarrow\!\shortmid X$, nach $\mathbf{Q}_2(\beta) := \mathbf{Q}_2[X]/(g(X))$, $\beta \longleftarrow\!\shortmid X$, d.h. wir suchen eine Nullstelle von $f(X)$ in $\mathbf{Q}_2(\beta)$. In anderen Worten, wir suchen eine primitive 7te Einheitswurzel in $\mathbf{Q}(\beta)$, die nicht Nullstelle von $g(X)$ ist, da die Nullstellen von $\Phi_7(X) = (X^7-1)/(X-1)$ genau alle primitiven 7ten Einheitswurzeln durchlaufen. Modulo 2 hat $g(X)$ die Nullstellen β, β^2 und β^4 (Frobenius!), und also nicht die Nullstellen

$$\begin{array}{rcl} \beta^3 & \equiv_{16} & 5\beta^2+6\beta+1 \\ \beta^5 & \equiv_{16} & -6\beta^2-\beta-1 \\ \beta^6 & \equiv_{16} & \beta^2-5\beta-6 \end{array}$$

welche daher Nullstellen von $f(X)$ modulo 2 sind. Dies bleibt auch über $\mathbf{Z}_2$ richtig.

(3) Sie kann die *verschiedenen* Minimalpolynome $f(X)$ und $g(X)$ haben. Beachte, daß $\mathbf{Q}_2(\zeta_7)$ in der Regel die Adjunktion einer primitiven 7ten Einheitswurzel *über* $\mathbf{Q}_2$ bedeutet (oben als $\mathbf{Q}_2(\alpha)$, $\mathbf{Q}_2(\beta)$ bezeichnet), und sich von $\mathbf{Q}_2 \otimes_{\mathbf{Q}} \mathbf{Q}(\zeta_7)$ unterscheidet, worin ζ_7 eine primitive 7te Einheitswurzel *über* $\mathbf{Q}$ war.

Aufgabe 5.

Sei $V = E^m$ der einfache $E \otimes_K D = E^{m \times m}$-Modul. Dann zerfällt $E \otimes_K D$ in eine direkte Summe von m isomorphen Kopien von V. Es wird $[E : K] = \dim_D E \otimes_K D = m \cdot \dim_D V$, speziell also $m \mid [E : K]$.