G. Nebe, M. Künzer

Übungen Algebra II, Sommersemester 03

Lösung 1

Aufgabe 1.

(a) Sei $\xi = a + b\sqrt{d}$ mit $a, b \in \mathbf{Q}$ ein allgemeines Element von $\mathbf{Q}(\sqrt{d})$. Dieses Element ist ganz (über $\mathbf{Z}$) genau dann, wenn sein Minimalpolynom in $\mathbf{Z}[X]$ liegt. Ist $b = 0$, so ist dies gegeben durch $\mu_{\xi,\mathbf{Q}}(X) = X - a$, und wir erhalten als Bedingung $a \in \mathbf{Z}$. Ist $b \neq 0$, so ist $\mu_{\xi,\mathbf{Q}}(X)$ von Grad 2, und wegen $\xi^2 = (a^2 + db^2) + 2ab\sqrt{d}$ ergibt sich

$$\mu_{\xi,\mathbf{Q}}(X) \;=\; X^2 - 2aX + (a^2 - db^2)\,.$$

Mit $2a =: a_0 \in \mathbf{Z}$ und $b = b_1/b_2$ mit $b_1, b_2 \in \mathbf{Z}$ in gekürzter Form wird aus der Forderung $a^2 - db^2 \in \mathbf{Z}$ die Bedingung, daß $a_0^2/4 - db_1^2/b_2^2$ ganz sei. Hieraus lesen wir zunächst $4db_1^2/b_2^2$ ganz ab. Da d quadratfrei ist, folgt zunächst, daß b_2 ein Teiler von 4 ist. Dann kann man noch $b_2 = 4$ ausschließen. Damit können wir auch $b = b_0/2$ mit $b_0 \in \mathbf{Z}$ schreiben (nicht notwendig gekürzt). Die Bedingung liest sich nun

$$a_0^2 \;\equiv_4\; db_0^2$$

Fall $d \equiv_4 1$. Wir erhalten $a_0 \equiv_2 b_0$. Der Ring der ganzen Zahlen ist als Menge gegeben durch $\{(a_0 + b_0\sqrt{d})/2 \;:\; a_0, b_0 \in \mathbf{Z}, a_0 \equiv_2 b_0\}$ (der Fall $b = 0$ ist hierbei mit abgedeckt). Als $\mathbf{Z}$-lineare Basis ergibt sich e.g. $(1, \frac{1}{2} + \frac{\sqrt{d}}{2})$, der Ring selbst ist gegeben durch $\mathbf{Z}[\frac{1}{2} + \frac{\sqrt{d}}{2}]$.

Fall $d \equiv_4 2$. Die Kongruenz ist nur lösbar für $a_0 \equiv_2 0$, was wegen d quadratfrei wiederum $b_0 \equiv_2 0$ impliziert. Der Ring der ganzen Zahlen ist also gegeben durch $\mathbf{Z}[\sqrt{d}]$, mit $\mathbf{Z}$-linearer Basis $(1, \sqrt{d})$.

Fall $d \equiv_4 3$. Wäre a_0 ungerade, so hätte auch b_0 ungerade zu sein, was auf den Widerspruch $1 \equiv_4 -1$ führte. Die Kongruenz ist also nur lösbar für $a_0, b_0 \equiv_2 0$. Der Ring der ganzen Zahlen ist mithin gegeben durch $\mathbf{Z}[\sqrt{d}]$, mit $\mathbf{Z}$-linearer Basis $(1, \sqrt{d})$.

(b) Bestimmen wir zunächst die *Einheiten.* Ein Element $a + b\sqrt{2}$ mit $a, b \in \mathbf{Z}$ ist genau dann eine Einheit, wenn seine Norm $\mathrm{N}_{\mathbf{Q}(\sqrt{2})|\mathbf{Q}}(a+b\sqrt{2}) = a^2 - 2b^2$ in $\mathbf{Z}^* = \{-1, +1\}$ liegt. Insbesondere ist mit $a + b\sqrt{2}$ stets auch $\pm a \pm b\sqrt{2}$ eine Einheit.

Ferner beobachten wir noch, daß $(1 + \sqrt{2})(-1 + \sqrt{2}) = 1$, beide Faktoren sind Einheiten von Norm -1.

Wir behaupten, daß jede Einheit von der Form $\pm(1 + \sqrt{2})^m$ mit $m \in \mathbf{Z}$ ist. Beachte, daß wenn $a + b\sqrt{2}$ von dieser Form ist, dann auch $\pm a \pm b\sqrt{2}$.

Sei $a + b\sqrt{2}$ eine Einheit, und seien $a, b \geq 0$. Wir haben zu zeigen, daß diese Einheit von der verlangten Form ist. Es wird

$$(a + b\sqrt{2})(-1 + \sqrt{2}) \;=\; (2b - a) + (a - b)\sqrt{2}\,.$$

Nun ist für $b > 0$

$$a - b \;=\; \sqrt{2b^2 \pm 1} - b \;\in\; [0, b)\;.$$

Also dürfen wir mit Induktion $b = 0$ annehmen. Dann aber ist $a = 1$.

Betrachten wir nun die *Primideale.* Zeigen wir zunächst, daß $\mathbf{Z}[\sqrt{2}]$ ein euklidischer Ring ist, und also insbesondere ein Hauptidealbereich. Sei dazu

$$\begin{array}{rcl} \mathbf{Z}[\sqrt{2}] \smallsetminus \{0\} & \xrightarrow{\|-\|} & \mathbf{Z}_{\geq 0} \\ a + b\sqrt{2} & \longmapsto & \|a + b\sqrt{2}\| := |\mathrm{N}_{\mathbf{Q}(\sqrt{2})|\mathbf{Q}}(a + b\sqrt{2})| = |a^2 - 2b^2|\;, \end{array}$$

wobei $a, b \in \mathbf{Z}$. Sicher ist $\|xy\| = \|x\|\|y\|$. Zu zeigen ist noch, daß für $x, y \in \mathbf{Z}[\sqrt{2}]$ mit $y \neq 0$ zwei Elemente $s, r \in \mathbf{Z}[\sqrt{2}]$ existieren mit $x = sy + r$, wobei $r = 0$ oder $\|r\| < \|y\|$. Schreiben wir $x/y = \xi + \eta\sqrt{2}$ mit $\xi, \eta \in \mathbf{Q}$, so finden wir $s = \sigma + \tau\sqrt{2}$ mit $\sigma, \tau \in \mathbf{Z}$ und $|\sigma - \xi|, |\tau - \eta| \leq 1/2$. Wir dürfen also $|\xi|, |\eta| \leq 1/2$ annehmen und haben

$$|\mathrm{N}_{\mathbf{Q}(\sqrt{2})|\mathbf{Q}}(\xi + \eta\sqrt{2})| \;<\; 1$$

zu zeigen, was aber unmittelbar folgt.

Zunächst ist nun 0 ein Primideal, und das ist das einzige Primideal, das über dem Nullideal in $\mathbf{Z}$ liegt.

Sei $p \in \mathbf{Z}$ eine Primzahl. Die Primideale, die über $p\mathbf{Z}$ liegen, entsprechen den Primidealen von $\mathbf{Z}[\sqrt{2}]/p\mathbf{Z}[\sqrt{2}] \simeq \mathbf{F}_p[X]/(X^2 - 2)$. Wir müssen also untersuchen, wie $f(X) := X^2 - 2 \in \mathbf{F}_p[X]$ in Faktoren zerfällt, und unterscheiden die folgenden Fälle.

$p = 2$. Hier ist $f(X) = X^2$. Es liegt also genau ein Primideal über 2, entsprechend $(X) \subseteq \mathbf{F}_2[X]$, und das läuft auf $(2, \sqrt{2}) = (\sqrt{2})$ hinaus.

$p \geq 3$, $p \equiv_8 3$ oder $p \equiv_8 5$. Wir behaupten, daß $p\mathbf{Z}[\sqrt{2}]$ ein Primideal ist. Wäre p nicht prim, so wäre, da $\mathbf{Z}[\sqrt{2}]$ als Hauptidealring primfaktoriell ist (cf. Aufg. 4 b), p auch reduzibel. Es hat Norm p^2, würde also in zwei Elemente von Norm $\pm p$ zerfallen. Nun gibt aber eine Fallunterscheidung nach Restklassen modulo 4, daß $p = a^2 - 2b^2$ mit $a, b \in \mathbf{Z}$ impliziert, daß $p \equiv_8 1$ oder $p \equiv_8 -1$. Also kann p nicht reduzibel sein, und muß mithin prim sein. Insbesondere ist $f(X)$ ein irreduzibles Polynom in $\mathbf{F}_p[X]$.

$p \geq 3$, $p \equiv_8 -1$. In $\mathbf{Z}[i]$ ist mit $p = 8n - 1$

$$(2^{2n})^2 \;=\; (1 + i)^p(1 + i) \;\equiv_p\; (1 + i^p)(1 + i) \;=\; (1 - i)(1 + i) \;=\; 2\;,$$

und diese Kongruenz gilt dann auch in $\mathbf{Z}$. Somit erhalten wir in $\mathbf{F}_p[X]$ die Zerlegung $f(X) = (X - 2^{2n})(X + 2^{2n})$, und entsprechend die Primideale $(p, \sqrt{2} - 2^{(p+1)/4})$ und $(p, \sqrt{2} + 2^{(p+1)/4})$. Beide sind natürlich Hauptideale, nur ist es wohl nicht möglich, einen Hauptidealerzeuger in geschlossener Form anzugeben.

Ist hingegen $p \equiv_8 1$, so ist mit $p = 8n + 1$ wegen

$$2^{4n+1} \;=\; (1 + i)^p(1 - i) \;\equiv_p\; (1 + i^p)(1 - i) \;=\; (1 + i)(1 - i) \;=\; 2$$

zumindest einmal $2^{4n} \equiv_p 1$. Da $\mathbf{F}_p^* \simeq C_{8n}$, ist 2 ein Quadrat in $\mathbf{F}_p$. Sei etwa $2 \equiv_p \alpha_p^2$, mit $\alpha_p \in \mathbf{Z}$. Dann wird $f(X) = (X - \alpha_p)(X + \alpha_p)$, und entsprechend die Primideale $(p, \sqrt{2} - \alpha_p)$ und $(p, \sqrt{2} + \alpha_p)$. Beide sind natürlich Hauptideale, nur ist es wohl nicht

möglich, einen Hauptidealerzeuger in geschlossener Form anzugeben. Auch die bloße Existenzaussage für α_p ist nicht zufriedenstellend.

Wir erhalten so die Primideale

$$0,\ (\sqrt{2}),\ (3),\ (5),\ (3+\sqrt{2}),\ (3-\sqrt{2}),\ (11),\ (13),\ (5-2\sqrt{2}),\ (5+2\sqrt{2}),\ (19),$$
$$(5-\sqrt{2}),\ (5+\sqrt{2}),\ (29),\ (7-3\sqrt{2}),\ (7+3\sqrt{2})\ ,\ \ldots\ ,$$

wobei wir nun in den angeführten Idealen geeignete Hauptidealerzeuger gesucht haben.

Aufgabe 2.

(a) Wir können $p \geq 3$ annehmen.

Sei $x \in \mathbf{Q}(\zeta_p)$ ganz über $\mathbf{Z}$. Dann ist die Spur $\mathrm{Tr}_{\mathbf{Q}(\zeta_p)|\mathbf{Q}}(x\zeta_p^i) \in \mathbf{Z}$ für alle $i \in [0, p-2]$. Schreiben wir $x = \sum_{j\in[0,p-2]} \alpha_j \zeta_p^{-j}$, so folgt, daß

$$\sum_{j\in[0,p-2]} \alpha_j \mathrm{Tr}_{\mathbf{Q}(\zeta_p)|\mathbf{Q}}(\zeta_p^{-j}\zeta_p^i) \ \in\ \mathbf{Z}$$

für alle $i \in [0, p-2]$. Mit Cramer ist also $\alpha_k \cdot \det(\mathrm{Tr}_{\mathbf{Q}(\zeta_p)|\mathbf{Q}}(\zeta_p^{i-j}))_{i,j} \in \mathbf{Z}$ für alle $k \in [0, p-2]$. Wir wollen diese Determinante berechnen.

Zunächst ist $\mathrm{Tr}_{\mathbf{Q}(\zeta_p)|\mathbf{Q}}(\zeta_p^j)$ gleich $p-1$ für $j \in p\mathbf{Z}$, und gleich -1 sonst. Eine elementare Rechnung zeigt, daß allgemein die Determinante einer Matrix in $\mathbf{Q}^{n\times n}$ mit $\xi-1$ auf der Hauptdiagonalen und -1 außerhalb der Hauptdiagonalen gleich $\xi^n - n\xi^{n-1}$ ist – subtrahiere die erste Spalte von den weiteren, dann addiere alle Zeilen zur ersten. Damit wird in unserem Fall

$$\det(\mathrm{Tr}_{\mathbf{Q}(\zeta_p)|\mathbf{Q}}(\zeta_p^{i-j}))_{i,j} \ =\ p^{p-1} - (p-1)p^{p-2} \ =\ p^{p-2}\ .$$

Bezeichnet $\mathcal{O}$ den Ring der ganzen Zahlen in $\mathbf{Q}(\zeta_p)$, so erhalten wir also $p^{p-2}\mathcal{O} \subseteq \mathbf{Z}[\zeta_p]$. Beachte ferner, daß $\mathcal{O} \simeq \mathbf{Z}^{p-1}$ als abelsche Gruppen.

Es ist $(\zeta_p^i - 1)/(\zeta_p - 1)$ für $i \in [1, p-1]$ eine Einheit in $\mathbf{Z}[\zeta_p]$ und also auch in $\mathcal{O}$. In der Tat, mit $j \in [1, p-1]$ so, daß $ij \equiv_p 1$ wird $(\zeta_p - 1)/(\zeta_p^i - 1) = ((\zeta_p^i)^j - 1)/(\zeta_p^i - 1) \in \mathbf{Z}[\zeta_p]$. Insbesondere unterscheiden sich $(\zeta_p - 1)^{p-1}$ und $\prod_{i\in[1,p-1]}(\zeta_p^i - 1) = \mathrm{N}_{\mathbf{Q}(\zeta_p)|\mathbf{Q}}(\zeta_p - 1) = (-1)^{p-1}\mu_{\zeta_p-1,\mathbf{Q}}(0) = (-1)^{p-1}\Phi_p(1) = (-1)^{p-1}p$ um eine Einheit in $\mathcal{O}$. Schreiben wir $\lambda := \zeta_p - 1$ und halten wir fest, daß $\lambda^{p-1}\mathcal{O} = p\mathcal{O}$.

Betrachten wir die absteigende Kette

$$\lambda^0\mathcal{O} \ \supseteq\ \lambda^1\mathcal{O} \ \supseteq\ \lambda^2\mathcal{O} \ \supseteq\ \cdots$$

Da $\mathcal{O} \supseteq p\mathcal{O} \supseteq p^2\mathcal{O} \supseteq \cdots$ eine echt absteigende Kette bildet, muß die Inklusion $\lambda^i\mathcal{O} \supseteq \lambda^{i+1}\mathcal{O}$ stets echt sein, da sonst die Kette an dieser Stelle stationär würde. Die Quotienten $\lambda^i\mathcal{O}/\lambda^{i+1}\mathcal{O}$ sind somit als $\mathbf{F}_p$-Vektorräume von Dimension ≥ 1. Da zusammen $\sum_{i\in[0,p-2]} \dim_{\mathbf{F}_p} \lambda^i\mathcal{O}/\lambda^{i+1}\mathcal{O} = \dim_{\mathbf{F}_p} \mathcal{O}/p\mathcal{O} = p-1$ erreicht wird, erhalten wir $\dim_{\mathbf{F}_p} \lambda^i\mathcal{O}/\lambda^{i+1}\mathcal{O} = 1$.

Speziell ist $\mathbf{F}_p \longrightarrow \mathcal{O}/\lambda\mathcal{O}$, $x \longmapsto x$, ein Isomorphismus. Hieraus entnehmen wir $\mathbf{Z} + \lambda\mathcal{O} = \mathcal{O}$ $(*)$. Das wiederum ergibt mit λ multipliziert $\lambda\mathbf{Z} + \lambda^2\mathcal{O} = \lambda\mathcal{O}$, und dies in $(*)$ eingesetzt liefert $\mathbf{Z} + \lambda^2\mathcal{O} = \mathcal{O}$. Das wiederum ergibt mit λ multipliziert $\lambda\mathbf{Z} + \lambda^3\mathcal{O} = \lambda\mathcal{O}$, und dies in $(*)$ eingesetzt liefert $\mathbf{Z} + \lambda^3\mathcal{O} = \mathcal{O}$. So fortfahrend erhalten wir $\mathcal{O} = \mathbf{Z} + \lambda^{(p-1)(p-2)}\mathcal{O} = \mathbf{Z} + p^{p-2}\mathcal{O} \subseteq \mathbf{Z}[\zeta_p]$. Insgesamt erhalten wir somit $\mathcal{O} = \mathbf{Z}[\zeta_p]$.

(b) Sei hierzu

$$\begin{array}{rcl} \mathbf{Z}[\zeta_3] \smallsetminus \{0\} & \xrightarrow{\|-\|} & \mathbf{Z}_{\geq 0} \\ a + b\zeta_3 & \longmapsto & \|a + b\zeta_3\| := \mathrm{N}_{\mathbf{Q}(\zeta_3)|\mathbf{Q}}(a + b\zeta_3) = a^2 - ab + b^2 \ , \end{array}$$

wobei $a, b \in \mathbf{Z}$. Beachte, daß in der Tat $a^2 - ab + b^2 \geq 0$ stets, da für $ab \geq 0$ gilt, daß $a^2 - ab + b^2 \geq (a-b)^2$. Ähnlich wie oben für $\mathbf{Z}[\sqrt{2}]$ bleibt nun zu zeigen, daß für $\xi, \eta \in \mathbf{Q}$ mit $|\xi|, |\eta| \leq 1/2$ gilt, daß

$$\mathrm{N}_{\mathbf{Q}(\sqrt{2})|\mathbf{Q}}(\xi + \eta\zeta_3) \ < \ 1 \ .$$

In der Tat ist

$$\begin{array}{rcl} \|\xi + \eta\zeta_3\| & = & \xi^2 - \xi\eta + \eta^2 \\ & \leq & 1/4 + 1/4 + 1/4 \\ & < & 1 \ . \end{array}$$

Aufgabe 3.

Mit $\|a + bi\| := \mathrm{N}(a + bi) = a^2 + b^2$, wobei $a, b \in \mathbf{Z}$, wird $\mathbf{Z}[i]$ ein euklidscher Ring, da für $\xi, \eta \in \mathbf{Q}$ mit $|\xi|, |\eta| \leq 1/2$

$$\mathrm{N}(\xi + \eta i) \ \leq 1/2 \ < \ 1 \ .$$

Zunächst ist nun $2 = 1^2 + 1^2$.

Primzahlen $p \geq 3$ mit $p \equiv_4 -1$ lassen sich sicher nicht als Summe zweier Quadrate schreiben, wie eine Betrachtung modulo 4 ergibt.

Wir behaupten umgekehrt, daß sich alle Primzahlen $p \geq 3$ mit $p \equiv_4 1$ als Summe zweier Quadrate schreiben lassen. Schreibe $p = 4n + 1$ mit $n \in \mathbf{Z}$. Es wird $(-1)^{2n} \equiv_p 1$, und somit ist $-1 \in (\mathbf{F}_p^*)^2$. In der Tat ist

$$(2n)!^2 \ \equiv_p \ 1 \cdot 2 \cdots 2n \cdot (p - 2n) \cdot (p - 2n + 1) \cdots (p - 1) \ \equiv_p \ -1 \ .$$

Somit teilt p das Element $((2n)! - i)((2n)! + i)$, ohne einen der Faktoren zu teilen. Also ist p nicht prim, und damit auch nicht irreduzibel. Somit finden wir $p = (a + bi)(c + di)$ mit weder $a + bi$ noch $c + di$ Einheit, $a, b, c, d \in \mathbf{Z}$. Also ist $a^2 + b^2 = \mathrm{N}_{\mathbf{Q}(i)|\mathbf{Q}}(a + bi)$ ein echter Teiler von $\mathrm{N}_{\mathbf{Q}(i)|\mathbf{Q}}(p) = p^2$, d.h. $a^2 + b^2 = p$.

Aufgabe 4.

(a) Sei R ein primfaktorieller Integritätsbereich. Sind π und π' zwei Primelemente, und teilt π das Element π', so ist π'/π eine Einheit. Denn aus $\pi' = a\pi$ mit $a \in R$ folgt $\pi' \mid a$ oder $\pi' \mid \pi$. Im ersteren Fall gäbe es ein $b \in R$ mit $\pi' = \pi\pi' b$, woraus sich nach Kürzen von π' ergäbe, daß π' eine Einheit wäre, was nicht der Fall ist. Im zweiteren Fall gibt es ein $b \in R$ mit $\pi = b\pi'$, woraus sich $1 = ab$ ergibt. Also ist a eine Einheit, wie behauptet.

Sei nun gegeben

$$\alpha\pi_1 \cdots \pi_m \ = \ \alpha'\pi'_1 \cdots \pi'_{m'}$$

mit Primelementen π_i und π'_i und Einheiten α, α'. Es teilt nun π_1 einen der Primfaktoren der rechten Seite, sagen wir π'_k. Mit $\alpha' = (\pi'_k/\pi_1)\alpha'$, was wiederum eine Einheit darstellt, erhalten wir

$$\alpha\pi_2 \cdots \pi_m \ = \ \tilde{\alpha}'\pi'_1 \cdots \pi'_{k-1}\pi'_{k+1} \cdots \pi'_{m'} \ .$$

Fahren wir so fort, so steht nach m Schritten auf der linken Seite eine Einheit. Also muß $m = m'$ gewesen sein, und wir haben die Eindeutigkeit einer Primfaktorzerlegung bis auf Multiplikation mit Einheiten (und Reihenfolge der Faktoren) gesehen.

Sei nun $K = \mathrm{Quot}(R)$, und sei $x \in K$ so gegeben, daß es ein Polynom $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ gibt mit $f(x) = 0$. Zu zeigen ist $x \in R$. Wir haben eine Primfaktorzerlegung $x = \alpha\pi_1^{k_1} \cdots \pi_m^{k_m}$ mit $k_i \in \mathbf{Z}$ und α einer Einheit, wobei nun π_i nicht π_j teile für $i \neq j$.

Nehmen wir an, es sei $k_l < 0$. Dann hat in

$$\pi_l^{n(-k_l)}x^n \;=\; \pi^{n(-k_l)}(-a_{n-1}x^{n-1} - \cdots - a_0)$$

die Primfaktorzerlegung der rechten Seite einen positiven Exponenten bei π_l, die linke aber nicht, Widerspruch. Also ist stets $k_l \geq 0$ und somit $x \in R$.

(b) Sei R ein Hauptidealbereich. Da jedes Ideal von endlich vielen Elementen erzeugt wird (viz. von einem), ist R noethersch. Jede Teilmenge der Menge aller Ideale in R hat also wenigstens ein maximales Element bezüglich der Inklusion.

Sei angenommen, es gebe Elemente in R ohne Primfaktorzerlegung. Sei $I \subseteq R$ ein Ideal, welches maximal bezüglich der Eigenschaft ist, daß sein Erzeuger (eindeutig bis auf Einheit) keine Primfaktorzerlegung besitzt, und sei $I = (x)$. Es liegt I in einem maximalen Ideal (π), und wegen $R/(\pi)$ Körper, insbesondere also Integritätsbereich, ist π prim. Wegen $(x) \subseteq (\pi)$ können wir $x = \pi y$ schreiben, und es ist auch $(x) \subseteq (y)$. Da π keine Einheit ist, ist diese Inklusion echt. Nach Wahl (x) hat y mithin eine Zerlegung in Primfaktoren. Wegen $x = \pi y$ gilt das auch für x, Widerspruch.

(c) Mit 2 a) können wir z.B. $R = \mathbf{Z}[\zeta_7]$ und $p = 7$ nehmen. Es ist $\mathbf{Z}[\zeta_7]/7\mathbf{Z}[\zeta_7] \simeq \mathbf{F}_7[X]/(\Phi_7(X))$, wobei $\Phi_7(X) = (X^7-1)/(X-1) \equiv_7 (X-1)^7/(X-1) = (X-1)^6$. Also hat $(X-1)^2$ Nilpotenzgrad 3, und das entspricht $(\zeta_7 - 1)^2$.

Alternativ, können wir zeigen, daß $\mathbf{Z}[\sqrt[3]{2}]$ ganzabgeschlossen ist – wir schreiben $\theta := \sqrt[3]{2}$ –, so erhalten wir modulo $p = 3$ den Isomorphismus

$$\mathbf{Z}[\theta]/3\mathbf{Z}[\theta] \xrightarrow{\sim} \mathbf{F}_3[X]/(X^3-2) \;=\; \mathbf{F}_3[X]/((X+1)^3)\;,$$

und das Element $X+1$ von Nilpotenzgrad 3, welches $\theta + 1$ entspricht.

Bleibt zu zeigen, daß $\mathbf{Z}[\theta]$ ganzabgeschlossen ist. Sei $\xi = a + b\theta + c\theta^2$ ein Element von $\mathbf{Q}(\theta)$, wobei $a, b, c \in \mathbf{Q}$, und sei ξ ganz über $\mathbf{Z}$. Wir haben zu zeigen, daß $a, b, c \in \mathbf{Z}$.

Nun ist entweder $b = 0$ und $c = 0$ und also $a \in \mathbf{Z}$, oder aber

$$\mu_{\xi,\mathbf{Q}}(X) \;=\; X^3 - 3aX^2 + 3(a^2 - 2bc)X + (6abc - a^3 - 2b^3 - 4c^3)\;.$$

Für $p \in \mathbf{Z}$ prim und $x \in \mathbf{Q} \smallsetminus \{0\}$ sei $v_p(x) \in \mathbf{Z}$ der Exponent von p in der Primfaktorzerlegung von x, i.e. $x = \prod_{p \text{ prim}} p^{v_p(x)}$. Wir setzen ferner noch $v_p(0) = +\infty$. Wir haben zu zeigen, daß $v_p(a) \geq 0$, $v_p(b) \geq 0$ und $v_p(c) \geq 0$ für alle $p \in \mathbf{Z}$ prim.

Fall $p \geq 5$. Aus $3a \in \mathbf{Z}$ folgt $v_p(a) \geq 0$. Aus $a^2 - 2bc \in \mathbf{Z}$ folgt nun $v_p(b) + v_p(c) \geq 0$ und damit aus $6abc - a^3 - 2b^3 - 4c^3 \in \mathbf{Z}$, daß zunächst auch $v_p(2b^3 + 4c^3) \geq 0$ gilt.

Es ist somit $v_p(b) < 0$ äquivalent zu $v_p(c) < 0$, was wegen $v_p(b) + v_p(c) \geq 0$ also nicht eintreten kann. Damit sind $v_p(b) \geq 0$ und $v_p(c) \geq 0$.

Fall $p = 2$. Aus $3a \in \mathbf{Z}$ folgt $v_2(a) \geq 0$. Aus $a^2 - 2bc \in \mathbf{Z}$ folgt nun $v_2(b) + v_2(c) \geq -1$, und damit aus $6abc - a^3 - 2b^3 - 4c^3 \in \mathbf{Z}$, daß zunächst auch $v_2(2b^3 + 4c^3) \geq 0$ gilt. Es ist somit $v_2(b) < 0$ äquivalent zu $v_2(c) < 0$. Wäre dies der Fall, so müßte wegen $v_2(2b^3 + 4c^3) \geq 0$ gelten, daß $1 \equiv_3 3v_2(b) + 1 = 3v_2(c) + 2 \equiv_3 2$, Widerspruch. Damit sind $v_2(b) \geq 0$ und $v_2(c) \geq 0$.

Fall $p = 3$. Aus $3a \in \mathbf{Z}$ folgt $v_3(a) \geq -1$.

Annahme $v_3(a) = -1$. Aus $a^2 - 2bc \in \mathbf{Z}$ folgt nun $v_3(b) + v_3(c) = -2$. Aus $6abc - (a^3 + 2b^3 + 4c^3) \in \mathbf{Z}$ folgt $v_3(b) = -1$ und $v_3(c) = -1$, da sonst $-2 = v_3(6abc) = v_3(a^3 + 2b^3 + 4c^3) \leq -6$. Wir schreiben $a = a_0/3$, $b = b_0/3$ und $c = c_0/3$ mit $a_0, b_0, c_0 \in \mathbf{Z}$, aber $a_0, b_0, c_0 \notin 3\mathbf{Z}$. Es folgt

$$6a_0b_0c_0 \equiv_{27} a_0^3 + 2b_0^3 + 4c_0^3 \equiv_3 a_0 - b_0 + c_0 .$$

Modulo 3 sehen wir, daß $b_0 \equiv_3 a_0 + c_0$. Da dazuhin $b_0 \not\equiv_3 0$, bleibt nur die Möglichkeit $a_0 \equiv_3 1$ und $c_0 \equiv_3 1$ oder aber die Möglichkeit $a_0 \equiv_3 -1$ und $c_0 \equiv_3 -1$ über. Beides würde, da $\mathbf{Z}[\theta]$ bereits aus ganzen Zahlen besteht, implizieren, daß $1 - \theta + \theta^2$ ganz ist, was aber nicht der Fall ist, da der konstante Koeffizient des Minimalpolynoms $-1/3$ beträgt. Damit ist die Annahme zum Widerspruch geführt, und wir haben $v_3(a) \geq 0$.

Aus $a^2 - 2bc \in \mathbf{Z}$ folgt nun $v_3(b) + v_3(c) \geq 0$. Aus $6abc - (a^3 + 2b^3 + 4c^3) \in \mathbf{Z}$ folgt nun $v_3(2b^3 + 4c^3) \geq 0$. Wäre $v_3(b) < 0$, so wäre $v_3(c) > 0$ und daher $v_3(2b^3 + 4c^3) < 0$, was nicht der Fall ist. Also $v_3(b) \geq 0$. Genauso sieht man $v_3(c) \geq 0$.