G. Nebe, M. Künzer

Übungen Algebra II, Sommersemester 03

Lösung 3

Aufgabe 1.

(a) Sei $G_{\mathbf{R}}$ die Teilmenge der reellen Einbettungen, sei $G_{\mathbf{C}}$ ein Repräsentantensystem in der Teilmenge der echt komplexen Einbettungen bezüglich komplexer Konjugation. Wir verwenden die Isometrie

$$\begin{array}{ccccc} K_{\mathbf{R}} & \xrightarrow[\sim]{f} & \prod_{\rho\in G_{\mathbf{R}}}\mathbf{R} & \times & \prod_{\sigma\in G_{\mathbf{C}}}(\mathbf{R}\times\mathbf{R}) \\ (z_\tau)_{\tau\in G} & \longmapsto & \Big((z_\rho)_{\rho\in G_{\mathbf{R}}} & , & ((\Re(z_\sigma),\Im(z_\sigma))_{\sigma\in G_{\mathbf{C}}}\Big) \end{array}$$

X_t ist sicher zentralsymmetrisch. Zeigen wir, daß X_t konvex ist. Es genügt zu zeigen, daß $f(X_t)$ konvex ist. Seien also $v = ((x_\rho)_\rho, (y_\sigma, \tilde{y}_\sigma)_\sigma)$ und $v' = ((x'_\rho)_\rho, (y'_\sigma, \tilde{y}'_\sigma)_\sigma)$ in $f(X_t)$ gegeben, und sei $\lambda \in [0,1]$. Zu zeigen ist

$$\lambda v + (1-\lambda)v' \overset{!}{\in} f(X_t)\ .$$

In der Tat wird

$$\begin{array}{ll} & \sum_\rho |\lambda x_\rho + (1-\lambda)x'_\rho| + 2\sum_\sigma |\lambda(y_\sigma + i\tilde{y}_\sigma) + (1-\lambda)(y'_\sigma + i\tilde{y}'_\sigma)| \\ \leq & \lambda\Big(\sum_\rho |x_\rho| + 2\sum_\sigma |y_\sigma + i\tilde{y}_\sigma|\Big) + (1-\lambda)\Big(\sum_\rho |x'_\rho| + 2\sum_\sigma |y'_\sigma + i\tilde{y}'_\sigma|\Big) \\ \leq & \lambda t + (1-\lambda)t \;=\; t\ . \end{array}$$

Zur Berechnung des Volumens betrachten wir ferner

$$f(X_t)^+ \;:=\; \left\{((x_\rho)_\rho, (y_\sigma,\tilde{y}_\sigma)_\sigma) \;:\; x_\rho \geq 0\,, \sum_\sigma x_\rho + 2\sum_\sigma |y_\sigma + i\tilde{y}_\sigma| \leq t\right\}\ .$$

Es ist das zu berechnende Volumen gleich dem 2^{r+s}-fachen des Volumens von $f(X_t)^+$ bezüglich des Standardmaßes. Der Faktor 2^r entspringt dem Vergleich von $f(X_t)$ mit $f(X_t)^+$, der Faktor 2^s dem Vergleich des induzierten Maßes von $K_{\mathbf{R}}$ mit dem Standardmaß.

Wir setzen das Volumen von $f(X_t)^+$ mit $v_t := \alpha_{r,s}t^n$ an.

Wir haben $\alpha_{1,0} = t$.

Falls $r > 1$, so wird

$$\begin{array}{rcl} v_t & = & \int_0^t \alpha_{r-1,s}(t-x)^{n-1}\,dx \\ & = & \int_0^t \alpha_{r-1,s}\tilde{x}^{n-1}\,d\tilde{x} \\ & = & \frac{\alpha_{r-1,s}}{n}\,t^n\ , \end{array}$$

i.e. $\alpha_{r,s} = \alpha_{r-1,s}/n$.

Falls $s > 0$, so wird

$$\begin{array}{rcl} v_t & = & \int_0^{2\pi}\int_0^{t/2} \alpha_{r,s-1}(t-2r)^{n-2} r\, dr d\varphi \\ & = & 2\pi \int_0^{t/2} \alpha_{r,s-1}(t-2r)^{n-2} r\, dr \\ & = & 2\pi \int_0^t \alpha_{r,s-1}\tilde{r}^{n-2}\frac{t-\tilde{r}}{2}\,\frac{1}{2}\, d\tilde{r} \\ & = & \frac{\pi}{2}\alpha_{r,s-1}t^n\left(\frac{1}{n-1}-\frac{1}{n}\right) \\ & = & \frac{\pi\alpha_{r,s-1}}{2n(n-1)}\, t^n\ , \end{array}$$

i.e. $\alpha_{r,s} = \pi\alpha_{r,s-1}/(2n(n-1))$.

Zusammen wird $\alpha_{r,s} = \pi^s 2^{-s}/n!$, und das gesuchte Volumen von $f(X_t)$ ergibt sich zu $2^r\pi^s t^n/n!$

(b) **Lemma.** *Sei $\mathfrak{b} \in \mathbf{Z}_K$ ein ganzes Ideal. Es gibt ein Element $b \in \mathfrak{b} \smallsetminus \{0\}$ mit*

$$|\mathrm{N}_{K|\mathbf{Q}}(b)| \;\leq\; \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \mathrm{N}_{K|\mathbf{Q}}(\mathfrak{b})\sqrt{|\Delta_{K|\mathbf{Q}}|}\ .$$

Beweis. Sei $j : K \longrightarrow K_{\mathbf{R}},\ x \longmapsto (x\tau)_{\tau\in G}$. Das Grundmaschenvolumen von $j(\mathfrak{b})$ ist gegeben durch $\mathrm{N}_{K|\mathbf{Q}}(\mathfrak{b})\sqrt{|\Delta_{K|\mathbf{Q}}|}$. Jede zentralsymmetrische konvexe Teilmenge von Volumen größer als $2^n\mathrm{N}_{K|\mathbf{Q}}(\mathfrak{b})\sqrt{|\Delta_{K|\mathbf{Q}}|}$ enthält mit Minkowski also einen Punkt ungleich Null von $j(\mathfrak{b})$.

Speziell, falls $t > t_0 := \left((4/\pi)^s n!\,\mathrm{N}_{K|\mathbf{Q}}(\mathfrak{b})\sqrt{|\Delta_{K|\mathbf{Q}}|}\right)^{1/n}$, dann gibt es mit (a) ein Element $b \in \mathfrak{b} \smallsetminus \{0\}$ mit $j(b) \in X_t$. Also finden wir eine Folge $b_i \in \mathfrak{b} \smallsetminus \{0\}$ mit $j(b_i) \in X_{t_0+1/i}$. Da X_{t_0+1} beschränkt ist, hat die Folge $j(b_i)$ einen Häufungspunkt im Abschluß von X_{t_0+1}, der aber notwendig in X_{t_0}. Da $j(\mathfrak{b}) \smallsetminus \{0\}$ eine abgeschlossene Teilmenge in $K_{\mathbf{R}}$ darstellt (Gitter ohne Ursprung), liegt dieser Häufungspunkt auch in $j(\mathfrak{b}) \smallsetminus \{0\}$. Insgesamt finden wir ein $b \in \mathfrak{b} \smallsetminus \{0\}$ mit

$$\sum_{\tau\in G} |b\tau| \;\leq\; t_0\ ,$$

woraus

$$\begin{array}{rcl} |\mathrm{N}_{K|\mathbf{Q}}(b)| & = & \prod_{\tau\in G}|b\tau| \\ & = & \left(\left(\prod_{\tau\in G}|b\tau|\right)^{1/n}\right)^n \\ & \overset{(1)}{\leq} & \left(\left(\sum_{\tau\in G}|b\tau|\right)/n\right)^n \\ & \leq & t_0^n/n^n \\ & = & (4/\pi)^s\frac{n!}{n^n}\mathrm{N}_{K|\mathbf{Q}}(\mathfrak{b})\sqrt{|\Delta_{K|\mathbf{Q}}|}\ . \end{array}$$

---

[1] Mit Induktion (Abspaltung eines Summanden resp. Faktors) genügt es zu zeigen: $p, q > 0$, $p + q = 1$, $x, y \geq 0$ seien gegeben, dann gilt

$$x^p y^q \;\leq\; px + qy\ .$$

Ohne Einschränkung sei $x > 0$. Setzt man $z = y/x$, so bleibt

$$z^q \;\leq\; p + qz$$

zu zeigen. Wir haben Gleichheit bei $z = 1$, und für die Ableitungen gilt $qz^{q-1} < q$ für $z > 1$, und $qz^{q-1} > q$ für $z < 1$.

Zurück zur Aufgabenstellung. Sei $\mathfrak{c}$ ein beliebiges gebrochenes Ideal in der fraglichen Idealklasse. Wähle ein $c \in \mathbf{Z}_K$ mit $\mathfrak{b} := c\mathfrak{c}^{-1} \subseteq \mathbf{Z}_K$. Das Lemma sichert die Existenz eines $b \in \mathfrak{b} \smallsetminus \{0\}$ mit

$$|\mathrm{N}_{K|\mathbf{Q}}(b)| \;\leq\; \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \mathrm{N}_{K|\mathbf{Q}}(\mathfrak{b})\sqrt{|\Delta_{K|\mathbf{Q}}|}\,.$$

Nun ist $\mathfrak{a} := b\mathfrak{b}^{-1}$ ein ganzes Ideal, wegen $\mathfrak{a} = bc^{-1}\mathfrak{c}$ ist $[\mathfrak{a}] = [\mathfrak{c}]$ die fragliche Idealklasse, und es gilt

$$\mathrm{N}_{K|\mathbf{Q}}(\mathfrak{a}) \;=\; |\mathrm{N}_{K|\mathbf{Q}}(b)|/\mathrm{N}_{K|\mathbf{Q}}(\mathfrak{b}) \;\leq\; \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\Delta_{K|\mathbf{Q}}|}\,.$$

(c) Nach Anwendung von (b) auf $\mathfrak{a} = \mathbf{Z}_K$ bleibt zu zeigen, daß $\frac{n^n}{n!}\left(\frac{\pi}{4}\right)^n > 1$ ist für $n \geq 2$. Die Ungleichheit gilt für $n = 2$, da $\pi > 3$. Mit Induktion nach n bleibt zu zeigen, daß

$$\left(1 + \frac{1}{n-1}\right)^{n-1} \;>\; \frac{4}{\pi}\,.$$

Das ist richtig für $n = 2$, und die Folge auf der linken Seite ist monoton wachsend.

(d) Wegen $2s \leq n$ ist stets $5^{-n}|\Delta_{K|\mathbf{Q}}| \geq 5^{-n}\left(\frac{n^n}{n!}\right)^2\left(\frac{\pi}{4}\right)^n$. Mit Stirling ergibt sich weiter, daß es für jedes $\varepsilon > 0$ ein N so gibt, daß für $n \geq N$

$$5^{-n}\left(\frac{n^n}{n!}\right)^2\left(\frac{\pi}{4}\right)^n \geq (1-\varepsilon)\left(\frac{e^2\pi}{20}\right)^n (2\pi n)^{-1} \;\geq\; (1-\varepsilon)(10/9)^n(2\pi n)^{-1}\,,$$

woraus das Ergebnis folgt.

Aufgabe 2

Sei $L|K$ eine Erweiterung von Zahlkörpern, sei R in K ein diskreter Bewertungsring mit Quotientenkörper K. Dann hat der ganze Abschluß S von R in L endlich viele Primideale, ist also ein Hauptidealbereich, und genauso der ganze Abschluß T von R in M (was zugleich den ganzen Abschluß von S in M darstellt).

Wir schreiben $l := [L:K]$ und $m := [M:L]$. Sei $(y_1,\ldots,y_m)$ eine Basis von T über S, und sei $(x_1,\ldots,x_l)$ eine Basis von S über R. Da S ein Hauptidealbereich ist, gibt es Basen $(y_1',\ldots,y_m')$ und $(y_1'',\ldots,y_m'')$, die aus $(y_1,\ldots,y_m)$ durch einen Basiswechsel mit je einer $\mathrm{SL}_m(S)$-Matrix hervorgehen, derart, daß $\mathrm{Tr}_{M|L}(y_i'y_j'')$ gleich 0 ist für $i \neq j$ und gleich einem γ_i falls $i = j$ (Elementarteilersatz).

Ist $A \in L^{m\times m}$, so ist $\det_K A = \mathrm{N}_{L|K}(\det_L A)$, wobei $\det_L$ die L-lineare und $\det_K$ die K-lineare Determinante bezeichnet, i.e. die Determinante der Abbildung $L^m \xrightarrow{A} L^m$, aufgefaßt als K-lineare Abbildung. (In Termen von Matrizen: man fixiere eine Basis von L über K und forme die Blockmatrix, die in den Blöcken die Matrix für die Multiplikation mit dem entsprechenden Element aus L stehen hat.) Zum Beweis dessen führen wir eine Gaußumformung von A in Zeilenstufenform durch. Für die hierzu benötigten Matrizen in $L^{m\times m}$ (Elementarmatrizen, Permutationsmatrizen, Diagonalmatrizen) gilt die zu beweisende Formel. Da die Formel in A multiplikativ ist, genügt es damit, sie für Matrizen in Zeilenstufenform zu zeigen, und auch hier trifft sie zu.

Nun sind $(x_i y_j)_{(i,j)}$, $(x_i y'_j)_{(i,j)}$ und $(x_i y''_j)_{(i,j)}$ Basen von T über R. Mit der eben gemachten Bemerkung folgt, daß die Basiswechselmatrizen von $(x_i y_j)_{(i,j)}$ zu $(x_i y'_j)_{(i,j)}$ und von $(x_i y_j)_{(i,j)}$ zu $(x_i y''_j)_{(i,j)}$ Determinante 1 haben.

Da $(x_i y_j)_{(i,j)}$ eine Basis von T über R darstellt, wird

$$\begin{array}{rcl}\Delta_{M|K} & = & \det\left(\mathrm{Tr}_{M|K}(x_i y_j x_{i'} y_{j'})\right)_{(i,j);(i',j')} \\ & = & \det\left(\mathrm{Tr}_{M|K}(x_i y'_j x_{i'} y''_{j'})\right)_{(i,j);(i',j')} \\ & = & \det\left(\mathrm{Tr}_{L|K}(x_i x_{i'} \mathrm{Tr}_{M|L}(y'_j y''_{j'}))\right)_{(i,j);(i',j')} \\ & = & \prod_{j\in[1,m]} \det\left(\mathrm{Tr}_{L|K}(\gamma_j x_i x_{i'})\right)_{i,i'} \; . \end{array}$$

Da $\prod_{j\in[1,m]} \gamma_j = \Delta_{M|L}$ ist, genügt es zu zeigen, daß für ein beliebiges $\gamma \in S$

$$\det\left(\mathrm{Tr}_{L|K}(\gamma x_i x_{i'})\right)_{i,i'} \;=\; \mathrm{N}_{L|K}(\gamma)\Delta_{L|K} \; .$$

In der Tat wird

$$\begin{array}{rcl}\det\left(\mathrm{Tr}_{L|K}(\gamma x_i x_{i'})\right)_{i,i'} & = & \det\left(((\gamma x_i)\sigma)_{i,\sigma}\left((x_i\sigma)_{i,\sigma}\right)^{\mathrm{t}}\right) \\ & = & \det\left((\gamma x_i)\sigma\right)_{i,\sigma} \det\left(x_i\sigma\right)_{i,\sigma} \\ & = & \det\left(\gamma\sigma\cdot x_i\sigma\right)_{i,\sigma} \det\left(x_i\sigma\right)_{i,\sigma} \\ & = & \left(\prod_\sigma \gamma\sigma\right) \det\left(x_i\sigma\right)_{i,\sigma} \det\left(x_i\sigma\right)_{i,\sigma} \\ & = & \mathrm{N}_{L|K}(\gamma) \det\left(\mathrm{Tr}_{L|K}(x_i x_{i'})\right)_{i,i'} \\ & = & \mathrm{N}_{L|K}(\gamma)\Delta_{L|K} \; , \end{array}$$

wobei σ jeweils über die Menge der Einbettungen von L nach $\mathbf{C}$ läuft, die zu einer fixierten Einbettung $K \subseteq \mathbf{C}$ einschränken.

Aufgabe 3

(a) Wir schreiben $b = a^{1/m}$ und behaupten, daß $Sb = S\mathfrak{a}$. Da b ganz über R ist, ist b in der Tat in S enthalten. Sei $\mathfrak{p}$ ein Primideal in S. Wir haben $v_\mathfrak{p}(b) = v_\mathfrak{p}(\mathfrak{a})$ zu zeigen. Wir zeigen, daß $mv_\mathfrak{p}(b) = mv_\mathfrak{p}(\mathfrak{a})$. Auf der einen Seite ist $mv_\mathfrak{p}(b) = v_\mathfrak{p}(b^m) = v_\mathfrak{p}(a)$. Auf der anderen Seite ist $mv_\mathfrak{p}(\mathfrak{a}) = v_\mathfrak{p}(\mathfrak{a}^m) = v_\mathfrak{p}(a)$.

(b) Für die Wohldefiniertheit der Abbildung ist zu zeigen, daß alle Ideale einer Klasse auf dasselbe Element gehen. Da die Abbildung multiplikativ ist, läuft das darauf hinaus, zu zeigen, daß $\mathfrak{a}$ Hauptideal impliziert, daß $\mathbf{Z}_L\mathfrak{a}$ Hauptideal.

Wir wissen, daß $\mathrm{Cl}(K)$ endlich ist. Seien $[\mathfrak{a}_1], \ldots, [\mathfrak{a}_n]$ Erzeuger von $\mathrm{Cl}(K)$, und sei m_i die Ordnung von $[\mathfrak{a}_i]$ in dieser endlichen Gruppe. Seien als Repräsentanten $\mathfrak{a}_i$ ferner ganze Ideale gewählt. Es genügt, eine Erweiterung zu finden, in der diese Erzeuger kapitulieren, da dann auch deren Produkte kapitulieren, und somit die auf den Klassengruppen induzierte Abbildung trivial wird. Nach Definition der Klassengruppe gibt es nun $a_i \in \mathbf{Z}_K$ mit

$$\mathfrak{a}_i^{m_i} \;=\; \mathbf{Z}_K a_i$$

für $i \in [1, n]$.

Wenn ein Ideal in einer Erweiterung kapituliert, dann auch in einer größeren, diese enthaltenden Erweiterung. Insbesondere kapitulieren mit (a) alle $\mathfrak{a}_i$ in

$$K(a_1^{1/m_1}, \ldots, a_n^{1/m_n}) \; .$$

(c) Es ist $[(2, 1+\sqrt{-5})]$ ein Erzeuger von $\mathrm{Cl}(\mathbf{Q}(\sqrt{-5}))$ von Ordnung 2, und es ist $(2, 1+\sqrt{-5})^2 = (2)$ (cf. Blatt 2, Aufgabe 3). Daher ist mit (b)

$$\mathrm{Cl}_{\mathbf{Q}(\sqrt{-5},\sqrt{2})|\mathbf{Q}(\sqrt{-5})}$$

trivial. Es ist in der Tat $\mathbf{Z}_{\mathbf{Q}(\sqrt{-5},\sqrt{2})}(2, 1+\sqrt{-5}) = \sqrt{2}\mathbf{Z}_{\mathbf{Q}(\sqrt{-5},\sqrt{2})}$, da

$$\begin{array}{rcl} 2 & = & \sqrt{2}\cdot\sqrt{2} \\ 1+\sqrt{-5} & = & \sqrt{2}\cdot\frac{\sqrt{2}}{2}(1+\sqrt{-5})\ , \end{array}$$

und da letzterer Faktor Minimalpolynom $X^2 + (2-\sqrt{-5})$ über $\mathbf{Z}[\sqrt{-5}]$ hat, sich also in $\mathbf{Z}_{\mathbf{Q}(\sqrt{-5},\sqrt{2})}$ befindet.

Aufgabe 4

$\mathbf{Z}[\sqrt{2}]$. Mit Dirichlet ist die Einheitengruppe von $\mathbf{Z}[\sqrt{2}]$ isomorph zu $C_2 \times \mathbf{Z}$, und mithin gegeben durch $\langle -1, \xi\rangle$, wobei ξ eine Untergruppe isomorph zu $\mathbf{Z}$ erzeugt. Da ξ sowohl durch $-\xi$ als auch durch das Galoiskonjugierte zu ξ ersetzt werden kann, dürfen wir $\xi = a + b\sqrt{2}$ mit $a, b \geq 0$ ansetzen. Da alle Einheiten von der Form $\pm\xi^m$ mit $m \in \mathbf{Z}$ sind, kann zwischen ξ und 1 keine weitere Einheit liegen. Damit folgt $\xi = 1+\sqrt{2}$ und $\mathbf{Z}[\sqrt{2}]^* = \langle -1,\, 1+\sqrt{2}\rangle$.

$\mathbf{Z}[\sqrt{3}]$. Mit Dirichlet ist die Einheitengruppe von $\mathbf{Z}[\sqrt{3}]$ isomorph zu $C_2 \times \mathbf{Z}$, und mithin gegeben durch $\langle -1, \xi\rangle$, wobei ξ eine Untergruppe isomorph zu $\mathbf{Z}$ erzeugt. Wir dürfen $\xi = a + b\sqrt{3}$ mit $a, b \geq 0$ ansetzen. Im Intervall $(1, \xi)$ kann keine weitere Einheit liegen. Damit folgt $\xi = 2+\sqrt{3}$ und $\mathbf{Z}[\sqrt{3}]^* = \langle -1,\, 2+\sqrt{3}\rangle$.

$\mathbf{Z}[(1+\sqrt{5})/2]$. Mit Dirichlet ist die Einheitengruppe von $\mathbf{Z}[(1+\sqrt{5})/2]$ isomorph zu $C_2\times\mathbf{Z}$, und mithin gegeben durch $\langle -1, \xi\rangle$, wobei ξ eine Untergruppe isomorph zu $\mathbf{Z}$ erzeugt. Wir dürfen $\xi = (a+b\sqrt{5})/2$ mit $a, b \geq 0$ und $a \equiv_2 b$ ansetzen. Im Intervall $(1, \xi)$ kann keine weitere Einheit liegen. Damit folgt $\xi = (1+\sqrt{5})/2$ und $\mathbf{Z}[(1+\sqrt{5})/2]^* = \langle -1,\, (1+\sqrt{5})/2\rangle$.

Für $\mathbf{Z}[\zeta_5]$ brauchen wir zunächst ein kleines

Lemma. *Ist $K \subseteq \mathbf{C}$ ein Zahlkörper mit fixierter Einbettung nach $\mathbf{C}$ und abelscher Galoisgruppe $\mathrm{Gal}(K|\mathbf{Q})$, so ist $\mathbf{Z}_K \cap \{z \in \mathbf{C} \,:\, |z| = 1\}$ endlich.*

Beweis. Das Bild von $M := K \cap \{z \in \mathbf{C} \,:\, |z| = 1\}$ unter $j : K \longrightarrow K_{\mathbf{R}}$, $x \longmapsto (x\tau)_\tau$, ist eine Teilmenge von $N := \{(z_\tau)_\tau \in K_{\mathbf{R}} \mid |z_\tau| = 1 \text{ stets}\}$. Nun ist N kompakt und $j(\mathbf{Z}_K)$ diskret (als Gitter), mithin $N \cap j(\mathbf{Z}_K)$ endlich, und somit erst recht $j(M \cap \mathbf{Z}_K) = j(M) \cap j(\mathbf{Z}_K)$ endlich, was schließlich $M \cap \mathbf{Z}_K$ endlich zur Folge hat.

Ist u eine Einheit in $\mathbf{Z}[\zeta_5]$, und ist $\mathbf{Q}(\zeta_5)$ via $\zeta_5 \longmapsto \exp(2\pi i/5)$ nach $\mathbf{C}$ eingebettet, so hat $u/\bar{u}$ den Betrag 1, ist also mit dem Lemma eine Einheit endlicher Ordnung. Mit Dirichlet ist die Einheitengruppe von $\mathbf{Z}[\zeta_5]$ isomorph zu $C_5 \times \mathbf{Z}$, so daß die Einheiten endlicher Ordnung gerade durch Elemente der Form $\pm\zeta_5^m$ mit $m \in \mathbf{Z}$ gegeben sind. Somit finden wir $u/\bar{u} = \varepsilon\zeta_5^m$ mit $\varepsilon \in \{-1, +1\}$. Ist $2k \equiv_5 -m$, so wird $v := \zeta_5^k u = \varepsilon\zeta_5^{m+k}\bar{u} = \varepsilon\overline{\zeta_5^k u}$.

Angenommen, es sei $\varepsilon = -1$. Aus $v = -\bar{v}$ schließen wir, daß wir $v = a(\zeta_5 - \zeta_5^{-1}) + b(\zeta_5^2 - \zeta_5^{-2})$ mit $a, b \in \mathbf{Z}$ schreiben können. Dieses Element ist aber teilbar durch $(\zeta_5 - \zeta_5^{-1})$, was wegen $\mathrm{N}_{\mathbf{Q}(\zeta_5)|\mathbf{Q}}(\zeta_5 - \zeta_5^{-1}) = 5$ keine Einheit ist. Widerspruch.

Beachte, daß $\zeta_5 + \zeta_5^{-1} = -(1+\zeta_5^2+\zeta_5^3) = (-1+\sqrt{5})/2$. Es ist $\mathbf{Q}(\zeta_5)^+ := \mathbf{Q}(\zeta_5+\zeta_5^{-1})$ der Fixkörper unter komplexer Konjugation in $\mathbf{Q}(\zeta_5)$, i.e. $\mathbf{Q}(\zeta_5)^+ = \mathbf{R}\cap\mathbf{Q}(\zeta_5)$, und es ist $\mathbf{Z}_{\mathbf{Q}(\zeta_5)^+} = \mathbf{Z}[\zeta_5+\zeta_5^{-1}] = \mathbf{Z}[(1+\sqrt{5})/2]$.

Damit ist $v \in \mathbf{Q}(\zeta_5)^+$, und mit obiger Überlegung folgt, daß $v = \pm((1+\sqrt{5})/2)^m = \pm(-\zeta_5^2 - \zeta_5^{-2})^m$ für ein $m \in \mathbf{Z}$. Insgesamt wird die Einheitengruppe zu

$$\mathbf{Z}[\zeta_5]^* \;=\; \langle \zeta_5,\, 1+\zeta_5 \rangle \;.$$

Beachte, daß wir Dirichlet für $\mathbf{Q}(\zeta_5)^+$ verwendet haben (zwei reelle Einbettungen), das Ergebnis aber auch den Voraussagen von Dirichlet für $\mathbf{Q}(\zeta_5)$ entspricht (zwei Paare echt komplexer Einbettungen). Weiterführende Literatur: Washington, Introduction to Cyclotomic Fields. Die Einheitengruppe von $\mathbf{Z}[\zeta_p]$ für p prim ist im allgemeinen unbekannt (dito die Klassengruppe).

$\mathbf{Z}[\sqrt[3]{2}]$. Wir schreiben $\theta := \sqrt[3]{2}$. Seien $a, b, c \in \mathbf{Z}$, sei $\xi = a + b\theta + c\theta^2$. Wir haben

$$\mathrm{N}_{\mathbf{Q}(\theta)|\mathbf{Q}}(\xi) \;=\; a^3 + 2b^3 + 4c^3 - 6abc \;.$$

Ist $\xi > 0$, so ist auch $\mathrm{N}_{\mathbf{Q}(\theta)|\mathbf{Q}}(\xi) = \xi(\xi\tau)\overline{(\xi\tau)} > 0$, wobei $\mathbf{Q}(\theta) \xhookrightarrow{\tau} \mathbf{C}$ eine echt komplexe Einbettung sei.

Ist ξ eine Einheit, so ist mithin $\mathrm{N}_{\mathbf{Q}(\theta)|\mathbf{Q}}(\xi) = 1$. Nach Dirichlet ist die Einheitengruppe von $\mathbf{Z}[\theta]$ von der Form $\langle -1, \xi \rangle$, wobei ξ eine Untergruppe isomorph zu $\mathbf{Z}$ erzeugt (cf. Lösung 1, Aufgabe 4 (c)). Insbesondere ist $\xi^{-1} = \mathrm{N}_{\mathbf{Q}(\theta)|\mathbf{Q}}(\xi)/\xi = (a^2 - 2bc) + (c^2 - ba)\theta + (b^2 - ca)\theta^2$.

Wir dürfen noch $\xi > 1$ annehmen. Dies hat dann $0 < \xi^{-1} < 1$ zur Folge.

Wir *behaupten,* daß $\xi > 1$ impliziert, daß $a > 0$, $b > 0$ und $c > 0$.

Annahme $a > 0$, $b > 0$ und $c \leq 0$. Wegen $a^2 - 2bc > 0$ und $b^2 - ca > 0$ muß wegen $\xi^{-1} < 1$ notwendig $c^2 - ba < 0$ sein. Wir erhalten

$$1 \;=\; \mathrm{N}_{\mathbf{Q}(\theta)|\mathbf{Q}}(\xi) \;=\; (a^3 - 2abc) + (4c^3 - 4abc) + 2b^3 \;\geq\; 3 \;,$$

Widerspruch.

Annahme $a > 0$, $b \leq 0$ und $c > 0$. Wegen $a^2 - 2bc > 0$ und $c^2 - ba > 0$ muß wegen $\xi^{-1} < 1$ notwendig $b^2 - ca < 0$ sein. Wir erhalten

$$1 \;=\; \mathrm{N}_{\mathbf{Q}(\theta)|\mathbf{Q}}(\xi) \;=\; (a^3 - 2abc) + (2b^3 - 2abc) + (2c^3 - 2abc) + 2c^3 \;\geq\; 4 \;,$$

Widerspruch.

Annahme $a > 0$, $b \leq 0$ und $c \leq 0$. Wegen $c^2 - ba \geq 0$ und $b^2 - ca \geq 0$ muß wegen $\xi^{-1} < 1$ notwendig $a^2 - 2bc \leq 0$ sein. Wir erhalten

$$1 \;=\; \mathrm{N}_{\mathbf{Q}(\theta)|\mathbf{Q}}(\xi) \;=\; (a^3 - 2abc) + (2b^3 - 2abc) + (2c^3 - 2abc) + 2c^3 \;\leq\; 0 \;,$$

Widerspruch.

Annahme $a \leq 0$, $b > 0$ und $c > 0$. Wegen $c^2 - ba > 0$ und $b^2 - ca > 0$ muß wegen $\xi^{-1} < 1$ notwendig $a^2 - 2bc < 0$ sein. Wir erhalten

$$1 \;=\; \mathrm{N}_{\mathbf{Q}(\theta)|\mathbf{Q}}(\xi) \;=\; (a^3 - 2abc) + (2b^3 - 2abc) + (2c^3 - 2abc) + 2c^3 \;\geq\; 6 \;,$$

Widerspruch.

Annahme $a \leq 0$, $b > 0$ und $c \leq 0$. Wegen $a^2 - 2bc \geq 0$ und $c^2 - ba \geq 0$ muß wegen $\xi^{-1} < 1$ notwendig $b^2 - ca \leq 0$ sein. Wir erhalten

$$1 \;=\; \mathrm{N}_{\mathbf{Q}(\theta)|\mathbf{Q}}(\xi) \;=\; (a^3 - 2abc) + (2b^3 - 2abc) + (2c^3 - 2abc) + 2c^3 \;\leq\; 0 \;,$$

Widerspruch.

Annahme $a \leq 0$, $b \leq 0$ und $c > 0$. Wegen $a^2 - 2bc \geq 0$ und $b^2 - ca \geq 0$ muß wegen $\xi^{-1} < 1$ notwendig $c^2 - ba \leq 0$ sein. Wir erhalten

$$1 \;=\; \mathrm{N}_{\mathbf{Q}(\theta)|\mathbf{Q}}(\xi) \;=\; (a^3 - 2abc) + (4c^3 - 4abc) + 2b^3 \;\leq\; 0\,,$$

Widerspruch.

Annahme $a \leq 0$, $b \leq 0$ und $c \leq 0$. Dann wäre $1 < \xi \leq 0$. Widerspruch.

Damit ist die Behauptung gezeigt.

Daher ist $\xi = 1 + \theta + \theta^2$, da θ, $1 + \theta$, θ^2, $1 + \theta^2$, $\theta + \theta^2$ die jeweilige Norm 2, 3, 4, 5 resp. 6 haben, und somit keine Einheiten sind. Das Ergebnis lautet

$$\mathbf{Z}[\theta]^* \;=\; \langle -1,\, 1 + \sqrt[3]{2} + \sqrt[3]{4} \rangle\;.$$

Einige Einheiten.

$$\begin{array}{rcrcrcr}
\xi^{-4} & = & (-7) & + & (-2)\theta & + & 6\theta^2 \\
\xi^{-3} & = & 1 & + & 3\theta & + & (-3)\theta^2 \\
\xi^{-2} & = & 1 & + & (-2)\theta & + & 1\theta^2 \\
\xi^{-1} & = & (-1) & + & 1\theta & + & 0\theta^2 \\
\xi^{0} & = & 1 & + & 0\theta & + & 0\theta^2 \\
\xi^{1} & = & 1 & + & 1\theta & + & 1\theta^2 \\
\xi^{2} & = & 5 & + & 4\theta & + & 3\theta^2 \\
\xi^{3} & = & 19 & + & 15\theta & + & 12\theta^2 \\
\xi^{4} & = & 73 & + & 58\theta & + & 46\theta^2 \\
\xi^{5} & = & 281 & + & 223\theta & + & 177\theta^2 \\
\xi^{6} & = & 1081 & + & 858\theta & + & 681\theta^2
\end{array}$$

Beachte, daß man auf diese Weise *alle* Lösungen von

$$a^3 + 2b^3 + 4c^3 \;=\; 1 + 6abc$$

in den ganzen Zahlen erhält.