Satz

1.) $\alpha \in \mathcal{O}_K \Rightarrow N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z} \wedge Tr_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$

2.) $N_{K/\mathbb{Q}}(x \cdot y) = N_{K/\mathbb{Q}}(x) \cdot N_{K/\mathbb{Q}}(y)$

Aufgabe 1

1. Zeigen oder widerlegen Sie, dass $(\sqrt[3]{13} + e^{[illegible]} + 17i(\frac{1+\sqrt{17}}{2}))$ eine ganzalgebraische Zahl (über $\mathbb{Z}$) ist.
2. Sei $K := \mathbb{Q}(\sqrt[3]{7})$ und $\alpha = 1 + \sqrt[3]{7} - \sqrt[3]{7}^2$. Berechnen Sie Norm und Spur von α.
3. Sei K ein algebraischer Zahlkörper und $\alpha \in \mathcal{O}_K$. Zeigen Sie, dass α genau dann eine Einheit in $\mathcal{O}_K$ ist, wenn $N_{K/\mathbb{Q}}(\alpha) = \pm 1$ ist.

Satz

$\alpha \in \mathcal{O}_K \Leftrightarrow \underset{\uparrow}{\Pi_{\alpha,\mathbb{Q}}} \in \mathbb{Z}[X]$

(d.h. α ganz) Minimalpolynom von α

3.)

„$\Rightarrow$"

Sei also $\alpha \in \mathcal{O}_K^\times$.

Zu zeigen: $N_{K/\mathbb{Q}}(\alpha) \in \{\pm 1\}$

Da $\alpha \in \mathcal{O}_K^\times$, so finden wir $\beta \in \mathcal{O}_K$ mit $\alpha \cdot \beta = 1$.

$$1 = N(1) = N(\alpha \cdot \beta) = \underbrace{N(\underset{\in \mathcal{O}_K}{\alpha})}_{\in \mathbb{Z}} \cdot \underbrace{N(\underset{\in \mathcal{O}_K}{\beta})}_{\in \mathbb{Z}}$$

$\Rightarrow \underline{\underline{N(\alpha) \in \{\pm 1\}}}$

„$\Leftarrow$"

zu 1.1) Noch zu zeigen: $\frac{1+\sqrt{17}}{2} \overset{!}{\in} \mathcal{O}_K$

$$\alpha = \frac{1+\sqrt{17}}{2} \quad | \cdot 2$$

$$2\alpha = 1 + \sqrt{17} \quad | -1$$

$$2\alpha - 1 = \sqrt{17} \quad | (\;)^2$$

$$4\alpha^2 - 4\alpha + 1 = 17$$

$$4\alpha^2 - 4\alpha - 16 = 0 \quad | : 4$$

$$\alpha^2 - \alpha - 4 = 0$$

$$\Pi_{\alpha,\mathbb{Q}} = X^2 - X - 4 \in \mathbb{Z}[X] \Rightarrow \alpha \in \mathcal{O}_K$$

Aufgabe 4

1. Sei K ein algebraischer Zahlkörper und $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ eine Basis von $K/\mathbb{Q}$, deren Elemente alle ganz sind. Zeigen Sie: Falls die Diskriminante $d(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$ quadratfrei ist, so ist $\alpha_1, \ldots, \alpha_n$ eine Ganzheitsbasis von $K/\mathbb{Q}$.

2. Sei $K = \mathbb{Q}(\alpha)$, wobei $\alpha^3 - \alpha - 1 = 0$ gelte. Bestimmen Sie eine Ganzheitsbasis von $\mathcal{O}_K$ über $\mathbb{Z}$.

3. Bestimmen Sie die Primidealfaktorisierungen der von den Primzahlen 2, 5, sowie 23 erzeugten Ideale in $\mathcal{O}_K$ (inkl. der Erzeuger der Ideale).

$$\alpha^2 \cdot \alpha^2 = \alpha^4 = \alpha^3 \cdot \alpha = (\alpha+1)\cdot\alpha = \alpha^2 + \alpha$$

zu 2) $(1, \alpha, \alpha^2)$ ist Basis von $\underbrace{\mathbb{Q}(\alpha)}_{= K}$ als $\mathbb{Q}$-Vektorraum, $1 \in \mathcal{O}_K$, $\alpha \in \mathcal{O}_K$, $\alpha^2 \in \mathcal{O}_K$

$$\mu_{\alpha,\mathbb{Q}} = X^3 - X - 1$$

$$d(1, \alpha, \alpha^2) = \det \begin{pmatrix} \mathrm{Tr}(1\cdot 1) & \mathrm{Tr}(1\cdot\alpha) & \mathrm{Tr}(1\cdot\alpha^2) \\ \mathrm{Tr} & \mathrm{Tr}(\alpha\alpha) & \mathrm{Tr}(\alpha\alpha^2) = \mathrm{Tr}(\alpha+1) \\ & & \mathrm{Tr}(\alpha^2\cdot\alpha^2) = \mathrm{Tr}(\alpha^2+\alpha) \end{pmatrix} = \det\begin{pmatrix} 3 & & \\ & & \\ & & \end{pmatrix}$$

$$\det \begin{array}{c|c} & \begin{array}{ccc} 1 & \alpha & \alpha^2 \end{array} \\ \hline & \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{array}{c} 1 \\ \alpha \\ \alpha^2 \end{array} \end{array} \qquad \det \begin{array}{c} \begin{array}{ccc} 1 & \alpha & \alpha^2 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \begin{array}{c} 1 \\ \alpha \\ \alpha^2 \end{array} \end{array}$$

$$\det \begin{array}{c} \begin{array}{ccc} 1 & \alpha & \alpha^2 \end{array} \\ \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \begin{array}{c} 1 \\ \alpha \\ \alpha^2 \end{array} \end{array} \qquad \det \begin{array}{c} \begin{array}{ccc} 1 & \alpha & \alpha^2 \end{array} \\ \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix} \begin{array}{c} 1 \\ \alpha \\ \alpha^2 \end{array} \end{array}$$

$$\alpha^2\cdot(\alpha+1) = \alpha^3 + \alpha^2 = \alpha + 1 + \alpha^2$$

$$= \det \begin{pmatrix} 3 & 0 & 2 \\ 0 & 2 & 3 \\ 2 & 3 & 2 \end{pmatrix} \begin{matrix} 3 & 0 \\ 0 & 2 \\ 2 & 3 \end{matrix}$$

$$= (12 + 0 + 0) - (8 + 27 + 0)$$

$$= -23 \text{ ist quadratfrei!}$$

$$\alpha\cdot(\alpha^2+\alpha) = \alpha^3 + \alpha^2 = \alpha + 1 + \alpha^2$$

$\Longrightarrow$ $1, \alpha, \alpha^2$ ist Ganzheitsbasis

Teilaufgabe a)

$$\mathcal{O}_K = \mathbb{Z}[\alpha] = \{ a + b\cdot\alpha \mid a, b \in \mathbb{Z} \}$$

$= \alpha + 2\alpha$

2. Sei $K = \mathbb{Q}(\alpha)$, wobei $\alpha^3 - \alpha - 1 = 0$ gelte. Bestimmen Sie eine Ganzheitsbasis von $\mathcal{O}_K$ über $\mathbb{Z}$.

3. Bestimmen Sie die Primidealfaktorisierungen der von den Primzahlen 2, 5 sowie 23 erzeugten Ideale in $\mathcal{O}_K$ (inkl. der Erzeuger der Ideale).

Proposition 6.10. Soient $\alpha \in \bar{\mathbb{Z}}$, $A = \mathbb{Z}[\alpha]$, p un nombre premier et $\bar{P} = \Pi_{\alpha,\mathbb{Q}} \in (\mathbb{Z}/p\mathbb{Z})[X]$ la réduction modulo p du polynôme minimal de α sur $\mathbb{Q}$.

(i) Si $Q \in (\mathbb{Z}/p\mathbb{Z})[X]$ est un diviseur de $\bar{P}$, et si $\tilde{Q} \in \mathbb{Z}[X]$ est un polynôme tel que $\tilde{Q} \bmod p = Q$, alors $I(Q) := pA + \tilde{Q}(\alpha)A$ est un idéal de A contenant p qui ne dépend pas du choix de $\tilde{Q}$.

(ii) L'application $Q \mapsto I(Q)$ est une bijection entre facteurs unitaires de $\bar{P}$ et idéaux de A contenant p ; elle satisfait $Q|Q' \Leftrightarrow I(Q') \subset I(Q)$.

(iii) L'anneau $A/I(Q)$ est isomorphe à $(\mathbb{Z}/p\mathbb{Z})[X]/(Q)$. En particulier, on a

$$|A/I(Q)| = p^{\deg(Q)}.$$

Ce résultat jouera un rôle important dans les applications. Considérons par exemple $\alpha = \sqrt{-5}$, de sorte que $\Pi_{\alpha,\mathbb{Q}} = X^2 + 5$, et cherchons les idéaux de $A = \mathbb{Z}[\alpha]$ contenant 2. On a $X^2 + 5 = (X+1)^2 \bmod 2$, les idéaux de $\mathbb{Z}[\alpha]$ contenant 2 sont donc $2A$, $2A + (\alpha+1)A$ et A. De même, comme $X^2 + 5 = (X-1)(X+1) \bmod 3$, les idéaux de A contenant 3 sont $3A$, A, $3A + (\alpha-1)A$ et $3A + (\alpha+1)A$. Enfin, si -5 n'est pas un carré modulo p, les idéaux de A contenant p sont simplement A et pA.

3.) $\mathcal{O}_K = \mathbb{Z}[\alpha]$

$X^3 - X - 1 \in \mathbb{Z}/2\mathbb{Z}[X]$

$= X^3 + X + 1$

$1^3 + 1 + 1 = 1 \neq 0$

$0^3 + 0 + 1 = 1 \neq 0$

Prop. 6.10 i) $\Rightarrow$ (2) ist einziges Ideal, was 2 enthält

Ergebnis:

$(2) = (2)$

ist die Primidealfaktorisierung von 2, da 2 schon selbst ein Primideal ist

$X^3 - X - 1 \in \mathbb{Z}/5\mathbb{Z}[X]$

$= X^3 + 4X + 4 = p(X)$

$= (X-2)(X^2 + 2X + 3)$

$p(0) = 4 \neq 0$

$p(1) = 4 \neq 0$

$p(2) = 8 + 8 + 4 = 20 = 0$

$p(3) = 27 + 12 + 4 \neq 0$

$p(4) = (-1)^3 + (-4) + 4 = -1 \neq 0$

$(X^3 + 4X + 4) : (X - 2) = X^2 + 2X + 3$

$-(X^3 - 2X^2)$

$2X^2 + 4X + 4$

$-(2X^2 - 4X)$

$3X + 4$

$-(3X - 6)$

$10 = 0$

Prop. 6.10 i $\Rightarrow$ Alle Ideale, die 5 enthalten sind

(5), $\underbrace{(5, \alpha - 2)}_{= \mathfrak{I}_1}$, $\underbrace{(5, \alpha^2 + 2\alpha + 3)}_{= \mathfrak{I}_2}$

Optionen:

$\mathfrak{I}_1^2 = (5)$ oder

$\mathfrak{I}_2^2 = (5)$ oder

$\mathfrak{I}_1 \cdot \mathfrak{I}_2 = (5)$

Wir zeigen:

$\mathfrak{I}_1^2 = (5)$

"$\subseteq$" ist klar

$(X-3)(X^2 + 3X + 8) = Q(X)$

$X^3 - X - 1 \in \mathbb{Z}/23\mathbb{Z}[X]$

$= p(X)$

$p(0) \neq 0$

$p(1) \neq 0$

$p(2) \neq 0$

$p(3) = 27 - 3 - 1 = 23 = 0$

$(X^3 - X - 1) : (X - 3) = X^2 + 3X + 8$

$-(X^3 - 3X^2)$

$3X^2 - X - 1$

$-(3X^2 - 9X)$

$8X - 1$

$-(8X - 24)$

$23 = 0$

$46 = 0$

$p(22) =$

$Q(0) \neq 0$

$Q(1) \neq 0$

$Q(2) \neq 0$

$Q(3) \neq 0$

$Q(4) \neq 0$

$Q(5) \neq 0$

$Q(6) \neq 0$

$Q(7) =$

Prop. 6.10 $\Rightarrow$ Einzige Ideale, die 23 enthalten sind

(23), $\underbrace{(23, \alpha - 3)}_{= \mathfrak{I}_1}$ und $\underbrace{(23, \alpha^2 + 3\alpha + 8)}_{= \mathfrak{I}_2}$

Ergebnis:

$(23) = \mathfrak{I}_1^2$ oder

$(23) = \mathfrak{I}_1 \cdot \mathfrak{I}_2$

oder

$(23) = \mathfrak{I}_2^2$

Blatt 4

$\Pi_{\sqrt{-5},\mathbb{Q}} = X^2 + 5 = X^2 - 1 = (X+1)(X-1) = (X+1)^2 \in \mathbb{Z}/2\mathbb{Z}$

$\overset{6.10}{\Rightarrow}$ Alle Ideale, die 2 enthalten, sind

(2), $(2, \sqrt{-5} + 1)$

Aufgabe 3 (10 Punkte)

Sei $K = \mathbb{Q}(\sqrt{-5})$ mit Ganzheitsring $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Wir wissen, dass $\mathcal{O}_K$ nicht faktoriell ist, da zum Beispiel $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ zeigt, dass wir zwei verschiedene nicht äquivalente Zerlegungen von 6 als Produkt irreduzibler Elemente haben.

Zeigen Sie, dass $(2) = \mathfrak{p}_1^2$, $(3) = \mathfrak{p}_2\mathfrak{p}_3$, $(1 + \sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_2$, $(1 - \sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_3$ mit den Idealen $\mathfrak{p}_1 = (2, 1 + \sqrt{-5})$, $\mathfrak{p}_2 = (3, 1 + \sqrt{-5})$, $\mathfrak{p}_3 = (3, 1 - \sqrt{-5})$ gilt.