ALG Üg

326) Sei D eine ganze Zahl und $R := \mathbb{Z}[\sqrt{D}]$ der von $\mathbb{Z}$ und $\sqrt{D}$ erzeugte Unterring von $\mathbb{C}$.

1) Man zeige, dass R mit der gewöhnlichen Addition und Multiplikation von $\mathbb{C}$ einen Integritätsbereich bildet.

2) Man bestimme für $D<0$ die Einheiten von R

3) Man zeige, dass für $D=2$ unendlich viele Einheiten in $\mathbb{Z}[\sqrt{D}] \subseteq R$ existieren.

Hinweis: Übersetzen Sie die Eigenschaft "z ist Einheit" in eine Eigenschaft von $N(z)$, siehe 5.1.3.1.(4)

Integritätsbereich ... nullteilerfreier, kommutativer Ring mit 1

Einheit ... $x \in R$ mit $x^{-1} \in R$ existiert

N ... Normfunktion $N: \mathbb{Z}[\sqrt{D}] \to \mathbb{Z}$, $a+b\sqrt{D} \mapsto (a+b\sqrt{D})(a-b\sqrt{D}) = a^2-b^2D$
wobei $D \neq 1$ eine Zahl mit $t^2 | D \Rightarrow t \in \{1,-1\}$

---

1) $R \subseteq \mathbb{C}$ ist klarerweise unter $+, 0, -, 1$ abgeschlossen. Sei $a+b\sqrt{D}, c+d\sqrt{D} \in R$ bel.

$(a+b\sqrt{D})(c+d\sqrt{D}) = (ac+bdD)+(ad+bc)\sqrt{D} \in R \Rightarrow (R,+,0,-,\cdot,1)$ ... Ring mit 1

Als Unterring von $\mathbb{C}$ ist auch R kommutativ und nullteilerfrei.

2) Sei $D<0$ bel. Sei $x = a+b\sqrt{D} \in R\setminus\{0\} \subseteq \mathbb{C}$ bel. Falls $x \in E(R)$ gilt

$N(x)\cdot N(x^{-1}) = N(1) = 1 \Rightarrow N(x^{-1}) = N(x)^{-1} \in \mathbb{N}^{\times}$ und $N(x) \in \mathbb{N}^{\times} \Rightarrow N(x) = 1$

Falls $N(x)=1$ gilt $a^2-b^2D=1$ und somit ist $\frac{a-b\sqrt{D}}{a^2-b^2D} = a-b\sqrt{D} \in R$ das inverse Element. $\Rightarrow x \in E(R)$

$\Rightarrow E(R) = \{x \in R \mid N(x) = 1\}$

3) $D=2$ $\quad x = a+b\sqrt{2} \in R\setminus\{0\}$ $\quad$ ges a,b mit $N(a+b\sqrt{2}) = a^2-2b^2 = 1$

Behauptung: $a_1 = 3$ $\quad b_1 = 2$ und $a_n = 3a_{n-1}+4b_{n-1}$ $\quad b_n = 2a_{n-1}+3b_{n-1}$

$\Rightarrow \forall n \in \mathbb{N}: a_n^2+2b_n^2 = 1$ vollständige Induktion nach n: $n=1$ $\quad 3^2-2\cdot 2^2 = 1$ ✓

$n+1$ $\quad (a_{n+1})^2-2(b_{n+1})^2 = (3a_n+4b_n)^2-2(2a_n+3b_n)^2 =$

$= 9a_n^2+24a_nb_n+16b_n^2-2(4a_n^2+12a_nb_n+9b_n^2) = a_n^2-2b_n^2 = 1$ ✓

$\Rightarrow (a+b\sqrt{2})\frac{a-b\sqrt{2}}{a^2-2b^2} = 1$ $\quad$ und $\quad \frac{a-b\sqrt{2}}{a^2-2b^2} = a-b\sqrt{2} \in R$

$\Rightarrow a+b\sqrt{2} \in E(R)$

ALG Ü9

330) Sei $R = \mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$

1) Zeigen Sie, dass die Elemente 2 und 3 in R irreduzibel aber nicht prim sind.

2) Finden Sie eine Primzahl $p \in \mathbb{Z}$, die im Ring $\mathbb{Z}[\sqrt{-5}]$ nicht irreduzibel ist.

Hinweis: Verwenden Sie die Normfunktion N aus 5.1.3. und zeigen Sie, dass genau jene $x \in R$ Einheiten sind, die $N(x) = 1$ erfüllen.

---

irreduzibel ... $p = a \cdot b \Rightarrow p \mid a \vee p \mid b \iff p = a \cdot b \Rightarrow a \in E(R) \vee b \in E(R)$

prim ... $p \mid a \cdot b \Rightarrow p \mid a \vee p \mid b$

---

1) Sei $x, y \in R$ mit $x \cdot y = 2$ bel. $\Rightarrow N(x) \cdot N(y) = N(2) = 4$

1. Fall $(N(x) = 1 \wedge N(y) = 4)$ oder $(N(x) = 4 \wedge N(y) = 1) \Rightarrow x \in E(R) \vee y \in E(R)$

2. Fall $N(x) = 2 \wedge N(y) = 2$

Damit $N(a + b\sqrt{-5}) = 2$ muss $a^2 + 5b^2 = 2$ was keine Lösung in $\mathbb{Z}$ hat $\lightning$

Sei $x, y \in R$ mit $x \cdot y = 3$ bel. $\Rightarrow N(x) \cdot N(y) = N(3) = 9$

1. Fall $(N(x) = 1 \wedge N(y) = 9)$ oder $(N(x) = 9 \wedge N(y) = 1) \Rightarrow x \in E(R) \vee y \in E(R)$

2. Fall $N(x) = 3 = N(y)$

Damit $N(a + b\sqrt{-5}) = 3$ muss $a^2 + 5b^2 = 3$ was keine Lsg in $\mathbb{Z}$ hat $\lightning$

$\Rightarrow$ 2, 3 sind irreduzibel in R

$\neg(2 \mid 1 + \sqrt{-5})$ aber $2 \mid (1 + \sqrt{-5})^2 = (1 + 2\sqrt{-5} - 5) = -4 + 2\sqrt{-5}$

$\neg(3 \mid 1 + \sqrt{-5}) \wedge \neg(3 \mid 2 + \sqrt{-5})$ aber $3 \mid (1 + \sqrt{-5})(2 + \sqrt{-5}) = -3 + 3\sqrt{-5}$

$\Rightarrow$ 2, 3 sind nicht prim in R

2) 5 ist prim in $\mathbb{Z}$ aber $5 = (-\sqrt{-5})(\sqrt{-5})$ und $N(-\sqrt{-5}) = N(\sqrt{-5}) = 5$

$\Rightarrow$ 5 ist nicht irreduzibel in R

ALG Ü9

332) Zeigen Sie, dass in $\mathbb{Z}[\sqrt{-5}]$ die Teilerkettenbedingung gilt.

Teilerkettenbedingung .. es gibt keine unendliche absteigende Folge echter Teiler

$\Leftrightarrow \forall (r_n)_{n\in\mathbb{N}}$ in R mit $\forall n\in\mathbb{N}: r_{n+1} | r_n \quad \exists n_0 \in \mathbb{N}: r_{n_0+1} \sim r_{n_0}$

$\Leftrightarrow \forall (r_n)_{n\in\mathbb{N}}$ in R mit $\forall n\in\mathbb{N}: r_{n+1} | r_n \quad \exists n_0 \in \mathbb{N}: \forall n \geq n_0: r_{n+1} \sim r_n$

Sei $(r_n)_{n\in\mathbb{N}}$ eine Folge in R mit $\forall n\in\mathbb{N}: r_{n+1} | r_n$ bel.

$\Rightarrow \forall n\in\mathbb{N} \ \exists s_n: \ s_n \cdot r_{n+1} = r_n \qquad \Rightarrow N(s_n)\cdot N(r_{n+1}) = N(r_n)$

Da $\forall a+b\sqrt{-5} \in R: \ N(a+b\sqrt{-5}) = a^2+5b^2 \in \mathbb{N}$ und in $\mathbb{N}$ die Teilerkettenbedingung gilt muss $N(s_{n_0}) = 1$ für ein $n_0 \in \mathbb{N}$

$\Rightarrow s_{n_0} \in E(R)$ (siehe Bsp 326)

$\Rightarrow r_{n_0+1} \sim r_{n_0}$

$\Rightarrow R$ erfüllt die Teilerkettenbedingung.

$\square$

ALG Ü9

2010) $\mathcal{V}$.. Varietät mit $\exists X \in \mathcal{V}: |X| \geq 2$ $F_i \in \mathcal{V}$ .. frei über (B_i, ι_i) $i=1,2$ $B_1 \cap B_2 = \emptyset$

(F, j_1, j_2) .. Koprodukt von F_1 und F_2

zz: a) $(j_1 \circ \iota_1)(B_1) \cap (j_2 \circ \iota_2)(B_2) = \emptyset$

Angenommen $\exists a \in (j_1 \circ \iota_1)(B_1) \cap (j_2 \circ \iota_2)(B_2) \neq \emptyset$

Sei $X \in \mathcal{V}$ mit $x_1, x_2 \in X$, $x_1 \neq x_2$ bel.

$$
\begin{tikzcd}
B_1 \arrow[r, "\iota_1"] \arrow[drr, bend right, "f_1"'] & F_1 \arrow[r, "j_1"] \arrow[dr, "g_1"] \arrow[dr, dashed, shift right=2, "\varphi_1"'] & F \arrow[d, dashed, "\varphi"] & F_2 \arrow[l, "j_2"'] \arrow[dl, "g_2"'] \arrow[dl, dashed, shift left=2, "\varphi_2"] & B_2 \arrow[l, "\iota_2"'] \arrow[dll, bend left, "f_2"] \\
 & & X & &
\end{tikzcd}
$$

$\forall X \, \forall f_1 \, \exists! \varphi_1$ $\forall X \, \forall f_2 \, \exists! \varphi_2$

$\forall X \, \forall g_1, g_2 \, \exists! \varphi$

$f_1: B_1 \to X$, $b \mapsto x_1$

$f_2: B_2 \to X$, $b \mapsto x_2$

$\Rightarrow \exists! \varphi_1: F_1 \to X$ $\exists! \varphi_2: F_2 \to X$

$\varphi_1 \circ \iota_1 = f_1 \wedge \varphi_2 \circ \iota_2 = f_2$

$\Rightarrow \exists! \varphi: F \to X: \varphi_1 = \varphi \circ j_1 \wedge \varphi_2 = \varphi \circ j_2$

$\Rightarrow \varphi \circ j_1 \circ \iota_1 = f_1 \wedge \varphi \circ j_2 \circ \iota_2 = f_2$

$a_1 \in B_1$, $a_2 \in B_2$ mit $(j_1 \circ \iota_1)(a_1) = a = (j_2 \circ \iota_2)(a_2)$

$\Rightarrow f_1(a_1) = x_1 = \varphi((j_1 \circ \iota_1(a_1)) = \varphi(a)$; $f_2(a_2) = x_2 = \varphi(j_2 \circ \iota_2(a_2)) = \varphi(a)$

$\Rightarrow \varphi(a) = x_1 \neq x_2 = \varphi(a)$ ↯ $\Rightarrow (j_1 \circ \iota_1)(B_1) \cap (j_2 \circ \iota_2)(B_2) = \emptyset$

---

b) $B = B_1 \,\dot\cup\, B_2$ $\iota := (j_1 \circ \iota_1) \,\dot\cup\, (j_2 \circ \iota_2)$ $\Rightarrow F$ .. frei über (B, ι)

Sei $X \in \mathcal{V}$ bel. Sei $f: B \to X$ bel. $f_1 = f|_{B_1}$, $f_2 = f|_{B_2}$

$\Rightarrow \exists! \varphi_i: F_i \to X$ mit $f_i = \varphi_i \circ \iota_i$ $i=1,2$

$\Rightarrow \exists! \varphi: F \to X$ mit $\varphi_i = \varphi \circ j_i$ $i=1,2$

$\Rightarrow f_i = \varphi \circ j_i \circ \iota_i = \varphi \circ \iota$ $i=1,2$

$$
\begin{tikzcd}
B \arrow[r, "\iota"] \arrow[dr, "f"'] & F \arrow[d, dashed, "\varphi"] \\
 & X
\end{tikzcd}
\qquad
\begin{tikzcd}
B_i \arrow[r, "\iota_i"] \arrow[dr, "f_i"'] & F_i \arrow[d, dashed, "\varphi_i"] \\
 & X
\end{tikzcd}
$$

Also $\forall X \in \mathcal{V} \; \forall f: B \to X \; \exists! \varphi: F \to X: f = \varphi \circ \iota$

$\Rightarrow F$ ist frei über (B, ι)

$\square$

ALG Üg

2011) R... Integritätsbereich $q,r,s \in R^\times$ mit $q = rs$

zz: $r \in E(R) \Leftrightarrow q \sim s$

($\Rightarrow$) $r \in E(R) \Rightarrow \exists r^{-1} \Rightarrow r^{-1}q = s \Rightarrow q|s \wedge s|q \Rightarrow q \sim s$

($\Leftarrow$) $q \sim s \Rightarrow \exists x \in R: xq = s \Rightarrow rxq = rs = q \Rightarrow rx = 1 \Rightarrow x = r^{-1} \Rightarrow r \in E(R)$

$p \in R^\times$ zz: folgende Aussagen sind äquivalent

(1) $\forall a,b \in R: \; p = ab \Rightarrow a \sim 1 \vee b \sim 1$

(1') $\forall a,b \in R: \; p = ab \Rightarrow a|1 \vee b|1$ $\quad$ (1) $\Rightarrow$ (1') klar

(2) $\forall a,b \in R: \; p = ab \Rightarrow a \sim p \vee b \sim p$

(1') $\Rightarrow \exists x \in R: a x = 1 \vee \exists y \in R: by = 1 \Rightarrow a \in E(R) \vee b \in E(R)$

$\Rightarrow$ nach oben $a \sim p \vee b \sim p \Leftrightarrow$ (2)

(2') $\forall a,b \in R: p = ab \Rightarrow p|a \vee p|b$ $\quad$ (2) $\Rightarrow$ (2') klar

(2') $\Rightarrow \exists x,y \in R: \; px = a \vee py = b \Rightarrow abx = a \vee bay = b$

$\Rightarrow bx = 1 \vee ay = 1 \Rightarrow a|1 \vee b|1 \Rightarrow a \sim 1 \vee b \sim 1 \Leftrightarrow$ (1)

$\Rightarrow$ (1) $\Leftrightarrow$ (1') $\Leftrightarrow$ (2) $\Leftrightarrow$ (2')

(3) $\forall a,b \in R: p = ab \Rightarrow$ a... triviale Teiler $\vee$ b... triviale Teiler

a... triviale Teiler $\Leftrightarrow a \sim p \vee a \sim 1$

(3) $\Rightarrow$ (1) $\vee$ (2) $\quad$ (1) $\Rightarrow$ (3) $\quad$ ((2) $\Rightarrow$ (3))

$\square$