Algebra I

Musterlösung 11

Euklidische und faktorielle Ringe

Ein Integritätsring R heiss **euklidisch**, wenn eine Abbildung $\delta : R \setminus \{0\} \to \mathbb{N}$ existiert mit folgender Eigenschaft:

Für alle $a, b \in R$ mit $b \neq 0$ existieren $q, r \in R$, sodass $a = b \cdot q + r$ mit $r = 0$ oder $\delta(r) < \delta(b)$.

68. (a) Zeige: Jeder euklidische Ring ist Hauptidealring.

(b) Zeige: $\mathbb{Z}[i]$ und $\mathbb{Z}[i\sqrt{2}]$ sind euklidisch.

Lösung: (a) Sei R ein euklidischer Ring und sei $\mathfrak{a} \subseteq R$ ein Ideal, das nicht das Nullideal ist. Sei $a \in \mathfrak{a}$ ein Element mit $\delta(a) = \min\{\delta(b) : b \in \mathfrak{a}\}$. Dieses existiert, da $\delta[\mathfrak{a} \setminus \{0\}] \subseteq \mathbb{N}$ ist und jede nichtleere Teilmenge von $\mathbb{N}$ ein Minimum besitzt. Sei $b \in \mathfrak{a}$. Dann existieren $q, r \in R$ mit $b = qa + r$ und $\delta(r) < \delta(a)$ oder $r = 0$. Mit $a, b \in \mathfrak{a}$ folgt $r \in \mathfrak{a}$. Aus der Minimalitätseigenschaft von $\delta(a)$ folgt $r = 0$ und somit ist $b \in (a)$. Da b beliebig gewählt war, haben wir $\mathfrak{a} = (a)$ bewiesen.

(b) Sei $d \in \{i, i\sqrt{2}\}$. Sei $R = \mathbb{Z}[d]$. Sei

$$\delta\colon R \setminus \{0\} \to \mathbb{N},\ \delta(a + ib) = a^2 - d^2b^2.$$

Wir überprüfen, dass δ eine euklidische Normfunktion ist. Seien dafür $x, y \in R$ mit $y \neq 0$. Es existieren $a, b \in \mathbb{R}$, so dass $\frac{x}{y} = a + bdi$ gilt (in der Tat liegen a und b in $\mathbb{Q}$). Wähle $m, n \in \mathbb{Z}$ mit

$$|a - m| \leq \frac{1}{2} \quad \text{und} \quad |b - n| \leq \frac{1}{2}$$

und setze $q := m + ndi$ und $r := x - yq$. Nach Konstruktion haben wir

$$\left|\frac{x}{y} - q\right|^2 = (a - m)^2 - d^2(b - n)^2 \leq \left(\frac{1}{2}\right)^2 - d^2 \cdot \left(\frac{1}{2}\right)^2 < 1.$$

Somit ist $x = yq + r$ mit

$$\delta(r) = |x - yq|^2 = \delta(y) \cdot \left|\frac{x}{y} - q\right|^2 < \delta(y).$$

Also ist δ eine euklidische Normfunktion auf R und R ist ein euklidischer Ring.

69. (a) Verallgemeinere den euklidischen Algorithmus zur Berechnung des ggT zweier Zahlen aus $\mathbb{N}$ auf euklidische Ringe.

(b) Berechne einen ggT von $X^3 + X^2 + X - 3$ und $X^4 - X^3 + 3X^2 + X - 4$ in $\mathbb{Q}[X]$.

(c) Stelle den ggT aus (b) als Linearkombination (mit Koeffizienten aus $\mathbb{Q}[X]$) der beiden Polynome $X^3 + X^2 + X - 3$ und $X^4 - X^3 + 3X^2 + X - 4$ dar.

(d) Finde mit Hilfe des euklidischen Algorithmus den ggT der Polynome

$$-3XY + 3X^2Y + Y^2 - 4XY^2 + Y^3 \quad \text{und} \quad -2X + 2X^2 - Y - XY - Y^2$$

in $\mathbb{Z}[X, Y]$.

Lösung: Sei R ein euklidischer Ring und $\delta\colon R \setminus \{0\} \to \mathbb{N}$ die entsprechende Funktion. Seien $a, b \in R \setminus \{0\}$. Nimm an, dass o.B.d.A. $\delta(a) \geq \delta(b)$ gilt. Seien q, r mit $a = bq + r$ und $\delta(q) < \delta(r)$ oder $r = 0$. Ein Teiler von a und b muss dann auch r teilen. Ausserdem teilt ein gemeinsamer Teiler von b und r sicher auch a. Daher gilt $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, r)$. Falls $r = 0$ ist, so ist $\mathrm{ggT}(a, b) = b$. Anderenfalls können wir dieses Argument mit (b, r) anstelle von (a, b) wiederholen. Wegen $\delta(a) + \delta(b) > \delta(b) + \delta(r)$ terminiert der Prozess irgendwann.

(b) Mit Polynomdivision finden wir

$$\begin{aligned} X^4 - X^3 + 3X^2 + X - 4 &= (X^3 + X^2 + X - 3) \cdot (X - 2) + (4X^2 + 6X - 10) \\ X^3 + X^2 + X - 3 &= (4X^2 + 6X - 10) \cdot (\frac{1}{4}X - \frac{1}{8}) + (\frac{17}{4}X - \frac{17}{4}) \\ 4X^2 + 6X - 10 &= (\frac{17}{4}X - \frac{17}{4}) \cdot (\frac{16}{17}X + \frac{40}{17}) + 0. \end{aligned}$$

Wenn wir mit der Einheit $\frac{4}{17}$ multiplizieren, erhalten wir

$$\mathrm{ggT}(X^4 - X^3 + 3X^2 + X - 4, X^3 + X^2 + X - 3) = X - 1.$$

(c) Wie in Aufgabe 52(b) berechnen wir mit dem Schema

		$X-2$	$\frac{1}{4}X - \frac{1}{8}$	$\frac{16}{17}X + \frac{40}{17}$
0	1	$X-2$	$\frac{1}{4}X^2 - \frac{5}{8}X + \frac{5}{4}$	
1	0	1	$\frac{1}{4}X - \frac{1}{8}$	

die Darstellung

$$17X - 17 = (-X + \frac{1}{2}) \cdot (X^4 - X^3 + 3X^2 + X - 4) + (X^2 - \frac{5}{2}X + 5) \cdot (X^3 + X^2 + X - 3).$$

(d) Da Y teilerfremd zum zweiten Polynom und prim ist, können wir das erste Polynom durch Y dividieren und berechnen

$$\begin{aligned} & \mathrm{ggT}(-3XY + 3X^2Y + Y^2 - 4XY^2 + Y^3, -2X + 2X^2 - Y - XY - Y^2) \\ \overset{\text{div. durch } Y}{=} \; & \mathrm{ggT}(-3X + 3X^2 + Y - 4XY + Y^2, -2X + 2X^2 - Y - XY - Y^2) \\ \overset{\text{add.}}{=} \; & \mathrm{ggT}(-2X + 2X^2 - Y - XY - Y^2, -5X + 5X^2 - 5XY) \\ \overset{\text{div. durch } -5X}{=} \; & \mathrm{ggT}(-2X + 2X^2 - Y - XY - Y^2, 1 - X + Y) \\ \overset{\text{mult. mit } Y \text{ und add.}}{=} \; & \mathrm{ggT}(1 - X + Y, -2X + 2X^2 - 2XY) \\ \overset{\text{div. durch } -2X}{=} \; & \mathrm{ggT}(1 - X + Y, 1 - X + Y) \\ = \; & 1 - X + Y. \end{aligned}$$

70. Zeige: $X^3 - X$ hat 6 Nullstellen in $\mathbb{Z}/6\mathbb{Z}$.

Lösung: Die Zahlen $0^3 - 0, 2^3 - 2, 3^3 - 3, (-2)^2 - (-2), (-1)^3 - (-1)$ sind alle durch 6 teilbar, somit sind alle Elemente aus $\mathbb{Z}/6\mathbb{Z}$ Nullstellen des besagten Polynoms.

71. Zeige: In einem faktoriellen Ring ist jedes irreduzible Element ein Primelement.

Sei R ein faktorieller Ring und sei $r \in R$ irreduziblel. Seien $a, b \in R$ mit $r|ab$. Wir können $a = p_1 \dots p_n$ und $b = q_1 \dots q_m$ eindeutig als Prudukt von irreduziblen Elementen schreiben. Sei $c \in R$ mit $rc = ab$ und schreibe $c = s_1 \dots s_k$ als Prudukt von irreduziblen Elementen. Dann ist $rc = rs_1 \dots s_k$ eine Darstellung von ab als Produkt von irreduziblen Elementen. Wegen der Eindeutigkeit muss es ein Element $p \in \{p_1, \dots, p_n, q_1, \dots, q_m\}$ geben, sodass r und p assoziiert sind. Das impliziert $r|a$ oder $r|b$ und somit ist r prim.

72. Sei K ein Körper. Finde alle maximalen Ideale in $K[X]$.

Lösung: Der Ring $K[X]$ ist ein Hauptidealring. Jedes Ideal ist also von der Form (P) mit $P \in K[X]$. In einem Hauptidealring ist jedes Primideal, das nicht das Nullideal ist, maximal. Ausserdem sind die Primideale genau die Ideale, die von Primelementen erzeugt werden. Nach der vorigen Aufgabe sind die Primelemente genau die irreduziblen Polynome. Das Ideal (P) ist daher genau dann maximal, wenn P ein irreduzibles Polynom ist.

Aliter: Sei $P \in K[X]$ ein nicht konstantes irreduzibles Polynom. Nach dem Euklidischen Algorithmus existiert für jedes $Q \in K[X]$ ein eindeutiges $R \in K[X]$ mit $\deg(R) < \deg(Q)$ und $R + (f) = Q + (f)$. Da P irreduzibel ist, sind P und R teilerfremd und somit ist nach dem Euklidischen Algorithmus $1 \in (P) + (R)$. Also ist (P) ein maximales Ideal.

Sei andererseits $P = P_1P_2$ mit $\deg(P_1), \deg(P_2) \geq 1$ ein reduzibles Polynom. Dann ist $P_1, P_2 \notin (P)$, da alle Elemente aus (P) mindestens Grad $\deg(P)$ haben, aber $P_1P_2 \in (P)$. Also ist (P) nicht prim und somit auch nicht maximal.

Die maximalen Ideale in $K[X]$ sind somit genau die Hauptideale, die von irreduziblen Polynomen erzeugt werden.

73. Im Ring $R := \mathbb{Z}[i\sqrt{5}] \subset \mathbb{C}$ gilt die Gleichheit

$$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5}).$$

Zeige:

(a) Die Funktion $N\colon R \to \mathbb{N}, z = a + bi\sqrt{5} \mapsto |z|^2 = a^2 + 5b^2$ ist multiplikativ (das heisst, $\forall \alpha, \beta \in R : N(\alpha\beta) = N(\alpha)N(\beta)$).

(b) $R^* = \{u \in R \mid N(u) = 1\} = \{\pm 1\}$.

(c) Die Elemente $2, 3, 1 + i\sqrt{5}, 1 - i\sqrt{5}$ sind unzerlegbar in R.

(d) Die Elemente $2, 3, 1 + i\sqrt{5}, 1 - i\sqrt{5}$ sind keine Primelemente in R.

(e) Für das Ideal $I = (2, 1 + i\sqrt{5})$ gilt $I \cdot I = (2)$.

(f) I ist kein Hauptideal von R.

(g) I ist ein maximales Ideal von R.

(h) Kein anderes Primideal enthält die Zahl 2.

(i) R ist nicht faktoriell.

Lösung: (a) Für alle $\alpha \in R$ gilt $N(\alpha) = |\alpha|^2$, wobei $|\cdot|$ den gewöhnlichen komplexen Absolutbetrag bezeichnet. Für alle $\alpha, \beta \in R$ folgt daraus

$$N(\alpha\beta) = |\alpha\beta|^2 = |\alpha|^2|\beta|^2 = N(\alpha)N(\beta),$$

wie gewünscht.

Variante: Seien $\alpha = a_1 + a_2 i\sqrt{5}$ und $\beta = b_1 + b_2 i\sqrt{5} \in R$. Dann ist

$$\begin{aligned} N(\alpha\beta) &= N(a_1b_1 - 5a_2b_2 + (a_1b_2 + a_2b_1)i\sqrt{5}) \\ &= (a_1b_1 - 5a_2b_2)^2 + 5(a_1b_2 + a_2b_1)^2 \\ &= a_1^2b_1^2 + 25a_2^2b_2^2 + 5a_1^2b_2^2 + 5a_2^2b_1^2 \\ &= (a_1^2 + 5b_1^2)(b_1^2 + 5b_2^2) \\ &= N(a_1 + a_2 i\sqrt{5})N(b_1 + b_2 i\sqrt{5}) = N(\alpha)N(\beta). \end{aligned}$$

(b) Betrachte eine Einheit $u = a + bi\sqrt{5} \in R$. Da N multiplikativ ist, gilt $N(u^{-1}) \cdot N(u) = N(u^{-1}u) = N(1) = 1$. Wegen $N(u^{-1}), N(u) \in \mathbb{N}$ muss daher $N(u) = a^2 + 5b^2 = 1$ sein. Daraus folgt sofort $b = 0$ und $a^2 = 1$, also $u = a = \pm 1$. Umgekehrt gilt für jedes Element $u = a + bi\sqrt{5} \in R$ mit $a^2 + 5b^2 = 1$ auch $(a + bi\sqrt{5})(a - bi\sqrt{5}) = 1$, also ist u eine Einheit in R.

(c) Falls $2 = \alpha\beta$ mit $\alpha, \beta \in R$ ist, folgt $4 = N(2) = N(\alpha)N(\beta)$. Wenn α und β keine Einheiten sind, ist $N(\alpha), N(\beta) > 1$ nach (b). Es gibt dann nur die Möglichkeit $N(\alpha) = N(\beta) = 2$. Diese kann aber nicht auftreten, da 2 wegen $a^2 + 5b^2 \neq 2$ für alle $a, b \in \mathbb{Z}$ nicht im Bild von N liegt. Somit ist 2 unzerlegbar in R.

Wegen $a^2 + 5b^2 \neq 3$ für alle $a, b \in \mathbb{Z}$ liegt auch 3 nicht im Bild von N. Wegen $N(3) = 9 = 3 \cdot 3$ folgt darum analog, dass 3 unzerlegbar in R ist.

Falls $1 + i\sqrt{5} = \alpha\beta$ mit $\alpha, \beta \in R$ ist, folgt $6 = N(1 + i\sqrt{5}) = N(\alpha)N(\beta)$. Wenn α und β keine Einheiten sind, dann müssen $N(\alpha), N(\beta) \in \{2, 3\}$ sein. Dies ist wiederum nicht möglich, da 2 und 3 nicht im Bild von N liegen. Daher ist $1 + i\sqrt{5}$ unzerlegbar. Mit der gleichen Argumentation folgt auch die Unzerlegbarkeit von $1 - i\sqrt{5}$.

(d) Wegen der Gleichheit $6 = 2 \cdot 3 = (1 + i\sqrt{5}) \cdot (1 - i\sqrt{5})$ sind 2 und 3 Teiler von $(1 + i\sqrt{5}) \cdot (1 - i\sqrt{5})$ und $1 + i\sqrt{5}$ und $1 - i\sqrt{5}$ Teiler von $2 \cdot 3$. Keines der vier Elemente ist aber ein Teiler eines anderen, weil sie nach (c) unzerlegbar sind, sich aber nach (b) nicht um Einheiten unterscheiden, da sie vershiedene Bilder unter N haben.

(e) Durch Multiplikation der Erzeuger erhalten wir

$$I \cdot I = (2, 1 + i\sqrt{5})(2, 1 + i\sqrt{5}) = (4, 2 + 2i\sqrt{5}, -4 + 2i\sqrt{5}).$$

Da $(2) = \{2a + 2bi\sqrt{5} \mid a, b \in \mathbb{Z}\}$ ist, haben wir $4, 2 + 2i\sqrt{5}, -4 + 2i\sqrt{5} \in (2)$ und daher $I \cdot I \subset (2)$. Umgekehrt ist

$$2 = (2 + 2i\sqrt{5}) - (-4 + 2i\sqrt{5}) - 4 \in I \cdot I.$$

Somit gilt $(2) = I \cdot I$.

(f) Wir nehmen an, dass I ein Hauptideal ist, d.h. $I = (2, 1 + i\sqrt{5}) = (\alpha)$ für ein $\alpha \in R$. Dann ist $2 = x\alpha$ für ein $x \in R$. Wegen der Unzerlegbarkeit von 2 ist entweder $x \in R^\times$ oder $\alpha \in R^\times$. Im ersten Fall ist 2 assoziiert zu α, also $(2) = (\alpha) = (2, 1 + i\sqrt{5})$. Dies ist ein Widerspruch, da $1 + i\sqrt{5}$ nicht in (2) liegt.

Es bleibt nur der Fall $\alpha \in R^\times$ übrig, in dem $I = (\alpha) = R$ ist. Auch dieser Fall kann nach (e) wegen des Widerspruchs

$$R = R \cdot R = I \cdot I = (2) \neq R$$

nicht auftreten. Somit ist I kein Hauptideal.

(g) Aus (f) folgt bereits, dass $I \neq (1)$, also ein echtes Ideal ist. Betrachte ein echt grösseres Ideal $I \subsetneq I' \subset R$ und wähle ein Element $a + bi\sqrt{5} \in I' \setminus I$. Die Rechnung $a + bi\sqrt{5} =$

$(a-b)+b\cdot(1+i\sqrt{5})$ zeigt dann, dass $a-b\notin I$ ist. Wegen $\mathbb{Z}\cap I=2\mathbb{Z}$ bedeutet dies, dass $a-b$ ungerade ist. Also ist

$$1 \;=\; (a+bi\sqrt{5}) - \tfrac{a-b-1}{2}\cdot 2 - b\cdot(1+i\sqrt{5}) \;\in\; (a+bi\sqrt{5})+I \;\subset\; I'.$$

Somit ist $I'=(1)$; und deshalb ist I maximal.

(h) Sei $\mathfrak{p}$ ein Primideal, das 2 enthält. Dann ist auch $2+2+2=6\in\mathfrak{p}$. Somit muss das Ideal $1+i\sqrt{5}$ oder $1-i\sqrt{5}$ enthalten. Wegen $1+i\sqrt{5}=2-(1-i\sqrt{5})$ enthält $\mathfrak{p}$ dann sowohl $1+i\sqrt{5}$ als auch $1-i\sqrt{5}$ und es folgt $I\subseteq\mathfrak{p}$. Da I maximal ist, folgt $I=\mathfrak{p}$.

(i) Mögliche Lösungen sind:

- Aus (c) und (d) folgt, dass in R unzerlegbare Elemente existieren, die nicht prim sind. Daher ist R nicht faktoriell.
- Die Gleichung $6=2\cdot 3=(1+i\sqrt{5})(1-i\sqrt{5})$ ergibt nach (c) zwei Zerlegungen von 6 in unzerlegbare Elemente. Bei (d) haben wir festgestellt, dass $2,3\nmid 1\pm i\sqrt{5}$ und $1\pm i\sqrt{5}\nmid 2,3$ gilt. Daher sind $2,3$ nicht zu $1\pm i\sqrt{5}$ assoziiert und die beiden obigen Zerlegungen sind nicht zueinander assoziiert. Deshalb kann R nicht faktoriell sein.

74. (a) Die komplexe Zahl $\omega=-\frac{1}{2}+\frac{1}{2}i\sqrt{3}$ ist algebraisch über $\mathbb{Q}$.
Finde ein Ideal $\mathfrak{a}\subseteq\mathbb{Q}[X]$ mit $\mathbb{Q}[\omega]\simeq\mathbb{Q}[X]/\mathfrak{a}$.

(b) Die reelle Zahl $t=\sqrt{2}+\sqrt{3}$ ist algebraisch über $\mathbb{Q}$.
Finde ein Ideal $\mathfrak{a}\subseteq\mathbb{Q}[X]$ mit $\mathbb{Q}[t]\simeq\mathbb{Q}[X]/\mathfrak{a}$.

Lösung: (a) Es gilt $\mathbb{Q}[\omega]=\{P(\omega):P\in\mathbb{Q}[X]\}\subseteq\mathbb{C}$. Sei $e\colon\mathbb{Q}[X]\to\mathbb{Q}[\omega]$, $e(P)=P(\omega)$ der Evaluationshomomorphismus. Nach dem 1. Isomorphiesatz ist $\mathfrak{a}=\ker(e)$ eine mögliche Lösung. Bezeichne mit $\bar{\omega}$ das komplex Konjugierte von ω. Die Zahl ω ist eine Nullstelle des Polynoms $X^2-(\omega+\bar{\omega})X+\omega\bar{\omega}=X^2+X+1$, aber keines linearen Polynoms, da $\omega\notin\mathbb{Q}$ ist. Also ist $\ker(e)=(X^2+X+1)$.

(b) Wir gehen wie in (a) vor. Aus $t^2=5+2\sqrt{6}$ und $(t^2-5)^2=25$ sehen wir, dass t eine Nullstelle von X^4-10X^2+1 ist, aber keines Polynoms von kleinerem Grad, da diess X^4-10X^2+1 teilen müsste. Allerdings hat X^4-10X^2+1 die vier verschiedenen Nullstellen $S=\{\pm(\sqrt{2}\pm\sqrt{3})\}$ und es ist nicht möglich, dass ein Polynom $\prod_{s\in S'}(X-s)$ für ein nichtleeres $S'\subsetneq S$ rationale Koeffizienten hat. Also ist $\mathfrak{a}=(X^4-10X^2+1)$ eine Lösung.

75. Sei $\mathfrak{a}=(3,X^3-X^2+2X-1)\subseteq\mathbb{Z}[X]$ ein Ideal in $\mathbb{Z}[X]$.

(a) Ist $\mathfrak{a}$ ein Hauptideal?

(b) Ist $\mathfrak{a}$ ein Primideal?

Lösung: (a) Sei $P\in\mathbb{Z}[X]$ mit $(P)=\mathfrak{a}$. Dann existiert ein $Q\in\mathbb{Z}[X]$ mit $PQ=a$. Da $\mathbb{Z}[X]$ ein Integritätsring ist, können wir die Gradformel anwenden und $P,Q\in\mathbb{Z}$ schliessen. Bis auf Assoziiertheit folgt damit $P=1$ oder $P=3$. Da alle Koeffizienten jedes Polynoms in (3) durch 3 teilbar sind, ist $P=3$ nicht möglich. Ausserdem ist muss jeder Koeffizient jedes Polonoms in $\mathfrak{a}$ vom Grad ≤ 2 durch 3 teilbar sein. Daher kann $P=1$ auch nicht sein. Somit ist $\mathfrak{a}$ kein Hauptidealring.

(b) Sei $\pi\colon\mathbb{Z}[X]\to\mathbb{Z}/3\mathbb{Z}[X]$ der Homomorphismus, der die Projektion $\mathbb{Z}\to\mathbb{Z}/3\mathbb{Z}$ mit $X\mapsto X$ fortsetzt. Dann ist $\pi[(X^3-X^2+2X-1)]=(X^3+\bar{2}X^2+\bar{2}X+\bar{2})$ ein Ideal in $\mathbb{Z}/3\mathbb{Z}[X]$ und der Kern der Projektion $\mathbb{Z}[X]\to(\mathbb{Z}[X]/(3))/(X^3+\bar{2}X^2+\bar{2}X+\bar{2})$

ist $\mathfrak{a}$. Somit ist $\mathbb{Z}[X]/\mathfrak{a}$ isomorph zu $\mathbb{Z}/3\mathbb{Z}[X]/(X^3 + \bar{2}X^2 + \bar{2}X + \bar{2})$. Durch Ausprobieren erkennen wir, dass das Polynom $X^3 + \bar{2}X^2 + \bar{2}X + \bar{2}$ keine Nullstellen in $\mathbb{Z}/3\mathbb{Z}$ hat. Da es Grad 3 hat, ist es somit irreduzibel und mit Aufgabe 72 folgt, dass der Faktorring $\mathbb{Z}/3\mathbb{Z}[X]/(X^3 + \bar{2}X^2 + \bar{2}X + \bar{2})$ ein Körper ist. Also ist auch $\mathbb{Z}[X]/\mathfrak{a}$ ein Körper und $\mathfrak{a}$ ist ein maximales Ideal. Insbesondere ist $\mathfrak{a}$ ein Primideal.