WS 05/06
Priv.-Doz. Dr. S. Wewers

Algebra I

7. Übungsblatt

Aufgabe 1: (1+1/2+1/2+1+1=4 P) Sei R ein kommutativer Ring. Zeigen Sie:

(a) Für alle $a, b, c \in R$ gilt:

   (i) $a \cdot (b - c) = a \cdot b - a \cdot c$,

   (ii) $a \cdot (-b) = (-a) \cdot b = -a \cdot b$,

   (iii) $a \cdot 0 = 0$.

(b) Der Polynomring $R[X]$ ist nullteilerfrei genau dann, wenn R nullteilerfrei ist.

(c) Sei R ein Integritätsbereich. Dann gilt

$$(R[X])^\times = R^\times,$$

d.h. die Einheiten von $R[X]$ sind genau die konstanten Polynome, welche als Elemente von R Einheiten sind.

(d) Mit $I_1, I_2 \lhd R$ sind auch die Teilmengen

$$I_1 \cap I_2, \quad I_1 + I_2 := \{\, a + b \mid a \in I_1,\, b \in I_2 \,\}$$

und

$$I_1 \cdot I_2 := \{\, \sum_{i=1}^{n} a_i b_i \;\mid\; a_i \in I_1,\, b_i \in I_2 \,\}$$

Ideale von R.

(e) Sei $I \lhd R$ ein Ideal. Wenn R/I ein Integritätsring ist, dann ist I ein Primideal. Und wenn R/I ein Körper ist, so ist I ein maximales Ideal.

Lösung:

(a) (i) Es wird unter Verwendung von (ii)

$$a \cdot (b - c) \;=\; a \cdot (b + (-c)) \;=\; a \cdot b + a \cdot (-c) \;=\; a \cdot b + (-a \cdot c) \;=\; a \cdot b - a \cdot c\,.$$

   (ii) Es wird unter Verwendung von (iii)

$$a \cdot (-b) \;=\; a \cdot (-b) + a \cdot b - a \cdot b \;=\; a \cdot (-b + b) - a \cdot b \;=\; a \cdot 0 - a \cdot b \;=\; 0 - a \cdot b \;=\; -a \cdot b\,.$$

   Eine analoge Rechnung zeigt $(-a) \cdot b = -a \cdot b$.

   (iii) Es wird

$$a \cdot 0 \;=\; a \cdot 0 + a \cdot 0 - a \cdot 0 \;=\; a \cdot (0 + 0) - a \cdot 0 \;=\; a \cdot 0 - a \cdot 0 \;=\; 0\,.$$

Bemerkung: Wir haben nicht verwendet, daß R kommutativ ist.

(b) Wegen $R \subseteq R[X]$ folgt aus der Nullteilerfreiheit von $R[X]$ die Nullteilerfreiheit von R. Es sei nun umgekehrt R nullteilerfrei. Es seien $f, g \in R[X]$ mit $f \neq 0$ und $g \neq 0$. Es seien etwa

$$f \;=\; \sum_{\nu=0}^{n} a_\nu X^\nu \;,\quad g \;=\; \sum_{\mu=0}^{m} b_\mu X^\mu$$

mit $a_n \neq 0$ und $b_m \neq 0$. Dann ergibt sich

$$f \cdot g \;=\; \sum_{\lambda=0}^{n+m} \left(\sum_{\nu=\max\{0,\lambda-m\}}^{\min\{n,\lambda\}} a_\nu b_{\lambda-\nu} \right) X^\lambda \;=\; a_n b_m X^{n+m} + \ldots \;.$$

Da R nullteierfrei ist, ist $a_n b_m \neq 0$. Daher ist $f \cdot g \neq 0$.

Bemerkung: Wir haben sogar beweisen, daß

$$\deg(f \cdot g) \;=\; \deg f + \deg g \;,$$

falls R nullteilerfrei ist. Dabei ist $\deg 0 := -\infty$ definiert.

(c) Die Inklusion $R^\times \subseteq (R[X])^\times$ ist klar, da jede Einheit von R ein Inverses in R besitzt, das dann auch Inverses in $R[X]$ ist. Es sei also umgekehrt $f \in R[X]^\times$ gegeben. Nach obiger Bemerkung gilt

$$0 \;=\; \deg 1 \;=\; \deg(f \cdot f^{-1}) \;=\; \deg f + \deg(f^{-1}) \;\geq\; \deg(f^{-1}) \;\geq\; 0 \;.$$

Daraus folgt $\deg f = \deg(f^{-1}) = 0$, d.h. $f \in R$ und $f^{-1} \in R$. Deshalb ist $f \in R^\times$.

(d) Die drei angebenen Mengen enthalten alle die 0.

- Es seien $a, b \in I_1 \cap I_2$ und $r \in R$. Dann gilt $a, b \in I_1$ und $a, b \in I_2$. Da I_1 und I_2 Ideale von R sind, folgt daraus $a - b \in I_1$, $ra \in I_1$, $a - b \in I_2$ und $ra \in I_2$. Daraus folgt $a - b \in I_1 \cap I_2$ und $ra \in I_1 \cap I_2$. Daher ist $I_1 \cap I_2$ ein Ideal von R.
- Es seien $x_1, x_2 \in I_1 + I_2$ und $r \in R$. Dann gibt es $a_1, a_2 \in I_1$ und $b_1, b_2 \in I_2$ so, daß $x_1 = a_1 + b_1$ und $x_2 = a_2 + b_2$. Da I_1 und I_2 Ideal von R sind, folgt daraus, daß $a_1 - a_2 \in I_1$, $b_1 - b_2 \in I_2$, $ra_1 \in I_1$ und $rb_1 \in I_2$. Daraus folgt

$$\begin{aligned} x_1 - x_2 &= (a_1 - a_2) + (b_1 - b_2) &\in\; I_1 + I_2 \;, \\ rx_1 &= (ra_1) + (rb_1) &\in\; I_1 + I_2 \;. \end{aligned}$$

  Also ist auch $I_1 + I_2$ ein Ideal von R.
- Es seien $x, y \in I_1 \cdot I_2$ und $r \in R$. Es seien etwa

$$x \;=\; \sum_{i=1}^{n} a_i b_i \;,\quad y \;=\; \sum_{i=1}^{m} c_i d_i$$

  für gewissen $n, m \in \mathbb{N}$, $a_i, c_i \in I_1$ und $b_i, d_i \in I_2$. Dann folgt

$$\begin{aligned} x - y &= \sum_{i=1}^{m} a_i b_i + \sum_{i=1}^{m} (-c_i) d_i &\in\; I_1 \cdot I_2 \;, \\ rx &= \sum_{i=1}^{m} (ra_i) b_i &\in\; I_1 \cdot I_2 \;. \end{aligned}$$

  Also ist auch $I_1 \cdot I_2$ ein Ideal von R.

(e)
- Es sei R/I ein Integritätsring. Insbesondere gilt $I \neq R$. Es seien $a, b \in R$ gegeben mit $ab \in I$. Zu zeigen: $a \in I$ oder $b \in I$. In R/I gilt
$$\overline{a} \cdot \overline{b} \;=\; \overline{ab} \;=\; \overline{0}\,.$$
Da R/I nullteilerfrei ist und $\overline{0}$ das Nullelement von R/I folgt daraus $\overline{a} = \overline{0}$ oder $\overline{b} = \overline{0}$. Dies impliziert aber $a \in I$ oder $b \in I$. Wegen der Beliebigkeit von a und B folgt, daß I ein Primideal ist.
- Es sei R/I ein Körper. Insbesondere gilt $I \neq R$. Es sei $J \supseteq I$ ein Ideal von R mit $J \neq I$. Zu zeigen: $J = R$. Nach der Wahl von J gibt es ein $a \in J \setminus I$. Dann ist $\overline{a} \neq \overline{0}$ in R/I. Da R/I ein Körper ist, besitzt $\overline{a}$ ein Inverses, d.h. es gibt ein $\overline{b} \in R/I$ so, daß $\overline{a} \cdot \overline{b} = \overline{1}$. Daraus folgt aber $\overline{ab} = \overline{1}$, d.h. $ab - 1 \in I$. Demanch gilt auch $ab - 1 \in J$ und $a \in J$. Da J ein Ideal ist, folgt $1 = ab - (ab - 1) \in J$. Aber aus $1 \in J$ folgt sofort $J = R$. Daher ist I maximales Ideal von R.

Aufgabe 2: (1+1+1+1=4 P) Es sei $\varphi : \mathbb{Z}[X] \to \mathbb{R}$ der Einsetzungshomomorphismus mit $\varphi(X) = \sqrt{3}$ und
$$\mathbb{Z}[\sqrt{3}] = \{\, x + y\sqrt{3} \mid x, y \in \mathbb{Z} \,\}$$
das Bild von φ. Sei $I := \mathrm{Kern}(\varphi) \lhd \mathbb{Z}[X]$ der Kern von φ.

(a) Zeigen Sie, dass I das von dem Polynom $X^2 - 3$ erzeugte Hauptideal ist,
$$I = (X^2 - 3).$$
(Hinweis: benutzen Sie Polynomdivision mit Rest.)

(b) Zeigen Sie, dass I ein Primideal, aber kein maximales Ideal ist.

(c) Sei $J := I + (11) \lhd \mathbb{Z}[X]$. Konstruieren Sie einen Isomorphismus
$$\mathbb{Z}[X]/J \xrightarrow{\sim} \mathbb{F}_{11} := \mathbb{Z}/\mathbb{Z} \cdot 11.$$
Schliessen Sie, dass J ein maximales Ideal ist. (Hinweis: finden Sie ein $a \in \mathbb{Z}$ mit $a^2 \equiv 3 \pmod{11}$.)

(d) Finden Sie ein Ideal $N \lhd \mathbb{Z}[\sqrt{3}]$ für das $\mathbb{Z}[\sqrt{3}]/N \cong \mathbb{F}_{11}$. Ist N Prim- bzw. maximales Ideal?

Lösung:

(a) Es gilt $\varphi(X^2 - 3) \;=\; 0$, d.h. es folgt $X^2 - 3 \in I$. Daher ist die Inklusion
$$I \;\supseteq\; (X^2 - 3)$$
gezeigt. Es sei nun umgekehrt $f \in I$ gegeben. Nach der Polynomdivision gilt
$$f \;=\; g \cdot (X^2 - 3) + h$$
mit Polynomen $g, h \in \mathbb{Z}[X]$, wobei $\deg h < 2$. Also ist $\deg h \leq 1$, d.h. wir können schreiben
$$h \;=\; cX + d$$
mit gewissen $c, d \in \mathbb{Z}$. Es folgt
$$0 \;=\; \varphi(f) \;=\; \varphi(g) \cdot 0 + \varphi(h) \;=\; c\sqrt{3} + d\,.$$
Wäre $c \neq 0$, so folgte daraus $\sqrt{3} \in \mathbb{Q}$, ein Widerspruch. Also ist $c = 0$ und folglich auch $d = 0$. Es gilt daher
$$f \;=\; g \cdot (X^2 - 3) \;\in\; (X^2 - 3)\,.$$
Wegen der Beliebigkeit von f folgt $I = (X^2 - 3)$.

(b) Es gilt $I \neq \mathbb{Z}[X]$, da z.B $X \notin I$ gilt. Und für $f, g \in \mathbb{Z}[X]$ mit $f \cdot g \in I$ folgt $0 = \varphi(fg) = \varphi(f)\varphi(g)$, also $\varphi(f) = 0$ oder $\varphi(g) = 0$, also $f \in I$ oder $g \in I$. Mithin ist I ein Primideal.

Alternativlösung: Nach dem Homomorphiesatz induziert φ einen Isomorphismus

$$\mathbb{Z}[X]/I \;\cong\; \mathbb{Z}[\sqrt{3}]\ .$$

Nun ist $\mathbb{Z}[\sqrt{3}] \subseteq \mathbb{C}$, also ist $\mathbb{Z}[\sqrt{3}]$ ein Integritätsring. Auch daraus folgt, daß I ein Primideal ist.

Andererseits besitzt $2 \in \mathbb{Z}[\sqrt{3}]$ kein Inverses, denn $\frac{1}{2} \neq \mathbb{Z}[\sqrt{3}]$. Also ist $\mathbb{Z}[\sqrt{3}]$ kein Körper. Mithin ist I kein maximales Ideal.

(c) Wie bereits in der Vorlesung erwähnt, stimmt die Aufgabe nicht. Wir wollen statt dessen ein maximales Ideal J finden mit $J \supseteq I$. Es sei z.B.

$$J \;:=\; (X-5, 11)$$

das von $X - 5$ und 11 erzeugte Ideal. Wegen

$$X^2 - 3 \;=\; (X-5)(X+5) + 11 \cdot 2$$

ist $X^2 - 3 \in J$ und damit $I \subseteq J$. Betrachte nun den Homomorphismus

$$\tau : \mathbb{Z}[X] \xrightarrow{\psi} \mathbb{Z} \xrightarrow{\kappa} \mathbb{Z}/11\mathbb{Z}\,.$$

Dabei sei ψ definiert durch $\psi(f) := f(5)$, und κ sei der kanonische Epimorphismus. Offenbar sind ψ und κ und damit auch τ surjektiv. Ferner gilt

$$\psi^{-1}(11\mathbb{Z}) \;=\; (X-5, 11) \;=\; J\ ,$$

wie man durch Polynomdivision durch $X - 5$ sieht. Also ist

$$\text{Kern}\ \tau \;=\; (\kappa \circ \psi)^{-1}(0) \;=\; \psi^{-1}(\tau^{-1}(0)) \;=\; \psi^{-1}(11\mathbb{Z}) \;=\; J\ .$$

Nach dem Homomorphiesatz induziert τ einen Isomorphismus

$$\mathbb{Z}[X]/J \;\cong\; \mathbb{Z}/11\mathbb{Z} \;=\; \mathbb{F}_{11}\ .$$

Da $\mathbb{F}_{11}$ ein Körper ist, ist J ein maximales Ideal.

(d) Wir wollen zeigen, daß es ein kommutatives Diagramm von Ringhomomorphismen gibt der Form

$$\begin{tikzcd} \mathbb{Z}[X] \arrow[r, two heads, "\tau"] \arrow[d, "\varphi"'] & \mathbb{F}_{11} \\ \mathbb{Z}[\sqrt{3}] \arrow[ur, dashed, "\alpha"] & \end{tikzcd}$$

Um die Kommutativität zu erhalten, ist $\alpha(\sqrt{3}) = \tau(X) = \overline{5}$ notwendig. Also definieren wir

$$\alpha : \mathbb{Z}[\sqrt{3}] \to \mathbb{F}_{11}\ ,\quad a + b\sqrt{3} \mapsto \overline{a + b \cdot 5}\ .$$

Diese Abbildung ist aufgrund der Eindeutigkeit von a, b wohldefiniert. Es gilt also

$$\alpha(\varphi(f)) \;=\; \tau(f)$$

für alle $f \in \mathbb{Z}[X]$. Daraus folgt die Kommutativität des Diagramms. Wegen der Surjektivität von φ folgt daraus auch, daß α ein Homomorphismus ist. Es folgt

$$\text{Kern } \alpha \;=\; \varphi(\varphi^{-1}(\alpha^{-1}(0))) \;=\; \varphi(\tau^{-1}(0)) \;=\; \varphi(J) \;=\; (\sqrt{3}-5, 11) \;:=\; N\ .$$

Nach dem Homomorphiesatz folgt

$$\mathbb{Z}[\sqrt{3}]/N \;\cong\; \mathbb{F}_{11}\ .$$

Da $\mathbb{F}_{11}$ ein Körper ist, ist N ein maximales Ideal (und somit auch ein Primideal).

Aufgabe 3: (1+1+2=4 P) Sei $R := \mathbb{Z}[i] \subset \mathbb{C}$ der Ring der ganzen Gauß'schen Zahlen. Sei $Q(R)$ der Quotientenkörper von R.

(a) Nach Satz 1.4 der Vorlesung setzt sich die natürliche Inklusion $R \hookrightarrow \mathbb{C}$ zu einer Inklusion $Q(R) \hookrightarrow \mathbb{C}$ fort. Zeigen Sie: das Bild von $Q(R)$ in $\mathbb{C}$ ist

$$\mathbb{Q}[i] = \{\, x + y \cdot i \mid x, y \in \mathbb{Q}\}.$$

(Insbesondere ist $\mathbb{Q}[i]$ ein Körper, den man mit dem Quotientenkörper $Q(R)$ identifizieren kann.)

(b) Finden Sie eine ganze Zahl a mit $a^2 \equiv -1 \pmod{41}$ und schreiben Sie das Ideal

$$I := (41, a - i) \lhd \mathbb{Z}[i]$$

als Hauptideal. Finden Sie $x, y \in \mathbb{Z}$ mit $x^2 + y^2 = 41$. Ist (41) ein Primideal? Ist I ein maximales Ideal?

(c) Zeigen Sie, dass das Ideal $(3) \lhd \mathbb{Z}[i]$ ein maximales Ideal (und damit auch ein Primideal) ist. (Hinweis: der euklidische Algorithmus zeigt, dass ein Ideal $J \lhd \mathbb{Z}[i]$ mit $(3) \subset J$, $(3) \neq J$, ein Element $a = x + y \cdot i$ enthält mit $|a| = 1$.)

Lösung:

(a)

- Es sei $\mathbb{Q}[i] := \{x + y \cdot i \mid x, y \in \mathbb{Q}\}$. Wir zeigen, daß gilt

  $$\mathbb{Q}[i] \;=\; \{ab^{-1} \mid a, b \in \mathbb{Z}[i],\ b \neq 0\} \;\subseteq\; \mathbb{C}\ .$$

  Es sei zuerst $z \in \mathbb{Q}[i]$, d.h. es gilt $z = \frac{x_1}{x_2} + \frac{y_1}{y_2} \cdot i$ für gewisse $x_1, x_2, y_1, y_2 \in \mathbb{Z}$. Dann folgt

  $$z \;=\; (x_1 y_2 + x_2 y_1 \cdot i)(x_2 y_2)^{-1} \;=\; ab^{-1}$$

  mit $a := x_1 y_2 + x_2 y_1 \cdot i \in \mathbb{Z}[i]$ und $b := x_2 y_2 \in \mathbb{Z}[i] \setminus \{0\}$.

  Es seien nun umgekehrt $a = x + y \cdot i$ und $b = c + d \cdot i$ mit $x, y, c, d \in \mathbb{Z}$, $b \neq 0$. Dann folgt

  $$ab^{-1} \;=\; \frac{x + y \cdot i}{c + d \cdot i} \;=\; \frac{(x + y \cdot i)(c - d \cdot i)}{c^2 + d^2} \;=\; \frac{xc + yd}{c^2 + d^2} + \frac{yc - xd}{c^2 + d^2} \cdot i \;\in \mathbb{Q}[i]\ .$$

- Nach Vorlesung gibt es einen Homomorphismus $\psi : Q(R) \hookrightarrow \mathbb{C}$, der die Inklusion $R \hookrightarrow \mathbb{C}$ fortsetzt. Ferner gilt nach Vorlesung $Q(R) \left\{\, \frac{a}{b} \,\middle|\, a, b \in R,\ b \neq 0 \right\}$. Also folgt für alle $a, b \in R$ mit $b \neq 0$

  $$\psi\left(\frac{a}{b}\right) \;=\; \psi\left(\frac{a}{1} \cdot \left(\frac{b}{1}\right)^{-1}\right) \;=\; \psi\left(\frac{a}{1}\right) \cdot \left(\psi\left(\frac{b}{1}\right)\right)^{-1} \;=\; ab^{-1}\ ,$$

  und das Bild von $Q(R)$ in $\mathbb{C}$ ist gleich der Menge

  $$\left\{ \psi\left(\frac{a}{b}\right) \,\middle|\, a, b \in R,\ b \neq 0 \right\} \;=\; \{ab^{-1} \mid a, b \in R,\ b \neq 0\} \;=\; \mathbb{Q}[i]\ .$$

(b) Es ist $a := 9$. Division mit Rest im Euklidischen Ring $\mathbb{Z}[i]$ ergibt

$$\begin{aligned} 41 &= 4 \cdot (9 - i) + 5 + 4 \cdot i \;, \quad |5 + 4 \cdot i|^2 < |9 - i|^2 \\ 9 - i &= (1 - i) \cdot (5 + 4 \cdot i) \;. \end{aligned}$$

Dies zeigt, daß $5 + 4 \cdot i$ ein ggT von 41 und $9 - i$ ist, d.h. es gilt

$$I \;=\; (41, 9 - i) \;=\; (5 + 4i) \;.$$

Formal gilt dies, da 41 und $9 - i$ Vielfache von $5 + 4i$ sind, und da $5 + 4i$ Linearkombination von 41 und $9 - i$ ist. Die Zahl $41 \in \mathbb{Z}[i]$ ist nicht irreduzibel wegen $41 = (5 + 4 \cdot i)(5 - 4 \cdot i)$. Also ist (41) auch kein Primideal.

Wir zeigen nun, daß $5 + 4 \cdot i$ irreduzibel ist. Zunächst ist $5 + 4 \cdot i$ keine Einheit. Es seien nun $a, b \in \mathbb{Z}[i]$ derart, daß $5 + 4 \cdot i = ab$. Dann folgt

$$41 \;=\; |5 + 4 \cdot i|^2 \;=\; |ab|^2 \;=\; |a|^2 |b|^2 \;,$$

und $|a|^2$ und $|b|^2$ sind natürliche Zahlen. Da 41 eine Primzahl ist, folgt daraus $|a| = 1$ oder $|b| = 1$, also $a \in \mathbb{Z}[i]^\times$ oder $b \in \mathbb{Z}[i]^\times$. (Denn die Einheiten ± 1 und $\pm i$ sind die einzigen Zahlen in $\mathbb{Z}[i]$ mit Norm 1). Daraus folgt, daß $5 + 4 \cdot i$ irreduzibel in $\mathbb{Z}[i]$ ist. Also ist $I = (5 + 4 \cdot i)$ ein maximales Ideal, da $\mathbb{Z}[i]$ ein Hauptidealring ist.

(c) Nach Vorlesung genügt es zu zeigen, daß 3 irreduzibel in $\mathbb{Z}[i]$ ist. Wir nehmen also an, es seien $a, b \in \mathbb{Z}[i]$ mit

$$3 \;=\; ab \;.$$

Dann folgt

$$9 \;=\; |3|^2 \;=\; |a|^2 |b|^2 \;.$$

Dabei sind $|a|^2$ und $|b|^2$ ganze Zahlen. Nun ist $|a|^2 = 3$ in $\mathbb{Z}[i]$ unmöglich, da die Summe zweier Quadratzahlen in $\mathbb{Z}$ niemals 3 ergibt. Also folgt $|a|^2 = 1$ oder $|b|^2 = 1$, also $a \in \{\pm 1, \pm i\} = (\mathbb{Z}[i])^\times$ oder $b \in \{\pm 1, \pm i\} = (\mathbb{Z}[i])^\times$. Also ist 3 irreduzibel in $\mathbb{Z}[i]$.

Abgabe: am Donnerstag, den 15.12. (in der Vorlesung, oder bei Herrn Martin).