Algebra I

Musterlösung 9

Isomorphiesätze, Primideale, Quotientenkörper

---

57. (a) Zeige: Ist $\varphi : R \to S$ ein Ringhomomorphismus und $\mathfrak{a} \subseteq S$ ein Ideal, dann ist $\varphi^{-1}[\mathfrak{a}]$ ein Ideal in R.

(b) Zeige: Ist $\varphi : R \to S$ ein surjektiver Ringhomomorphismus und $\mathfrak{a} \subseteq R$ ein Ideal, dann ist $\varphi[\mathfrak{a}]$ ein Ideal in S.

Lösung: (a) Aus der Gruppentheorie wissen wir bereits, dass $(\varphi^{-1}[\mathfrak{a}], +)$ eine Untergruppe von $(R, +)$ ist. Sei nun $a \in \varphi^{-1}[\mathfrak{a}]$, d.h. $\varphi(a) \in \mathfrak{a}$, und sei $r \in R$. Weil $\mathfrak{a}$ ein Ideal ist, gilt $\varphi(ra) = \varphi(r)\varphi(a) \in \mathfrak{a}$. Also ist auch $ra \in \varphi^{-1}[\mathfrak{a}]$. Somit ist $\varphi^{-1}[\mathfrak{a}]$ ein Ideal in R.

(b) Aus der Gruppentheorie wissen wir bereits, dass $(\varphi[\mathfrak{a}], +)$ eine Untergruppe von $(S, +)$ ist. Sei nun $a \in \varphi[\mathfrak{a}]$, d.h. es existiert ein $b \in \mathfrak{a}$ mit $a = \varphi(b)$, und sei $s \in S$. Da φ surjektiv ist, existiert ein $r \in R$ mit $\varphi(r) = s$. Daher gilt $sa = \varphi(r)\varphi(b) = \varphi(rb) \in \varphi[\mathfrak{a}]$. Somit ist $\varphi[\mathfrak{a}]$ ein Ideal in R.

58. (a) Zeige: Jedes maximale Ideal ist Primideal.

(b) Zeige: Jeder endliche Integritätsring ist ein Körper.

(c) Zeige: Ist $\mathfrak{p} \subseteq R$ ein Primideal und ist $R/\mathfrak{p}$ endlich, dann ist $\mathfrak{p}$ ein maximales Ideal.

Lösung: (a) Ein Ideal ist genau dann ein Primideal, wenn der entsprechende Faktorring ein Integritätsring ist. Ein Ideal ist genau dann maximal, wenn der entsprechende Faktorring ein Körper ist. Da jeder Körper nullteilerfrei ist, folgt die Aussage.

(b) Sei R ein endlicher Integritätsring. Wir müssen zeigen, dass $(R \setminus \{0\}, \cdot)$ eine Gruppe ist. In Aufgabe 15c) haben wir bewiesen, dass für jede Gruppe G und endliche nichtleere Teilmenge U folgendes gilt. Ist $UU \subseteq U$, so ist U eine Untergruppe von G. Nun folgt die Aussage mit $U = R \setminus \{0\}$ und $G = \mathrm{Quot}(R) \setminus \{0\}$.

(c) Da $\mathfrak{p}$ ein Primideal ist, ist $R/\mathfrak{p}$ ein Integritätsring. Nach Teil b) ist es somit ein Körper. Also ist $\mathfrak{p}$ maximal.

59. Sei R ein kommutativer Ring und sei $S \subseteq R \setminus \{0\}$ ein multiplikatives Monoid, *d.h.* es ist $1 \in S$ und mit $x, y \in S$ ist auch $x \cdot y \in S$. Ferner sei $\mathfrak{p} \subseteq R$ ein Ideal mit $\mathfrak{p} \cap S = \emptyset$, das bezüglich dieser Eigenschaft maximal ist.

Zeige: $\mathfrak{p}$ ist ein Primideal.

Lösung: Wegen $1 \in S$ ist $\mathfrak{p} \neq R$. Es bleibt zu zeigen, dass für alle $a, b \in R \setminus \mathfrak{p}$ gilt $ab \notin \mathfrak{p}$. Wegen der Maximalität von $\mathfrak{p}$ gilt $(\mathfrak{p} + (a)) \cap S \neq \emptyset$. Daher existieren $p \in \mathfrak{p}$ und $x \in R$ mit $p + xa \in S$. Analog existieren $q \in \mathfrak{p}$ und $y \in R$ mit $q + yb \in S$. Da S abgeschlossen unter Multiplikation ist folgt $(p + xa)(q + yb) = pq + xaq + pyb + xyab \in S$. Wegen $\mathfrak{p} \cap S = \emptyset$ impliziert das $ab \notin p$.

60. Seien R ein kommutativer Ring, $\mathfrak{a} \subseteq R$ ein Ideal und $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \subseteq R$ Primideale in R mit $\mathfrak{a} \subseteq \mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_r$.

Zeige: Dann existiert ein $i \in \{1, \ldots, r\}$ mit $\mathfrak{a} \subseteq \mathfrak{p}_i$.

Lösung: Wir verwenden vollständige Induktion. Für $r = 1$ ist die Aussage offensichtlich. Sei nun $r > 1$. Falls es ein $k \in \{1, \ldots, r\}$ gibt, sodass bereits

$$\mathfrak{a} \subseteq \bigcup_{\substack{i=1 \\ i \neq k}}^{r} \mathfrak{p}_i$$

gilt, sind wir laut Induktionsannahme fertig. Wir können daher annehmen, dass es für jedes k ein Element

$$a_k \in \mathfrak{a} \setminus \bigcup_{\substack{i=1 \\ i \neq k}}^{r} \mathfrak{p}_i$$

gibt. Wegen $\mathfrak{a} \subseteq \mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_r$ folgt daraus $a_k \in \mathfrak{p}_k$. Sei

$$a := \sum_{k=1}^{r} \prod_{\substack{i=1 \\ i \neq k}}^{r} a_i .$$

Offensichtlich liegt $a \in \mathfrak{a}$ und somit existiert ein l mit $a \in \mathfrak{p}_l$. Da für jedes $k \neq l$ das Element $\prod_{\substack{i=1 \\ i \neq k}}^{r} a_i$ den Faktor a_l hat und deshalb in $\mathfrak{p}_l$ liegt, muss auch

$$a - \sum_{\substack{k=1 \\ k \neq l}}^{r} \prod_{\substack{i=1 \\ i \neq k}}^{r} a_i = \prod_{\substack{i=1 \\ i \neq l}}^{r} a_i$$

ein Element von $\mathfrak{p}_l$ sein. Da $\mathfrak{p}_l$ ein Primideal ist, impliziert das, dass es ein $i \neq l$ gibt mit $a_i \in \mathfrak{p}_l$. Das ist ein Widerspruch zur Definition von a_i.

61. Gegeben sei der Ring $R = \big(\mathscr{P}(\mathbb{N}), \emptyset, \mathbb{N}, +, \cdot\big)$ mit $+$ und $\cdot$ wie in Aufgabe 48 und sei

$$\mathfrak{a} = \{X \subseteq \mathbb{N} : X \text{ ist endlich}\} \subseteq R .$$

Weiter sei

$$S = \Big\{ \bigcup_{n \in Y} \{2n, 2n+1\} : Y \subseteq \mathbb{N} \Big\}$$

ein Unterring von R.

(a) Zeige, dass $\mathfrak{a}$ ein Ideal in R ist.

(b) Zeige, dass $\mathfrak{a}$ kein Primideal ist.

(c) Finde mit dem 1. Isomorphiesatz einen von $(S+\mathfrak{a})/\mathfrak{a}$ verschiedenen, aber zu $(S+\mathfrak{a})/\mathfrak{a}$ isomorphen, Ring und bestimme den entsprechenden Isomorphismus.

(d) Finde einen surjektiven Ringhomomorphismus $\varphi : R \to S$ mit $\ker(\varphi) = \mathscr{P}(4\mathbb{N})$.

(e) Sei φ der surjektive Ringhomomorphismus $\varphi : R \to S$ aus Aufgabe (d) und sei $\mathfrak{b} := \mathscr{P}(2\mathbb{N})$.

Bestimme den Isomorphismus zwischen $R/\mathfrak{b}$ und $S/\varphi[\mathfrak{b}]$.

(f) Finde zwei Primideale in R.

(g) Wo liegt die Schwierigkeit, das Ideal $\mathfrak{a}$ zu einem Primideal zu erweitern?

Lösung: (a) Wegen $\emptyset \in \mathfrak{a}$ ist $\mathfrak{a} \neq \emptyset$. Weiter ist die Vereinigung zweier endlicher Mengen immer endlich. Ausserdem ist jede Teilmenge einer endlichen Menge endlich. Somit sind alle Bedingungen aus Aufgabe 48b) erfüllt und $\mathfrak{a}$ ist ein Ideal in R.

(b) Es ist $(\mathbb{N} \setminus \{0\}) \cdot (N \setminus \{1\}) = \{0, 1\} \in \mathfrak{a}$, aber weder $\mathbb{N} \setminus \{0\}$ noch $\mathbb{N} \setminus \{1\}$ liegen in $\mathfrak{a}$.

(c) Sei $\iota\colon S \to S + \mathfrak{a}$ die Inklusion und $\pi\colon S + \mathfrak{a} \to S + \mathfrak{a}/\mathfrak{a}$ die Projektion. Dann ist die Verknüpfung

$$\varphi := \pi \circ \iota\colon S \to (S + \mathfrak{a})/\mathfrak{a},\ \varphi(s) = s + \mathfrak{a}$$

ein Ringhomomorphismus. Offensichtlich gilt $\ker(\varphi) = S \cap \mathfrak{a}$. Seien $s \in S$ und $a \in \mathfrak{a}$. Dann gilt $(s + a) + \mathfrak{a} = s + \mathfrak{a}$ und somit $\varphi(s) = (s + a) + \mathfrak{a}$. Also ist φ surjektiv und mit dem 1. Isomorphiesatz folgt

$$(S + \mathfrak{a})/\mathfrak{a} \cong S/(S \cap \mathfrak{a}).$$

(d) Wir bemerken zuerst, dass R und S via

$$\psi\colon R \to S, \quad \psi(A) = \bigcup_{a \in A} \{2a, 2a + 1\}$$

isomorph sind. Es genügt also, einen Ringautomorphismus $R \to R$ mit Kern $4\mathbb{N}$ zu finden. Die Idee hierfür ist, aus $\mathbb{N}$ einfach alle durch 4 teilbaren Zahlen zu streichen und dann neu zu nummerieren. Sei $\lceil x \rceil := \min\{y \in \mathbb{N} : y \geq x\}$ für jedes $x \in \mathbb{R}$. Definiere

$$\rho\colon R \to R,\ A \mapsto \bigcup_{a \in A \setminus 4\mathbb{N}} \left\{a - \left\lceil \frac{a}{4} \right\rceil \right\}.$$

Dann ist $\psi \circ \rho$ der gesuchte Homomorphismus. Dass es sich tatsächlich um einen Homomorphismus handelt, folgt aus der folgenden Aussage mit $f\colon \mathbb{N} \setminus 4\mathbb{N} \to \mathbb{N},\ f(a) = a - \left\lceil \frac{a}{4} \right\rceil$. Seien X, Y zwei Mengen und $f\colon X \to Y$ eine injektive Funktion. Dann gilt für alle Teilmengen $X_1, X_2 \subseteq X$, dass $f[X_1 \cup X_2] = f[X_1] \cup f[X_2]$ und $f[X_1 \cap X_2] = f[X_1] \cap f[X_2]$, sowie $f[X_1 \setminus X_2] = f[X_1] \setminus f[X_2]$ ist.

(e) Da φ surjektiv ist, ist auch die Verknüpfung mit der Projektion $\pi\colon S \to S/\varphi[\mathfrak{b}]$ surjektiv. Es gilt $\ker(\pi \circ \varphi) = \varphi^{-1}[\varphi[\mathfrak{b}]]$. Wegen $4\mathbb{N} = \ker \varphi \subset \mathfrak{b}$ ist $\varphi^{-1}[\varphi[\mathfrak{b}]] = \mathfrak{b}$. Daher induziert $\pi \circ \varphi$ nach dem 1. Isomorphiesatz einen Isomorphismus $\psi\colon R/\mathfrak{b} \to S/\varphi[\mathfrak{b}]$.

Wir wollen diesen explizit bestimmen. Sei zuerst $\{a\} \subset \mathbb{N}$ mit ungeradem a, also $a = 2b+1$. Dann gilt

$$\psi(\{a\} + \mathfrak{b}) = \begin{cases} \{3b, 3b + 1\} + \varphi[\mathfrak{b}] & b \text{ gerade} \\ \{3b + 2, 3b + 3\} + \varphi[\mathfrak{b}] & b \text{ ungerade.} \end{cases}$$

Für beliebiges $A \subset \mathbb{N}$ gilt $A + \mathfrak{b} = A \cap (\mathbb{N} \setminus 2\mathbb{N}) + \mathfrak{b}$ und wir können ψ in offensichtlicher Weise auf A erweitern, nämlich

$$\psi(A + \mathfrak{b}) = \bigcup_{4b+1 \in A} \{3b, 3b + 1\} \cup \bigcup_{4b+3 \in A} \{3b + 2, 3b + 3\} + \varphi[\mathfrak{b}].$$

(f) Sei $A \in R$. Dann ist $(A) = \mathscr{P}(A)$. Nimm nun an, es gebe $x, y \in \mathbb{N} \setminus A$ mit $x \neq y$. Dann ist $(A \cup \{x\}) \cdot (A \cup \{y\}) = A \in (A)$. Daher ist ein Hauptideal genau dann ein Primideal, wenn sein Komplement Kardinalität 1 hat. Zwei Beispiele sind $(\mathbb{N} \setminus \{0\})$ und $(\mathbb{N} \setminus \{353761\})$.

(g) Seien $A, B \in R$ mit $|A \cap B| < \infty$. Dann muss A oder B in $\mathfrak{a}$ sein. Sei $C \in R$ mit $|\mathbb{N} \setminus C| < \infty$. Dann ist $\mathbb{N} \setminus C \in \mathfrak{a}$ und $\mathbb{N} = C + (\mathbb{N} \setminus C)$. Deshalb folgt $C \notin \mathfrak{a}$. Wenn wir jetzt annehmen, dass $A \cup B = \mathbb{N}$ gilt, dürfen nicht sowohl A als auch B in $\mathfrak{a}$ liegen, denn $|\mathbb{N} \setminus (A + B)| < \infty$. Wir müssen also von allen solchen Paaren A, B in konsistenter Weise eines auwählen. Dazu benötigt man das Auswahlaxiom.

62. Sei $d \in \mathbb{N}$ mit $\sqrt{d} \notin \mathbb{N}$.

Bestimme den Quotientenkörper $\mathrm{Quot}\big(\mathbb{Z}[\sqrt{d}]\big)$ des Ringes $\mathbb{Z}[\sqrt{d}]$, wobei

$$\mathbb{Z}[\sqrt{d}] := \left\{a + \sqrt{d} \cdot b : a, b \in \mathbb{Z}\right\}.$$

Lösung: Es gibt eine offensichtliche Einbettung $\varphi \colon \mathbb{Z}[\sqrt{d}] \to \mathbb{R}$. Nach der universellen Eigenschaft des Quotientenkörpers setzt sich diese zu einer Einbettung $\mathrm{Quot}\big(\mathbb{Z}[\sqrt{d}]\big) \to \mathbb{R}$ fort. Wir können daher annehmen, dass $\mathrm{Quot}\big(\mathbb{Z}[\sqrt{d}]\big) \subseteq \mathbb{R}$ ist. Seien $a, b \in \mathbb{Z}$ nicht beide gleich 0. Wir berechnen

$$\frac{1}{a + \sqrt{d} \cdot b} = \frac{a - \sqrt{d} \cdot b}{a^2 - db^2} = \frac{a}{a^2 - db^2} + \sqrt{d} \cdot \frac{-b}{a^2 - db^2}.$$

Mit dieser Rechnung sehen wir, dass

$$\frac{1}{a + \sqrt{d} \cdot b} \in \mathbb{Q}[\sqrt{d}] := \left\{x + \sqrt{d} \cdot y : x, y \in \mathbb{Q}\right\}$$

ist und dass $\mathbb{Q}[\sqrt{d}] \setminus \{0\}$ abgeschlossen unter Inversenbildung ist. Ausserdem ist es offensichtlich abgeschlossen unter Addition, Subtraktion und Multiplikation, also ist $\mathbb{Q}[\sqrt{d}]$ ein Körper, der $\mathbb{Z}[\sqrt{d}]$ enthält. Es bleibt zu zeigen, dass es der kleinste ist. Offensichtlich ist es der kleinste Körper, der für alle $p \in \mathbb{Z}, q \in \mathbb{Z}^*$ die Zahlen $\frac{p}{q}$ und $\sqrt{d} \cdot \frac{p}{q}$ enthält. Diese müssen aber wegen $\frac{p}{q} = pq^{-1}$ in $\mathrm{Quot}\big(\mathbb{Z}[\sqrt{d}]\big)$ enthalten sein. Somit sind wir fertig.