Prof. Dr. Lorenz Halbeisen

Musterlösung Serie 11

PRIMIDEALE, QUOTIENTENKÖRPER

---

58. Zeige:

(a) Ist R nullteilerfrei, so ist $\operatorname{char}(R) = 0$ oder $\operatorname{char}(R)$ ist eine Primzahl.

(b) Ist $\operatorname{char}(R) = n > 0$, so gilt $n \cdot a = 0$ fuer alle $a \in R$.

Lösung: (a) Sei $n := \operatorname{char}(R)$. Wir müssen nur zeigen, dass falls $n > 0$ ist, so ist n eine Primzahl. Angenommen, n ist keine Primzahl, sondern ein Produkt $n = a \cdot b$ mit $a, b \in \mathbb{Z}$, wobei $a, b < n$ gilt. Nach Definition der Charakteristik gilt $0 = n \cdot 1_R = a \cdot b \cdot 1_R$. Weil R aber Nullteilerfrei ist, muss $a \cdot 1_R = 0$ oder $b \cdot 1_R = 0$ gelten. Nach Definition der Charakteristik gilt dann $n|a$ oder $n|b$, was ein Widerspruch zu unserer Annahme ist. Daher muss n eine Primzahl sein.

(b) Es gilt $n \cdot a = n \cdot (1_R \cdot a) = (n \cdot 1_R) \cdot a = 0 \cdot a = 0$.

59. Zeige:

(a) Jedes maximale Ideal ist Primideal.

(b) Jeder endliche Integritätsring ist ein Körper.

(c) 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 $(R\backslash\{0\}, \cdot)$ eine Gruppe ist. In Aufgabe 16c) 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 $U = R\backslash\{0\}$ und $G = \operatorname{Quot}(R)\backslash\{0\}$.

(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.

60. Gegeben sei der Ring $R = \big(\mathscr{P}(\mathbb{N}), \varnothing, \mathbb{N}, +, *\big)$ mit $+$ und $*$ wie in Aufgabe 50 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 $\varnothing \in \mathfrak{a}$ ist $\mathfrak{a} \neq \varnothing$. Weiter ist die Vereinigung zweier endlicher Mengen immer endlich. Ausserdem ist jede Teilmenge einer endlichen Menge endlich. Somit sind alle Bedingungen aus Aufgabe 50b) erfüllt und $\mathfrak{a}$ ist ein Ideal in R.

(b) Sei $X \in R$ die Menge aller geraden Zahlen und $Y \in R$ die Menge aller ungeraden Zahlen. Dann gilt $X * Y = \varnothing \in \mathfrak{a}$, jedoch liegt weder X noch Y 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 $\lceil x\rceil := \min\{y \in \mathbb{N} : y \geqslant x\}$ 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 $A + \mathfrak{b} = A \cap (\mathbb{N} \backslash 2\mathbb{N}) + \mathfrak{b}$ 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 $x, y \in \mathbb{N} \backslash A$ 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 $(\mathbb{N} \backslash \{0\})$ und $(\mathbb{N} \backslash \{353761\})$.

(g) Sei $\mathfrak{p} \subset R$ ein Primideal mit $\mathfrak{a} \subset \mathfrak{p}$. Seien $A, B \in R$ mit $|A \cap B| < \infty$. Dann muss A oder B in $\mathfrak{p}$ sein. Sei $C \in R$ mit $|\mathbb{N} \backslash C| < \infty$. Dann ist $\mathbb{N} \backslash C \in \mathfrak{a}$ und $\mathbb{N} = C + (\mathbb{N} \backslash C)$. Deshalb folgt $C \notin \mathfrak{p}$ weil andernfalls $1_R = \mathbb{N} \in \mathfrak{p}$ und somit $\mathfrak{p} = R$ gilt. Wenn wir jetzt annehmen, dass $A \cup B = \mathbb{N}$ gilt, dürfen nicht sowohl A als auch B in $\mathfrak{p}$ liegen, denn $|\mathbb{N} \backslash (A + B)| < \infty$. Wir müssen also von allen solchen Paaren A, B in konsistenter Weise eines auwählen. Dazu benötigt man das Auswahlaxiom.

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

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

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

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 $\operatorname{Quot}\big(\mathbb{Z}[\sqrt{d}]\big) \to \mathbb{R}$ fort. Wir können daher annehmen, dass $\operatorname{Quot}\big(\mathbb{Z}[\sqrt{d}]\big) \subseteq \mathbb{R}$ 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

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

ist und dass $\mathbb{Q}[\sqrt{d}] \backslash \{0\}$ 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 $\operatorname{Quot}\big(\mathbb{Z}[\sqrt{d}]\big)$ enthalten sein. Somit sind wir fertig.

Das sogenannte Teichmüllerprinzip ist eine Aussage, welche äquivalent zum Auswahlaxiom ist, und welche sich besonders für Anwendungen in der Algebra eignet. Für die Formulierung des Teichmüllerprinzips müssen wir folgenden Begriff einführen:

Eine Menge M hat **endlichen Charakter**, wenn gilt:

$$X \text{ ist in } M \iff \text{jede endliche Teilmenge von } X \text{ ist in } M.$$

TEICHMÜLLERPRINZIP: Ist M eine Menge mit endlichem Charakter, so hat M bezüglich der Inklusion $\subseteq$ ein maximales Element.

62. Sei R ein Ring.

(a) Zeige, dass die Menge $M := \big\{S \subseteq R : 1_R \notin (S)\big\}$ endlichen Charakter hat.

(b) Zeige, dass R ein maximales Ideal besitzt.

(c) Zeige, dass jedes Ideal $\mathfrak{a} \subseteq R$ mit $\mathfrak{a} \neq R$ zu einem maximalen Ideal erweitert werden kann.

Lösung: (a) Ist $S \in M$, so gilt für jede endliche Teilmenge $S' \subseteq S$ wegen $(S') \subseteq (S)$ offensichtlich $1_R \notin (S')$. Sei andererseits $S \subseteq R$ mit der Eigenschaft, dass für jede endliche Teilmenge $S' \subseteq S$ gilt, dass $1_R \notin (S')$ ist. Sei $s \in (S)$. Dann exisiteren $r_1, \dots, r_n \in R$ und $s_1, \dots, s_n \in S$ mit $s = \sum_{i=1}^{n} r_i s_i$. Somit ist $s \in (\{s_1, \dots, s_n\})$ und es folgt $s \neq 1$. Also ist $1_R \notin (S)$.

(b) Sei $M := \big\{S \subseteq R : 1_R \notin (S)\big\}$. Dann ist $\{0\} \in M$, also $M \neq \emptyset$. Mit (a) hat M ein bezüglich Inklusion maximales Element S_{max}. Für alle $r \in R$ gilt nun entweder $r \in (S_{\text{max}})$ oder $(S_{\text{max}} \cup \{r\}) = R$, und somit ist (S_{max}) ein maximales Ideal in R.

(c) Sei $M_{\mathfrak{a}} := \big\{S \subseteq R : 1_R \notin (S \cup \mathfrak{a})\big\}$. Dann ist $\{0\} \in M_{\mathfrak{a}}$, also $M_{\mathfrak{a}} \neq \emptyset$. Mit (a) hat $M_{\mathfrak{a}}$ ein bezüglich Inklusion maximales Element S_{max}. Wie in (b) folgt dann, dass $(S_{\text{max}} \cup \mathfrak{a})$ ein maximales Ideal in R ist, welches $\mathfrak{a}$ enthält.