D-MATH | Algebra I | HS20
Prof. Manfred Einsiedler

Lösung 3

Faktorringe, Primideale, maximale Ideale

1. Ein *Pythagoreisches Tripel* ist ein Tripel von ganzen Zahlen $(x, y, z) \in \mathbb{Z}^3 \setminus \{(0,0,0)\}$ mit $x^2 + y^2 = z^2$. Wir nennen, ein Pythagoreisches Tripel (x, y, z) *primitiv*, falls x, y, z paarweise teilerfremd sind.

   (a) (**SAGE**) Erstellen Sie einen Plot aller Punkte (x, y), $|x|, |y| \leqslant 500$, die Teil eines Pythagoreischen Tripels sind.

   (b) Wie lassen sich Regelmässigkeiten in diesem Plot erklären?

   (c) Können Sie eine Vermutung über die Anzahl der primitiven Pythagoreischen Tripel aufstellen?

2. Sei R ein kommutativer Ring und I, J Ideale in R. Wir definieren das Ideal

$$IJ := (\{ij : i \in I, j \in J\}) .$$

   (a) Zeigen Sie, dass die Menge $\{ij : i \in I, j \in J\}$ nicht notwendigerweise ein Ideal in R ist.

   (b) Zeigen Sie, dass $IJ \subset I \cap J$ und finden Sie ein Beispiel, bei dem die Inklusion strikt ist.

   (c) Zeigen Sie, dass falls I und J koprim sind, dann gilt $I \cap J = IJ$.

3. (a) Welche der folgenden Ideale von $\mathbb{Z}/4\mathbb{Z}[X]$ sind prim? Welche sind maximal? *Hinweis*: Betrachten Sie den Faktorring.

      i. $(X, 2) \subset \mathbb{Z}/4\mathbb{Z}[X]$;

      ii. $(X) \subset \mathbb{Z}/4\mathbb{Z}[X]$.

   (b) Sei $a \in \mathbb{R}$. Untersuche, wann der Ring $\mathbb{R}[X]/(X^2 + a)$ isomorph zu $\mathbb{R} \times \mathbb{R}$, beziehungsweise zu $\mathbb{C}$, beziehungsweise zu keinem der beiden ist.

4. Sei R ein kommutativer Ring. Wir nehmen an, dass ein Ideal $I \subset R$ existiert, so dass

$$R^\times = R \setminus I \tag{1}$$

   (a) Zeigen Sie, dass I ein maximales Ideal ist.

   (b) Zeigen Sie, dass I das eindeutige maximale Ideal von R ist.

(c) Umgekehrt nehmen wir an, dass I das eindeutige maximale Ideal eines kommutativen Ringes R ist. Zeigen Sie, dass $R^\times = R \smallsetminus I$ gilt.

Einen kommutativen Ring mit der Eigenschaft (1) nennt man einen *lokalen* Ring.

5. (a) Seien R und S kommutative Ringe.

i. Sei $\varphi : R \to S$ ein Ringhomomorphismus und $I \subset R$ und $J \subset S$ Ideale, so dass $\varphi(I) \subset J$. Zeigen Sie, dass ein eindeutiger Ringhomomorphismus $\overline{\varphi} : R/I \longrightarrow S/J$ existiert, so dass das folgende Diagramm

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, "p_I"'] & S \arrow[d, "p_J"] \\ R/I \arrow[r, "\overline{\varphi}"'] & S/J \end{tikzcd}$$

kommutiert, wobei wir mit p_I und p_J die kanonischen Projektionen bezeichnen, d.h. $\overline{\varphi} \circ p_I = p_J \circ \varphi$.

ii. Was können wir über $\overline{\varphi}$ schliessen, wenn $I = \varphi^{-1}(J)$?

Lösung:

i. Sei $\psi = p_J \circ \varphi$. Dann ist $\psi(I) = p_J(\varphi(I)) \subseteq p_J(J) = \{0_{S/J}\}$, und damit ist $I \subseteq \ker(\psi)$. Nach dem ersten Isomorphissatz existiert ein eindeutiger Ringhomomorphismus $\overline{\varphi} : R/I \longrightarrow S/J$, so dass $\overline{\varphi} \circ p_I = \psi = p_J \circ \varphi$.

ii. Da $\varphi^{-1}(J) = \varphi^{-1}(p_J^{-1}(\{0_{S/J}\})) = \psi^{-1}(\{0_{S/J}\}) = \ker(\psi)$, falls $I = \varphi^{-1}(J)$, sagt uns der erste Isomorphisatz, dass $\overline{\varphi}$ injektiv ist.

(b) Sei R ein kommutativer Ring und $I_0 \subset R$ ein Ideal.

i. Zeigen Sie, dass es eine Korrespondenz zwischen Idealen in R/I_0 und Idealen in R, die I_0 enthalten, gibt. (siehe Vorlesung)

ii. Zeigen Sie, dass für ein Ideal $I \subset R$, das I_0 enthält, ein Ringisomorphismus

$$(R/I_0)/(I/I_0) \xrightarrow{\sim} R/I$$

existiert.

iii. Sei $I_0 \neq R$. Zeigen Sie, dass die maximalen (bzw. Prim-) Ideale von R/I_0 die Ideale I/I_0 sind, wobei $I \subset R$ ein maximales (bzw. Prim-) Ideal ist, das I_0 enthält.

iv. Finden Sie alle Ideale von $\mathbb{Z}/8\mathbb{Z}$. Welche sind prim? Welche sind maximal?

Lösung:

i. Sei I ein Ideal in R, das I_0 enthält. Dann können wir den Faktorring I/I_0 betrachten. Wir zeigen zuerst, dass $p_{I_0}(I) = I/I_0$ ein Ideal in R/I_0 ist, wobei wir mit $p_{I_0} : R \to R/I_0$ die kanonische Projektion bezeichnen. Es

gilt $0+I_0 \in I/I_0$, da $I_0 \subseteq I$. Seien nun $a, b \in I$, dann gilt $(a+I_0)+(b+I_0) = (a+b)+I_0 \in I/I_0$, da I ein Ideal in R. Analog gilt für $a \in I$ und $r \in R$, dass $(a+I_0)(r+I_0) = (ar)+I_0 \in I/I_0$, da I ein Ideal in R.
Sei nun J ein Ideal in R/I_0. Dann ist $I := p_{I_0}^{-1}(J)$ ein Ideal in R, da Urbilder von Idealen unter Ringhomomorphismen wieder Ideale sind. Es gilt $I_0 \subseteq I = p_{I_0}^{-1}(J)$, falls $p_{I_0}(I_0) \subseteq p_{I_0}(I) = p_{I_0} \circ p_{I_0}^{-1}(J) = J$, da p_{I_0} surjektiv ist. Es gilt $p_{I_0}(I_0) = 0 \in R/I_0$ und, da J ein Ideal, ist $0 \in J$ und somit $I_0 \subseteq I$. Da p_{I_0} surjektiv ist, gilt $p_{I_0}(I) = p_{I_0} \circ p_{I_0}^{-1}(J) = J$.

ii. Da $I_0 \subseteq I$ und I der Kern der kanonischen Projektion $p_I : R \to R/I$ ist, faktorisiert die Abbildung p_I durch R/I_0 (siehe (a)i.), d.h. das folgende Diagramm kommutiert.

$$\begin{tikzcd} R \arrow[r, "\mathrm{id}"] \arrow[d, "p_{I_0}"'] & R \arrow[d, "p_I"] \\ R/I_0 \arrow[r, "f"'] & R/I \end{tikzcd}$$

Der Ringhomomorphismus $f : R/I_0 \to R/I$ ist surjektiv, da p_I surjektiv ist. Ausserdem gilt

$$\ker(f) = \{r+I_0,\, r \in R : r+I = I\} = \{r+I_0,\, r \in I\} = I/I_0,$$

das heisst nach dem ersten Isomorphiesatz induziert die Abbildung f einen Ringsisomorphismus

$$\varphi : (R/I_0)/(I/I_0) \xrightarrow{\sim} R/I.$$

iii. Aus (b)i. wissen wir, dass die Ideale von R/I_0 von der Form I/I_0 sind, wobei I ein Ideal in R ist, das I_0 enthält. Für ein Ideal $I_0 \subset I \subset R$ ist I/I_0 in R/I_0 maximales (bzw. Prim-) Ideal genau dann, wenn $(R/I_0)/(I/I_0)$ ein Körper (bzw. ein Integritätsbereich) ist. Dies ist äquivalent dazu, dass R/I ein Körper (bzw. ein Integritätsbereich) ist wegen des Isomorphismus aus ii. Dies ist wieder äquivalent dazu, dass I in R ein maximales (bzw. Prim-) Ideal ist, was zu zeigen war.

iv. Alle Ideale von $\mathbb{Z}/8\mathbb{Z}$ sind von der Form $I/8\mathbb{Z}$ wobei $I \subset \mathbb{Z}$ ein Ideal ist, das $8\mathbb{Z}$ enthält (siehe i). Da alle Ideale von $\mathbb{Z}$ Hauptideale sind, suchen wir $I = a\mathbb{Z} \subset 8\mathbb{Z}$, was äquivalent dazu ist, dass $a \mid 8$. Wir können annehmen, dass a positiv ist, da $-a\mathbb{Z} = a\mathbb{Z}$, und somit bleiben vier Möglichkeiten: $a \in \{1, 2, 4, 8\}$. Dies liefert 4 Ideale $\mathbb{Z}/8\mathbb{Z}$, $2\mathbb{Z}/8\mathbb{Z}$, $4\mathbb{Z}/8\mathbb{Z}$ and $8\mathbb{Z}/8\mathbb{Z} = (0)$.
Aus iii. wissen wir, dass das Ideal $I/8\mathbb{Z} \subset \mathbb{Z}/8\mathbb{Z}$ prim bzw. maximal ist, genau dann wenn $I \subset \mathbb{Z}$ prim bzw. maximal ist. Es folgt:

- Das Ideal $2\mathbb{Z} \subset \mathbb{Z}$ ist ein Primideal und maximal, also ist $2\mathbb{Z}/8\mathbb{Z} \subset \mathbb{Z}/8\mathbb{Z}$ ein Primideal und maximal.

- Die Ideale $\mathbb{Z}, 4\mathbb{Z}, 8\mathbb{Z} \subset \mathbb{Z}$ sind weder maximal noch Primideale, also sind die Ideale $\mathbb{Z}/8\mathbb{Z}, 4\mathbb{Z}/8\mathbb{Z}, (0) \subset \mathbb{Z}/8\mathbb{Z}$ weder maximal noch Primideale.

6. Sei R ein kommutativer Ring. Ein Element $x \in R$ heisst *nilpotent*, falls ein $n \geqslant 1$ mit $x^n = 0$ existiert.

   (a) Beweisen oder widerlegen Sie: Die Menge der Nullteiler von R zusammen mit 0 ist ein Ideal von R.

   (b) Beweisen oder widerlegen Sie: Die Menge I der nilpotenten Elemente von R ist ein Ideal von R.

   (c) Beweisen Sie: Für I wie in (b) enthält der Faktorring R/I ausser 0 keine nilpotenten Elemente.

   Lösung:

   (a) Sei $R = \mathbb{Z}/6\mathbb{Z}$. Dann sind 2 und 3 Nullteiler, da $2 \cdot 3 = 0$, aber $2 + 3 = 5$ ist eine Einheit, da $5 \cdot 5 = 25 \equiv 1 \mod 6$, und somit kein Nullteiler, das heisst die Menge der Nullteiler ist kein Ideal.

   (b) Offensichtlich ist 0 nilpotent, d.h. $0 \in I$. Seien nun $a \in I$, d.h. a ist nilpotent mit $a^n = 0$, und $r \in R$ beliebig. Da R kommutativ ist, ist $(ar)^n = a^n r^n = 0r = 0$, und somit ist $ar \in I$.

   Seien nun $a, b \in I$ mit $a^n = 0$ und $b^m = 0$. Da R kommutativ ist, gilt für alle $l \in \mathbb{N}$, dass
   $$(a+b)^l = \sum_{i=0}^{l} \binom{l}{i} a^i b^{l-i}$$
   (siehe Vorlesung). Ist nun $l \geqslant 2\max\{n, m\}$, dann ist für jedes $i = 0, \ldots, l$ entweder $i \geqslant \max\{n, m\} \geqslant n$ oder $l - i \geqslant \max\{n, m\} \geqslant m$, und folglich $a^i = 0$ oder $b^{l-i} = 0$ und damit $(a+b)^l = 0$.

   Wir haben gezeigt, dass I ein Ideal in R ist.

   (c) Angenommen es existiert $x \in R$, so dass $x + I \in R/I$ nilpotent ist. Das bedeutet es existiert $n \in \mathbb{N}$ mit $(x + I)^n = 0 + I = I$. In anderen Worten, $x^n + I = I$ oder auch $x^n \in I$. Dies bedeutet, dass x^n nilpotent in R ist und damit existiert $m \in \mathbb{N}$ mit $(x^n)^m = 0$. Damit folgt $x^{nm} = (x^n)^m = 0$ und somit $x \in I$, und damit $x + I = 0 + I$.