Karlsruher Institut für Technologie
Institut für Algebra und Geometrie
PD Dr. Stefan Kühnlein Dipl.-Math. Jochen Schröder

Einführung in Algebra und Zahlentheorie – Übungsblatt 11 – Musterlösung

Aufgabe 1 (4 Punkte)

a) Seien R ein Hauptidealring und $Q = \mathrm{Quot}(R)$ sein Quotientenkörper. Weiterhin seien $f \in R[X]$ ein normiertes Polynom und $q \in Q$ eine Nullstelle von f. Zeige, dass q bereits in R liegt.[1]

b) Zeige mit Hilfe von Aufgabenteil a), dass $\sqrt{3}$ irrational ist.

Lösung: Korrektur In der ersten Version fehlte das Wort „normiert“ in Aufgabenteil a). Dann ist die Aussage natürlich falsch, denn $\frac{1}{2}$ ist eine Nullstelle von $2X - 1 \in \mathbb{Z}[X]$.

a) Sei $f = X^n + \sum_{i=0}^{n-1} a_i X^i \in R[X]$ mit Nullstelle $\frac{p}{q}$ mit „Zähler“ p und „Nenner“ q aus R.
Im Hauptidealring können wir uns den Bruch vollständig gekürzt wünschen, denn wir haben eine eindeutige Primzerlegung von Zähler und Nenner.
Also gilt $\frac{p^n}{q^n} + \sum_{i=0}^{n-1} a_i \frac{p^i}{q^i} = 0$ und wir multiplizieren die Gleichung mit q^n und erhalten:
$0 = p^n + \sum_{i=0}^{n-1} a_i p^i q^{n-i} = p^n + q \cdot (\sum_{i=0}^{n-1} a_i p^i q^{n-i-1}) \Rightarrow p^n = p \cdot (-\sum_{i=0}^{n-1} a_i p^i q^{n-i-1})$.
Also ist q ein Teiler von p^n und wegen der Teilerfremdheit ist also $q \in R^\times$ und damit $\frac{p}{q} = pq^{-1} \in R$.

b) $\sqrt{3}$ ist eine Nullstelle von $X^2 - 3 \in \mathbb{Z}[X]$. Wäre $\sqrt{3} \in \mathbb{Q}$, so wäre nach a) sogar $\sqrt{3} \in \mathbb{Z}$, aber wegen $|1|^2 < 3 < |2|^2$ kann das nicht sein.

Aufgabe 2 (4 Punkte)
Seien $R \neq \{0\}$ ein kommutativer Ring und $I \subseteq R$ ein Ideal.[2] Zeige die folgenden Aussagen:

a) I ist genau dann ein Primideal, wenn R/I nullteilerfrei ist.

b) I ist genau dann ein maximales Ideal, wenn R/I ein Körper ist.

Folgere, dass jedes maximale Ideal ein Primideal ist, und finde ein Beispiel dafür, dass die andere Richtung nicht gilt.

Lösung: In beiden Aufgabenteilen a) und b) können wir uns auf $I \subsetneq R$ beschränken, denn $I = R$ erfüllt keine der vier Bedingungen. Dann ist stets $R/I \neq \{0\}$ ein kommutativer Ring.
Beachte: Es ist $0_{R/I} = 0 + I$ und für $r \in R$ gilt $r + I = 0 + I \Leftrightarrow r \in I$.
Seien stets $a, b \in R$:

a) „$\Rightarrow$:“ Sei $(a + I)(b + I) = (0 + I), a + I \neq 0$. Zu zeigen ist $b + I \overset{(!)}{=} 0 + I$.
Wegen $(a + I)(b + I) = ab + I$ ist $ab + I = 0 + I$, also $ab \in I$, und desweiteren $a \notin I$ wegen $a + I \neq 0 + I$. Dann ist $b \in I$, denn I ist ein Primideal, also ist $b + I = 0 + I$.

[1] Man sagt, R ist in Q *ganz abgeschlossen*.

[2] Die Aussage ist auch richtig für $R = \{0\}$. Dann gibt es keine Primideale und keine maximalen Ideale und alle Faktorringe sind weder nullteilerfrei noch Körper – das ist ein recht langweiliger Fall.

„⇐:“ Sei $ab \in I$, $a \notin I$. Zu zeigen ist $b \overset{(!)}{\in} I$.
Wegen $ab \in I$ ist $0 + I = ab + I = (a + I)(b + I)$, aber $a + I \neq 0 + I$, denn $a \notin I$. Also ist $b + I = 0 + I$, denn R/I ist nullteilerfrei, also ist $b \in I$.

b) „⇒:“ Es reicht zu zeigen, dass jedes Element in R/I ungleich 0 invertierbar ist.
Sei $x + I \neq 0 + I$, also $x \notin I$. Dann aber ist $I \subsetneq I + \langle x \rangle$, also $I + \langle x \rangle = R$, denn I war ein maximales Ideal. Insbesondere ist $1 \in I + \langle x \rangle$, also $1 = i + rx$ für ein $i \in I$, $r \in R$. Damit aber ist
$1_{R/I} = 1 + I = (i + rx) + I = rx + I = (r + I)(x + I)$, also $(x + I)$ invertierbar in R/I.
„⇐:“ Sei $I \subsetneq J$ für ein Ideal J. Dann gibt es $x \in J \setminus I$ und wegen $x + I \neq 0 + I$ und da R/I ein Körper ist, ist $x + I$ invertierbar in R/I. Also gilt $1 + I = (x + I)(y + I) = xy + I$ für ein $y \in R$ und wir folgern $1 = xy + i$ für ein $i \in I \subseteq J$.
Wegen $x \in J$ ist $xy \in J$ und wegen $i \in J$ also $1 = xy + i \in J$, also $J = R$, was zu zeigen war.

Da jeder Körper insbesondere nullteilerfrei ist, ist die Folgerung offensichtlich:
Sei I ein maximales Ideal, dann ist R/I ein Körper, also R/I nullteilerfrei, also I ein Primideal.
Das Nullideal in $\mathbb{Z}$ ist ein Primideal – $\mathbb{Z}/\{0\} \cong \mathbb{Z}$ ist nullteilerfrei – aber nicht maximal, denn $\{0\} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$.

Aufgabe 3 (4 + 1 Punkte)
Die Menge R der stetigen reellwertigen Funktionen auf dem Intervall $[0, 1]$ wird zu einem Ring[3] durch

$$(f + g)(x) = f(x) + g(x) \text{ und } (f \cdot g)(x) = f(x) \cdot g(x) \text{ für alle } f, g \in R, x \in [0, 1].$$

Für $a \in [0, 1]$ definieren wir $I_a := \{f \in R : f(a) = 0\}$. Zeige die nachfolgenden Aussagen:

a) Für jedes $a \in [0, 1]$ ist I_a ein maximales Ideal von R.

b) Jedes Ideal $I \neq R$ ist in einem der I_a enthalten.

c) I_a wird nicht vom Polynom $X - a$ erzeugt.

d) Einen *Zusatzpunkt* erhältst du, wenn du zeigst, dass I_a kein Hauptideal ist.

Lösung: Vorüberlegung: Das Einselement ist die konstante Funktion E mit $E(x) = 1$ für alle $x \in [0, 1]$.
Die Einheiten des Rings sind diejenigen Abbildungen ohne Nullstellen:
Ist $f \in R^\times$ mit inverser Abbildung f^{-1}, so ist $1 = (f \cdot f^{-1})(x) = f(x) \cdot f^{-1}(x)$ für alle $x \in [0, 1]$, also $f(x) \neq 0$.
Andersrum definieren wir zu einer Abbildung f ohne Nullstellen die Abbildung f^{-1} durch $f^{-1}(x) = \frac{1}{f(x)}$ für alle $x \in [0, 1]$. f^{-1} ist nach Analysis 1 ebenfalls stetig, also in R, und nach Definition gilt $f \circ f^{-1} = E$.

a) Sei $a \in [0, 1]$ fest. Wir betrachten die Einsetzabbildung $\varphi_a \colon R \to \mathbb{R}, f \mapsto f(a)$. Die Ringstruktur von R ist gerade so gemacht (das wissen wir oder rechnen es nach...), dass φ_a ein Ringhomomorphismus ist. Der Kern ist I_a und als Kern ist I_a sicher ein Ideal.
Weiterhin ist φ_a surjektiv, denn die konstanten Funktionen sind in R enthalten.
Nach dem Homomorphiesatz ist dann $\mathbb{R} \cong R/I_a$ und damit R/I_a ein Körper und nach Aufgabe 3 ist I_a maximal.

Alternativ rechnen wir es eben doch einfach nach. Für $f, g \in I_a$ und $r \in R$ ist $(rf - g)(a) = r(a)f(a) - g(a) = 0$, also $rf - g \in I_a$ und weil $I_a \neq \emptyset$ (die Nullfunktion ist zum Beispiel enthalten) , ist I_a ein Ideal.
Sei nun $I \subsetneq J$, dann gibt es $h \in I \setminus J$. Es ist $h(a) \neq 0$ und damit $h(x)^2 + (|x - a|) > 0$ für alle $x \in [0, 1]$, also ist $h^2 + (x \mapsto |x - a|) \in J$ eine Einheit – also ist $J = R$ und damit I maximal.

[3] Das darf man glauben.

b) Sei I ein Ideal, das in keinem der I_a liegt. Dann finden wir für jedes $a \in [0,1]$ ein $f_a \in I$ mit $f_a(a) \neq 0$. Weil jedes f_a stetig ist, gibt es für jedes a eine (hinreichend kleine) Umgebung U_a von a (das ist ein Intervall U_a mit a im Inneren von U_a), so dass $f_a(x) \neq 0$ für alle $x \in U_a$.
Es ist $[0,1] = \bigcup_{a\in[0,1]} U_a$, aber – weil $[0,1]$ kompakt ist – sogar schon $[0,1] = \bigcup_{i=1}^{n} U_{a_i}$ für eine endliche Auswahl $a_1, ..., a_n \in [0,1]$.
Dann ist $f = \sum_{i=1}^{n} f_{a_i}^2 \in I$ nach Konstruktion eine Funktion ohne Nullstelle, denn für alle $x \in [0,1]$ ist $f_{a_i}^2(x) = (f_{a_i}(x))^2 \geq 0$ für alle $i = 1, ..., n$ und $(f_{a_{i_0}}(x))^2 > 0$ für dasjenige i_0 mit $x \in U_{a_{i_0}}$.
Also enthält nach der Vorüberlegung I eine Einheit und damit ist $I = R$ kein echtes Ideal.

c) Das folgt natürlich auch aus d), aber hier bringen wir ein anderes (einfacheres?) Argument.
In I_a liegt eine stetige Funktion, die in a nicht differenzierbar ist:

- Für $a \in (0,1)$ ist $x \mapsto |x - a|$ eine solche,
- für $a = 0$ ist $f(x) = x \cdot \cos(1/x)$ für $x \neq 0$ stetig ergänzt mit $f(0) = 0$ eine solche
- und analog für $a = 1$ die Abbildung gegeben durch $x \mapsto f(x - 1)$.

(**Nach der Übung...** habe ich mir noch sagen lassen, dass die stetige Wurzelfunktion $x \mapsto \sqrt{x}$ in 0 auch nicht differenzierbar ist. $x \mapsto \sqrt{1 - x}$ ist in 1 nicht differenzierbar. Das ist etwas einfacher als die beiden Funktionen oben. Danke für den Tipp!)
Wir zeigen, dass jedes $g \cdot (x - a) \in \langle x - a\rangle$ differenzierbar in a ist, dann folgt, dass $\langle x - a\rangle \subsetneq I_a$.
Die Differenzierbarkeit in a sehen wir über den Differenzenquotienten:
$\lim_{x\to a} \frac{g(x)(x-a)-g(a)(a-a)}{x-a} = \lim_{x\to a} g(x) = g(a)$, denn g ist stetig.
Also ist $\langle x - a\rangle \subsetneq I_a$ eine echte Teilmenge.

d) Ein allgemeines Argument sieht so aus:
Annahme: Sei $I_a = \langle f\rangle = \{gf : g \in R\}$ für ein $f \in R$. Dann gilt sicher $f(a) = 0$, aber auch $f(b) \neq 0$ für alle $b \in [0,1], b \neq a$ $(*)$: Wäre nämlich $f(b) = 0$ für ein $b \neq a$, so wäre b Nullstelle von allen $gf \in \langle f\rangle$, aber $x \mapsto x - a \in I_a$ hat keine weitere Nullstelle.

Es ist $\sqrt{|f|} \in I_a = \langle f\rangle$ ein Vielfaches von f, also $\sqrt{|f|} = g \cdot f$ für ein $g \in R$.
Also gilt $\sqrt{|f(x)|} = f(x)g(x)$ für alle $x \in [0,1]$ und wegen $(*)$ können wir $g(x) = \frac{\sqrt{|f(x)|}}{f(x)}$ für alle $x \in [0,1], x \neq a$ ausrechnen.
Aber wegen $\lim_{x\to a} \frac{\sqrt{|f(x)|}}{f(x)} = \infty$ gibt es keine solche stetige Funktion g.

Aufgabe 4 (4 Punkte) (*Irreduzibilitätskriterium von Eisenstein*)

a) Sei $f = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X], a_n \neq 0$ mit $\mathrm{ggT}(a_0, ..., a_n) = 1$. Sei weiterhin $p \in \mathbb{P}$ eine Primzahl, so dass $p \mid a_i$ für alle $i = 0, ..., n-1$, aber $p^2 \nmid a_0$. Zeige, dass f in $\mathbb{Z}[X]$ irreduzibel ist.
(*Bemerkung:* $\mathbb{Z}$ kann hierbei durch jeden Hauptidealring ersetzt werden, wenn wir den Begriff „Primzahl“ durch „Primelement“ ersetzen. Man kann die Aussage dann genauso beweisen.)

b) Finde ein irreduzibles Polynom vom Grad 42 in $\mathbb{Z}[X]$.

Lösung

a) Sei $f = gh$ mit $g = \sum_{i=0}^{k} b_i X^i, h = \sum_{i=0}^{m} c_i X^i$ mit $b_k, c_m \neq 0$. Dann gilt:
$p|a_0 = b_0 c_0$ und da p prim ist, gilt $p|b_0$ oder $p|c_0$. Aber wegen $p^2 \nmid b_0 c_0$ kann p nicht beides teilen:
Ohne Einschränkung gelte $p|b_0, b \nmid c_0$. Wegen $p \nmid a_n = b_k c_m$ gilt aber $p \nmid b_k$.
Also gibt es ein minimales $i_0 \in 1, ..., k$, so dass $p|b_0$, ..., $p|b_{i_0-1}$, aber $p \nmid b_{i_0}$.

Nun gilt $a_{i_0} = \sum_{j=0}^{i_0} b_j c_{i_0-j} \equiv b_{i_0} c_0$ modulo p. Aber $p \nmid b_{i_0} c_0$, denn $p \nmid c_0$, $p \nmid b_{i_0}$ und p ist prim.
Da p ein Teiler von $a_0, ..., a_{n-1}$ ist, folgt $i_0 = n$, was nur möglich ist für $k = n$ und die Gradformel der Polynom-Multiplikation verrät $m = 0$, also ist $h = c_0$ konstant.
Aber wegen $c_0 | a_i$ für alle i und wegen $\text{ggT}(a_0, ..., a_n) = 1$, muss c_o eine Einheit in R, also $h \in R[X]^\times$ sein. Das war zu zeigen.

b) $X^{42} - 7$ ist irreduzibel, denn für $p = 7$ kann das Eisensteinkriterium angewendet werden.