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

Einführung in Algebra und Zahlentheorie – Übungsblatt 10[1]

Aufgabe 1 (4 Punkte)
Sei R ein kommutativer Ring mit genau drei Assoziiertenklassen. Zeige:

a) R besitzt genau ein Ideal m mit $m \neq R, m \neq \{0\}$.

b) R/m ist ein Körper.

c) Für jedes $x \in m$ gilt $x^2 = 0$.

Lösung Aufgabe 1

a) 0 und $R^\times$ sind stets Assoziiertenklassen. Da alle Assoziiertenklassen eine disjunkte Zerlegung von R sind (Äquivalenzklassen!), ist $T := R \setminus (R^\times \cup \{0\})$ (die Menge aller nichttrivialen Nichteinheiten) die dritte Assoziiertenklasse. Insbesondere ist R kein Körper, denn T ist nicht leer. (Es gibt genau zwei Assoziiertenklassen, wenn R ein Körper ist.)
Existenz: Für ein $x \in T$ ist das von x erzeugte Ideal $\langle x \rangle = Rx \notin \{0, R\}$, wir haben also ein drittes Ideal gefunden.

Eindeutigkeit: Sei nun $m \neq R, 0$ ein Ideal. Wir zeigen $m \overset{(!)}{=} T \cup \{0\} = R \setminus R^\times$, dann sind wir fertig. Sicher enthält m wegen $m \neq R$ keine Einheit, also gilt „$\subseteq$“.
Desweiteren enthält m mindestens ein Element $x_0 \in T$, denn $m \neq 0$. Jedes $t \in T$, $t \neq 0$ ist assoziiert zu x_0, also $t = rx_0$ für ein $r \in R^\times$ und wegen $Rm \subseteq m$ ist $t \in m$. Da $0 \in m$ sowieso klar ist, gilt auch „$\supseteq$“.

b) **Vorbemerkung:** Da hier schon einmal die lange Lösung stand, werde ich diese gerne stehenlassen. Mein Beweis gilt bereits mit einer schwächeren Voraussetzung, nämlich wenn m ein sogenanntes *maximales Ideal* ist, ein Ideal $m \neq R$, so dass kein Ideal I echt zwischen m und R passt. Das Ideal m aus der Aufgabe erfüllt dies sicher, es gibt aber viele weitere: Zum Beispiel ist jedes $p\mathbb{Z}$ in $\mathbb{Z}$ ein maximales Ideal, wobei $\mathbb{Z}$ sicher nicht die Voraussetzung an R aus der Aufgabe erfüllt.
In unserem Fall geht der Beweis direkter, wie dankenswerterweise in der Übung angemerkt wurde.

R/m ist kommutativ und es reicht, für jedes $\overline{x} \neq 0$ ein Inverses zu finden.
Die „komplizierte“ Übungsleiterlösung (siehe Vorspann) geht so:
$\overline{x} \neq 0 \Rightarrow x \notin m$ (das ist wohldefiniert!) und damit $m \subsetneq \langle m, x \rangle = m + Rx = \{m_0 + rx : m_0 \in m, r \in R\}$. Aber es gibt nur ein Ideal größer als m, also $m + Rx = R$, insbesondere ist 1 von der Form $1 = m_0 + rx$ für passende m_0, r. Dann aber ist $\overline{r} \cdot \overline{x} = \overline{1}$ in R/m, also x invertierbar.

Die kurze Lösung der schlauen Studenten geht so:
$x \notin m$, dann ist $x \in R^\times$ (Das gilt aber wirklich nur hier wegen der speziellen Form von m!), also gibt es ein Inverses $x^{-1} \in R$ und $\overline{x^{-1}}$ ist das Inverse in R/m. Fertig.

c) Ohne Einschränkung sei $x \neq 0$, also $x \in T$. x^2 ist in einer der Assoziiertenklassen enthalten. Es gilt:

- $x^2 \notin R^\times$, denn das Produkt zweier Nichteinheiten ist niemals eine Einheit.
  (Wären y, z keine Einheiten, aber yz eine Einheit mit Inversem $(yz)^{-1}$, so wäre $y \cdot (z \cdot yz^{-1}) = 1$, y also doch eine Einheit. WIDERSPRUCH)
- **Annahme:** $x^2 \in T$. Dann sind x, x^2 assoziiert, also $x = rx^2 \Rightarrow 0 = rx^2 - x = x(rx - 1)$ für eine Einheit $r \in R$. Da x weder 0 noch eine Einheit war, sind beide Faktoren $x, rx - 1 \neq 0$, also echte Nullteiler, insbesondere kann auch $rx - 1$ keine Einheit sein, also $rx - 1 \in T$, wiederum assoziiert zu x.
  Also gibt es eine weitere Einheit s mit $sx = rx - 1 \Rightarrow 1 = rx - sx = (r - s)x$ und x war eben doch eine Einheit. WIDERSPRUCH

$x^2 \notin R^\times, x^2 \notin T \Rightarrow x^2 = 0$.

[1] Auf diesem Übungsblatt gibt es bis zu 17 Punkte zu holen. Warum nicht?

Aufgabe 2 (4 Punkte) **(Neufassung)**
Sei $R \subseteq \mathbb{C}$ ein Teilring von $\mathbb{C}$ und $|\cdot| : \mathbb{C} \to \mathbb{R}_{\geq 0}$ der Standardbetrag von $\mathbb{C}$.
Zeige, dass R genau dann eine Division mit Rest bezüglich $|\cdot|^2$ besitzt[2], wenn folgende Eigenschaft gilt:
Für alle $x \in R, y \in R \setminus \{0\}$ gibt es ein $z \in R$ mit $|\frac{x}{y} - z| < 1$.
(*Hinweis:* Wiederhole das geometrische Argument für den Ring $\mathbb{Z}[i]$ aus der Vorlesung.)

Wegen $|x|^2 = 0 \Leftrightarrow x = 0$ ist R dann also euklidisch nach Definition, wenn zusätzlich das Bild von R unter $|\cdot|^2$ eine Teilmenge von $\mathbb{N}_0$ ist.

Seien $a_1 = \sqrt{3}, a_2 = \sqrt{3}i, a_3 = \frac{-1+\sqrt{3}i}{2}$. Für $j = 1, 2, 3$ sei $R_j = \mathbb{Z}[a_j]$ der kleinste Teilring von $\mathbb{C}$, der $\mathbb{Z}$ und a_j umfasst.
Zeige jeweils, dass jedes Element in R_j eindeutig als $x + ya_j$, $x, y \in \mathbb{Z}$ dargestellt werden kann.
Beweise oder widerlege jeweils, ob der Ring R_j eine Division mit Rest bezüglich $|\cdot|^2$ besitzt und ob er euklidisch ist.

Lösung Aufgabe 2
Vorbemerkung: In der alten Fassung der Aufgabe wurde die Bedingung für einen euklischen Ring vergessen, dass $|\cdot|^2$ jeweils in $\mathbb{N}_0$ landet. Um den euklidischen Algorithmus zu benutzen, benötigen wir, dass die absteigende Kette der Restbeträge schließlich 0 wird. Der Ring R_1 ist ein Beispiel, in dem wir mit Rest teilen können, in dem die Bedingung, dass die Reste betragsmäßig kleiner werden, aber nicht ausreichend für den euklidischen Algorithmus ist.

Seien $x, y \in R$, $y \neq 0$ beliebig.
x ist durch y mit Rest teilbar $\Leftrightarrow$ es gibt $z \in R$: $x = zy + r$ mit einem Rest r mit $|r|^2 < |y|^2 \overset{r=x-zy}{\Leftrightarrow}$ es gibt $z \in R$: $|x - zy|^2 < |y|^2 \Leftrightarrow$ es gibt $z \in R$: $|x - zy| < |y| \overset{\cdot|\frac{1}{y}|}{\Leftrightarrow}$ es gibt $z \in R$ $|\frac{x}{y} - z| < 1$.
Da R eine Division mit Rest besitzt, wenn die Aussage für alle x, y, $y \neq 0$ gilt, folgt die Behauptung.
(Ein solches geometrisch gefundenes z ist also ein geeigneter Koeffizient vor y beim Teilen mit Rest.)

Nun zeigen wir, dass die Elemente aus R_j eindeutig von der gegebenen Form sind. Wir haben diese Argumentation in ähnlicher Form früher schon gesehen. (Könnte das klausurrelevant sein, wenn es mehrfach auftritt? Zumindest die Argumentation zu verstehen, sollte wichtig sein!)
Klar: Für $j = 1, 2, 3$ gilt jeweils, dass alle $x + ya_j \in R_j$ sein müssen, denn R_j ist abgeschlossen unter Multiplikation und Addition. Dies zeigt jeweils $\{x + ya_j : x, y \in \mathbb{Z}\} \subseteq R_j$.
Da R_j der kleinste Ring ist, der $\mathbb{Z}$ und a_j umfasst, reicht es, zu zeigen, dass die links Seite bereits ein Ring ist (der dann offensichtlich $\mathbb{Z}$ und a_j umfasst), dann folgt automatisch $\supseteq$. Es gilt:
$0, 1$ sind in der linken Seite enthalten, die Summe zweier Elemente ist wieder in der linken Seite enthalten und es verbleibt zu zeigen, dass die Menge multiplikativ abgeschlossen sind:
$j = 1$: $(a + b\sqrt{3})(c + d\sqrt{3}) = ac + 3bd + (ad + bc)\sqrt{3} \in R_1$.
$j = 2$: $(a + b\sqrt{3}i)(c + d\sqrt{3}i) = ac - 3bd + (ad + bc)\sqrt{3}i \in R_2$.
$j = 3$: Schreibe $\zeta := \frac{-1+\sqrt{3}i}{2}$ und rechne nach: $\zeta^2 = -\zeta - 1$. Dann ist
$(a + b\zeta)(c + d\zeta) = ac + (ad + bc)\zeta + bd\zeta^2 = ac - bd + (ad + bc - bd)\zeta \in R_3$.

Es verbleibt die Eindeutigkeit der Darstellung, aber auch dieses Argument haben wir bereits gesehen und können es für $j = 1, 2, 3$ zeitgleich durchführen:
Sei $x + ya_j = x' + y'a_j$, so sind die Darstellungen sicher gleich, falls $y = y'$. Für $y \neq y'$ aber wäre $a_j = \frac{x-x'}{y'-y} \in \mathbb{Q}$, aber $a_j \notin \mathbb{Q}$. (Die letzte Aussage ist klar für die nicht-reellen Zahlen a_2, a_3, für $\sqrt{3}$ glauben wir dies...)

Nun testen wir, welcher der Ringe eine Division mit Rest haben. Dafür untersuchen wir für jedes R_j die Brüche $\frac{x}{y}$, $x, y \in R_j, y \neq 0$, die im Allgemeinen nicht in R_j liegen. Gibt es für jeden Bruch ein hinreichend nahes $z \in R_j$? Hinreichend nah bedeute dabei stets Abstand echtkleiner 1.
(**Achtung:** Dies ist sicher der Fall, wenn wir für jedes $c \in \mathbb{C}$ ein hinreichend nahes z finden, siehe R_3 und $\mathbb{Z}[i]$ aus der Vorlesung. Dies ist aber kein notwendiges Kriterium, wie etwa R_1 zeigt.)

[2]das heißt, für $x, y \in R, y \neq 0$ gibt es z, so dass $x = zy + r$ mit einem r mit $|r|^2 < |y|^2$

- Es gilt $R_1 \subseteq \mathbb{R}$. Damit aber ist auch jeder Quotient $\frac{x}{y} \in \mathbb{R}$, also insbesondere die Gaußklammer $z = [\frac{x}{y}]$ ein geeignetes $z \in R_1$.
  R_1 besitzt also Division mit Rest für $|\cdot|^2$, ist aber wegen $|1+\sqrt{3}|^2 \notin \mathbb{N}_0$ nicht euklidisch.

- Hier hilft es, sich R_2 geometrisch als Gitterpunkte in der komplexen Ebene aufzuzeichnen. Die Punkte sind Rechteck-Ecken von Rechtecken mit Seitenlänge 1 und $\sqrt{3}$. Der maximale Abstand eines beliebigen Punktes in $\mathbb{C}$ zu R_2 tritt auf, wenn wir einen Rechteckmittelpunkt wählen, dieser hat dann Abstand $\frac{1}{2}^2 + \frac{\sqrt{3}}{2}^2 = 1$.
  R_2 besitzt also genau dann eine Division mit Rest bezüglich $|\cdot|^2$, wenn kein Rechteckmittelpunkt als Bruch auftritt, aber für $x = 1+\sqrt{3}i$, $y = 2$ ist $\frac{x}{y}$ ein Mittelpunkt und wir finden kein z mit Abstand < 1 von $\frac{x}{y}$ in R_2.
  Insbesondere ist der Ring auch nicht euklidisch.

- Für R_3 können wir wieder die stärkere Aussage zeigen, dass wir für jedes $c \in \mathbb{Z}$ ein $z \in R_3$ finden, so dass $|c - z| < 1$ ist. Dazu betrachten wir wieder R_3 als Gitterpunkte in der Ebene.
  Eine *Grundmasche* des Gitters ist das Parallelogramm mit den Ecken 0, 1, ζ, $\zeta+1$. Die Seitenlängen des Parallelogramms sind 1.
  Gibt es für jedes Punkt innerhalb dieser Grundmasche eine Ecke (dies sind ja die Elemente aus R_3) z, die hinreichend nah ist, so gibt es für jeden Punkt $c \in \mathbb{C}$ ein solches $z \in R_3$.
  Wir verbinden 0 und $\zeta + 1$ durch eine Linie l, die das Parallelogramm in drei Abschnitte aufteilt: Zwei halboffene Dreiecke (ohne l) und l selbst. (Das sollte man sich aufmalen!)
  Jeder Punkt im Dreieck oben links ist hinreichend nahe an ζ, jeder Punkt im Dreieck unten rechts ist hinreichend nah an 1. Da l Länge 1 hat (nachrechnen), ist jeder Punkt von l hinreichend nah an einem der beiden Endpunkte 0 oder $1 + \zeta$.
  R_3 besitzt also eine Division mit Rest und ist sogar euklidisch, denn für beliebiges $a + b\zeta$ gilt:
  $|a+b\frac{-1+\sqrt{3}i}{2}|^2 = (a-\frac{b}{2})^2+(\frac{b\sqrt{3}}{2})^2 = a^2+ab+\frac{b^2}{4}+\frac{3b^2}{4} = a^2-ab+b^2 \in \mathbb{Z}$ und da das Betragsquadrat nichtnegativ ist sogar $\in \mathbb{N}_0$.

Aufgabe 3 (3 Punkte)
Zeige, dass für einen Körper K der Ring $K[[X]]$ der formalen Potenzreihen[3] ein euklidischer Ring ist.

Lösung Aufgabe 3
Für $f = \sum_{i=0}^{\infty} a_i X^i \neq 0$ definieren wir den Untergrad $\mathrm{Ug}(f) = \min(i \geq 0 : a_j = 0 \text{ für alle } j < i\}$. Es gilt also $\sum_{i=0}^{\infty} a_i X^i = \sum_{i=\mathrm{Ug(f)}}^{\infty} a_i X^i$.
Behauptung: $\gamma(f) = \mathrm{Ug} + 1$, falls $f \neq 0$, $\gamma(0) = 0$ ist eine euklidische Funktion.
Erinnerung an Blatt 8: Einheiten in $K[[X]]$ sind die $\sum_{i=0}^{\infty} a_i X^i$ mit $a_0 \in K^\times$, also $a_0 \neq 0$.
Sei nun $f = \sum_{i=\mathrm{Ug(f)}}^{\infty} a_i X^i \neq 0$. Dann ist $f = \sum_{i=\mathrm{Ug(f)}}^{\infty} a_i X^i = X^{\mathrm{Ug}} \cdot \sum_{i=0}^{\infty} a_{\mathrm{Ug(f)}+i} X^i \sim X^{\mathrm{Ug}}$. $(*)$
Seien nun f und $g \neq 0$ beliebige Potenzreihen, wir müssen zeigen, dass wir f durch g mit Rest teilen können. Offensichtlich reicht es $f \neq 0$ und $\mathrm{Ug}(f) \geq \mathrm{Ug}(g)$ zu betrachten.
Nach $(*)$ sind $f = X^{\mathrm{Ug}(f)} \cdot f_1, g = X^{\mathrm{Ug}(g)} \cdot g_1$, mit Einheiten f_1, g_1 und wir sehen, dass
$f = g \cdot X^{\mathrm{Ug}(f)-\mathrm{Ug}(g)} \cdot g_1^{-1} \cdot f_1 + 0$.

Nachtrag: Der euklidische Algorithmus ist hier also stets nach spätestens einem Schritt fertig, der ggT zweier nichttrivialer Potenzreihen ist einfach die Potenzreihe mit kleinerem Untergrad.

Aufgabe 4 (3 Punkte)
Erinnerung: $\mathbb{R}[X]$ ist euklidisch bezüglich γ mit $\gamma(0) = 0$, $\gamma(f) = \mathrm{Grad}(f) + 1$ für $f \neq 0$.
Bestimme mit Hilfe des euklidischen Algorithmus einen größten gemeinsamen Teiler der Polynome

$$X^3 - 2X^2 - X + 2 \text{ und } X^3 - 4X^2 + 3X \in \mathbb{R}[X]$$

und stelle den ggT als Linearkombination der beiden Polynome dar.

Lösung Aufgabe 4:
$(X^3 - 2X^2 - X + 2) : (X^3 - 4X^2 + 3X) = 1$ mit Rest $2X^2 - 4X + 2$,
also ist $(X^3 - 2X^2 - X + 2) = 1 \cdot (X^3 - 4X^2 + 3X) + (2X^2 - 4X + 2)$ (i).

$(X^3 - 4X^2 + 3X) : (2X^2 - 4X + 2) = \frac{1}{2}X - 1$ mit Rest $-2X + 2$,
also ist $(X^3 - 4X^2 + 3X) = (\frac{1}{2}X - 1) \cdot (2X^2 - 4X + 2) + (-2X + 2)$ (ii).

$(2X^2 - 4X^2 + 3X) : (-2X + 2) = -X + 1$ mit Rest 0.

Ein ggT ist $-2X + 2$. Da -2 eine Einheit ist, ist auch $X - 1$ ein ggT, dies ist der naheliegende Vertreter der Assoziationsklasse aller ggTs.

Wie im 'normalen' Fall können wir eine Linearkombination des ggT erhalten, indem wir rückwärts rechnen und dabei die Gleichungen (i) und (ii) benutzen:
$-2X + 2 = (X^3 - 4X^2 + 3X) - (\frac{1}{2}X - 1)(2X^2 - 4X + 2) = (X^3 - 4X^2 + 3X) - (\frac{1}{2}X - 1)((X^3 - 2X^2 - X + 2) - (X^3 - 4X + 3X)) = \frac{1}{2}X(X^3 - 4X^2 + 3X) - (\frac{1}{2}X - 1)(X^3 - 2X^2 - X + 2)$.
Eine Linearkombination von $X-1$ erhalten wir, indem wir die Gleichung beidseitig mit $-\frac{1}{2}$ multiplizieren.

[3] Vergleiche Übungsblatt 8!

Aufgabe 5 (3 Punkte)
Zeige, dass ein Polynom $f \in \mathbb{C}[X]$ genau dann eine doppelte Nullstelle besitzt, wenn f und die Ableitung f' nicht teilerfremd sind.
(*Hinweis:* Benutze, dass in $\mathbb{C}$ jedes nichtkonstante Polynom in Linearfaktoren zerfällt, und die Produktregel, die du aus der Analysis 1 kennst.)

Lösung Aufgabe 5
Für zwei Polynome $f, g \neq 0$ gilt über $\mathbb{C}[X]$:

f, g sind nicht teilerfremd $\Leftrightarrow$ es gibt Polynom h vom Grad ≥ 2: $h|f$ und $h|g \overset{(!)}{\Leftrightarrow}$ es gibt Linearfaktor $(X-a)$: $(X-a)|f, (X-a)|g \Leftrightarrow f, g$ haben gemeinsame Nullstelle in $\mathbb{C}$.
Für die spannende Richtung $\Rightarrow$ unter dem (!) benutzen wir dabei, dass h in Linearfaktoren zerfällt und jeder Teiler von h ein Teiler von f und von g ist.

Wir müssen also zeigen, dass f genau dann eine doppelte Nullstelle besitzt, wenn f und f' eine gemeinsame Nullstelle haben. Die Aussage ist klar, wenn f konstant oder linear ist, insbesondere auch für $f = 0$.
Sei also f ein beliebiges Polynom vom Grad $n \geq 2$. Wir faktorisieren $f = \prod_{i=1}^{n} (X - a_i)$. Dann ist f' nach der Produktregel $\sum_{j=1}^{n} \prod_{i=1, i\neq j}^{n} (X - a_i)$.

Besitzt f eine doppelte Nullstelle, also ohne Einschränkung $a_1 = a_2$, so ist der Linearfaktor $(X - a_1)$ in jedem Summanden mindestens einmal vorhanden, kann also ausgeklammert werden. f' und f besitzen also die gemeinsame Nullstelle a_1, also sind f und f' nicht teilerfremd. Dies zeigt „$\Rightarrow$“.

Haben nun f, f' eine gemeinsame Nullstelle. Eine solche ist eine Nullstelle von f. Ohne Einschränkung sei a_1 eine gemeinsame Nullstelle.
Wir betrachten jeden Summanden von $\sum_{j=1}^{n} \prod_{i=1, i\neq j}^{n} (X - a_i)$ ausgewertet an der Stelle a_1. Für $j \neq 1$ ist das hintere Produkt 0, enthält es doch den Faktor $a_1 - a_1$. Also ist
$0 = f'(a_1) = \sum_{j=1}^{n} \prod_{i=1, i\neq j}^{n} (a_1 - a_i) = \prod_{i=1, i\neq 1}^{n} (a_1 - a_i)$, also ist einer der Linearfaktoren des letzten Produktes 0 und damit $a_1 \in \{a_2, ..., a_n\}$. Also ist a_1 doppele Nullstelle von f, womit „$\Leftarrow$“ gezeigt wäre.