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

Einführung in Algebra und Zahlentheorie – Übungsblatt 8

Aufgabe 1 (3 Punkte)
Sei R ein Integritätsbereich[1]. Zeige die Äquivalenz der folgenden Aussagen:

(i) R ist ein Körper.

(ii) R besitzt genau zwei Ideale.

(iii) R besitzt nur endlich viele Ideale.

Folgere, dass jeder endliche Integritätsbereich ein Körper ist.
Lösung:
„$(i) \Rightarrow (ii)$“: $\{0\} \neq R$ sind zwei verschiedene Ideale. Dies sind alle, denn:
Ist $I \neq \{0\}$ ein Ideal, so gibt es $x \in I$, $x \neq 0$, also ist $x \in R^\times$, denn R ist ein Körper.
Dann ist $r = (rx^{-1})x \in R \cdot I \subseteq I$ für alle $r \in R$, also $R = I$.
„$(ii) \Rightarrow (iii)$“: Das glauben wir!
„$(iii) \Rightarrow (i)$“: Da $R \neq \{0\}$ kommutativ ist, reicht es zu zeigen, dass alle $x \neq 0$ invertierbar sind.
Sei $x \neq 0$. Für $n \in \mathbb{N}$ sei I_n das von x^n erzeugte Ideal, also $I_n = x^n \cdot R$.
Da es nur endlich viele Ideale gibt, ist $I_j = I_k$ für passende $j < k$. Insbesondere ist dann $x^j \in I_k = I_j$, also $x^j = x^k \cdot r$ für ein $r \in R$. Umstellen ergibt

$$0 = x^k \cdot r - x^j = x^j \cdot (x^{k-j} \cdot r - 1).$$

Wegen der Nullteilerfreiheit ist zunächst $x^j \neq 0$ und dann $x^{k-j} \cdot r - 1 = 0$. Erneut Umstellen und Ausklammern von x ergibt

$$x(x^{k-j-1} \cdot r) = 1$$

und wir haben das Inverse von x gefunden.

Die Folgerung ist offensichtlich, denn ein endlicher Integritätsbereich enthält nur endlich viele Teilmengen, also erst Recht nur endliche viele Ideale, also gilt (iii) und damit (i).

Aufgabe 2 (4 Punkte)
Sei $\mathbb{Z}[\sqrt{2}]$ der kleinste Teilring von $\mathbb{R}$, der $\mathbb{Z}$ und $\sqrt{2}$ enthält. Zeige die nachfolgenden Aussagen:

a) $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$.

b) Die Abbildung $N : (\mathbb{Z}[\sqrt{2}], \cdot) \to (\mathbb{Z}, \cdot)$, $a + b\sqrt{2} \mapsto a^2 - 2b^2$ ist ein Monoid-Homomorphismus.

c) $a + b\sqrt{2}$ ist genau dann in $\mathbb{Z}[\sqrt{2}]^\times$, wenn $a^2 - 2b^2 \in \{\pm 1\}$. Bestimme das Inverse von $7 + 5\sqrt{2}$.

d) Es gibt unendlich viele Einheiten in $\mathbb{Z}[\sqrt{2}]$.

Lösung:

[1] Insbesondere ist dann $R \neq \{0\}$.

a) Wegen der Abgeschlossenheit ist jedes Element der Form $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, das zeigt „⊇“.
„⊆“: Es reicht zu zeigen, dass $H := \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ ein Ring ist (!), dann sind wir fertig, denn dann ist H ein Ring, der $\mathbb{Z}$ und $\sqrt{2}$ enthält, und darum gilt „⊆“, denn $\mathbb{Z}[\sqrt{2}]$ ist minimal mit dieser Eigenschaft.
Die meisten Ringaxiome vererben sich von $\mathbb{R}$ – Kommutativität von +, Assoziativität von + und · und die Distributivgesetze. Seien nun $a + b\sqrt{2}, c + d\sqrt{2} \in H$ beliebig.
Das Einselement $1 = 1 + 0\sqrt{2} \in H$, insbesondere ist H nicht leer. Außerdem ist
$(a + b\sqrt{2}) - (c + d\sqrt{2}) = (a - c) + (b - d) \in H$. Damit ist H eine Gruppe.
Weiterhin ist $(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = ac + 2bd + (ad + bc)\sqrt{2} \in H$ und wegen $1 \in H$ ist $(H, \cdot)$ ein Monoid.

b) Zunächst ist $a^2 + 2b^2 \in \mathbb{Z}$, also N wohldefiniert.
Wir berechnen $N(1) = N(1 + 0\sqrt{2}) = 1$. (Das sollte man bei Monoidhomomorphismen nicht vergessen!)
Für $a + b\sqrt{2}, c + d\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ gilt
$N((a + b\sqrt{2}) \cdot (c + d\sqrt{2})) = N(ac + 2bd + (ad + bc)\sqrt{2}) = (ac + 2bd)^2 - 2(ad + bc)^2 = a^2c^2 + 4abcd + 4b^2d^2 - 2a^2d^2 - 4abcd - 2b^2c^2 = a^2c^2 + 4b^2d^2 - 2a^2d^2 - 2b^2c^2$ und
$N(a+b\sqrt{2})\cdot N(c+d\sqrt{2}) = (a^2-2b^2)(c^2-2d^2) = a^2c^2-2a^2d^2-2b^2c^2+4b^2d^2$, was nach Umstellen die Behauptung zeigt.

c) Es ist $N(a + b\sqrt{2}) = a^2 - 2b^2 = (a + b\sqrt{2})(a - \sqrt{2})$.
Ist nun $a^2 - 2b^2 = \pm 1$, so ist $(a + b\sqrt{2})^{-1} = \pm a - b\sqrt{2}$, also $a + b\sqrt{2}$ eine Einheit.
Ist hingegen $a + b\sqrt{2}$ eine Einheit, so ist das Bild $N(a + b\sqrt{2}) = a^2 - 2b^2$ eine Einheit in $\mathbb{Z}$, also ± 1, denn N ist ein Monoidhomomorphismus.

Wegen $N(7 + 5\sqrt{2}) = -1$ ist $(7 + 5\sqrt{2})^{-1} = -(7 - 5\sqrt{2})$.

d) Der reelle Absolutbetrag von $7 + 5\sqrt{2}$ ist nicht 1 – also sind alle Potenzen $(7 + 5\sqrt{2})^n$ paarweise verschieden und natürlich alles Einheiten in $Z[\sqrt{2}]$.

Aufgabe 3 (3 Punkte)
Zeige, dass es keinen Ring mit genau 5 Einheiten geben kann.
(*Hinweis:* Was ist die Charakteristik eines solchen Ringes? Untersuche für eine Einheit a der Ordnung 5 das Element $1 + a^2 + a^3$!)

Lösung: In dieser Aufgabe sei ord stets die multiplikative Ordnung.
Sei R ein solcher Ring mit $\#R^\times = 5$. Nach dem Satz von Lagrange ist $\mathrm{ord}(a) = 5$ für alle $a \in R^\times, a \neq 1$. Ein solches a gibt es.
Insbesondere ist wegen $(-1)^2 = 1$ die Ordnung $\mathrm{ord}(-1) \leq 2$, was $\mathrm{ord}(-1) = 1$ und somit $-1 = 1$ erzwingt. Also hat R die Charakteristik 2 (denn $1 \neq 0$, aber $1 + 1 = 0$) und wir berechnen die Potenzen von $1 + a^2 + a^3$. Dafür benutzen wir folgende Tatsachen:
(1): $a^5 = 1$,
(2): $x = -x$ bzw. $x + x = 0$ für alle $x \in R$ (denn $x + x = (1 + 1) \cdot x = 0x = 0$),
(3): für $i, j \in \{0, ..., 4\}, i \neq j$ ist $a^i \neq a^j$ (sonst wäre $\mathrm{ord}(a) < 5$).

Es ist $1 + a^2 + a^3 \overset{(2),(3)}{\neq} 1$.
$(1+a^2+a^3)^2 = 1+a^2+a^3+a^2+a^4+a^5+a^3+a^5+a^6 \overset{(1)}{=} 1+a^2+a^3+a^2+a^4+1+a^3+1+a \overset{(2)}{=} 1+a+a^4 \overset{(2),(3)}{\neq} 1$.
$(1 + a^2 + a^3)^3 = (1 + a + a^4)(1 + a^2 + a^3) = 1 + a^2 + a^3 + a + a^3 + a^4 + a^4 + a^6 + a^7 \overset{(1)}{=} 1 + a^2 + a^3 + a + a^3 + a^4 + a^4 + a + a^2 \overset{(2)}{=} 1$.

Also ist $1 + a^2 + a^3$ invertierbar mit Ordnung 3 – das geht nach Lagrange nicht und wir haben einen WIDERPSPRUCH.

Aufgabe 4 (3 Punkte)

a) Seien R und S Ringe mit Charakteristik $\neq 0$. Zeige, dass $\text{char}(S)$ ein Teiler von $\text{char}(R)$ ist, wenn es einen Ringhomomorphismus zwischen R und S gibt.

b) Finde und beweise ein Kriterium, wann es einen Ringhomomorphismus zwischen den Restklassenringen $\mathbb{Z}/N\mathbb{Z}$ und $\mathbb{Z}/M\mathbb{Z}$ mit $M, N \in \mathbb{Z}$ gibt.[2] (*Stichwort Homomorphiesatz*)

Lösung:

a) φ ist ein Gruppenhomomorphismus von $(R, +)$ nach $(S, +)$ und die Charakteristik von R bzw. S ist die additive Ordnung von 1_R in R bzw. von $1_S = \varphi(1_R)$ in S.
Die Aussage lässt sich nun ganz genau wie die Aufgabe 1 von Übungsblatt 4 lösen, das rechne ich hier nicht noch einmal vor.
(**Bemerkung:** In der alten Aufgabe waren endliche Gruppen gefragt – deswegen ist das hier kein Spezialfall davon, aber wenn wir die Ringe jeweils auf den von 1 erzeugten Ring einschränken, dann klappt es doch wieder. Der von 1 erzeugte Ring in R ist übrigens isomorph zu $\mathbb{Z}/\text{char}(R)\mathbb{Z}$, das ist klar, oder?)

b) **Behauptung:** Es gibt genau dann einen Ringhomomorphismus von $\mathbb{Z}/N\mathbb{Z}$ und $\mathbb{Z}/MZ$, wenn M ein Teiler von N ist.
Fall 1: M, N beide $\neq 0$. Um das Vorzeichen müssen wir uns keine Gedanken machen, denn weder die Restklassenringe noch die Teilereigenschaft sehen das Vorzeichen. Ohne Einschränkung sind also $M, N \in \mathbb{N}$.
„$\Rightarrow$“ ist eine direkte Folgerung von a), denn $\text{char}(\mathbb{Z}/N\mathbb{Z}) = N, \text{char}(\mathbb{Z}/M\mathbb{Z}) = M$.
„$\Leftarrow$“ Sei M ein Teiler von N, etwa $kM = N$ für ein $k \in \mathbb{Z}$.
$\varphi\colon \mathbb{Z} \to \mathbb{Z}/M\mathbb{Z}, z \mapsto [z]_M = z + M\mathbb{Z}$ ist ein Ringhomomorphismus laut Vorlesung.
Sei $x \in N\mathbb{Z}$, etwa $x = lN$ mit $l \in \mathbb{Z}$, gilt $\varphi(x) = \varphi(lN) = \varphi(lkM) = 0$, also ist $N\mathbb{Z} \subseteq \text{Kern}(\varphi)$.
Dann folgt die Behauptung mit Hilfe des Homomorphiesatzes.
Fall 2: Ist $N = 0$, so ist $\mathbb{Z}//N\mathbb{Z} = \mathbb{Z}$ und es gibt einen Ringhomomorphismus von $\mathbb{Z}/N\mathbb{Z}$ nach $\mathbb{Z}/M\mathbb{Z}$ für alle $M \in \mathbb{Z}$. Andererseits ist jedes solche M auch ein Teiler von 0, womit die Äquivalenz auch in diesem Fall gezeigt wäre.
Fall 3: Es verbleibt $N \neq 0, M = 0$. Dann ist N kein Teiler vom M und es gibt aber auch keinen Homomorphismus von $\mathbb{Z}/N\mathbb{Z}$ nach $\mathbb{Z}/M\mathbb{Z} = \mathbb{Z}$, denn die additive Ordnung der 1 in $\mathbb{Z}$ müsste doch kleinergleich N sein – ganz analog zum Beweis aus a). Auch hier stimmt die Äquivalenz.

Zusatz: Der Homomorphismus – sofern existent – ist stets eindeutig gegebenden durch $[x]_N \mapsto [x]_N$. Da $[1]_N$ die Gruppe $\mathbb{Z}/n\mathbb{Z}$ erzeugt und das Bild von $[1]_N$ festgelegt ist (denn das Einselement wird auf das Einselement abgebildet), ist das die einzige Möglichkeit für einen Homomorphismus. In der Vorlesung haben wir gesehen, dass es von $\mathbb{Z}$ in jedem Ring R genau einen Ringhomomorphismus gibt. Es gibt höchstens einen Ringhomomorphismus von $\mathbb{Z}/N\mathbb{Z}$ nach R, die Existenz hängt dann von der Charakteristik von R ab.

[2] Es gibt dann sogar genau einen!

Aufgabe 5 (3 Punkte)
Sei R ein kommutativer Ring und I ein Ideal. Wir definieren das *Radikal* $\sqrt{I}$ von I durch

$$\sqrt{I} = \{a \in R : a^r \in I \text{ für ein } r \in \mathbb{N}\}.$$

Zeige, dass $\sqrt{I}$ ein Ideal ist.

Lösung:
Wir zeigen, dass $(\sqrt{I}, +) \overset{(!)}{\leq} (R, +)$ eine Untergruppe ist und dass $R \cdot \sqrt{I} \overset{(!)}{\subseteq} \sqrt{I}$.
(**Bemerkung am Rande:** Weil wir in Ringen stets $1 \in R$ fordern, gilt sogar Gleichheit $RJ = J$ für jedes Ideal J von R. Nachfolgende würde aber stets auch „$\subseteq$“ reichen.)
Seien dazu $a, b \in \sqrt{I}$, $r \in R$ beliebig:
Es gibt also $n \in \mathbb{N}$, so dass $a^n \in I$ und insbesondere ist dann auch $a^{n'} = a^{n'-n} \cdot a^n \in RI = I$ für alle $n' > n$.
Analog gibt es ein $m \in \mathbb{N}$, so dass $a^m \in I$ und $a^{m'} \in I$ für alle $m' > m$.

(*i*) Zunächst ist $\sqrt{I} \neq \emptyset$, denn zum Beispiel $0 \in \sqrt{I}$ – es gilt offensichtlich sogar $I \subseteq \sqrt{I}$, nicht wahr?
(*ii*) Es ist $(-a)^n = (-1)^n \cdot a^n \in RI = I$, also $(-a)^n \in I$, also $-a \in \sqrt{I}$.
(*iii*) Außerdem ist $(a+b)^{n+m} = \sum_{j=0}^{m+n} \binom{m+n}{j} a^j b^{m+n-j} = \sum_{j=0}^{n-1} \binom{m+n}{j} a^j b^{m+n-j} + \sum_{j=n}^{m+n} \binom{m+n}{j} a^j b^{m+n-j} \in I$, denn alle Summanden der ersten Summe sind in $RI = I$ wegen $b^{m+n-j} \in I$, alls Summanden der zweiten Summe sind in $IR = I$ wegen $a^j \in I$. Also ist $a + b \in \sqrt{I}$.
(*iv*) Es ist $(ra)^n = r^n a^n \in RI = I$, also $ra \in \sqrt{I}$.

Mit (*i*), (*ii*) , (*iii*) und dem Untergruppenkriterium folgt, dass $\sqrt{I}$ eine Untergruppe ist, mit (*iv*) dann die zusätzliche Idealeigenschaft.

Zusatzaufgabe (4 Punkte) – Alle Jahre wieder . . .
. . . versuchen wir, Schneewittchens Hochzeitspläne zu verstehen und zu berechnen, wann sie und ihr Prinz sich endlich das Ja-Wort geben können. Selbstverständlich scheitert die Hochzeit jedes Jahr erneut, nicht an der Mathematik, sondern an Schneewittchens Launen.[3]

Dieses Jahr ist alles anders. Schneewittchen hat geheiratet. Gerümpel konnte es noch gar nicht glauben, aber es war so. Vor wenigen Tagen war die Hochzeit nach jahrelanger Planung endlich über die Bühne gegangen und alle waren sie da gewesen: Die Zwerge, die Großmutter des Prinzen, Schneewittchens chinesischer Freund Li und sogar Dornröschen war rechtzeitig wach geworden.
Leider sah auch die Zwergenhöhle dementsprechend aus. Alle Ecken waren vollgestellt mit Zeugs und Gerümpel war eingeteilt, hier aufzuräumen – warum gerade er diesen Auftrag bekommen hatte, war ihm unklar, aber einer musste es halt machen. Glücklicherweise war er wenigstens nicht damit beauftragt worden, die Stühle der Tafel fortzuräumen, an der das Heer des Prinzen gesessen hatte. Das war Stapels und Schleppels Job – die zwar geflucht hatten, aber immerhin war der Prinz ja nur Herrscher[4] eines kleinen Landes und mehr als 1000 Soldaten hatte er nicht. Das wussten alle, auch wenn nicht einmal der Prinz genau zu sagen vermochte, wie groß sein Heer nun eigentlich genau war.

Oh, das Heer, Gerümpel erinnerte sich genau. Schneewittchen hatte darauf bestanden, dass die Soldaten in Reih' und Glied in den Ballsaal marschierten. „Kein Problem," hatte der Prinz gerufen und alle Soldaten sollten sich in einer Zweierreihe aufstellen, was auch wunderbar aufging, aber – wer hätte es anders erwartet – das gefiel Schneewittchen nicht. „Geht das nicht auch quadratisch?" nörgelte sie, aber da war natürlich nichts zu machen.
„Eine Dreierreihe geht auch nicht," berechnete Oberschlau schnell, „da würden zwei überbleiben, bei einer Fünferreihe gar drei."

[3] Vielleicht liest dein Tutor dir diese Geschichte vor?
[4] Böse Zungen behaupten, nach der Hochzeit sah die Rollenverteilung ganz anders aus.

Gerümpel erinnerte sich an den verzweifelten Gesichtsausdruck des Prinzen, als auch die Siebenerreihe scheiterte, doch bevor er auf die Idee kommen könnte, die übrig gebliebenen fünf Soldaten einfach in den Kerker zu werfen – wenn es um die Hochzeit ging, verstand der Prinz inzwischen keinen Spaß mehr – reihten sich die Soldaten zu acht nebeneinander und sogar Schneewittchen war zufrieden.

Doch wieviele Soldaten besitzt der Prinz nun eigentlich genau? Da es eh Zeit für eine Pause war – war es das nicht immer? – schnappte sich Gerümpel Zettel und Stift und hatte bald die richtige Anzahl berechnet.

Als die Zwerge später beim Abendessen zusammensaßen, erzählte Gerümpel den anderen von seiner Berechnung. Außer Oberschlau interessierte sich aber keiner wirklich dafür. „Dann hätte es ja doch eine prima[5] Aufstellung gegeben," ärgerte sich Oberschlau, der mit der Achterlösung von Anfang an nicht wirklich zufrieden gewesen war.
Doch gerade als sich Gerümpel an Teilbarkeitsregeln erinnerte, klingelte der Wecker…

Hätte Gerümpel nicht schon nach „Schneewittchen hat geheiratet." wissen müssen, dass es nur ein Traum sein kann? Wie reagierte Schneewittchen, als Gerümpel am Frühstückstisch von seinem Traum erzählte? Und wie viele Soldaten waren es denn nun wirklich? Für die Beantwortung der letzten Frage kannst du dir vier Punkte verdienen, für die vorherigen Fragen bekommst du höchstens einen finsteren Blick von Schneewittchen und vielleicht einen Apfel.

Lösung: Sei $0 \leq x < 1000$ die Anzahl der Soldaten. Dann gilt laut Text:
(1): $x \equiv 0\ (2)$ und $x \equiv 0\ (8)$, wobei die zweite Aussage die erste impliziert, die wir also weglassen können – **Achtung!** Wäre etwa $x \equiv 1\ (2)$, so würde sich das mit $x \equiv 0\ (8)$ beißen. Der chinesische Restsatz funktioniert ja nur bei teilerfremden Zahlen.
Also ist $x = 8l$ für ein $l \in \mathbb{Z}$ (und das sind genau die Lösungen der ersten Kongruenz(en)).
(2): Weiterhin gilt $x \equiv 2\ (3)$, also $8l \equiv 2\ (3)$. Äquivalenzumformungen modulo 8 ergeben:
$8l \equiv 2l \equiv 2\ (3) \overset{\cdot 2}{\Leftrightarrow} l \equiv 1\ (3)$, also $l = 3m + 1$ für ein $m \in \mathbb{Z}$.
Insgesamt erhalten wir $x = 8l = 24m + 8$ und dies sind die Lösungen der ersten beiden Kongruenzen.
(3): Weiterhin gilt $x \equiv 3\ (5)$, also $24m + 8 \equiv 3\ (5) \Leftrightarrow -m \equiv 0\ (5) \overset{\cdot(-1)}{\Leftrightarrow} m \equiv 0\ (5)$, also $m = 5n$ für ein $n \in \mathbb{Z}$.
Insgesamt erhalten wir $x = 120n + 8$ als Lösungen der bisherigen Kongruenzen.
(4): Die letzte Kongruenz ist $x \equiv 5\ (7)$, also $120n + 8 \equiv n + 1 \equiv 5\ (7) \Leftrightarrow n \equiv 4\ (7)$, also $n = 7o + 4$ für ein $o \in \mathbb{Z}$ und wir erhalten $x = 840o + 488$.
Das sind alle Lösungen des Kongruenzensystems und wegen $0 \leq x < 1000$ ist $x = 488$ die richtige Anzahl der Soldaten.

Nachtrag: Dem Übungsleiter ist rechentechnisch ein Faux-Pas passiert. Eigentlich sollten in der Siebenerreihe zwei Soldaten überbleiben. Das Kongreuenzsystem wäre dann von allen $x = 128 + 840o$ gelöst worden und mathematisch hätte es zwei Lösungen gegeben. Der schlaue Zwerg hätte dann aber erkannt, dass es für $128 = 2^7$ keine „prima Aufstellung" gibt und die Lösung wäre 968 Soldaten gewesen, was – erinnern wir uns an die alternierende Quersumme – wegen $9 - 6 + 8 = 11$ durch 11 teilbar gewesen wäre – prima gedacht, schlecht gerechnet, lieber Übungleiter. Er ist eben nicht Oberschlau.

Und noch ein Nachtrag: Dieses Verfahren, das nacheinander die Kongruenzen abarbeitet, gelingt immer, wenn Kongruenzen modulo paarweise teilerfremden Zahlen vorliegen. Zwischendurch müssen wir Inverse in Restklassenringen berechnen, wenn wir die Kongruenzbedingungen auflösen. Die Inversen existieren wegen der Teilerfremdheit – da schaue man sich noch einmal an, was da genau in was invertiert wird. Berechnen können wir sie zum Beispiel mit Hilfe des euklidischen Algorithmus.

[5] Oberschlau meinte wohl „prime". [Anm. des Autors]