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

# Einführung in Algebra und Zahlentheorie – Übungsblatt 6+1

**Aufgabe 1** (3 Punkte)
$R$ sei 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 Aufgabe 1**
„(i) $\Rightarrow$ (ii)“ $R \neq 0$, also sind $R, 0$ zwei verschiedene Ideale. Wir erinnern uns, dass jedes Ideal $I$, das eine Einheit enthält, bereits der ganze Ring ist, denn mit $x \in R^\times \cap I$ ist wegen $RI \subseteq I$ zunächst $x^{-1} \cdot x = 1 \in I$ und damit für alle $r \in R$ auch $r \cdot 1 = r \in I$, also $I = R$. Da aber jedes Körperelement ungleich 0 invertierbar ist, folgt aus $I \neq 0$ direkt, dass $I = R$ gilt, wir haben also genau zwei Ideale.
„(ii) $\Rightarrow$ (iii)“ glauben wir sofort, oder?
Für „(iii) $\Rightarrow$ (i)“ müssen wir etwas arbeiten. Es reicht zu zeigen, dass jedes $x \neq 0$ invertierbar ist, denn $R \neq 0$ ist bereits kommutativ.
Für ein solches $x$ betrachten wir die Ideale, die von $x^j$, $j \in \mathbb{N}$ erzeugt werden. Ein solches Ideal $(x^j)$ ist bekanntlich von der Form $R \cdot x^j$.
Wegen $x^{j+1} = x \cdot x^j \in (x^j)$ ist $R = (x^0) \supseteq (x^1) \supseteq (x^2) \supseteq ...$, aber da nur endlich viele von diesen Idealen verschieden sind, muss es auch $i > j$ geben, so dass $(x^i) = (x^j)$.
Dann aber ist $(x^j) \supseteq (x^{j+1}) \supseteq (x^i) = (x^j)$ und wir folgern $(x^j) = (x^{j+1})$, also insbesondere $x^j \in (x^{j+1})$. Es gibt also ein $r \in R$, so dass $x^j = rx^{j+1}$ und Umstellen und Ausklammern ergibt $(rx - 1)x^j = 1$. Aber wegen der Nullteilerfreiheit ist zunächst $x^j \neq 0$ und anschließend folgt $rx - 1 = 0$, also $rx = 1$, womit $x \in R^\times$ gezeigt wäre.

Die Folgerung ist dann natürlich trivial, hat jeder endliche Integritätsbereich doch nur endlich viele Teilmengen, also erst recht nur endlich viele Ideale.

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

**Aufgabe 2** (4 Punkte) *und schon wieder eine alte Klausur-Aufgabe*
Seien $R, S$ kommutative Ringe, $I \trianglelefteq R, J \trianglelefteq S$ Ideale in $R$ beziehungsweise $S$. Desweiteren sei $\varphi : R \to S$ ein Ring-Homomorphismus.

a) $\varphi^{-1}(J)$ ist ein Ideal in $R$.

b) Ist $\varphi$ surjektiv, so ist $\varphi(I)$ ein Ideal in $S$.

c) Ist $\varphi(I)$ immer ein Ideal in $S$? Beweise dies oder finde ein Gegenbeispiel.

**Lösung Aufgabe 2**
Je nachdem, was wir aus der linearen Algebra oder unserer Vorlesung mitbringen, ist der Beweis gegebenenfalls sehr kurz. Wir erinnern uns, dass Bilder und Urbilder von Untergruppen (Ideale sind ja insbesondere dieses) unter Gruppenhomomorphismen (Ringhomomorphismen sind ja insbesondere dieses) wieder Untergruppen sind. Wer sich nicht erinnert, kann (und sollte!) dies kurz hinschreiben.

a) $\varphi^{-1}(J)$ ist eine Untergruppe von $(R, +)$ nach der Vorüberlegung.
Seien nun $r \in R$, $i \in \varphi^{-1}(J)$, das heißt, $\varphi(i) \in J$:
$\varphi(ri) = \varphi(r)\varphi(i) \in J$, da $\varphi(r) \in S$, $\varphi(i) \in J$ und $J$ ein $S$-Ideal ist. Damit aber ist $ri \in \varphi^{-1}(J)$, was zu zeigen war.

b) $\varphi(I)$ ist eine Untergruppe von $(S, +)$ nach der Vorüberlegung.
Seien nun $s \in S$, $j \in \varphi(I)$ beliebig, das heißt, $j = \varphi(i)$ für ein $i \in I$ und wegen der Surjektivität von $\varphi$ ist $s = \varphi(r)$ für ein $r \in R$:
$sj = \varphi(r)\varphi(i) = \varphi(ri) \in \varphi(I)$, da $ri \in I$, da $I$ ein $R$-Ideal ist.

c) Betrachte die natürliche Einbettung $i$ von $\mathbb{Z}$ nach $\mathbb{Q}$, die jedes $z \in \mathbb{Z}$ auf sich selbst abbildet.
Dann ist $\mathbb{Z}$ in $\mathbb{Z}$ ein Ideal (klar), aber $i(\mathbb{Z}) = \mathbb{Z}$ kein Ideal in $\mathbb{Q}$, was etwa wegen $\frac{1}{2} \cdot 1 \notin \mathbb{Z}$ klar sein dürfte.

**Aufgabe 3** (5 Punkte)
Sei $R$ ein Integritätsbereich, $n$ eine natürliche Zahl $> 1$. Dann ist $R^{n\times n}$ ein nicht-kommutativer Ring.

a) Finde einen $R^{n\times n}$-Untermodul in $R^{n\times n}$, der kein Ideal ist.[2]

b) Zeige, dass die Ideale in $R^{n\times n}$ gerade die $J^{n\times n}$ sind, wobei $J$ ein Ideal von $R$ ist.

c) Sei $J^{n\times n}$ ein Ideal in $R^{n\times n}$, $J$ wie in Aufgabenteil b).
Zeige, dass $R^{n\times n}/J^{n\times n} \cong (R/J)^{n\times n}$.

d) Sei nun $R$ ein Körper, $S \neq 0$ ein Ring und $\varphi : R^{n\times n} \to S$ ein Ringhomomorphismus. Zeige, dass $\varphi$ injektiv ist.

**Lösung Aufgabe 3**
Wir legen zunächst ein paar Schreibweisen fest. Man muss sich das gegebenenfalls als Pünktchenmatrix aufschreiben, dann sollten die Definitionen klar sein.

- Für eine Matrix $A \in R^{n\times n}$ sei $i, j \in \{1, ..., n\}$ mit $A_{i,j}$ der Eintrag in der $i$-ten Zeile, $j$-ten Spalte von $A$ bezeichnet.
- Mit $P(k,l)$ sei die Vertauschungsmatrix gemeint, die die $k$-te Zeile (bzw. Spalte) und $l$-te Zeile (bzw. Spalte) vertauscht. Gegeben ist sie durch $P(k,l)_{i,i} = 1$ für $i \notin \{k,l\}$ und $P(k,l)_{k,l} = P(k,l)_{l,k} = 1$, sonstige Einträge sind 0.
- Schließlich sei $E(k,l)$ die Elementarmatrix mit $E(k,l)_{k,l} = 1$, restliche Einträge 0.
Insbesondere ist dann $r \cdot E(k,l)$ die Matrix, die genau einen Eintrag $r$ enthält, dieser steht in der $k$-ten Zeile, $l$-ten Spalte.

Nun widmen wir uns dem Beweis, der nicht allzu schwer ist, man muss es nur sauber aufschreiben. In dieser Lösung werden wir viel mit den Matrizentypen oben arbeiten, als handschriftliche Lösung (in der Übung oder wenn du diese Lösungen nachvollziehst) sollte man sich auf jeden Fall die Matrizen (mit Pünktchen) hinschreiben und sich die gegebenen Rechenschritte in Ruhe klar machen. Gerade bei der Multiplikation mit Elementarmatrizen passiert eigentlich nichts kompliziertes, aber man muss doch genau schauen, um mit den Indizes zurecht zu kommen.

a) Setze $M = \{A \in R^{n\times n} : A_{i,1} = 0 \text{ für alle } i = \{1, ..., n\}\}$, $M$ ist die Menge aller Matrizen, deren erste Spalte die Nullspalte ist. $M$ ist sicher eine Gruppe bezüglich $+$, und nach der Definition der Matrizenmultiplikation gilt $R^{n\times n} \cdot M \subseteq M$. Aber zum Beispiel $E(1,n) \in M$ und $E(1,n) \cdot P(1,n) = E(1,1)$ ist kein Element aus $M$, also $M \cdot R^{n\times n} \not\subseteq M$.

b) Zunächst zeigen wir, dass für ein Ideal $J$ von $R$ $J^{n\times n}$ ein Ideal in $R^{n\times n}$ ist. Das ist nicht schwer einzusehen, denn bei komponentenweiser Berechnung von Matrizenaddition bzw. Matrizenmultiplikation werden ausschließlich Rechnungen durchgeführt, die das Ideal $J$ nicht verlassen. Konkret heißt das folgendes:
$J^{n\times n}$ ist sicher nicht leer, enthält etwa die Nullmatrix.
Seien $A, B \in J^{n\times n}$ und $T \in R^{n\times n}$ beliebig. Seien stets $i, j \in \{1, ..., n\}$ beliebig:
$A, B \in J^{n\times n}$, also sind $A_{i,j}, B_{i_j} \in J$. Damit ist $(A - B)_{i,j} = A_{i-j} - B_{i-j} \in J$, also $A - B \in J^{n\times n}$.
$(TA)_{i,j} = \sum\limits_{k=1}^{n} T_{i,k}A_{k,j} \in J$, da alle $A_{k,j}$ und damit jeder Summand und damit die Summe in $J$ liegt, denn $J$ ist ein Ideal in $R$. Also $TA \in J^{n\times n}$.
Analog gilt $(AT)_{i,j} = \sum\limits_{k=1}^{n} A_{i,k}T_{k,j} \in J \Rightarrow AT \in J^{n\times n}$.
Insgesamt folgt, dass $J^{n\times n}$ ein $R^{n\times n}$-Ideal ist.

Es verbleibt zu zeigen, dass zu einem Ideal $I$ von $R^{n\times n}$ ein Ideal $J$ von $R$ existiert, so dass $I = J^{n\times n}$.
Wir zeigen, dass $J := \{r \in R : A_{i,j} = r \text{ für ein } A \in I, i, j \text{ passend}\}$ ein Ideal ist, das die Bedingung erfüllt.

[2] Wenn man von links- und rechtsseitigen Idealen spricht, dann suchen wir hier ein Linksideal, das kein Rechtsideal ist. Für ein Linksideal $I$ von einem Ring $S$ fordern wir dabei nur $SI \subseteq I$, aber nicht $IS \subseteq I$. Man beachte, dass für einen Untermodul gerade die erste Abgeschlossenheit wichtig ist.
Bei kommutativen Ringen sind (zweiseitige) Ideale, Linksideale, Rechtsideale sowieso alle gleich und man überzeugt sich schnell, dass man in der nicht kommutativen Welt lieber gar nicht nach Idealen schaut. Aber es ist trotzdem gut, so etwas einmal gesehen zu haben.

Vorher zeigen wir folgende **Behauptung:** Für ein $r \in J$ ist jede Matrix $r \cdot E(k,l) \in I$ enthalten, denn:
Nach Definition von $J$ gibt es $A \in I, i, j$, so dass $A_{i,j} = r$ ist. Dann aber ist $E(k,i) \cdot A \cdot E(j,l) = r \cdot E(k,l)$ wie behauptet.
Damit ist der Beweis plötzlich sehr einfach geworden. Wir benutzen stets, dass $I$ ein Ideal ist.
$J$ ist nicht leer und für $r, s \in J$ sind $rE(1,1)$, $sE(1,1) \in I$ und damit $rE(1,1) - sE(1,1) = (r-s)E(1,1) \in I$, womit $r - s \in J$.
Für $r \in J, t \in R$ ist $rE(1,1) \in I$, $tE(1,1) \in R$ und damit $tE(1,1)rE(1,1) = trE(1,1) \in I$, womit $tr \in J$.
Also ist $J$ ein Ideal und wir müssen noch zeigen, dass $I = J^{n\times n}$ ist.

„$\subseteq$" ist nach Definition von $J$ klar. Ist aber nun $A \in J^{n\times n}$ beliebig, so ist wegen der Behauptung jede Matrix $A_{i,j} \cdot E(i,j) \in I$ und $A$ gerade die Summe davon, also auch in $I$ enthalten. Dies zeigt „$\supseteq$".

c) Wir definieren $\psi : R^{n\times n}/J^{n\times n} \to (R/J)^{n\times n}$ wie folgt:
$\overline{\begin{pmatrix} r_{1,1} & ... & r_{1,n} \\ ... & ... & ... \\ r_{n,1} & ... & r_{n,n} \end{pmatrix}} \mapsto \begin{pmatrix} \overline{r_{1,1}} & ... & \overline{r_{1,n}} \\ ... & ... & ... \\ \overline{r_{n,1}} & ... & \overline{r_{n,n}} \end{pmatrix}$.
Wir wollen einsehen, dass dies ein Ring-Isomorphismus ist.

Zunächst sehen wir ein, dass $\psi$ wohldefiniert ist.
Es ist $\overline{A} = \overline{B} \Leftrightarrow A - B \in J^{n\times n} \Leftrightarrow A_{i,j} - B_{i,j} \in J$ für alle $i, j \in \{1, ..., n\} \Leftrightarrow \begin{pmatrix} \overline{A_{1,1}} & ... & \overline{A_{1,n}} \\ ... & ... & ... \\ \overline{A_{n,1}} & ... & \overline{A_{n,n}} \end{pmatrix} = \begin{pmatrix} \overline{B_{1,1}} & ... & \overline{B_{1,n}} \\ ... & ... & ... \\ \overline{B_{n,1}} & ... & \overline{B_{n,n}} \end{pmatrix}$.
Da dies Äquivalenzen sind, zeigt das, dass die Zuordnung $\begin{pmatrix} \overline{r_{1,1}} & ... & \overline{r_{1,n}} \\ ... & ... & ... \\ \overline{r_{n,1}} & ... & \overline{r_{n,n}} \end{pmatrix} \mapsto \overline{\begin{pmatrix} r_{1,1} & ... & r_{1,n} \\ ... & ... & ... \\ r_{n,1} & ... & r_{n,n} \end{pmatrix}}$ ebenfalls wohldefiniert ist, offensichtlich ist die Zuordnung zu $\psi$ invers, $\psi$ also bijektiv.

Es verbleibt die Homomorphie-Eigenschaften nachzurechnen:
Dass die Eins $\overline{I}$ auf die Eins abgebildet wird, ist offensichtlich.
Für $\overline{A}, \overline{B}$ gilt schließlich für beliebige $i, j \in \{1, ..., n\}$:
$\psi(\overline{A} + \overline{B})_{i,j} = \psi(\overline{A + B})_{i,j} = \overline{A_{i,j} + B_{i,j}} = \overline{A_{i,j}} + \overline{B_{i,j}} = \psi(\overline{A}) + \psi(\overline{B})$ und
$\psi(\overline{A} \cdot \overline{B})_{i,j} = \psi(\overline{A \cdot B})_{i,j} = \overline{\sum_{k=1}^{n} A_{i,k} \cdot B_{k,j}} = \sum_{k=1}^{n} \overline{A_{i,k}} \cdot \overline{B_{k,j}} = \psi(\overline{A}) \cdot \psi(\overline{B})$.

d) Nach all der Vorarbeit ist dieser Teil nun einfach. Wir wissen, dass der Kern von $\varphi$ ein Ideal in $R^{n\times n}$ ist, also nach b) ist der Kern ein $J^{n\times n}$ mit einem Ideal $J$ von $R$. Aber da gibt es doch nur $R$ und 0, da $R$ ein Körper ist. Wegen $1 \mapsto 1$ ist der Kern aber nicht $R^{n\times n}$ und es verbleibt nur $J = 0$, also ist der Kern trivial und als Gruppenhomomorphismus also $\varphi$ injektiv.

**Aufgabe 4** (4 vergiftete Äpfel)

**Die Vorgeschichte**
Manche behaupten, Zwerge hätten in der modernen Welt der Mathematik nichts verloren. Das mag tatsächlich stimmen. Eine Geschichte haben wir aber noch versprochen, die soll hier noch erzählt werden. Erinnert ihr euch an Schneewittchens Hochzeitspläne? In grauer Vorzeit, manche mögen es letzte Woche nennen, hatte Schneewittchen einen Termin gesucht, an dem sie heiraten wollte...

„Ich werde nur Donnerstag heiraten, das ist mein Glückstag", bestimmte Schneewittchen. „Heute ist Dienstag, der 29. Mai", sinnierte der Prinz, „wir können also übermorgen hei –" „Nein, nein!" wurde er unterbrochen. „Du denkst daran, dass meine Trauzeugin dann schläft? Du weißt doch, seit dem Unfall mit der Spindel schläft Dornröschen eigentlich nur noch."
„Sie ist nur alle 11 Tage wach", warf Rumpel ein, „am zweiten Juni das nächste Mal. Aber das ist ein Samstag."
„Kein Problem", sagte Oberschlau, „wir werden einen Donnerstag finden, an dem Dornröschen wach ist. Das nächste mal müsste das doch bereits in wenigen Tagen der Fall sein." Er begann zu rechnen...
Erleichterung machte sich im Gesicht des Prinzen breit, doch wie immer setzte Schneewittchen noch einen drauf: „Du weißt aber, dass hier nur alle 4 Tage saubergemacht wird, mein Lieber? Nur an einem solchen Tag werde ich heiraten!" „Wir haben heute morgen gewischt!" rief Kumpel dazwischen.
Doch Schneewittchen wäre nicht Schneewittchen, wenn sie nicht noch mehr Wünsche hätte. „Ohne meinen alten Freund Li aus China werde ich nicht heiraten!" intonierte sie. „Er kann morgen hier sein. Danach wieder Samstag, Dienstag... Alle drei Tage eben.„

Der sonst so beherrschte Prinz begann mit dem Kopf zu schütteln. "Willst du mich überhaupt heiraten? Ich glaube kaum, dass wir einen passenden Termin finden werden...„ murmelte er. Schneewittchen - die eigentlich gerade ihre weiteren Bedingungen anbringen wollte - nahm ihn bei der Hand und versprach, dass sie es sicher noch dieses Jahr schaffen würden.

Oberschlau wollte sich gerade räuspern, hielt sich aber tatsächlich zurück. Eigentlich war jedem aus dem Raum klar, dass die Hochzeit wohl kaum vor 2027 stattfinden würde, wenn sich Schneewittchen nicht bescheidener zeigen würde. Und Bescheidenheit war ja nicht ihre Stärke, nur bei Äpfeln hielt sie sich immer sehr zurück. (Das allerdings ist auch wieder eine andere Geschichte. Die lasst ihr euch bitte von euren Eltern erzählen.)

Aber wie sieht das eigentlich mathematisch aus? In wievielen Tagen können der Prinz und die Prinzessin unter den gegebenen Umständen frühestens heiraten – wird es im Jahr 2012 möglich sein? Wie viele Tage müssen sie danach warten, bis sie wieder einen passenden Termin finden?
Wann kauft sich Dornröschen endlich einen besseren Wecker?

Wie sieht das eigentlich aus, wenn der Lieferant der Hochzeitstorte – wir erinnern uns, dass die Zwerge gewisse Probleme hatten, selbst eine herzustellen – nur alle 6 Tage liefern könnte? Wann sollte er liefern können, damit die Hochzeit überhaupt theoretisch Chancen hat, tatsächlich einmal stattzufinden?

**Lösung Aufgabe 4**
Die Anzahl der Tage, die vergehen, bis sich ein geeigneter Termin findet, bezeichnen wir mit $x$. Der Text enthält dann vier Kongruenzen, die $x$ erfüllen muss.
Die Prinzessin heiratet estmals übermorgen, dann wöchentlich: $x \equiv 2(7)$.
Dornröschen wacht in vier Tagen auf, ist danach alle elf Tage wach: $x \equiv 4(11)$.
Heute wurde geputzt, danach alle vier Tage: $x \equiv 0(4)$.
Li kann am nächsten Tag kommen, danach alle drei Tage: $x \equiv 1(3)$.

Wir erinnern uns, dass die Kongruenzen in beliebiger Reihenfolge abgearbeitet werden können. Hier erkennt das gute Auge zum Beispiel sofort, dass 4 die letzten drei Kongruenzen erfüllt, diese also äquivalent zu $x \equiv 4(11 \cdot 4 \cdot 3)$ ist. (!)

Um das Verfahren zu lernen, werden wir hier aber auf gut-gesehen-Lösungen verzichten und das Verfahren Schritt für Schritt durchführen. Es gibt verschiedene Verfahren, die jeweils darauf beruhen, eine

Kongruenz nach der anderen dazuzunehmen und mit den bisherigen Erkenntnissen zu verarbeiten.
Ich werde hier ein anderes Verfahren verwenden, als es der Beweis des chinesischen Restsatzes vorschlägt, das funktioniert natürlich genauso und liefert das gleiche Ergebnis.

- $x \equiv 2(7)$, also ist $x = 7n + 2$ für $n \in \mathbb{Z}$. (Dies sind genau die Lösungen der ersten Kongruenz.)

- Die zweite Kongruenz $x \equiv 4(11)$ gibt Einschränkungen an $n$, die wir durch Äquivalenzumformungen modulo 11 erhalten.
  $7n + 2 \equiv 4(11) \Leftrightarrow 7n \equiv 2(11) \overset{7\cdot 8\equiv 1(11)}{\Leftrightarrow} n \equiv 16(11) \equiv 5(11)$. Also ist $n = 11m + 5$ für $m \in \mathbb{Z}$, eingesetzt ergibt sich $x = 7n + 2 = 77m + 37$ für $m \in \mathbb{Z}$. (Dies sind genau die Lösungen der ersten beiden Kongruenzen.)

- $x \equiv 0(4)$ gibt nun folgende Bedingung an $m$:
  $77m + 37 \equiv 0(4) \Leftrightarrow m + 1 \equiv 0(4) \Leftrightarrow m \equiv 3(4)$, also ist $m$ von der Form $m = 4l + 3$.
  Eingesetzt erhalten wir $x = 308l + 268$, $l \in \mathbb{Z}$. (Dies sind genau die Lösungen der ersten drei Kongruenzen.)

- $x \equiv 1(3)$ schließlich gibt folgende Bedingung an $l$:
  $308l + 268 \equiv 1(3) \Leftrightarrow 2l + 1 \equiv 1(3) \Leftrightarrow 2l \equiv 0(3) \Leftrightarrow l \equiv 0(3)$, also ist $l = 3k$, eingesetzt $x = 924k + 268$, $k \in \mathbb{Z}$ und dies sind die Lösungen aller Kongruenzen.

Zurück in der Anwendung interessieren uns die nichnegativen Lösungen. Unser Ergebnis heißt, dass die beiden frühestens in 268 Tagen heiraten können, danach erst wieder 924 Tage später, danach wieder 924 Tage später und so weiter.

Widmen wir uns der Zusatzfrage nach der Hochzeitstorte. Wann sollte diese geliefert werden können? Die Kongruenzen $x \equiv 0(4)$ und $x \equiv 1(3)$ legen die Kongruenz modulo 6 bereits eindeutig fest, denn wir folgern $x \equiv 4(12)$ und wenn $x$ bei Teilen durch 12 Rest 4 lässt, lässt es diesen auch bei Teilen durch 6. Wir folgern, dass die Hochzeit nur stattfinden kann, wenn die Hochzeitstorte in vier Tagen (also am Samstag, den 2. Juni) das nächste mal geliefert werden kann.