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

Einführung in Algebra und Zahlentheorie – Übungsblatt 9

Aufgabe 1 (4 Punkte)
Sei R ein kommutativer Ring und $(S,\cdot) \subseteq (R,\cdot)$ ein Untermonoid. Weiterhin sei A ein kommutativer Ring und $\varphi : R \to A$ ein Ringhomomorphismus mit $\varphi(S) \subseteq A^\times$.
Wir definieren $\tilde{R} := \{\varphi(r)\varphi(s)^{-1} : r \in R, s \in S\} \subseteq A$.

a) Zeige, dass $\tilde{R}$ ein Teilring von A ist.

b) Sei $\tilde{I}$ ein Ideal in $\tilde{R}$. Zeige, dass es als Ideal von $\varphi(\varphi^{-1}(\tilde{I}))$ erzeugt wird.

c) Zeige, dass jedes Ideal in $\tilde{R}$ endlich erzeugt ist, wenn dies für alle Ideale in R gilt.

d) Schließlich sei konkret $A \subseteq \mathbb{Q}$, $R = \mathbb{Z}$, $S = \mathbb{Z} \cap A^\times$.
Erinnere dich, dass in diesem Fall φ eindeutig bestimmt ist, und zeige $A = \tilde{R}$.

Lösung Aufgabe 1
Zunächst stellen wir fest, dass $\varphi(R) \subseteq \tilde{R}$ ist $((*))$, denn für alle r ist $\varphi(r) = \varphi(r)\varphi(1)^{-1} \in \tilde{R}$.

a) Dass $\tilde{R} \subseteq A$ ist offensichtlich.
$\tilde{R}$ enthält $1 = \varphi(1)\varphi(1)^{-1}$, ist insbesondere nicht leer.
Seien nun $\varphi(r)\varphi(s)^{-1}, \varphi(r')\varphi(s')^{-1} \in \tilde{R}$ beliebig, dabei seien $r, r' \in R, s, s' \in S$.
Dann ist $\varphi(r)\varphi(s)^{-1} \cdot \varphi(r')\varphi(s')^{-1} = \varphi(rr')\varphi(ss')^{-1} \in \tilde{R}$, wobei wir die Kommutativität von A ausnutzen. Weiterhin ist
$\varphi(r)\varphi(s)^{-1} - \varphi(r')\varphi(s')^{-1} = \varphi(r)\varphi(s)^{-1} \cdot (\varphi(s')\varphi(s')^{-1}) - \varphi(r')\varphi(s')^{-1} \cdot (\varphi(s)\varphi(s)^{-1}) = (\varphi(r)\varphi(s') - \varphi(r')\varphi(s)) \cdot \varphi(s)^{-1}\varphi(s')^{-1} = \varphi(rs' - r's)\varphi(ss')^{-1} \in \tilde{R}$.

Alle Aussagen zusammen ergeben, dass $\tilde{R}$ ein Ring ist.

b) Sei $\varphi(r)\varphi(s)^{-1} \in \tilde{I}$ beliebig. Es gilt:
$\varphi(s) \in \tilde{R}$ nach $(*)$ und damit ist $\varphi(r) = \varphi(s)(\varphi(r)\varphi(s)^{-1}) \in \tilde{I}$, da $\tilde{I}$ ein $\tilde{R}$-Ideal ist.
$\Rightarrow \varphi(r) \in \varphi(R) \cap \tilde{I} \overset{(!)}{=} \varphi(\varphi^{-1}(\tilde{I}))$, wobei die letzte Gleichheit aus der LA bekannt sein sollte:
„$\supseteq$“ gilt offensichtlich, denn die rechte Seite ist stets Teilmenge von $\tilde{I}$.
„$\subseteq$“: Sei $i = \varphi(r) \in \tilde{R}$ (mit $r \in R$), dann ist $r \in \varphi^{-1}(\tilde{I})$ und damit $i = \varphi(r)$ in der rechten Menge enthalten...
Dann aber ist $\varphi(r)\varphi(s)^{-1} = (\varphi(1)\varphi(s)^{-1})\varphi(r)$ im Erzeugnis von $\varphi(\varphi^{-1}(\tilde{I}))$ als $\tilde{R}$-Ideal.

c) Sei $\tilde{I}$ beliebiges Ideal in $\tilde{R}$. Dann ist $\varphi^{-1}(\tilde{I})$ ein R-Ideal, denn: Sicher ist es eine abelsche Gruppe und ist $r \in R$, $j \in \varphi^{-1}(\tilde{I})$, so ist $\varphi(rj) = \varphi(r)\varphi(j) \in \tilde{I}$, da $\varphi(r)$ wegen $(*)$ in $\tilde{R}$ liegt und $\varphi(j)$ natürlich in $\tilde{I}$ nach Wahl von j. Also ist $rj \in \varphi^{-1}(\tilde{I})$.

$\varphi^{-1}(\tilde{I})$ wird aber endlich erzeugt, etwa von $\{i_1, ..., i_k\}$ und es reicht zu zeigen, dass $\tilde{I}$ dann von $J = \{\varphi(i_1), ..., \varphi(i_k)\} \subseteq \tilde{I}$ erzeugt wird.
Wegen b) reicht es aber, zu zeigen, dass jedes $x \in \varphi(\varphi^{-1}(\tilde{I}))$ im Erzeugnis von J liegt. Sei also $x = \varphi(t)$ für ein $t \in \varphi^{-1}(\tilde{I})$. Dann existieren $r_j \in R$ mit $t = \sum_{j=1}^{k} r_j i_j$ und damit ist $x = \varphi(t) = \sum_{j=1}^{k} \varphi(r_j)\varphi(i_j)$ im Erzeugnis von J als $\tilde{R}$-Ideal, denn die r_j liegen wegen $(*)$ in $\tilde{R}$.

d) Wir müssen nur $A \overset{(!)}{\subseteq} \tilde{R}$ zeigen.
Wegen $\varphi(z) = z$ für alle $z \in \mathbb{Z}$ (Wegen der Bedingung $\varphi(1) = 1$ gibt es doch nur diesen einen Ringhomomorphismus!) ist $\tilde{R} = \{\frac{r}{s} \in \mathbb{Q} : r \in \mathbb{Z}, s \in \mathbb{Z} \cap A^\times\}$.

Sei nun $a \in A(\subseteq \mathbb{Q})$, ohne Einschränkung $a \neq 0$, dann ist $a = \frac{z}{n}$ für passende teilerfremde $z, n \in \mathbb{Z}$, $n \neq 0$. Aber dann gibt es $b, c \in \mathbb{Z} : 1 = bz + cn$ und wegen $\frac{z}{n}, \frac{n}{n} = 1, b, c \in A$ ist dann auch $b\frac{z}{n} + c\frac{n}{n} = \frac{1}{n} \in A$, also $n \in A^\times$ und damit $a \in \tilde{R}$.

Aufgabe 2 (4 Punkte)

a) Bestimme den ggT von 7854 und 5015 und stelle ihn als ganzzahlige Linearkombination dieser Zahlen dar.

b) Überlege dir, wie du den euklidischen Algorithmus verwenden kannst, um multiplikative Inverse in den Ringen $\mathbb{Z}/n\mathbb{Z}$ zu berechnen. Bestimme anschließend das Inverse zu 42 in $\mathbb{Z}/59\mathbb{Z}$ und $\mathbb{Z}/71\mathbb{Z}$.

Lösung Aufgabe 2
In der Lösung erlauben uns Zwischenschritte mit negativem Rest, um gegebenenfalls Schritte zu sparen. Dies ist erlaubt, denn die Funktion in $\mathbb{Z}$ als euklidischer Ring ist doch der Betrag, wir fordern also nur einen Rest der betragsmäßig kleiner ist.
Dies kann sinnvoll sein, um den Rest betragsmäßig schneller klein zu kriegen, vergleiche auch Aufgabe 3. Natürlich kommen wir auch mit ausschließlich nicht-negativen Resten zum Ziel.

a) $7854 = 5015 + 2839$
$5015 = 2839 + 2176$
$2839 = 2176 + 663$
$2176 = 3 \cdot 663 + 187$
$663 = 3 \cdot 187 + 102$
$187 = 2 \cdot 102 - 17$
$102 = 6 \cdot 17 + 0$, der ggT ist 17.
Rückwärtsrechnend finden wir $17 = 2 \cdot 102 - 187 = 2 \cdot (663 - 3 \cdot 187) - 187 = -7 \cdot 187 + 2 \cdot 663 = -7 \cdot (2176 - 3 \cdot 663) + 2 \cdot 663 = 23 \cdot 663 - 7 \cdot 2176 = 23 \cdot (2839 - 2176) - 7 \cdot 2176 = 23 \cdot 2839 - 30 \cdot 2176 = 23 \cdot 2839 - 30 \cdot (5015 - 2839) = 53 \cdot 2839 - 30 \cdot 5015 = 53 \cdot (7854 - 5015) - 30 \cdot 5015 = 53 \cdot 7854 - 83 \cdot 5015$.

b) Ist m teilerfremd zu n (und zwar genau dann), so können wir 1 als Linearkombination von m, N darstellen:
$1 = am + bn$ mit $a, b \in \mathbb{Z}$. Modulo n ist dann $\overline{1} = \overline{am} = \overline{a}\ \overline{m}$ und wir haben das Inverse zu $\overline{m}$ gefunden.

Konkret heißt das modulo 71:
$71 = 42 + 29$
$42 = 29 + 13$
$29 = 2 \cdot 13 + 3$
$13 = 4 \cdot 3 + 1$
und wir rechnen zurück: $1 = 13 - 4 \cdot 3 = 13 - 4 \cdot (29 - 2 \cdot 13) = 9 \cdot 13 - 4 \cdot 29 = 9 \cdot (42 - 29) - 4 \cdot 29 = 9 \cdot 42 - 13 \cdot 29 = 9 \cdot 42 - 13 \cdot (71 - 42) = 22 \cdot 42 - 13 \cdot 71 \Rightarrow 42^{-1} = 22$.

Modulo 59 bekommen wir folgendes:
$59 = 42 + 17$
$42 = 2 \cdot 17 + 8$
$17 = 2 \cdot 8 + 1$
und wir rechnen zurück: $1 = 17 - 2 \cdot 8 = 17 - 2 \cdot (42 - 2 \cdot 17) = 5 \cdot 17 - 2 \cdot 42 = 5 \cdot (59 - 42) - 2 \cdot 42 = 5 \cdot 59 - 7 \cdot 42 \Rightarrow 42^{-1} = -7 = 52$.

Aufgabe 3 (4 Punkte)
Die bekannten Fibonacci-Zahlen F_n sind wie folgt gegeben:

$$F_0 = 0, F_1 = 1 \text{ und dann rekursiv durch } F_n := F_{n-2} + F_{n-1} \text{ für } n \geq 2.$$

Wir untersuchen, wie sich der euklidische Algorithmus verhält, wenn er auf benachbarte Fibonacci-Zahlen angewendet wird. Alle Reste seien dabei stets nicht-negativ, das Abbruch-Kriterium sei Rest 0.

Bestimme zunächst für $n \in \mathbb{N}_0$ den größten gemeinsamen Teiler von F_{n+1}, F_n und stelle ihn als Linearkombination dieser beiden Zahlen dar.
Ab sofort sei $n \geq 3$. Zeige, dass für die Berechnung des ggTs von F_n, F_{n+1} genau $n-1$ Schritte benötigt werden. Ist hingegen $0 < a \leq b < F_n$, so werden höchstens $n-2$ Schritte benötigt, um den ggT von a und b zu berechnen.

Lösung Aufgabe 3
Für $n = 0, 1, 2$ ist eine der beteiligten Zahlen 1, der ggT ist also 1 und die Linearkombination ist schnell gefunden.
Sei nun $n \geq 3$. Wir geben direkt eine Linearkombination der 1 aus F_n und F_{n+1} an, dies zeigt gleich, dass 1 der größte gemeinsame Teiler ist. Dafür stellen wir zunächst eine Vermutung auf, indem wir die Linearkombination für ein paar mögliche n hinschreiben. Wir erhalten eine Formel, die wir mit Induktion zeigen, indem wir einen Euklidschritt anwenden.

Es ist $F_0 = 0, F_1 = 1, F_2 = 1, F_3 = 2, F_4 = 3, F_5 = 5, F_6 = 8, F_7 = 13$ und das soll vorerst genügen.
$n = 3$: $1 = -1 \cdot 2 + 1 \cdot 3 = (-1)^{\textbf{ungerade}} \cdot F_2 \cdot F_3 + (-1)^{\textbf{gerade}} \cdot F_1 \cdot F_4$
$n = 4$: $1 = 2 \cdot 3 - 1 \cdot 5 = (-1)^{\textbf{gerade}} \cdot F_3 \cdot F_4 + (-1)^{\textbf{ungerade}} \cdot F_2 \cdot F_5$
$n = 5$: $1 = -3 \cdot 5 + 2 \cdot 8 = (-1)^{\textbf{ungerade}} \cdot F_4 \cdot F_5 + (-1)^{\textbf{gerade}} \cdot F_3 \cdot F_6$
$n = 6$: $1 = 5 \cdot 8 - 3 \cdot 13 = (-1)^{\textbf{gerade}} \cdot F_5 \cdot F_6 + (-1)^{\textbf{ungerade}} \cdot F_4 \cdot F_7$
Vermutung: Für alle $n \geq 3$ ist $1 = (-1)^n \cdot F_{n-1} \cdot F_n + (-1)^{n+1} \cdot F_{n-2} \cdot F_{n+1}$ die Linearkombination der 1 aus F_n und F_{n+1}.
Beweis durch Induktion: Induktionsanfang ist mehrfach erledigt. Sei die Aussage wahr für ein $n \in \mathbb{N}$. Wir führen einen Euklidschritt durch, um die Linearkombination aus F_{n+1}, F_{n+2} zu berechnen. Dazu verwenden wir, dass der erste Schritt $F_{n+2} = 1 \cdot F_{n+1} + 1 \cdot F_n$ war, beim Rückwärtsrechnen heißt dies also, dass wir F_n durch $F_{n+2} - F_{n+1}$ ersetzen müssen. Dies ergibt mit der Induktionsvoraussetzung
$1 = (-1)^n \cdot F_{n-1} \cdot F_n + (-1)^{n+1} \cdot F_{n-2} \cdot F_{n+1} = (-1)^n \cdot F_{n-1} \cdot (F_{n+2} - F_{n+1}) + (-1)^{n+1} \cdot F_{n-2} \cdot F_{n+1} = (-1)^n \cdot F_{n-1} \cdot F_{n-2} + (-1)^n F_{n-1} \cdot (-F_{n+1}) + (-1)^{n+1} \cdot F_{n-2} \cdot F_{n+1} = (-1)^n \cdot F_{n-1} \cdot F_{n+2} + (-1)^{n+1} \cdot (F_{n-1} + F_{n-2}) \cdot F_{n+1} = (-1)^n \cdot F_{n-1} \cdot F_{n+2} + (-1)^{n+1} \cdot F_n \cdot F_{n+1}$, was nach Vertauschen der Summanden zu zeigen war.

Für $n = 3$ benötigen wir $2 = 3 - 1$ Schritte, um Rest 0 zu erhalten. $3 = 2 + 1, 2 = 2 \cdot 1 + 0$.
Sei nun die Anzahl der Schritte für die Berechnung von $\text{ggT}(F_n, F_{n+1}) = n-1$ für ein n. Der erste Schritt zur Berechnung von ggT von F_{n+1}, F_{n+2} ist $F_{n+2} = F_{n+1} + F_n$ und wir benötigen nach Induktionsvoraussetzung weitere $n-1$ Schritte, um den Algorithmus mit den Resten F_n, F_{n+1} fortzuführen. Insgesamt brauchen wir n Schritte, was zu zeigen war.

Schließlich zeigen wir die letzte Aussage wieder per Induktion nach n:
$n = 3$, $b < F_3 = 2$, also ist $F_3 = 0$ oder $F_3 = 1$ und wir benötigen höchstens einen Schritt.
$n = 4$, $b < F_4 = 3$: Für $b = 0, 1$ ist die Aussage klar, für $b = 2$ ist $a = 0, 1$ oder 2 und wir sehen schnell ein, dass wir höchstens 2 Schritte brauchen.
Sei die Aussage wahr für $n-1, n-2$ und $a \leq b < F_n$ gegeben. Der erste Schritt ist $b = k \cdot a + r$ mit $r < a$.
Fall 1: $a < F_{n-1}$. Der Algorithmus wird fortgeführt mit $r < a < F_{n-1}$ und benötigt nach Induktionsvoraussetzung höchstens $(n-1) - 2 = n - 3$ weitere Schritte, mit dem Startschritt brauchen wir insgesamt also höchstens $n - 2$ Schritte.
Fall 2: $a \geq F_{n-1}$. In diesem Fall ist sicher $k = 1$, denn $2 \cdot F_{n-1} > F_n > b$. Desweiteren ist $r = b - a < F_n - F_{n-1} = F_{n-2}$.
Der zweite Schritt ist $a = k_1 \cdot r + r_1$ mit $r_1 < r < F_{n-2}$.
Nun können wir die Induktionsvoraussetzung anwenden, der restliche Algorithmus benötigt höchstens $(n-2) - 2 = n - 4$ Schritte, der Gesamtalgorithmus mit den beiden Startschritten also höchstens $n - 2$ Schritte.

Aufgabe 4 (4 Punkte)
Seien $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) = \{A \in \mathbb{Z}^{2\times 2} : \det(A) = 1\}$ gegeben.
Berechne für alle $k \in \mathbb{Z}$ die Potenzen S^k, T^k. Zeige, dass S und T die Gruppe $\mathrm{SL}_2(\mathbb{Z})$ erzeugen.

Lösung Aufgabe 4:
Für alle $a, b \in \mathbb{Z}$ ist $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}$, insbesondere gilt also für für $k \in \mathbb{N}$: $T^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ (Beweis induktiv), $T^{-k} = (T^k)^{-1} = \begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix}$. Also gilt allgemein $T^z = \begin{pmatrix} 1 & -z \\ 0 & 1 \end{pmatrix}$ für alle $z \in \mathbb{Z}$.
S besitzt Ordnung 4, denn es ist $S^2 = -I, S^3 = -S, S^4 = I$.

Wir zeigen, dass wir jede Matrix A durch Multiplikation von links mit S- und T-Potenzen in eine T-Potenz überführen können. Dies zeigt die Behauptung der Aufgabe.
Behauptung: Wir können jede Matrix $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ in eine Matrix der Form $\begin{pmatrix} a_1 & * \\ b_1 & * \end{pmatrix}$ überführen mit $a_1 = 0$ oder $b_1 = 0$. Wir zeigen die Aussage mit Induktion nach dem Produkt $|a| \cdot |b| \in \mathbb{N}_0$ der Beträge der Einträge der ersten Spalte.
Induktionsanfang: Die Aussage ist sicher richtig für $|a| \cdot |b| = 0$, denn dann ist bereits einer der Einträge 0. Sei die Aussage richtig für alle Matrizen aus $\mathrm{SL}_2(\mathbb{Z})$, deren Produkt der ersten Spalte betragsmäßig kleiner als $|a| \cdot |b|$ ist.
Fall 1: $|a| \leq |b|$: Nach dem euklidischen Algorithmus gibt es $s \in \mathbb{Z}$, so dass $b = as + r$ mit einem Rest r mit $|r| < |a|$.
$T^{-s}A = \begin{pmatrix} a & * \\ r & * \end{pmatrix}$ und wegen $|a| \cdot |r| < |a| \cdot |b|$ kann diese Matrix nach Induktionsvoraussetzung in eine Matrix wie gefordert überführt werden.
Fall 2: $|a| > |b|$. Setze $A' = S \cdot A = \begin{pmatrix} -b & -d \\ a & c \end{pmatrix}$. Das Produkt der ersten Spalte ist betragsmäßig gleich geblieben und wir können nun Fall 1 anwenden.

Nach Überführen in einer Matrix wie in der Behauptung verbleibt eine Matrix von der Form $A_1 = \begin{pmatrix} a & c \\ 0 & d \end{pmatrix}$ beziehungsweise $A_2 = \begin{pmatrix} 0 & c \\ b & d \end{pmatrix}$. Da die Determinante 1 sein muss (Determinanten-Multiplikationssatz), gilt $1 = a \cdot d$ beziehungsweise $1 = \det(A) = -b \cdot c$. Die Matrix aus der Behauptung hat also sogar eine der Formen
$A_1 = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$ oder $A_2 = \begin{pmatrix} -1 & c \\ 0 & -1 \end{pmatrix}$ oder $A_3 = \begin{pmatrix} 0 & -1 \\ 1 & d \end{pmatrix}$ oder $A_4 = \begin{pmatrix} 0 & 1 \\ -1 & d \end{pmatrix}$.
Durch geeignete Multiplikation mit einer S-Potenz $(A_1, S^2 \cdot A_2, S^3 \cdot A_3, S \cdot A_4)$ kann jede dieser Matrizen in eine Matrix der Form $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ überführt werden, letztere ist eine T-Potenz, was die Behauptung zeigt.