

Anmerkungen und Lösungen zu  
**Einführung in die Algebra**  
Blatt 6

Jendrik Stelzner

Letzte Änderung: 21. Dezember 2017

### Aufgabe 3

Es sei  $R$  ein euklidischer Ring und es seien  $a_1, \dots, a_n \in R$  paarweise teilerfremd. Wir wollen erklären, wie man für  $b_1, \dots, b_n \in R$  das System simultaner Kongruenzen

$$\begin{cases} x \equiv b_1 & \text{mod } a_1, \\ x \equiv b_2 & \text{mod } a_2, \\ \vdots \\ x \equiv b_n & \text{mod } a_n, \end{cases}$$

löst. Nach dem chinesischen Restsatz ist die Lösungsmenge von der Form

$$b + (a_1 \cdots a_n)R,$$

wobei  $b$  eine konkrete Lösung ist. Es gilt also, eine entsprechende Lösung zu finden. Wir geben zwei Möglichkeiten an, wie dies mithilfe des euklidischen Algorithmus getan werden kann:

- ◦ Wir betrachten zunächst den Fall  $n = 2$ , also das System von Kongruenzen

$$\begin{cases} x \equiv b_1 & \text{mod } a_1, \\ x \equiv b_2 & \text{mod } a_2. \end{cases} \quad (1)$$

Da  $a_1$  und  $a_2$  teilerfremd sind, gibt es  $c_1, c_2 \in R$  mit  $1 = c_1 a_1 + c_2 a_2$ . Dann gilt

$$\begin{cases} c_2 a_2 \equiv 1 & \text{mod } a_1, \\ c_1 a_1 \equiv 1 & \text{mod } a_2, \end{cases}$$

und somit

$$\begin{cases} b_1 c_2 a_2 \equiv b_1 & \text{mod } a_1, \\ b_2 c_1 a_1 \equiv b_2 & \text{mod } a_2. \end{cases}$$

Also ist  $b := b_1 c_2 a_2 + b_2 c_1 a_1$  eine der gesuchten Lösungen. Nach dem chinesischen Restsatz ist (3) somit äquivalent zu der einzelnen Kongruenz

$$x \equiv b \pmod{(a_1 a_2)}.$$

◦ Im allgemeinen Fall

$$\begin{cases} x \equiv b_1 \pmod{a_1}, \\ x \equiv b_2 \pmod{a_2}, \\ x \equiv b_3 \pmod{a_3}, \\ \vdots \\ x \equiv b_n \pmod{a_n}, \end{cases} \quad (2)$$

können wir betrachten Fall eine Lösung  $b$  der Systems

$$\begin{cases} x \equiv b_1 \pmod{a_1}, \\ x \equiv b_2 \pmod{a_2}, \end{cases} \quad (3)$$

finden. Nach dem chinesischen Restsatz ist dann das System (3) äquivalent zu der einzelnen Kongruenz

$$x \equiv b \pmod{(a_1 a_2)}.$$

Wir können daher das System (2) durch das äquivalente System

$$\begin{cases} x \equiv b \pmod{(a_1 a_2)}, \\ x \equiv b_3 \pmod{a_3}, \\ \vdots \\ x \equiv b_n \pmod{a_n}, \end{cases}$$

ersetzen. Da  $a_1 a_2, a_3, \dots, a_n$  teilerfremd sind, können wir dieses Vorgehen fortsetzen, um eine Lösung von (2) zu erhalten.

- Für alle  $i = 1, \dots, n$  sind  $a_i$  und  $a_1 \cdots a_{i-1} a_{i+1} \cdots a_n$  teilerfremd, weshalb sich mit dem euklidischen Algorithmus  $c_1^{(i)}, c_2^{(i)} \in R$  bestimmen lassen, so dass

$$c_1^{(i)} a_i + c_2^{(i)} a_1 \cdots a_{i-1} a_{i+1} \cdots a_n = 1$$

gilt. Für das Element  $k_i := c_2^{(i)} a_1 \cdots a_{i-1} a_{i+1} \cdots a_n$  gilt dann

$$\begin{cases} k_i \equiv 0 \pmod{a_1}, \\ \vdots \\ k_i \equiv 1 \pmod{a_i}, \\ \vdots \\ k_i \equiv 0 \pmod{a_n}, \end{cases}$$

Deshalb ist

$$b := b_1 k_1 + \cdots + b_n k_n$$

eine konkrete Lösung.

## Aufgabe 4

Für ein Element  $x \in R$  bezeichnen wir im Folgenden eine Zerlegung  $x = \varepsilon p_1 \cdots p_n$  in eine Einheit  $\varepsilon \in R^\times$  und irreduzible Elemente  $p_1, \dots, p_n \in R$  als eine *Primfaktorzerlegung* von  $x$ . Man beachte, dass a priori nicht gefordert wird, dass die  $p_i$  prim sind.

### (a)

Wir formulieren zunächst einige (intuitive) Aussagen über Primfaktorzerlegungen in faktoriellen Ringen:

**Lemma 1.** *Es seien  $x, y \in R$  mit  $x, y \neq 0$ , so dass  $x$  ein Teiler von  $y$  ist. Dann lässt sich jede Primfaktorzerlegung  $x = \varepsilon p_1 \cdots p_n$  von  $x$  zu einer Primfaktorzerlegung  $y = \varepsilon' p_1 \cdots p_n p_{n+1} \cdots p_m$  von  $y$  ergänzen.*

*Beweis.* Es gibt  $z \in R$  mit  $xz = y$ , und es gilt  $z \neq 0$ , da  $y \neq 0$  gilt. Also besitzt  $z$  eine Primfaktorzerlegung  $z = \delta p_{n+1} \cdots p_m$ . Dann gilt

$$y = xz = \varepsilon \delta p_1 \cdots p_n p_{n+1} \cdots p_m,$$

und die Aussage ergibt sich mit  $\varepsilon' := \varepsilon \delta$ . □

Für  $x \in R$ ,  $x \neq 0$  mit Primfaktorzerlegung  $x = \varepsilon p_1 \cdots p_n$  bezeichnen wir mit  $\nu(x) := n$  die Anzahl der insgesamt vorkommenden Primfaktoren (inklusive Vielfachheit). Die Zahl  $\nu(x)$  ist wohldefiniert, da die Primfaktorzerlegung von  $x$  bis auf Permutation und Einheiten eindeutig ist.

**Lemma 2.** *Es seien  $x, y \in R$  mit  $x, y \neq 0$ .*

1. *Es gilt genau dann  $\nu(x) = 0$ , wenn  $x$  eine Einheit ist.*
2. *Es gilt  $\nu(xy) = \nu(x) + \nu(y)$ .*
3. *Ist  $x$  ein Teiler von  $y$ , so gilt  $\nu(x) \leq \nu(y)$ .*
4. *Ist  $x$  ein echter Teiler von  $y$ , also  $(y) \subsetneq (x)$ , so gilt  $\nu(x) < \nu(y)$ .*

*Beweis.*

1. In der Primfaktorzerlegung  $x = \varepsilon p_1 \cdots p_n$  gilt  $n = 0$  und somit  $x = \varepsilon \in R^\times$ . Falls  $x$  eine Einheit ist, so ist für die Einheit  $\varepsilon := x$  die Zerlegung  $x = \varepsilon$  bereits eine Primfaktorzerlegung.
2. Da  $R$  ein Integritätsbereich ist, gilt auch  $xy \neq 0$ , weshalb  $\nu(xy)$  definiert ist. Es seien  $x = \varepsilon p_1 \cdots p_n$  und  $y = \delta q_1 \cdots q_m$  Primfaktorzerlegungen. Dann ist

$$xy = (\varepsilon \delta) p_1 \cdots p_n q_1 \cdots q_m$$

eine Primfaktorzerlegung von  $xy$  und somit

$$\nu(xy) = n + m = \nu(x) + \nu(y).$$

3. Es gibt  $z \in R$  mit  $y = xz$ . Es gilt  $z \neq 0$ , da  $y \neq 0$  gilt, weshalb  $\nu(z)$  definiert ist. Somit gilt

$$\nu(y) = \nu(xz) = \nu(x) + \nu(z) \geq \nu(x).$$

4. In der obigen Situation gilt andernfalls  $\nu(z) = 0$ , weshalb  $z$  dann eine Einheit ist. Deshalb gilt dann

$$(y) = (xz) = (x). \quad \square$$

**(i)**

Es sei  $p \in R$  irreduzibel, und es seien  $x, y \in R$  mit  $p \mid xy$ . Gilt  $x = 0$  oder  $y = 0$ , so gilt  $p \mid x$  oder  $p \mid y$ .

Andernfalls gibt es Primfaktorzerlegungen  $x = \delta q_1 \cdots q_n$  und  $y = \delta' q'_1 \cdots q'_m$ . Dann ist

$$xy = (\delta \delta') q_1 \cdots q_n q'_1 \cdots q'_m \quad (4)$$

eine Primfaktorzerlegung von  $xy$ . Da  $p$  irreduzibel ist und  $p \mid xy$  gilt, lässt sich  $p$  nach Lemma 1 zu einer Primfaktorzerlegung

$$xy = \varepsilon p p_2 \cdots p_r \quad (5)$$

ergänzen. Da  $R$  faktoriell ist, sind die beiden Primfaktorzerlegungen (4) und (5) eindeutig bis auf Einheiten und Permutation. Es gilt deshalb  $p \mid q_i$  oder  $p \mid q'_i$  für passendes  $i$ , und somit  $p \mid x$  oder  $p \mid y$ .

**(ii)**

Wir nehmen an, dass nicht jede aufsteigende Kette von Hauptidealen stabilisieren würde. Dann gibt es eine unendliche, echt aufsteigende Kette von Hauptidealen

$$(a_0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq (a_4) \subsetneq \cdots$$

Dann gilt  $a_i \neq 0$  für alle  $i \geq 1$  (denn sonst wäre  $(a_i) = 0$  für ein solches  $i$ , und dann würde  $(a_i) = \cdots = (a_0) = 0$  gelten). Nach Lemma 2 erhalten wir eine unendliche absteigende Kette

$$\nu(a_1) > \nu(a_2) > \nu(a_3) > \nu(a_4) > \cdots$$

Dies ist aber nicht möglich.

**(b)**

Wir müssen zeigen, dass es für jedes Element  $x \in R$  mit  $x \neq 0$  eine Primfaktorzerlegung

$$x = \varepsilon p_1 \cdots p_n$$

gibt, und dass diese eindeutig bis auf Einheiten und Permutation ist.

## Existenz

**Lemma 3.** *Es sei  $x \in R$ , und es sei  $x = yz$  eine Zerlegung mit  $z \notin R^\times$ . Dann gilt  $(x) \subsetneq (y)$ .*

*Beweis.* Es gilt  $y \mid x$  und somit  $(x) \subseteq (y)$ . Wäre  $(x) = (y)$ , so gebe es ein  $z' \in R$  mit  $y = xz'$ . Dann wäre  $x = yz = xzz'$  und somit  $1 = zz'$ , da  $R$  ein Integritätsbereich ist. Dann wäre  $z$  eine Einheit mit  $z^{-1} = z'$ , im Widerspruch zu  $z \notin R^\times$ .  $\square$

Wir nehmen an, dass es ein Element  $x \in R$  mit  $x \neq 0$  gibt, dass keine Primfaktorzerlegung besitzt. Dann ist  $x$  insbesondere keine Einheit und auch nicht irreduzibel. Es gibt deshalb nicht-Einheiten  $y, z \in R$  mit  $x = yz$ ; dabei gelten  $y, z \neq 0$  da  $x \neq 0$  gilt. Würden  $x$  und  $z$  beide eine Primfaktorzerlegung besitzen, so würden sich diese zu einer Primfaktorzerlegung von  $x$  kombinieren lassen. Also hat  $x$  oder  $y$  keine Primfaktorzerlegung; wir können o.B.d.A. davon ausgehen, dass  $y$  keine hat. Da  $z$  keine Einheit ist, gilt  $(x) \subsetneq (y)$  nach Lemma 3.

Wir setzen  $a_0 := x$  und  $a_1 := y$ . Durch induktives Wiederholen der obigen Argumentation erhalten wir eine unendliche aufsteigende Kette von Hauptidealen

$$(a_0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots$$

Dies steht im Widerspruch zur Annahme (ii).

## Eindeutigkeit

Für zwei Primfaktorzerlegungen

$$x = \varepsilon p_1 \cdots p_n = \delta q_1 \cdots q_m$$

zeigen wir die gewünschte Eindeutigkeit per Induktion über  $n$ :

Gilt  $n = 0$ , so ist  $x = \varepsilon \in R^\times$  eine Einheit. Dann gilt  $q_j \mid x \mid 1$  für alle  $j$ , weshalb jedes  $q_j$  eine Einheit ist. Irreduzible Elemente sind aber per Definition keine Einheiten, weshalb  $m = 0$  gelten muss. Dann ist also  $x = \varepsilon = \delta$ , und die beiden Zerlegungen stimmen überein.

Es sei nun  $n > 0$ . Nach Annahme (i) ist  $p_1$  prim. Aus

$$p_1 \mid x = \delta q_1 \cdots q_m$$

folgt damit, dass  $p_1 \mid \delta$  gilt, oder dass  $p_1 \mid q_j$  für ein  $j$  gilt. Würde  $p_1 \mid \delta$  gelten, so wäre  $p_1$  eine Einheit, im Widerspruch zur Irreduzibilität von  $p_1$ . Also gilt  $p_1 \mid q_j$  für ein  $j$ ; wir können o.B.d.A. davon ausgehen, dass  $p_1 \mid q_1$  gilt. Es gibt also  $\delta' \in R$  mit  $q_1 = p_1 \delta'$ . Da  $q_1$  irreduzibel ist, folgt dabei, dass bereits  $p_1$  oder  $\delta'$  eine Einheit ist;  $p_1$  ist wegen Irreduzibilität keine Einheit, so dass  $\delta'$  eine Einheit ist. Also sind  $p_1$  und  $q_1$  bis auf die Einheit  $\delta'$  gleich.

Es gilt nun

$$x = \varepsilon p_1 \cdots p_n = \delta q_1 \cdots q_m = \delta \delta' p_1 q_2 \cdots q_m. \quad (6)$$

Da  $R$  ein Integritätsbereich ist, können wir die obige Gleichung durch  $p_1 \neq 0$  teilen, und erhalten, dass bereits

$$\varepsilon p_2 \cdots p_n = (\delta \delta') q_2 \cdots m \tag{7}$$

gilt. Nach Induktionsvoraussetzung sind beide Seiten von (7) bis auf Einheiten und Permutation gleich. Damit sind in (6) bereits beide Zerlegungen bis auf Einheiten und Permutation gleich, da auch  $p_1$  und  $q_1$  bis auf Einheit gleich ist.