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

Einführung in Algebra und Zahlentheorie – Übungsblatt 10 – Musterlösung

Aufgabe 1 (4 Punkte)

a) Sei R ein Integritätsbereich. Zeige die Äquivalenz der nachfolgenden Aussagen:
   (i) R ist ein Körper.
   (ii) R besitzt genau zwei Assoziiertenklassen.
   (iii) R besitzt nur endlich viele Assoziiertenklassen.

b) Finde einen Ring R mit genau drei Assoziiertenklassen.

Lösung:

a) Als Integritätsbereich ist $R \neq \{0\}$.
„$(i) \Rightarrow (ii)$“: In jedem Ring ist $\{0\}$ eine Assoziiertenklasse (klar) und ebenso $R^\times$, denn für $r, s \in R^\times$ ist $r = (rs^{-1})s \in R^\times \cdot s$, also sind r, s assoziiert.
Wegen $R = R^\times \dot\cup \{0\}$ sind das die einzigen Assoziationsklassen. „$(ii) \to (iii)$“ Das glauben wir wieder! (Diese Argumentation kennen wir von einer früheren Übungsaufgabe.)
„$(iii) \to (i)$“: Es reicht zu zeigen, dass alle $x \in R \setminus \{0\}$ invertierbar sind. Sei $x \neq 0$.
Für $n \in \mathbb{N}$ betrachte wir die Assoziiertenklasse $A_n = R^\times \cdot x^n$ von x^n. Da es nur endlich viele Assoziationsklassen gibt, gibt es $j < k$ mit $A_j = A_k$, also $A_k \ni x^j = r \cdot x^k$ mit $r \in R^\times$. Umstellen ergibt

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

und wegen der Nullteilerfreiheit und $x \neq 0$ ist $x^j \neq 0$ und dann $1 - rx^{k-j} = 0$ und wir stellen um zu

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

und wir haben das Inverse zu x gefunden.

b) $R = \mathbb{Z}/4\mathbb{Z}$ ist ein solcher Ring. $\{0\}$ und die Einheiten $\{1, 3\}$ bilden (in jedem Ring) eine Assoziiertenklasse, das verbleibende Element $\{2\}$ muss die dritte und letzte Klasse bilden – das können wir natürlich mit $2 = 1 \cdot 2 = 3 \cdot 2$ auch vorrechnen.

Aufgabe 3 (4 Punkte) (Zum Abschluss gibt es etwas zum Knobeln!)
Finde einen kommutativen Ring R und Elemente $a, b \in R$, die sich gegenseitig teilen, aber nicht assoziiert sind.

Lösung: Ein solcher Ring ist zum Beispiel $\mathbb{Z}[X]/(5X)$ mit den Elementen $\overline{2X}$ und $\overline{X}$, die sich wegen $\overline{3} \cdot \overline{2X} = \overline{X}$ und $\overline{2} \cdot \overline{X} = \overline{2X}$ gegenseitig teilen.

Es ist $\overline{\sum_{i=0}^{<\infty} a_i X^i} = \overline{\sum_{i=0}^{<\infty} b_i X^i} \Leftrightarrow \overline{\sum_{i=0}^{<\infty} (a_i - bi) X^i} = 5X \cdot f$ für ein $f \in \mathbb{Z}[X] \Leftrightarrow a_0 - b_0 = 0$ und $a_i - b_i \in 5\mathbb{Z}$ für alle $i \geq 1$. $(*)$
Insbesondere gilt: Jedes Element $f \in R$ besitzt einen eindeutigen Vertreter $\sum_{i=0}^{<\infty} a_i X^i$ mit $a_0 \in \mathbb{Z}$, $a_i \in \{0, ..., 4\}$ für $i \geq 1$.

Behauptung: Die Einheiten in R sind $\overline{\pm 1}$.
Dann folgt wegen $\overline{X} \neq \pm\overline{2X}$ (mit $(*)$), dass R, $\overline{X}$, $\overline{2X}$ tun, was sie tun sollen.

Beweis der Behauptung: Seien $f = \overline{\sum_{i=0}^{m} a_i X^i}, g = \overline{\sum_{i=0}^{n} b_i X^i} \in R \setminus \{\overline{0}\}$ mit $m, n \in \mathbb{N}_0$ und $a_i, b_i \in \{0, ..., 4\}$ für alle $i \geq 1$. m, n seien dabei so gewählt, dass $a_m, b_n \neq 0$.
Es ist $\overline{1} = f \cdot g = \overline{a_m b_n X^{m+n} + ...}$ und da 5 eine Primzahl, also $a_n b_m \notin 5\mathbb{Z}$ ist, folgt (mit $(*)$, dass $X^{m+n} = X^0$, also $m = n = 0$. Weiterhin gilt dann $a_0 b_0 = 1$, also $a_0 = b_0 \in \{\pm 1\}$ wie behauptet.

Aufgabe 2 (8 Punkte)
Sei $\mathcal{A}$ der Ring der arithmetischen Funktionen. Die eulersche φ-Funktion, die konstante Funktion $\eta \equiv 1$ und die kanonische Einbettung $\mathrm{Id}_{\mathbb{N}}$ sind Elemente aus $\mathcal{A}$. Zeige:

a) Das Produkt zweier multiplikativer arithmetischer Funktionen ist multiplikativ.

b) Die Inverse einer multiplikativ arithmetischen Funktion ist multiplikativ.
(*Hinweis:* Überlege dir zunächst, wieso es reicht, zu zeigen, dass $\beta(p^e \cdot m) = \beta(p^e) \cdot \beta(m)$ für alle $p \in \mathbb{P}$, $e \in \mathbb{N}_0$ und für alle zu p teilerfremden $m \in \mathbb{N}$ gilt. Diese Aussage kann etwa mit doppelter Induktion nach e und m bewiesen werden.)

c) Die Menge aller multiplikativen arithmetischen Funktionen ist eine Untergruppe von $\mathcal{A}^\times$.

d) Es ist $\mathrm{Id}_{\mathbb{N}} = \eta * \varphi$.

e) Für alle $k \in \mathbb{N}_0$ ist die *Teilerpotenzsummenfunktion* $\sigma_k \colon \mathbb{N} \to \mathbb{N}$, gegeben durch $\sigma_k(n) = \sum\limits_{d|n} d^k$, multiplikativ.

Lösung:
Vorüberlegung 1: Sind $m, n \in \mathbb{N}$ teilerfremde Zahlen, so ist die Abbildung $(e, f) \mapsto ef$ eine Bijektion zwischen $\{e \in \mathbb{N} : e|m\} \times \{f \in \mathbb{N} : f|n\}$ und $\{d \in \mathbb{N} : d|mn\}$.
Das sehen wir direkt an der Primzerlegung und haben es schon im Tutorium diskutiert.
Vorüberlegung 2: Stimmen zwei multiplikative arithmetische Funktionen ψ_1, ψ_2 auf allen Primpotenzen überein, so gilt $\psi_1 = \psi_2$, denn für alle $n = \prod\limits_{p\in\mathbb{P}} p^{v_p(n)}$ gilt dann

$$\psi_1(n) = \psi_1(\prod_{p\in\mathbb{P}} p^{v_p(n)}) \overset{\text{Mult.}}{=} \prod_{p\in\mathbb{P}} \psi_1(p^{v_p(n)}) = \prod_{p\in\mathbb{P}} \psi_2(p^{v_p(n)}) \overset{\text{Mult.}}{=} \psi_2(\prod_{p\in\mathbb{P}} p^{v_p(n)}) = \psi_2(n).$$

a) Wir benutzen die Vorüberlegung 1. Seien ψ_1, ψ_2 multiplikative arithmetische Funktionen. Sicher ist $(\psi_1 * \psi_2)(1) = \sum\limits_{d|1} \psi_1(d) \cdot \psi_2(\frac{1}{d}) = \psi_1(1) \cdot \psi_2(1) = 1 \cdot 1 = 1$.
Seien nun m, n teilerfremd. Dann ist
$(\psi_1 * \psi_2)(m) \cdot (\psi_1 * \psi_2)(n) = \left(\sum\limits_{e|m} \psi_1(e) \cdot \psi_2(\frac{m}{e})\right) \cdot \left(\sum\limits_{f|n} \psi_1(f) \cdot \psi_2(\frac{n}{f})\right) = \sum\limits_{e|m} \sum\limits_{f|n} \psi_1(e) \cdot \psi_1(f) \cdot$
$\psi_2(\frac{m}{e}) \cdot \psi_2(\frac{n}{f}) \overset{\text{Mult.}}{=} \sum\limits_{e|m} \sum\limits_{f|n} \psi_1(ef) \cdot \psi_2(\frac{mn}{ef}) \overset{V1}{=} \sum\limits_{d|mn} \psi_1(d) \cdot \psi_2(\frac{mn}{d}) = (\psi_1 * \psi_2)(mn)$.
Dabei benutzen wir, dass auch e und f beziehungsweise $\frac{m}{e}$ und $\frac{n}{f}$ als Teiler teilerfremder Zahlen teilerfremd sind.

b) Sei nun ψ multiplikativ und $\xi := \psi^{-1}$ ihre Inverse. Zu zeigen ist, dass ξ multiplikativ ist.
Wegen $\psi(1) = 1$ und da $\xi * \psi$ das Einselement (also $(\xi * \psi)(1) = 1, (\xi * \psi)(n) = 0$ für $n > 1$) ist, berechnen wir

$$\xi(1) = \xi(1)\psi(1) = (\xi * \psi)(1) = 1.$$

Es verbleibt zu zeigen, dass $\xi(mn) \overset{(!)}{=} \xi(m)\xi(n)$ für teilerfremde m, n ist.

Behauptung: Es reicht, zu zeigen, dass wir Primpotenzen abspalten können, also

$$\xi(p^e \cdot m) \overset{(!)}{=} \xi(p^e)\xi(m) \text{ für } p \nmid m, m \in \mathbb{N}, e \in \mathbb{N}_0.(*)$$

Beweis der Behauptung: Unter dieser Voraussetzung können wir dann beliebige teilerfremde Produkte zerlegen: Jedes $n \in \mathbb{N}$ zerfällt in Primpotenzen $n = p_1^{e_1} \cdot ... \cdot p_r^{e_r}$ mit paarweise verschiedene Primzahlen p_i, die nicht in der Primzerlegung von m vorkommen, e_r in $\mathbb{N}$, $r \in \mathbb{N}_0$).
Mit der Voraussetzung können wir diese einzeln abspalten. Anschließend können wir sie dann einzeln wieder anfügen. Formal liest sich das etwa so:
$\xi(m \cdot n) = \xi(m \cdot \prod_{i=1}^{r} p_i^{e_i}) = \xi((m \cdot \prod_{i=2}^{r} p_i^{e_i}) \cdot p_1^{e_1}) \overset{(*)}{=} \xi(m \cdot \prod_{i=2}^{r} p_i^{e_i}) \cdot \xi(p_1^{e_1}) \overset{(*)}{=} \xi(m \cdot \prod_{i=3}^{r} p_i^{e_i}) \cdot \xi(p_2^{e_2}) \cdot \xi(p_1^{e_1}) = ... = \xi(m) \cdot \prod_{i=1}^{r} \xi(p_i^{e_i}) = ...$
Aber dies gilt doch für alle m und für $m = 1$ (mit $\xi(m) = 1$) lesen wir gerade $\xi(n) = \prod_{i=1}^{r} \xi(p_i^{e_i})$, womit der letzte Term also
$... = \xi(m)\xi(n)$ ist. (Wer den Trick mit $m = 1$ nicht mag, zieht die Potenzen analog wie vorher mit $(*)$ Stück für Stück wieder zusammen.) □ (Behauptung)

Die Bedingung $\xi(p^e \cdot m) = \xi(p^e)\xi(m)$ zeigen wir per Induktion nach $m \cdot e$.

Induktionsanfang:
Die Aussage ist offensichtlich richtig für $m \cdot e = 0$: Dann ist $e = 0$, also $p^e = 1$.
Außerdem ist sie richtig für $m \cdot e = 1$: Dann ist $m = 1$.
In beiden Fällen können wir den Faktor 1 wegen $\xi(1) = 1$ abspalten.

Induktionsschritt:
Sei $em \geq 2$ und die Aussage richtig **für alle** e', m' mit $e'm' < em$.
Für die nachfolgenden Rechnungen benutzen wir

- die Induktionsvoraussetzung (markiert mit $(*)$) und dass ψ multiplikativ ist,
- dass $(\psi * \xi)(n) = 0$ für $n > 1$ ist und
- dass die Teiler von mp^e nach Vorüberlegung 1 genau die Zahlen dp^k mit $d|m$, $0 \leq k \leq m$ sind.

(Damit man beim Lesen nicht den roten Faden verliert, sollte man sich klar machen, was hier geschieht. Auf die meisten $\xi(...)$ können wir die Induktionsvoraussetzung anwenden. Dazu zerlegen wir die Summen und betrachten diejenigen Werte, für die das nicht geht, einzeln. So zum Beispiel spalten wir den Summanden für den Teiler $d = 1$ von m als erstes ab. Später spalten wir den Summanden für $k = 0$ ab.)

$0 \overset{p^e m > 1}{=} (\psi * \xi)(p^e m) = \sum_{d|m} \sum_{k=0}^{e} \psi(dp^k)\xi(\frac{m}{d}p^{e-k}) = \sum_{d|m, d\neq 1} \sum_{k=0}^{e} \psi(dp^k)\xi(\frac{m}{d}p^{e-k}) + \sum_{k=0}^{e} \psi(p^k)\xi(mp^{e-k})$
$\overset{(*)}{=} \sum_{d|m, d\neq 1} \sum_{k=0}^{e} \psi(d)\psi(p^k)\xi(\frac{m}{d})\xi(p^{e-k}) + \sum_{k=0}^{e} \psi(p^k)\xi(mp^{e-k}) = ...$

(**Nebenrechnung 1:** Es ist

$$\sum_{d|m, d\neq 1} \sum_{k=0}^{e} \psi(d)\psi(p^k)\xi(\frac{m}{d}))\xi(p^{e-k}) = \left(\sum_{d|m, d\neq 1} \psi(d)\xi(\frac{m}{d})\right) \cdot \left(\sum_{k=0}^{e} \psi(p^k)\xi(p^{e-k})\right)$$

$= \left(\sum_{d|m, d\neq 1} \psi(d)\xi(\frac{m}{d}) \right) \cdot (\psi * \xi)(p^e) \overset{p^e>1}{=} \left(\sum_{d|m, d\neq 1} \psi(d)\xi(\frac{m}{d}) \right) \cdot 0 = 0.$

Damit vereinfacht sich der Term oben stark:$\Big)$

$0 = ... = \sum_{k=0}^{e} \psi(p^k)\xi(mp^{e-k}) = \psi(p^0)\xi(mp^e) + \sum_{k=1}^{e} \psi(p^k)\xi(mp^{e-k})$
$\overset{(*)}{=} \xi(mp^e) + \sum_{k=1}^{e} \psi(p^k)\xi(m)\xi(p^{e-k}) = ...$

$\Big($ **Nebenrechnung 2:** Dabei ist

$\sum_{k=1}^{e} \psi(p^k)\xi(m)\xi(p^{e-k}) = \xi(m)\cdot\left(\sum_{k=1}^{e} \psi(p^k)\xi(p^{e-k}) \right) = \xi(m)\cdot\left(\sum_{k=1}^{e} \psi(p^k)\xi(p^{e-k}) + \psi(1)\xi(p^e) - \psi(1)\xi(p^e) \right)$
$= \xi(m) \cdot \left(\sum_{k=0}^{e} \psi(p^k)\xi(p^{e-k}) - \xi(p^e) \right) = \xi(m) \cdot ((\xi * \psi)(p^e) - \xi(p^e)) \overset{p^e>1}{=} -\xi(m)\xi(p^e)$

und damit vereinfachen wir zu$\Big)$

$0 = ... = \xi(mp^e) - \xi(m)\xi(p^e)$ und genau das war zu zeigen. Uff!

c) Die Menge der multiplikativen arithmetischen Funktionen ist eine Teilmenge von $\mathcal{A}^\times$. Sie ist nicht leer, zum Beispiel ist φ nach Vorlesung multiplikativ.
Mit a) und b) und dem Untergruppenkriterium folgt dann die Aussage.

d) Alle beteiligten Funktionen sind multiplikativ – das ist offensichtlich oder aus der Vorlesung bekannt. Insbesondere ist nach a) auch $\eta * \varphi$ multiplikativ.
Nach der Vorüberlegung 2 reicht es, $(\eta * \varphi)(p^e) \overset{(!)}{=} \mathrm{Id}_{\mathbb{N}}(p^e)$ zu zeigen. Die Teiler von p^e sind $p^j, 0 \leq j \leq e$ und wir erhalten
$(\eta * \varphi)(p^e) = \sum_{j=0}^{e} \varphi(p^j) \cdot \eta(p^{e-j}) = \sum_{j=0}^{e} \varphi(p^j) = \varphi(1) + \sum_{j=1}^{e} \varphi(p^j) = 1 + \sum_{j=1}^{e} (p^j - p^{j-1}) =$
$1 + \sum_{j=1}^{e} p^j - \sum_{j=1}^{e} p^{j-1} = 1 + \sum_{j=1}^{e} p^j - \sum_{j=0}^{e-1} p^j = 1 + p^e - p^0 = 1.$

e) Die Abbildung $hk\colon \mathbb{N} \to \mathbb{N}, n \mapsto n^k$ ist (sogar strikt) multiplikativ, denn $hk(1) = 1^k = 1$ und $hk(mn) = (mn)^k = m^k n^k = hk(m) \cdot hk(n)$ für alle $m, n \in \mathbb{N}$.
Für alle $n \in \mathbb{N}$ gilt $\sigma_k(n) = \sum_{d|n} d^k = \sum_{d|n} hk(d) \cdot \eta(\frac{n}{d}) = (hk * \eta)(n)$, also gilt $\sigma_k = hk * \eta$ und damit ist σ_k als Produkt multiplikativer arithmetischer Funktionen wieder eine solche.