D-MATH Algebra I HS 2022
Prof. Richard Pink

Musterlösung Serie 6

Ringe, Homomorphismen, Unterringe, Produkte

1. In jedem Ring R wird das additive Inverse eines Elements x mit $-x$ bezeichnet. Zeige nur mittels der Ringaxiome die folgenden Grundregeln für alle $x, y, z \in R$:

   (a) $0 \cdot x = 0$.

   (b) $(-1) \cdot x = -x$.

   (c) $-xy = (-x)y$.

   (d) $(x - y)z = xz - yz$.

   Lösung: Mit $u := 0 \cdot x$ gilt

   $$u + u \;=\; 0 \cdot x + 0 \cdot x \;=\; (0 + 0) \cdot x \;=\; 0 \cdot x \;=\; u$$

   und folglich

   $$u \;=\; 0 + u \;=\; ((-u) + u) + u \;=\; (-u) + (u + u) \;=\; (-u) + u \;=\; 0,$$

   also gilt (a). Unter Benutzung von (a) folgt (b) aus der Rechnung

   $$(-1) \cdot x + x \;=\; (-1) \cdot x + 1 \cdot x \;=\; ((-1) + 1) \cdot x \;=\; 0 \cdot x \;=\; 0.$$

   Durch zweimalige Anwendung von (b) erhalten wir nun (c) durch

   $$-xy \;=\; (-1) \cdot (xy) \;=\; ((-1) \cdot x)y \;=\; (-x)y.$$

   Daraus wiederum folgt (d) mittels

   $$(x - y)z \;=\; (x + (-y))z \;=\; xz + (-y)z \;=\; xz + (-yz) \;=\; xz - yz.$$

2. Zeige, dass ein Ringhomomorphismus $\psi : R \to S$ genau dann ein Isomorphismus ist, wenn er bijektiv ist.

   Lösung: Sei $\psi : R \to S$ ein bijektiver Ringhomomorphismus. Für alle $s_1, s_2 \in S$ setze $r_1 := \psi^{-1}(s_1)$ und $r_2 := \psi^{-1}(s_2)$. Dann gilt $s_1 = \psi(r_1)$ und $s_2 = \psi(r_2)$. Aus der Homomorphieeigenschaft von ψ folgt

   $$\begin{aligned} s_1 + s_2 &= \psi(r_1) + \psi(r_2) = \psi(r_1 + r_2), \\ s_1 \cdot s_2 &= \psi(r_1) \cdot \psi(r_2) = \psi(r_1 \cdot r_2), \end{aligned}$$

also haben wir

$$\begin{aligned} \psi^{-1}(s_1 + s_2) &= r_1 + r_2 = \psi^{-1}(s_1) + \psi^{-1}(s_2), \\ \psi^{-1}(s_1 \cdot s_2) &= r_1 \cdot r_2 = \psi^{-1}(s_1) \cdot \psi^{-1}(s_2). \end{aligned}$$

Zudem gilt $\psi^{-1}(1_S) = 1_R$ wegen $\psi(1_R) = 1_S$. Somit ist $\psi^{-1} : S \to R$ ebenfalls ein Ringhomomorphismus. Deshalb ist ψ ein Isomorphismus.

Umgekehrt ist ein Ringisomorphismus $\psi\colon R \to S$ insbesondere ein Isomorphismus der unterliegenden Mengen, und folglich bijektiv.

3. Welche der Unterringe

$$\mathbb{Z}[i, \tfrac{1}{5}], \quad \mathbb{Z}[\tfrac{i}{25}], \quad \mathbb{Z}[\tfrac{4i}{5}], \quad \mathbb{Z}[\tfrac{4i}{5}, 4 + 3i]$$

von $\mathbb{C}$ sind gleich?

Lösung: Zuerst bemerken wir, dass sich der Unterring $\mathbb{Z}[i, \frac{1}{5}] \subset \mathbb{C}$ in der Form

$$\mathbb{Z}[i, \tfrac{1}{5}] = \left\{ \tfrac{a+bi}{5^k} \;\middle|\; a, b \in \mathbb{Z},\ k \in \mathbb{Z}^{\geqslant 0} \right\}$$

schreiben lässt. In der Tat ist die rechte Seite ein Unterring von $\mathbb{C}$, da sie unter Addition, Bildung von additiven Inversen und Multiplikation abgeschlossen ist und das Einselement enthält. Zudem enthält sie die Erzeugenden i und $\frac{1}{5}$ und ist wegen $\frac{a+bi}{5^k} = (\frac{1}{5})^k \cdot (a + bi)$ in der linken Seite enthalten. Also ist sie gleich $\mathbb{Z}[i, \frac{1}{5}]$.

Insbesondere ersehen wir daraus, dass die Elemente $\frac{i}{25}$, $\frac{4i}{5}$, $4 + 3i$ alle in $\mathbb{Z}[i, \frac{1}{5}]$ liegen. Somit sind die drei anderen Ringe alle in $\mathbb{Z}[i, \frac{1}{5}]$ enthalten. Umgekehrt liegen die Erzeuger $i = 25 \cdot \frac{i}{25}$ und $\frac{1}{5} = -125 \cdot (\frac{i}{25})^2$ in dem zweiten Ring und wegen $i = 5(\frac{4i}{5}) - (4 + 3i) + 4$ und $\frac{1}{5} = -5(\frac{4i}{5})^2 - 3$ auch in dem vierten Ring. Somit gilt für diese auch die umgekehrte Inklusion, und es gilt

$$\mathbb{Z}[i, \tfrac{1}{5}] = \mathbb{Z}[\tfrac{i}{25}] = \mathbb{Z}[\tfrac{4i}{5}, 4 + 3i].$$

Für den dritten Ring behaupten wir

$$\mathbb{Z}[\tfrac{4i}{5}] = \left\{ \tfrac{a+4bi}{5^k} \;\middle|\; a, b \in \mathbb{Z},\ k \in \mathbb{Z}^{\geqslant 0} \right\}.$$

In der Tat ist die rechte Seite ein Unterring von $\mathbb{C}$, da sie unter Addition, Bildung von additiven Inversen und Multiplikation abgeschlossen ist und das Einselement enthält. Zudem enthält sie $\mathbb{Z}$ und das Erzeugende $\frac{4i}{5}$ des Unterrings $\mathbb{Z}[\frac{4i}{5}]$; somit gilt die Inklusion „$\subset$“. Umgekehrt sind sowohl $\frac{1}{5} = -5 \cdot (\frac{4i}{5})^2 - 3$ als auch $4i = 5 \cdot \frac{4i}{5}$ in der linken Seite enthalten und daher auch $\frac{a+4bi}{5^k} = (\frac{1}{5})^k \cdot (a + b \cdot 4i)$. Darum gilt auch die umgekehrte Inklusion und wir haben die Gleichheit gezeigt.

Aus dieser Gleichung folgt nun, dass i kein Element von $\mathbb{Z}[\frac{4i}{5}]$ ist. Somit ist dieser Ring verschieden von den anderen.

4. Zeige, dass jeder endlich erzeugte unitäre Unterring von $\mathbb{Q}$ die Form $\mathbb{Z}[\frac{1}{n}]$ für ein $n \in \mathbb{Z}^{>0}$ hat. Folgere daraus, dass $\mathbb{Q}$ als Ring über $\mathbb{Z}$ nicht endlich erzeugt ist.

   Lösung: Sei $R \subset \mathbb{Q}$ ein endlich erzeugter unitärer Unterring mit Erzeugenden $\alpha_1, \ldots, \alpha_k \in \mathbb{Q}$. Wegen $1 \in R$ enthält R den Unterring $\mathbb{Z}$, also ist $R = \mathbb{Z}[\alpha_1, \ldots, \alpha_k]$.

   Wir können jedes α_i auf eindeutige Weise schreiben als $\alpha_i = \frac{p_i}{q_i}$ für teilerfremde $p_i \in \mathbb{Z}$ und $q_i \in \mathbb{Z}^{>0}$. Sei $n := \mathrm{kgV}(q_1, \ldots, q_k)$. Dann ist $\alpha_i = \frac{p_i}{q_i} = \frac{p_i d_i}{n}$ für $1 \leqslant i \leqslant k$ mit der ganzen Zahl $d_i := \frac{n}{q_i}$. Also sind alle Erzeugende ganzzahlige Vielfache von $\frac{1}{n}$, und daraus folgt $R = \mathbb{Z}[\alpha_1, \ldots, \alpha_k] \subset \mathbb{Z}[\frac{1}{n}]$.

   Sodann sind für jedes $1 \leqslant i \leqslant k$ die Zahlen p_i und q_i teilerfremd, also existieren nach dem chinesischen Restsatz $a_i, b_i \in \mathbb{Z}$ mit $a_i p_i + b_i q_i = 1$. Daraus folgt dann $\frac{1}{q_i} = a_i \alpha_i + b_i \in R$. Zudem ist n ein Teiler von $q_1 \cdots q_k$, also ist $\frac{1}{n} = \ell \frac{1}{q_1} \cdots \frac{1}{q_k}$ für ein $\ell \in \mathbb{Z}$ und daher auch $\frac{1}{n} \in R$. Dies impliziert die umgekehrte Inklusion; es folgt also $R = \mathbb{Z}[\frac{1}{n}]$.

   Ist nun $R = \mathbb{Z}[\frac{1}{n}] \subset \mathbb{Q}$ ein beliebiger endlich erzeugter unitärer Unterring, so existiert eine Primzahl p mit $p \nmid n$; dann ist $\frac{1}{p} \in \mathbb{Q} \smallsetminus R$, also $R \neq \mathbb{Q}$. Dies zeigt, dass $\mathbb{Q}$ als Ring über $\mathbb{Z}$ nicht endlich erzeugt ist.

*5. Zeige, dass die Einheitengruppe $\mathbb{Z}[\sqrt{3}]^\times \subset \mathbb{R}$ unendlich ist, und bestimme sie.

   Lösung: Wie in der Vorlesung bemerken wir zuerst, dass $\{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$ ein Unterring ist, der einerseits $\mathbb{Z} \cup \{\sqrt{3}\}$ enthält und andererseits in $\mathbb{Z}[\sqrt{3}]$ enthalten ist. Also gilt

$$\mathbb{Z}[\sqrt{3}] \;=\; \big\{a + b\sqrt{3} \;\big|\; a, b \in \mathbb{Z}\big\}.$$

   Sodann gilt für beliebige Elemente $a + b\sqrt{3}$, $c + d\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$

$$(a + b\sqrt{3})(c + d\sqrt{3}) \;=\; (ac + 3bd) + (ad + bc)\sqrt{3}.$$

   Somit ist $a + b\sqrt{3}$ genau dann eine Einheit von $\mathbb{Z}[\sqrt{3}]$, wenn ganze Zahlen c, d existieren mit $ac + 3bd = 1$ und $ad + bc = 0$, und dann hat $a + b\sqrt{3}$ das Inverse $c + d\sqrt{3}$. In diesem Fall gilt

$$(a - b\sqrt{3})(c - d\sqrt{3}) \;=\; (ac + 3bd) - (ad + bc)\sqrt{3} \;=\; 1,$$

   also ist dann $a - b\sqrt{3}$ eine Einheit mit dem Inversen $c - d\sqrt{3}$. Somit ist dann auch $(a+b\sqrt{3})(a-b\sqrt{3}) = a^2 - 3b^2$ eine Einheit mit dem Inversen $(c+d\sqrt{3})(c-d\sqrt{3}) = c^2 - 3d^2$. Da diese beiden Elemente in $\mathbb{Z}$ liegen, sind sie dann schon Einheiten in $\mathbb{Z}$. Für jede Einheit $a + b\sqrt{3}$ gilt also $a^2 - 3b^2 = \pm 1$.

   Wir suchen Lösungen dieser Gleichung mit ein paar kleinen Werten von b:

$$\begin{array}{rcll} b = 0 & \Rightarrow & a^2 = \pm 1 & \Rightarrow\; a = \pm 1 \\ |b| = 1 & \Rightarrow & a^2 = 3 \pm 1 & \Rightarrow\; a = \pm 2 \\ |b| = 2 & \Rightarrow & a^2 = 12 \pm 1 & \Rightarrow\; \text{nicht möglich.} \end{array}$$

Also sind -1 und $w_0 := 2 + \sqrt{3}$ Einheiten. Deshalb ist

$$\left\{\pm(2+\sqrt{3})^n \;\middle|\; n \in \mathbb{Z}\right\} \;\subset\; \mathbb{Z}[\sqrt{3}]^\times. \tag{1}$$

Wegen $w_0 > 1$ ist zudem $w_0^n \to \infty$ für $n \to \infty$; also hat w_0 unendliche Ordnung. Insbesondere ist $\mathbb{Z}[\sqrt{3}]^\times$ daher unendlich.

Schliesslich behaupten wir, dass in (1) schon Gleichheit gilt. Betrachte dafür ein beliebiges $w \in \mathbb{Z}[\sqrt{3}]^\times$. Um zu zeigen, dass w in der linken Seite enthalten ist, können wir nach etwaigem Ersetzen von w durch $-w$ annehmen, dass $w > 0$ ist. Sodann können wir nach Ersetzen von w durch w/w_0^n für ein geeignetes $n \in \mathbb{Z}$ annehmen, dass $\frac{1}{\sqrt{w_0}} \leqslant w \leqslant \sqrt{w_0}$ ist.

Nun schreiben wir $w = a + b\sqrt{3}$. Wegen $(a+b\sqrt{3})(a-b\sqrt{3}) = a^2 - 3b^2 = \pm 1$ ist dann $w^{-1} = \pm(a - b\sqrt{3})$. Insbesondere gilt $|-a+b\sqrt{3}\,| = |w^{-1}| = w^{-1} \leqslant \sqrt{w_0}$. Daraus folgt nun

$$2|b|\sqrt{3} \;\leqslant\; \left|a+b\sqrt{3}\,\right| + \left|-a+b\sqrt{3}\,\right| \;=\; w + w^{-1} \;\leqslant\; 2\sqrt{w_0}$$

und folglich

$$|b| \;\leqslant\; \frac{\sqrt{w_0}}{\sqrt{3}} \;=\; \sqrt{\frac{2+\sqrt{3}}{\sqrt{3}}} \;=\; 1.46... \;<\; 2.$$

Da b eine ganze Zahl ist, lässt dies nur die bereits oben behandelten Fälle übrig, das heisst, die Zahlen ± 1 und $\pm 2 \pm \sqrt{3}$ mit unabhängigen Vorzeichen. Dies sind genau die Zahlen ± 1 und $\pm w_0^{\pm 1}$, also bereits in der linken Seite von (1) enthalten. Somit gilt die gesuchte Gleichheit.

6. Ein Element e eines Rings R mit $e^2 = e$ heisst *idempotent*. Zeige:

   (a) Für jedes Idempotente e ist $e' := 1 - e$ idempotent und es gilt $ee' = e'e = 0$.

   (b) Die Zerlegungen von R in ein Produkt $S \times T$ von Ringen S und T entsprechen eineindeutig den Darstellungen $1 = e + e'$ mit Idempotenten e und e'.

   Hinweis: Die Faktoren S und T entsprechen den Teilmengen Re und Re'. Diese sind aber im Allgemeinen keine Unterringe, weil sie das Einselement nicht enthalten.

   Lösung: Aussage (a) folgt direkt aus den Rechnungen

$$\begin{aligned}(1-e)^2 \;&=\; 1 - 2e + e^2 \;=\; 1 - 2e + e \;=\; 1 - e,\\ e(1-e) \;&=\; (1-e)e \;=\; e - e^2 \;=\; e - e \;=\; 0.\end{aligned}$$

   Für (b) betrachten wir zuerst einen Isomorphismus $\varphi\colon S \times T \xrightarrow{\sim} R$. Dann sind $(1,0)$ und $(0,1)$ idempotent in $S \times T$ und ihre Summe ist das Einselement $(1,1)$. Folglich sind $e := \varphi((1,0))$ und $e' := \varphi((0,1))$ idempotente Elemente von R mit

$e + e' = \varphi((1,1)) = 1$. Zudem gilt dann $S \times \{0\} = (S \times T) \cdot (1,0)$ und folglich $\varphi(S \times \{0\}) = Re$ und analog $\varphi(\{0\} \times T) = Re'$.

Seien umgekehrt Idempotente e, $e' \in R$ gegeben mit $e + e' = 1$. Setze $S := Re$ und $T := Re'$ und betrachte die Abbildungen

$$\varphi\colon S \times T \longrightarrow R, \quad (s,t) \mapsto s + t,$$
$$\psi\colon R \longrightarrow S \times T, \quad r \mapsto (re, re').$$

Wegen $\varphi(\psi(r)) = re + re' = r(e + e') = r1 = r$ ist ψ ein Rechtsinverses von φ. Ausserdem impliziert (a) für jedes $s = re \in S$ sowohl $se = re^2 = re = s$ als auch $se' = see' = s0 = 0$. Für jedes $t \in T$ folgt analog $te = 0$ und $te' = t$. Die Rechnung $\psi(\varphi((s,t))) = ((s+t)e, (s+t)e') = (se + te, se' + te') = (s,t)$ zeigt nun, dass ψ auch ein Linksinverses von φ ist. Darum sind sie zueinander inverse Bijektionen.

Weiter sind für alle $r, r' \in R$ sowohl $re + r'e = (r + r')e$ als auch $(re)(r'e) = rr'ee$ in Re, und es gilt $e(re) = re^2 = re$. Für alle $s, s' \in S$ gilt daher $s + s'$, $ss' \in S$ und $es = s$. Ausserdem ist $0 = 0e \in Re = S$. Die Ringaxiome für R implizieren dann direkt, dass S mit der Einschränkung von $+$ und $\cdot$ und dem Nullelement 0 sowie dem Einselement e ein Ring ist. (Es ist im Allgemeinen aber kein Unterring, weil es das Einselement von R nicht enthält). Analog ist T ein Ring mit dem Einselement e'.

Nun ist $S \times T$ ein Ring mit komponentenweiser Addition und Multiplikation sowie dem Nullelement $(0,0)$ und dem Einselement (e,e'). Sodann ist $\psi(1) = (e,e')$, und für alle r, $r' \in R$ gilt

$$\begin{aligned}
\psi(r) + \psi(r') &= (re, re') + (r'e, r'e') = (re + r'e, re' + r'e') = \psi(r + r'),\\
\psi(r) \cdot \psi(r') &= (re, re') \cdot (r'e, r'e') = (rer'e, re'r'e') = (rr'e, rr'e') = \psi(rr').
\end{aligned}$$

Darum ist ψ ein Ringhomomorphismus. Nach Aufgabe 2 ist es daher ein Ringisomorphismus, und folglich gilt dasselbe für sein Inverses φ.

Schliesslich bemerken wir, dass die beiden Konstruktionen zueinander invers sind, bis auf Isomorphie der Ringe S und T. Somit entsprechen die Zerlegungen von R in ein Produkt von Ringen $S \times T$ eineindeutig den Darstellungen $1 = e + e'$ mit Idempotenten e und e'.

7. Vereinfache die folgenden Ausdrücke im Polynomring $\mathbb{Z}[X,Y,Z]$ für jede natürliche Zahl d, wobei in der Summe jeweils $i, j, k \geqslant 0$ sind:

   (a) $(X - Y) \cdot \sum_{i+j=d} X^i Y^j$.

   (b) $(X - Y)(X - Z)(Y - Z) \cdot \sum_{i+j+k=d} X^i Y^j Z^k$.

Lösung: In (a) haben wir die Teleskopsumme

$$\begin{aligned}(X-Y)\cdot\sum_{i+j=d}X^iY^j &= (X-Y)\cdot\sum_{i=0}^{d}X^iY^{d-i}\\ &= \sum_{i=0}^{d}X^{i+1}Y^{d-i}-\sum_{i=0}^{d}X^iY^{d-i+1}\\ &= \sum_{i=1}^{d+1}X^iY^{d-i+1}-\sum_{i=0}^{d}X^iY^{d-i+1}\\ &= X^{d+1}-Y^{d+1}.\end{aligned}$$

Dies setzen wir mehrfach in (b) ein und erhalten:

$$\begin{aligned}(X-Y)(X-Z)(Y-Z)\cdot\sum_{i+j+k=d}X^iY^jZ^k &= (X-Z)(Y-Z)\cdot\sum_{k=0}^{d}\left((X-Y)\cdot\sum_{i+j=d-k}X^iY^j\right)Z^k\\ &\overset{(a)}{=} (X-Z)(Y-Z)\cdot\sum_{k=0}^{d}\left(X^{d-k+1}-Y^{d-k+1}\right)Z^k\\ &= (X-Z)(Y-Z)X\cdot\sum_{\ell+k=d}X^\ell Z^k-(X-Z)(Y-Z)Y\cdot\sum_{\ell+k=d}Y^\ell Z^k\\ &\overset{(a)}{=} (Y-Z)X(X^{d+1}-Z^{d+1})-(X-Z)Y(Y^{d+1}-Z^{d+1})\\ &= YX^{d+2}-YXZ^{d+1}-ZX^{d+2}+XZ^{d+2}-XY^{d+2}+XYZ^{d+1}+ZY^{d+2}-YZ^{d+2}\\ &= YX^{d+2}-ZX^{d+2}+XZ^{d+2}-XY^{d+2}+ZY^{d+2}-YZ^{d+2}\\ &= (Y-Z)X^{d+2}+(Z-X)Y^{d+2}+(X-Y)Z^{d+2}.\end{aligned}$$