D-MATH Algebra I HS 2015
Prof. Richard Pink

Musterlösung 2

Einheiten, Produkte, Quotientenkörper

1. Bestimme die Einheitengruppe $\mathbb{Z}[\sqrt{3}]^\times \subset \mathbb{R}$, und zeige, dass sie unendlich ist.

   Lösung: Zunächst stellen wir fest, dass $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$ ist, da die rechte Seite in der linken enthalten ist und schon selbst ein Unterring von $\mathbb{R}$ ist. Da 1 und $\sqrt{3}$ linear unabhängig über $\mathbb{Q}$ sind, ist dabei die Darstellung $a + b\sqrt{3}$ eindeutig. Daher ist durch $a+b\sqrt{3} \mapsto a-b\sqrt{3}$ eine eindeutige bijektive Abbildung $\mathbb{Z}[\sqrt{3}] \to \mathbb{Z}[\sqrt{3}]$ definiert. Direkte Rechnung zeigt, dass diese ein Homomorphismus ist. Wegen Serie 1, Aufgabe 2, ist sie somit ein Automorphismus.

   Für jede Einheit $a + b\sqrt{3}$ ist also auch $a - b\sqrt{3}$ eine Einheit, und somit auch $(a + b\sqrt{3}) \cdot (a - b\sqrt{3}) = a^2 - 3b^2$. Insbesondere ist $a^2 - 3b^2 \neq 0$, und auch sein Inverses ist eine Einheit in $\mathbb{Z}[\sqrt{3}]$. Aber $a^2 - 3b^2$ und sein Inverses liegen auch in $\mathbb{Q}$. Daher liegen sie in $\mathbb{Z}$, also in $\mathbb{Z}^\times$, und es gilt $a^2 + 3b^2 = \pm 1$.

   Der Fall $b = 0$ liefert die Möglichkeiten $a = \pm 1$, der Fall $b = \pm 1$ die Möglichkeiten $a = \pm 2$. Insbesondere ist $w_0 := 2 + \sqrt{3}$ eine Einheit. Da die Einheiten eine Gruppe bilden, folgt

   $$\mathbb{Z}[\sqrt{3}]^\times \supset \{\pm(2 + \sqrt{3})^n \mid n \in \mathbb{Z}\}.$$

   Wir behaupten umgekehrt, dass jedes $w \in \mathbb{Z}[\sqrt{3}]^\times$ in der rechten Seite enthalten ist. Jedenfalls ist $w \neq 0$. Nach etwaigem Ersetzen von w durch $-w$ können wir oBdA $w > 0$ annehmen. Da $w_0 > 1$ ist, existiert dann ein $n \in \mathbb{Z}$ mit $w_0^{n-\frac{1}{2}} \leqslant w \leqslant w_0^{n+\frac{1}{2}}$. Nach Ersetzen von w durch w/w_0^n gilt dann oBdA $\frac{1}{\sqrt{w_0}} \leqslant w \leqslant \sqrt{w_0}$. Für jede Wahl der Vorzeichen gilt also $\pm w^{\pm 1} \leqslant \sqrt{w_0}$.

   Schreibe nun $w = a + b\sqrt{3}$. Wegen $(a + b\sqrt{3}) \cdot (a - b\sqrt{3}) = a^2 - 3b^2 = \pm 1$ ist dann $w^{-1} = \pm(a - b\sqrt{3})$. Wegen $\pm w^{\pm 1} \leqslant \sqrt{w_0}$ gilt dann auch $\pm a \pm b\sqrt{3} \leqslant \sqrt{w_0}$ für jede Wahl der Vorzeichen. Insbesondere ist $|a| + |b|\sqrt{3} \leqslant \sqrt{w_0} = 1.91...$. Wegen $b \in \mathbb{Z}$ folgt daraus $|b| \leqslant 1$. Wir haben schon gesehen, dass dies nur die Möglichkeiten $w = \pm 1$ und $\pm 2 \pm \sqrt{3} = \pm w_0^{\pm 1}$ lässt. Von diesen erfüllt aber nur $w = 1$ die Bedingung $\frac{1}{\sqrt{w_0}} \leqslant w \leqslant \sqrt{w_0}$. Da dieses in der rechten Seite liegt, sind wir fertig. Es gilt also

   $$\mathbb{Z}[\sqrt{3}]^\times = \{\pm(2 + \sqrt{3})^n \mid n \in \mathbb{Z}\}.$$

   Wegen $2 + \sqrt{3} > 1$ sind die Werte $\pm(2 + \sqrt{3})^n \in \mathbb{R}$ paarweise verschieden; also ist $\mathbb{Z}[\sqrt{3}]^\times$ unendlich.

2. Sei $n \in \mathbb{Z}^{>0}$.

   (a) Bestimme die Einheitengruppe $\mathbb{Z}[\frac{1}{n}]^\times$.

   (b) Bestimme alle Primelemente von $\mathbb{Z}[\frac{1}{n}]$.

Lösung: An arbitrary element of $\mathbb{Z}[\frac{1}{n}]$ has the form $\sum_{i=0}^{k} a_i(\frac{1}{n})^i = \frac{a_k+a_{k-1}n+...+a_0n^k}{n^k}$ where the $a_i \in \mathbb{Z}$. Thus

$$\mathbb{Z}[\tfrac{1}{n}] = \{\frac{a}{n^i} \mid a, i \in \mathbb{Z}, i \geqslant 0\}$$

.

(a) Let $n = p_1^{e_1}p_2^{e_2}...p_k^{e_k}$ be the prime factorization of n. We claim that

$$\mathbb{Z}[\tfrac{1}{n}]^\times = \{\pm p_1^{i_1}p_2^{i_2}...p_k^{i_k} \mid (i_1, ..., i_k) \in \mathbb{Z}^k\}.$$

Suppose $a = \pm p_1^{i_1}p_2^{i_2}...p_k^{i_k}$ is of the above form and let $m \in \mathbb{Z}$ be such that $r_j := me_j - i_j \geqslant 0$ for $j = 1, ..., k$. Then $x := \pm p_1^{r_1}p_2^{r_2}...p_k^{r_k} \cdot n^{-m} \in \mathbb{Z}[\frac{1}{n}]$ and $ax = 1$. Thus a is a unit.

Conversely, suppose $a \in \mathbb{Z}[\frac{1}{n}]^\times$. Since the property of being a unit is preserved by association, we may assume that a is positive. By definition, there exists an $x \in \mathbb{Z}[\frac{1}{n}]$ such that $ax = 1$. Writing $a = \frac{a'}{n^s}$ and $x = \frac{x'}{n^t}$, we see that $a'x' = n^{r+s}$. Thus $a'|n^{r+s}$ and $a' = p_1^{i_1}p_2^{i_2}...p_k^{i_k}$ for some $i_j \geqslant 0$ for each $j = 1, ..., k$. Thus

$$a = p_1^{i_1-e_1s}p_2^{i_2-e_2s}...p_k^{i_k-e_3s}$$

is of the desired form.

(b) We claim that the prime elements of $\mathbb{Z}[\frac{1}{n}]$ are exactly the elements associated to prime numbers $p \in \mathbb{Z}$ such that $p \nmid n$.

Let p be a prime number not dividing n, and let $a, b \in \mathbb{Z}[\frac{1}{n}]$ be such that $p|ab$. Then there exists an $x \in \mathbb{Z}[\frac{1}{n}]$ such that $px = ab$. Writing $a = \frac{a'}{n^s}$ and $b = \frac{b'}{n^t}$ and $x = \frac{x'}{n^u}$, we attain $px'n^{(s+t)} = n^u a'b'$. Therefore $p|n^u a'b'$ in $\mathbb{Z}$. Since $p \nmid n$, we must have $p|a'b'$ in $\mathbb{Z}$. Since p is a prime number, we have $p|a'$ or $p|b'$ in $\mathbb{Z}$. WLOG suppose $p|a'$. Then there exists a $y \in \mathbb{Z}$ such that $py = a'$. Then $p\frac{y}{n^s} = \frac{a'}{n^s} = a$ and so $p|a$ and is thus prime in $\mathbb{Z}[\frac{1}{n}]$. Since association preserves primeness, every element associated to p is also prime.

Now let $p \in \mathbb{Z}[\frac{1}{n}]$ be a prime element. We may assume without loss of generality that p is positive. Write $p = \frac{p'}{n^i}$. Since n^i is a unit in $\mathbb{Z}[\frac{1}{n}]$, we may further assume that p is an integer.

Let $q \in \mathbb{Z}$ be a prime number dividing both p and n. Then q is a unit by (a) and we may replace p by $\frac{p}{q}$. After repeating this process finitely many times, we may assume that p and n are relatively prime.

Let $a, b \in \mathbb{Z}$ be such that $p|ab$. Since p is a prime element, we must have $p|a$ or $p|b$ in $\mathbb{Z}[\frac{1}{n}]$. Without loss of generality, we assume $p|a$. Then there is an element $x \in \mathbb{Z}[\frac{1}{n}]$ such that $px = a$. Writing $x = \frac{x'}{n^t}$, we attain $px' = an^t$
Thus $p|an^t$ in $\mathbb{Z}$. Since n and p are relatively prime, we must have $p|a$ in $\mathbb{Z}$. As $a, b \in \mathbb{Z}$ were arbitrary, we conclude that p is a prime number.

3. Sei R ein Ring. Ein Element $e \in R$ mit $e^2 = e$ heisst *idempotent*. Zeige, dass die Zerlegungen von R in ein Produkt $S \times T$ von Ringen S und T eineindeutig den Darstellungen $1 = e + e'$ mit e und e' idempotent entsprechen.

   Lösung: Sei $1 = e + e'$ mit $e, e \in R$ idempotent. Wir setzen $S := Re$ und $T := Re'$. Für $s_1, s_2 \in S$ gibt es $r_1, r_2 \in R$, so dass $s_1 = r_1 e$ und $s_2 = r_2 e$ sind. Dann ist $s_1 - s_2 = r_1 e - r_2 e = (r_1 - r_2)e \in S$ und $s_1 s_2 = (r_1 e)(r_2 e) = r_1 r_2 e^2 = r_1 r_2 e \in S$. Somit ist S unter $+, -$ und $\cdot$ geschlossen. Wegen $s_1 e = e s_1 = e(r_1 e) = (r_1 e)e = r_1 e^2 = r_1 e = s_1$, ist S ein nicht-trivialer Ring mit Einselement e. Analog ist T ein Ring mit Einselement e'.

   Wir zeigen nun, dass R das direkte Produkt von S und T ist, d.h. dass die natürliche Abbildung

$$\begin{array}{rccc} \varphi: & S \times T & \longrightarrow & R \\ & (x, y) & \longmapsto & x + y \end{array}$$

   ein Ringisomorphismus ist. Für $r_1 e, r_2 e \in S$ und $r_1' e', r_2' e' \in T$ mit $r_1, r_2, r_1', r_2' \in R$ gilt wegen $ee' = e(1 - e) = e - e^2 = 0$

$$\begin{aligned} \varphi(r_1 e, r_1' e')\varphi(r_2 e, r_2' e') &= (r_1 e + r_1' e')(r_2 e + r_2' e') = (r_1 e)(r_2 e) + (r_1' e')(r_2' e') \\ &= \varphi((r_1 e, r_1' e')(r_2 e, r_2' e')). \end{aligned}$$

   Somit ist φ multiplikativ und wegen der Kommutativität der Addition auch additiv. Zudem ist $\varphi(1_{S \times T}) = \varphi(e, e') = e + e' = 1_R$. Also ist φ ein Ringhomomorphismus.

   Da sich jedes Element $r \in R$ durch $r = r \cdot 1 = r(e + e') = re + re'$ als Summe von Elementen in S und T schreiben lässt, ist φ surjektiv.

   Sei weiter $\varphi(re, r'e') = re + r'e' = 0$. Dann folgt durch Multiplikation mit e von rechts $0 = re^2 + r'e'e = re$, wobei wir wiederum $ee' = e'e = 0$ benutzt haben. Analog folgt $r'e' = 0$ durch Multiplikation mit e'. Somit ist φ auch injektiv. Nach Serie 1, Aufgabe 2 ist daher φ ein Ringisomorphismus.

   Falls umgekehrt es einen Isomorphismus $\varphi : S \times T \to R$ gibt, setzen wir $e := \varphi(1_S, 0)$ und $e' := \varphi(0, 1_T)$. Dann sind e und e' idempotent. Zudem bildet φ als Ringhomomorphismus das Einselement (e, e') von $S \times T$ auf 1_R ab, also gilt $1_R = e + e'$.

   Zudem gilt in diesem Fall $\varphi(S \times \{0\}) = Re$ und $\varphi(\{0\} \times T) = Re'$. Denn für $re \in Re$ mit $r = \varphi(s, t)$ gilt wegen der Multiplikativität von φ

$$re = \varphi(s, t)\varphi(1_S, 0) = \varphi(s, 0) = s \in S$$

und umgekehrt ist $s = se \in Re$ für jedes $s \in S$. Analog folgt $\varphi(T) = Re'$.

Es folgt daraus, dass die natürliche Ringisomorphismus $Re \times Re' \to R$ einen natürlichen Isomorphismus $Re \times Re' \cong S \times T$ ergibt.

Insgesamt haben wir somit gezeigt, dass die Zerlegungen von R in ein Produkt $S \times T$ von Ringen S und T eineindeutig den Darstellungen $1 = e + e'$ mit $e, e' \in R$ idempotent entsprechen.

4. Sei K ein Körper, und sei $K((X))$ die Menge aller beidseitig unendlichen Folgen $(a_n)_{n\in\mathbb{Z}}$ in K, für die ein $N \in \mathbb{Z}$ existiert, so dass $a_n = 0$ für alle $n < N$ ist. Diese Folgen schreiben wir als *formale Laurentreihen mit endlichem Hauptteil* $\sum_{n=N}^{\infty} a_n X^n$.

   (a) Definiere Rechenoperationen + und $\cdot$ auf $K((X))$ in Analogie zu $K[[X]]$ und zeige, dass damit $K((X))$ ein Körper ist.

   (b) Konstruiere einen natürlichen Isomorphismus $\mathrm{Quot}(K[[X]]) \cong K((X))$.

   Lösung:

   (a) Die Operationen auf $K((X))$ definieren wir gleich wie auf dem Ring der formalen Potenzreihen:

$$\begin{aligned} (a_n) + (b_n) &:= (a_n + b_n) \\ (a_n)(b_n) &:= \left(\textstyle\sum_{i+j=n} a_i b_j\right) \end{aligned}$$

   Beachte, dass die Summe in der Definition der Multiplikation nur über endlich viele Terme geht, da $N, M \in \mathbb{Z}$ existieren mit $a_i = 0$ für $i < N$ und $b_j = 0$ für $j < M$.

   Wie bei den formalen Potenzreihen prüft man nach, dass $K((X))$ mit diesen Operationen ein Ring ist. Zudem können wir $K[[X]]$ mit dem Unterring von $K((X))$ der Folgen $(a_n)_{n\in\mathbb{Z}}$ mit $a_n = 0$ für $n < 0$ identifizieren.

   Es bleibt zu zeigen, dass jedes von Null verschiedene Element $f \in K((X))$ invertierbar ist. Ein solches Element lässt sich als $f = \sum_{n=N}^{\infty} a_n X^n$ mit $a_N \neq 0$ schreiben und erfüllt $f = X^N g$, wobei $g = \sum_{n=0}^{\infty} b_n X^n \in K[[X]]$ mit $b_n := a_{n+N}$ ist. Wegen $b_0 = a_N \neq 0$ ist g nach Aufgabe 5. b) der Serie 1 in $K[[X]]$ invertierbar, es gibt also ein $h \in K[[X]]$ mit $hg = 1$. Dafür ist

$$(hX^{-N})f = hX^{-N}X^N g = hg = 1.$$

   Deshalb ist f in $K((X))$ invertierbar mit $f^{-1} = hX^{-N}$.

   (b) Nach oben ist $K[[X]]$ im Körper $K((X))$ enthalten. Nach der universellen Eigenschaft des Quotientenkörpers gibt es darum einen Körperhomomorphismus $i : \mathrm{Quot}(K[[X]]) \to K((X))$ mit Bild

$$Q_{K[[X]]} = \left\{ \frac{g}{h} \;\middle|\; g, h \in K[[X]],\, h \neq 0 \right\}.$$

In (a) haben wir festgestellt, dass sich jedes Element $f \in K((X))$ als $f = X^N g$ mit $N \in \mathbb{Z}$ und $g \in K[[X]]$ schreiben lässt. Falls $N \geqslant 0$ ist, liegt f in $K[[X]]$ und daher in $Q_{K[[X]]}$. Andernfalls ist $-N > 0$ und $f = \frac{g}{X^{-N}} \in Q_{K[[X]]}$. Es ist also $Q_{K[[X]]} = K((X))$ und i ist surjektiv. Als Körperhomomorphismus ist i aber auch injektiv und somit ein Isomorphismus $\mathrm{Quot}(K[[X]]) \xrightarrow{\sim} K((X))$.

5. Sei S die Menge aller Funktionen $\mathrm{dom}(f) \to \mathbb{R}$ für alle Teilmengen $\mathrm{dom}(f) \subset \mathbb{R}$ mit $|\mathbb{R} \smallsetminus \mathrm{dom}(f)| < \infty$, so dass $u, v \in \mathbb{R}[X]$ existieren mit $\forall x \in \mathrm{dom}(f)\colon v(x) \neq 0$ und $f(x) = \frac{u(x)}{v(x)}$.

   Wir nennen zwei Funktionen $f, g \in S$ *äquivalent*, wenn ihre Werte auf einer geeigneten Teilmenge $X \subset \mathrm{dom}(f) \cap \mathrm{dom}(g)$ mit $|\mathbb{R} \smallsetminus X| < \infty$ übereinstimmen.

   (a) Zeige, dass dies eine Äquivalenzrelation auf S ist. Sei K die Menge ihrer Äquivalenzklassen.

   (b) Definiere Operationen $+$ und $\cdot$ auf K sowie Elemente $0, 1 \in K$, und zeige, dass das Tupel $(K, +, \cdot, 0, 1)$ ein Körper ist.

   (c) Konstruiere einen natürlichen Isomorphismus $\mathbb{R}(X) \xrightarrow{\sim} K$.

   In diesem Sinn ist es berechtigt, die Elemente von $\mathbb{R}(X)$ *rationale Funktionen* zu nennen.

   Lösung:

   (a) That $\sim$ is symmetric and reflexive is clear. For transitivity, suppose that $f \sim g$ and $g \sim h$. Take subsets $X \subset \mathrm{dom}(f) \cap \mathrm{dom}(g)$ and $Y \subset \mathrm{dom}(g) \cap \mathrm{dom}(h)$ with $|\mathbb{R} \smallsetminus X| < \infty$ and $|\mathbb{R} \smallsetminus Y| < \infty$, such that $f|_X = g|_X$ and $g|_Y = h|_Y$. Then $Z := X \cap Y \subset \mathrm{dom}(f) \cap \mathrm{dom}(h)$ with $|\mathbb{R} \smallsetminus Z| < \infty$ and $f|_Z = g|_Z = h|_Z$. Therefore $f \sim h$.

   (b) For any f, $g \in S$ we define

$$\begin{aligned} f + g &\colon \mathrm{dom}(f) \cap \mathrm{dom}(g) \to \mathbb{R}, \quad x \mapsto f(x) + g(x), \\ f \cdot g &\colon \mathrm{dom}(f) \cap \mathrm{dom}(g) \to \mathbb{R}, \quad x \mapsto f(x) \cdot g(x). \end{aligned}$$

   These functions again lie in S. Consider any $f, f', g, g' \in S$ with $f \sim f'$ and $g \sim g'$. Take subsets $X \subset \mathrm{dom}(f) \cap \mathrm{dom}(f')$ and $Y \subset \mathrm{dom}(g) \cap \mathrm{dom}(g')$ with $|\mathbb{R} \smallsetminus X| < \infty$ and $|\mathbb{R} \smallsetminus Y| < \infty$, such that $f|_X = f'|_X$ and $g|_Y = g'|_Y$. Then $Z := X \cap Y$ satisfies $|\mathbb{R} \smallsetminus Z| < \infty$, and we have $(f+g)|_Z = f|_Z + g|_Z = f'|_Z + g'|_Z = (f'+g')|_Z$ and likewise $(f \cdot g)|_Z = \ldots = (f' \cdot g')|_Z$. Therefore $f + g \sim f' + g'$ and $f \cdot g \sim f' \cdot g'$. Thus the operations yield well-defined maps

$$\begin{aligned} K \times K \to K, \quad ([f], [g]) &\mapsto [f] + [g] := [f + g], \\ K \times K \to K, \quad ([f], [g]) &\mapsto [f] \cdot [g] := [f \cdot g]. \end{aligned}$$

Let $0, 1 \in S$ denote the constant functions $\mathbb{R} \to \mathbb{R}$ with values $0, 1$, respectively. We claim that with these operations and the elements [0] and [1] the set K becomes a field.

The associativity, commutativity, and distributivity laws as well as the laws for the identity elements follow by direct, if tedious, calculation from the ring axioms for the values of the functions at any $x \in \mathbb{R}$.

The additive inverse of an element $[f]$ is $[-f]$, because on $\mathrm{dom}(f)$ we have $(f + (-f))(x) = f(x) - f(x) = 0$ and therefore $f + (-f) \sim 0$ in S and hence $[f] + [-f] = [0]$.

Next the functions 0 and 1 do not agree anywhere on $\mathbb{R}$; in particular not on a subset $X \subset \mathbb{R}$ with $|\mathbb{R} \smallsetminus X| < \infty$. Thus $0 \not\sim 1$; in other words $[0] \neq [1]$.

Finally consider any $[f] \in K \smallsetminus \{[0]\}$. Choose $u, v \in \mathbb{R}[X]$ with $\forall x \in \mathrm{dom}(f) : v(x) \neq 0$ und $f(x) = \frac{u(x)}{v(x)}$. In the case $u = 0$ we would have $f(x) = 0$ for all $x \in \mathrm{dom}(f)$ and hence $f \sim 0$ and $[f] = [0]$, contrary to the assumption. Thus $u \neq 0$. As a non-zero polynomial it has at most finitely many zeros in $\mathbb{R}$. Thus $X := \{x \in \mathrm{dom}(f) \mid u(x) \neq 0\}$ again satisfies $|\mathbb{R} \smallsetminus X| < \infty$. Define $f' \colon X \to \mathbb{R}$ by $f'(x) := \frac{v(x)}{u(x)}$. Then $f' \in S$, and the fact that $\forall x \in X \colon f(x) \cdot f'(x) = 1$ implies that $f \cdot f' \sim 1$, or equivalently $[f] \cdot [f'] = [1]$. This proves the last of the field axioms.

(c) To any polynomial $u \in \mathbb{R}[X]$ we associate the polynomial function $\tilde{u} \colon \mathbb{R} \to \mathbb{R}$, $x \mapsto u(x)$. By the definition of the ring structure of K this defines a ring homomorphism $\mathbb{R}[X] \to K$, $u \mapsto [\tilde{u}]$. For any distinct $u, v \in \mathbb{R}[X]$ the polynomial $u - v$ has at most finitely many zeros in $\mathbb{R}$; hence the set $\{x \in \mathbb{R} \mid u(x) = v(x)\}$ is finite. Thus $\tilde{u} \not\sim \tilde{v}$; in other words $[\tilde{u}] \neq [\tilde{v}]$. Thus the homomorphism $\mathbb{R}[X] \to K$ is injective. By the universal property of the quotient field, it extends to a unique field homomorphism $\mathbb{R}(X) := \mathrm{Quot}(\mathbb{R}[X]) \to K$. As a field homomorphism this is automatically injective. On the other hand, for any $[f] \in K$ by definition there exist $u, v \in \mathbb{R}[X]$ with $\forall x \in \mathrm{dom}(f) \colon v(x) \neq 0$ und $f(x) \cdot v(x) = u(x)$. This means that $[f] \cdot [\tilde{v}] = [\tilde{u}]$ with $[\tilde{v}] \neq [0]$, or equivalently $[f] = [\tilde{u}]/[\tilde{v}]$. Thus $[f]$ lies in the image, and so the homomorphism is surjective. It is therefore an isomorphism.