Lösung 2

Quotientenkörper, Polynomringe, Ideale

1. (a) (**SAGE**) Erstellen Sie eine Liste aller Zahlen bis 100, die sich als Summe von 3 Quadratzahlen (ohne Vielfachheiten) schreiben lassen.
   Hinweis:
   i. Erstellen Sie zuerst eine ungeordnete Liste L aller Summen von 3 Quadratzahlen bis 100. Hier ist der Befehl *in range($n+1$)* (dies geht alle Zahlen von 0 bis n durch) hilfreich.
   ii. Gehen Sie im nächsten Schritt alle Zahlen von 1 bis 100 durch und überprüfen Sie, ob sie in der Liste L sind. Hier ist der Befehl *in* L (dies überprüft, ob ein Element in L liegt) hilfreich.

   (b) Verwenden Sie (a), um die Gesetzmässigkeit für die Darstellbarkeit von m als Summe von 3 Quadratzahlen zu erkennen.

2. Seien R und S zwei kommutative Ringe.

   (a) Zeigen Sie, dass die Menge $R \times S$, bezüglich komponentenweiser Addition und Multiplikation ein kommutativer Ring ist.

   (b) Bestimmen Sie $(R \times S)^\times$.

   (c) Zeigen Sie, dass jedes Ideal in $R \times S$ von der Form $I \times J$ ist, wobei I ein Ideal in R, und J ein Ideal in S ist.

   (d) Zeigen Sie, dass es einen Ringisomorphism

   $$(R \times S)/(R \times \{0\}) \xrightarrow{\sim} S.$$

   gibt.

   (e) Finden Sie alle Ringhomomorphismen $\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$.

3. Sei R ein kommutativer Ring.

   (a) Zeigen Sie, dass für jeden Integritätsbereich R gilt $(R[X])^\times = R^\times$. Kann $R[X]$ ein Körper sein?

   (b) Finde einen Ring R mit $(R[X])^\times \neq R^\times$.

   (c) Zeigen Sie, dass ein Polynom $f = a_n X^n + \ldots + a_0 \in R[X]$ genau dann invertierbar ist, wenn a_0 in R invertierbar ist und die Koeffizienten a_i für $1 \leqslant i \leqslant n$ nilpotent sind, wobei ein Element $a \in R$ *nilpotent* heisst, falls $a^m = 0$ für ein $m \in \mathbb{N}$.

4. Sei R ein Integritätsbereich.

   (a) Zeigen Sie, dass $R[[X]]$ ein Integritätsbereich ist.

   (b) Zeigen Sie, dass $1 - X \in R[[X]]^\times$.

   (c) Als Verallgemeinerung von (b), zeigen Sie, dass

$$R[[X]]^\times := \left\{ \sum_{n\in\mathbb{N}} a_n X^n | a_0 \in R^\times \right\}.$$

   Hinweis: Finden Sie die Koeffizienten der inversen formalen Potenzreihe induktiv.

5. Sei R ein kommutativer Ring und sei $S \subseteq R$ eine Teilmenge, die bezüglich der Ringmultiplikation ein Untermonoid ist. (Es gilt also $1 \in S$ und $ss' \in S$ für alle $s, s' \in S$.) Auf der Menge $R \times S$ betrachten wir die durch

$$(r, s) \sim (r', s') \iff \exists t \in S : (rs' - r's)t = 0$$

   definierte Relation.

   (a) Zeige, dass die Relation $\sim$ eine Äquivalenzrelation ist.

   (b) Es bezeichne $R[S^{-1}]$ die Menge der Äquivalenzklassen bezüglich $\sim$ und $\frac{r}{s}$ die Äquivalenzklasse eines Elementes (r, s). Zeige, dass die durch

$$\frac{r}{s} + \frac{r'}{s'} := \frac{rs' + r's}{ss'} \text{ und } \frac{r}{s} \cdot \frac{r'}{s'} := \frac{rr'}{ss'}$$

   definierten Verknüpfungen wohldefiniert sind und aus $R[S^{-1}]$ einen kommutativen Ring mit Nullelement $\frac{0}{1}$ und Einselement $\frac{1}{1}$ machen, die *Lokalisierung von R nach S*.

   (c) Zeigen Sie, dass $\varphi : R \to R[S^{-1}]$, $r \mapsto \frac{r}{1}$ einen Ringhomomorphismus mit der folgenden Eigenschaft definiert: Für jeden Homomorphismus kommutativer Ringe $\psi : R \to R'$ mit der Eigenschaft $\psi(S) \subseteq (R')^\times$ existiert ein eindeutig bestimmter Ringhomomorphismus $\psi_S : R[S^{-1}] \to R'$ mit $\psi_S \circ \varphi = \psi$. Ist φ immer injektiv?

   (d) Falls R ein Integritätsbereich ist und $S = R \setminus \{0\}$, zeigen Sie, dass $R[S^{-1}] = \mathrm{Quot}(R)$.

   (e) Sei $S = 2\mathbb{Z} \setminus \{0\} \subseteq \mathbb{Z}$. Zeigen Sie, dass $\mathbb{Z}[S^{-1}] = \mathbb{Q}$.

   Lösung:

   (a) i. $(r, s) \sim (r, s)$: Dies ist wahr für jedes $t \in S$, denn $(rs - rs)t = 0t = 0$.

   ii. $(r, s) \sim (r', s') \implies (r', s') \sim (r, s)$: Sei $t \in S$, so dass $(rs' - r's)t = 0$. Dann gilt auch $(r's - rs')t = 0$ und somit $(r', s') \sim (r, s)$.

iii. $(r,s) \sim (r',s'), (r',s') \sim (r'',s'') \implies (r,s) \sim (r'',s'')$: Seien $t, t' \in S$, so dass $(rs' - r's)t = 0$ und $(r's'' - r''s')t' = 0$. Wir überprüfen, dass $(rs'' - r''s)(tt's') = 0$ mit $tt's' \in S$, da $t, t', s \in S$ und S abgeschlossen unter Multiplikation ist.

(b) Seien $(r,s) \sim (u,v)$ und $(r',s') \sim (u',v')$ in $R \times S$. Wir zeigen, dass $\frac{r}{s} + \frac{r'}{s'} \sim \frac{u}{v} + \frac{u'}{v'}$ und $\frac{r}{s}\frac{r'}{s'} \sim \frac{u}{v}\frac{u'}{v'}$. Seien dazu $t, t' \in S$ mit $(rv - su)t = 0$ und $(r'v' - s'u')t' = 0$. Dann gilt $((rs' + r's)vv' - (uv' + u'v)ss')(tt') = 0$ und $(rr'vv' - ss'uu')(tt') = 0$ mit $tt' \in S$, da die Menge S multiplikativ abgeschlossen ist. Somit folgt, dass $\frac{r}{s} + \frac{r'}{s'} \sim \frac{u}{v} + \frac{u'}{v'}$ und $\frac{r}{s}\frac{r'}{s'} \sim \frac{u}{v}\frac{u'}{v'}$ und damit ist Addition und Multiplikation wohl-definiert.

Die Assoziativität, Kommutativität und Distributivität der Operationen auf $R[S^{-1}]$ folgen aus der Assoziativität, Kommutativität und Distributivität der Operationen in R.

Es gilt $\frac{0}{1} + \frac{r}{s} = \frac{0s+1r}{1s} = \frac{r}{s}$ und $\frac{1}{1}\frac{r}{s} = \frac{1r}{1s} = \frac{r}{s}$, und somit ist $\frac{0}{1}$ das Nullelement und $\frac{1}{1}$ das Einselement in $R[S^{-1}]$. Ausserdem ist $\frac{-r}{s} + \frac{r}{s} = \frac{-rs+sr}{ss} = \frac{0}{ss} = \frac{0}{1}$ und somit ist $\frac{-r}{s}$ ein additives Inverses von $\frac{r}{s} \in R[S^{-1}]$.

(c) Sei $\psi : R \to R'$ ein Homomorphismus kommutativer Ringe mit der Eigenschaft $\psi(S) \subseteq (R')^\times$. Damit die Ringhomomorphismen kommutieren muss $\psi_S\left(\frac{1}{s}\right) = \psi(s)^{-1}$ und damit $\psi_S\left(\frac{r}{s}\right) = \psi(r)\psi(s)^{-1}$ sein. Es kann also maximal einen solchen Ringhomomorphismus geben, der durch die letzte Gleichung definiert sein muss. Wir definieren demnach $\psi_S : R[S^{-1}] \to R'$ durch

$$\psi_S\left(\frac{r}{s}\right) := \psi(r)\psi(s)^{-1}.$$

Wir müssen zeigen, dass diese Abbildung wohldefiniert und ein Ringhomomorphismus mit der Eigenschaft $\psi_S \circ \varphi = \psi$ ist.

Seien dazu $\frac{r}{s} = \frac{r'}{s'}$, d.h. es existiert $t \in S$ mit $(rs' - r's)t = 0$. Wir müssen zeigen, dass $\psi(r)\psi(s)^{-1} = \psi(r')\psi(s')^{-1}$, denn daraus folgt direkt $\psi_S\left(\frac{r}{s}\right) = \psi_S\left(\frac{r'}{s'}\right)$ und damit ist ψ_S wohldefiniert. Es gilt $(\psi(r)\psi(s') - \psi(r')\psi(s))\psi(t) = 0$. Da $t \in S$ und $\psi(S) \subseteq (R')^\times$, folgt, dass $\psi(r)\psi(s') - \psi(r')\psi(s) = 0$, was zu zeigen war.

Es folgt aus der Definition von ψ_S und der Kommutativität von R, dass

$$\begin{aligned}
\psi_S\left(\frac{1}{1}\right) &= \psi(1)\psi(1)^{-1} = 1, \\
\psi_S\left(\frac{r}{s} + \frac{u}{v}\right) &= \psi_S\left(\frac{rv + su}{sv}\right) = \psi(rv + su)\psi(sv)^{-1} \\
&= \psi(r)\psi(s)^{-1} + \psi(u)\psi(v)^{-1} = \psi_S\left(\frac{r}{s}\right) + \psi_S\left(\frac{u}{v}\right),
\end{aligned}$$

und analog für die Multiplikation

$$\psi_S\left(\frac{r}{s}\frac{u}{v}\right) = \psi_S\left(\frac{ru}{sv}\right) = \psi(ru)\psi(sv)^{-1}$$
$$= \psi(r)\psi(s)^{-1}\psi(u)\psi(v)^{-1} = \psi_S\left(\frac{r}{s}\right)\psi_S\left(\frac{u}{v}\right),$$

woraus folgt, dass ψ_S ein Ringhomomorphismus ist.
Für $r \in R$ gilt

$$\psi_S \circ \varphi(r) = \psi_S\left(\frac{r}{1}\right) = \psi(r)\psi(1)^{-1} = \psi(r),$$

und damit folgt, dass $\psi_S \circ \varphi = \psi$, da $r \in R$ beliebig.
Im Allgemeinen ist $\varphi : R \to R[S^{-1}]$ nicht injektiv. Der Kern der Abbildung besteht aus allen Elementen $r \in R$ für die ein $t \in S$ existiert mit $rt = 0$. Ist R ein Integritätsbereich und enthält S nicht die 0, dann ist φ injektiv.

(d) Wir müssen nur überprüfen, dass wir die gleiche Äquivalenzrelation auf $R \times (R \setminus \{0\})$ definieren. Dazu zeigen wir, dass für $r, r' \in R, s, s' \in R \setminus \{0\}$ die Bedingungen $\exists t \in R \setminus \{0\} : (rs' - r's)t = 0$ und $rs' - r's = 0$ äquivalent sind. Der Rest der Konstruktion ist analog.
Es ist klar, dass falls $rs' - r's = 0$, dann gilt $(rs' - r's)t = 0$ für alle $t \in R \setminus \{0\}$.
Andererseits, sei $t \in R \setminus \{0\}$ mit $(rs' - r's)t = 0$. Da R ein Integritätsbereich ist, folgt $rs' - r's = 0$, da $t \in R \setminus \{0\}$ gewählt.

(e) Da $\mathbb{Z}$ ein Integritätsbereich ist und $S \subseteq \mathbb{Z} \setminus \{0\}$, kann man sich schnell davon überzeugen, dass $\mathbb{Z}[S^{-1}] \subseteq \mathrm{Quot}(\mathbb{Z}) = \mathbb{Q}$ nach (d). Wir bemerken, dass jedes $\frac{p}{q} \in \mathbb{Q}$ so erweitert werden kann, dass der Nenner gerade ist. Damit ist $\mathbb{Q} \subseteq \mathbb{Z}[S^{-1}]$.

6. (a) (**SAGE**) Verwenden Sie SAGE, um herauszufinden für welche Zahlen $m \in \{2, \ldots, 100\}$ ein $g \in \mathbb{Z}/m\mathbb{Z}$ existiert so dass

$$(\mathbb{Z}/m\mathbb{Z})^\times = \{g^k : k \in \mathbb{N}_0\}.$$

Hinweis: Es genügt, die rechte Menge für $k < m$ zu betrachten.

(b) Verwenden Sie (a), um eine Vermutung auszusprechen, wie man diese m charakterisieren könnte.

Lösung:

(a) Ein möglicher Code könnte wie folgt aussehen:

```
def einheit(n):
    return any(n*m==1 for m in R)
```

```
ListeZyklischeEinheiten = list();
for m in range(101):
    if m != 0 and m !=1:
        R = Integers(m)
        ListeEinheiten = [r for r in R if einheit(r)]
        for r in R:
            if r != 0:
                ErzeugteUntergruppe = [r^k for k in range(m)]
                if Set(ErzeugteUntergruppe)==Set(ListeEinheiten):
                    ListeZyklischeEinheiten.append(i)
                    break
```

Wir erhalten, dass die folgenden Zahlen $2 \leqslant m \leqslant 100$ die Eigenschaft haben, dass ein $g \in \mathbb{Z}/m\mathbb{Z}$ existiert mit $(\mathbb{Z}/m\mathbb{Z})^\times = \{g^k : k \in \mathbb{N}_0\}$:

```
ListeZyklischeEinheiten
= [2, 3, 4, 5, 6, 7, 9, 10, 11, 13, 14, 17, 18, 19, 22, 23, 25, 26,
    27, 29, 31, 34, 37, 38, 41, 43, 46, 47, 49, 50, 53, 54, 58,
    59, 61, 62, 67, 71, 73, 74, 79, 81, 82, 83, 86, 89, 94, 97, 98]
```

(b) Wir sehen zuerst, dass alle Primzahlen in der Liste sind und betrachten die restlichen Zahlen.

```
ListeZyklischeEinheitenOhnePrimzahlen
= [m for m in ListeZyklischeEinheiten if m not in Primes()]
= [4, 6, 9, 10, 14, 18, 22, 25, 26, 27, 34, 38, 46, 49, 50, 54,
      58, 62, 74, 81, 82, 86, 94, 98]
```

Wir betrachten die geraden Zahlen und teilen durch 2:

```
ListeZyklischeEinheitenOhnePrimzahlenGerade
= [m/2 for m in ListeZyklischeEinheitenOhnePrimzahlen if
     any(m==2*k for k in range(m))]
= [2, 3, 5, 7, 9, 11, 13, 17, 19, 23, 25, 27, 29, 31, 37, 41, 43,
     47, 49]
```

Wir sehen, dass alle Zahlen in der Liste ausser die 2 ungerade sind. Ausserdem sind alle Zahlen entweder selbst Primzahlen oder Potenzen von ungeraden Primzahlen.

Nun betrachten wir die ungeraden Zahlen in der Liste, die nicht prim sind.

```
ListeZyklischeEinheitenOhnePrimzahlenUngerade
= [m for m in ListeZyklischeEinheitenOhnePrimzahlen if m/2 not
      in ListeZyklischeEinheitenOhnePrimzahlenGerade]
= [9, 25, 27, 49, 81]
```

Auch diese Zahlen sind Potenzen ungerader Primzahlen.

Wir stellen folgende Vermutung auf: Eine Zahl $m \in \mathbb{N}, m > 1$ hat die Eigenschaft, dass $(\mathbb{Z}/m\mathbb{Z})^\times = \{g^k : k \in \mathbb{N}_0\}$ für ein $g \in \mathbb{Z}/m\mathbb{Z}$, genau dann wenn

$$m \in \{2, 4, p^l, 2p^l \mid p \text{ prim und ungerade}, l \in \mathbb{N}\}.$$