1 Unterringe und Ideale

Sei im folgenden R immer ein Ring.

1. Eine echte Teilmenge $M \subset R$ ist kein Ideal, wenn es ein Unterring ist. Denn wäre M ein Ideal, so wäre es ein Ideal, das 1 enthält. Jedes Ideal, das 1 enthält ist aber der ganze Ring.
   Eine echte Teilmenge $M \subset R$, die ein Ideal ist, ist kein Unterring. Denn M enthält nicht $1 \in R$.

2. Sei M eine Teilmenge von R. Bezeichnen wir mit $U(M)$ den kleinsten Unterring von R, der M enthält und mit $I(M)$ das kleinste Ideal, das M enthält, so heißt M minimale erzeugenden Menge, wenn für jede echte Teilmenge N von M gilt:

   $$U(N) \neq U(M)$$

   entsprechend für I. Um für einen konkreten Unterring $U \subset R$ zu zeigen, dass $U(M) = U$ gilt, muss man nur $M \subset U$ und $U \subset U(M)$ zeigen. Dann ist U ein Unterring, der M enthält, aber es gibt keinen echten Unterring von $U(M)$, der M enthält.

3. Um für eine Teilmenge $N \subset R$ zu zeigen, dass $I(M) = N$ gilt, hat man nun also folgende Strategie:

   - Zeige N ist eine Ideal
   - Zeige $M \subset N$
   - Zeige $N \subset I(M)$

   Entsprechendes Erhält man für erzeugte Unterringe.

4. Minimale erzeugende Mengen müssen nicht eindeutig sein. Für Ideale zum Beispiel ist $\{3, 5\}$ eine minmale Erzeugende Menge des Ideals $\mathbb{Z} \subset \mathbb{Z}$, aber ebenso $\{1\}$. Also nicht einmal die Anzahl der Elemente ist eindeutig.

2 Ringhomomorphismen

1. Seien R, S Ringe und $I \subset R$ ein Ideal. Wenn man zeigen möchte, dass $R/I \cong S$ gilt, dann zeigt man für gewöhnlich:

   - es gibt einen surjektiven Ringhomomorphismus $\phi : R \to S$
   - für den obigen Ringhomomorphismus ϕ gilt: $\ker \phi = I$

2. Es sei an folgenden Satz erinnert: Sei R ein kommutativer Ring und $R[x]$ der Polynomring in einer Unbekannten. Für jeden Ringhomomorphismus $\sigma : R \to S$ und jedes $b \in S$ gibt es genau einen Ringhomomorphismus $\phi = \phi_{\sigma,b} : R[x] \to S$ mit

$$\phi \mid_R = \sigma \qquad \text{und} \qquad \phi(x) = b$$

Dieser Satz sagt einem, dass man einen Ringhomomorphismus, der auf einem Polynomring definiert ist, nur auf den Unbestimmten definieren muss. Meistens ist klar, was der Homomorphismus σ ist, deswegen wird dieser häufig nicht angegeben. Der Homomorphismus ϕ wird dann kurz angegeben mit

$$\phi : R[x] \to S, x \mapsto b$$

In Aufgabe 3 ist $\sigma = \iota : \mathbb{Q} \to \mathbb{Q}(\sqrt{2}), a \mapsto a + 0 \cdot \sqrt{2}$.
In Aufgabe 4 ist $\sigma : k \to k[M_\ell], \lambda \mapsto \lambda \cdot s^0 t^0$.

3 Lösungen

3.1 Aufgabe 1

Seien im folgenden $a = \sum_{n\in\mathbb{N}} a_n x^n$, $b = \sum_{n\in\mathbb{N}} b_n x^n$, $c = a + b$ und $d = a \cdot b$.

1. Sei $M = \left\{\sum_{n\in\mathbb{N}} a_n x^n \mid a_n \in k\,\mathbb{Z}, k > 1\right\}$. M ist kein Unterring, weil k nicht 1 teilt. Aber M ist ein Ideal, denn

   - 0 ist durch k teilbar, also ist $M \neq \emptyset$
   - Wenn a_n und b_n für alle n durch k teilbar sind, dann auch $c_n = a_n + b_n$
   - Wenn a_n für alle n durch k teilbar sind, dann auch $d_n = \sum_{i+j=n} a_i b_j$

   $M = I(k)$, denn $k \in M$ und mit k ist auch $k \cdot a \in I(k)$, dieses Polynom ist aber offensichtlich in M, also $M \subset I(k)$.

2. Sei $M = \left\{\sum_{n\in\mathbb{N}} a_n x^n \mid n \notin k\,\mathbb{Z} \Longrightarrow a_n = 0, k > 1\right\}$. M enthält 1 und ist eine echte Teilmenge von $\mathbb{Z}[x]$ also kein Ideal, aber M ist ein Unterring, denn

   - Sei $n \notin k\,\mathbb{Z}$, dann ist $a_n = b_n = 0$, also $c_n = 0$
   - Sei $n \notin k\,\mathbb{Z}$ und $i + j = n$. Angenommen i teil k, dann teilt j nicht k, also ist $a_i \cdot b_j = 0$, womit $d_n = 0$ gilt.

   $M = U(x^k)$, denn $x^k \in M$. $U(x^k)$ enthält auch die 1 (sonst wäre es kein Unterring) und weil $U(x^k)$ unter Addition und bilden von additiven Inversen abgeschlossen ist, enthält es auch $\mathbb{Z}$ (1 ist Erzeuger von $\mathbb{Z}$).

Da $U(x^k)$ unter Multiplikation abgeschlossen ist, sind auch alle $x^{nk} = x^k \cdots x^k$ für $n \in \mathbb{N}$ enthalten.
Somit enthält $U(x^k)$ auf jeden Fall die Menge

$$\left\{ \sum_{n \in \mathbb{N}} a_n x^{kn} \mid a_n \in \mathbb{Z} \right\} = M$$

3. Sei $M = \left\{ \sum_{n \in \mathbb{N}} a_n x^n \mid 2k \mid a_0, k \mid a_1, k \mid a_2, k > 1 \right\}$. M enthält 1 nicht, ist also kein Unterring, aber M ist ein Ideal

   - $2k \mid 0$, also $M \neq \emptyset$
   - Wenn a_0 und b_0 von $2k$ geteilt werden, dann auch ihre Summe c_0. Gleiches gilt für a_i, b_i, c_i und k mit $i = 1, 2$.
   - Seien a_0, a_1, a_2 wie in den Voraussetzungen. Es ist $d_0 = a_0 b_0$ (wird von $2k$ geteilt, weil a_0 von $2k$ geteilt wird), $d_1 = a_0 b_1 + a_1 b_0$ (wird von k geteilt, weil a_0 von k geteilt wird und a_1 auch), $d_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$ (wird von k geteilt, wie bei den anderen beiden).

   $M = I(2k, kx, x^3)$. Dass $\left\{ 2k, kx, x^3 \right\} \subset M$ gilt ist klar. Ist nun $f \in M$, so ist es von der Form $f = 2kf_0 + kf_1 x + kf_2 x \cdot x + \sum_{n \in \mathbb{N}} f_{n+3} x^n \cdot x^3$ mit $f_i \in \mathbb{Z}$ für $i \in \mathbb{N}$, also in $I(2k, kx, x^3)$.

4. Sei für ein $y \in \mathbb{Z}$ die Menge $M = \{p \in \mathbb{Z}[x] \mid p(y) = 0\}$ definiert. M ist kein Unterring, weil $1 \notin M$, aber M ist ein Ideal

   - $0 \in M$
   - Seien $p, q \in M$, dann gilt $(p + q)(y) = p(y) + q(y) = 0 + 0$
   - Sei $p \in M$ und $r \in \mathbb{Z}[x]$, dann gilt $(pr)(y) = p(y)r(y) = 0 \cdot r(y) = 0$

   $M = I(x - y)$. $x - y \in M$ ist klar. Sei nun $p \in M$, dann ist p durch $x - y$ teilbar also in $I(x - y)$.

3.2 Aufgabe 2

Seien A, B Ringe. $R := A \times B$ wird zum Ring durch komponentenweise erklärte Verknüpfung. Also $(a, b) + (c, d) := (a + c, b + d)$, für $\cdot$ entsprechend. Das Nullelement ist $(0, 0)$ und das Einselement ist $(1, 1)$. Dass die Assoziativ- und Distributivgesetze gelten, folgt sofort aus der Gültigkeit in den Komponenten und der Definition der Verknüpfungen. Gleiches gilt für die Kommutativität der Addition.
Sei nun $I \subset R$ ein Ideal. Definiere $J := \{a \in A \mid (a, 0) \in I\}$ und $K :=$

$\{b \in B \mid (0,b) \in I\}$. Wir zeigen, dass dies Ideale in A bzw. B sind.
Seien $a \in J$ und $c \in A$, dann ist $(a,0) \in I$ und damit

$$(c,0)(a,0) = (ca,0) \in I$$

, also $ca \in J$.
Seien $a, b \in J$, dann sind $(a,0), (b,0) \in I$ also auch

$$(a,0) + (b,0) = (a+b,0) \in I$$

also $a + b \in J$.
Dass $I = J \times K$ gilt, ist nach Definition klar.

3.3 Aufgabe 3

Wir zeigen zunächst, dass $\mathbb{Q}(\sqrt{2})$ ein Unterring von $\mathbb{R}$ ist:

- Es ist $1 \in \mathbb{Q}(\sqrt{2})$
- mit $a + b\sqrt{2}$ und $c + d\sqrt{2}$ ist die Summe $(a+c) + (b+d)\sqrt{2}$ und das Produkt $(ac + 2bd) + (ad + bc)\sqrt{2}$ wieder in $\mathbb{Q}(\sqrt{2})$.

Wir betrachten $\phi : \mathbb{Q}[x] \to \mathbb{Q}(\sqrt{2}), x \mapsto \sqrt{2}$.
Er ist offenbar surjektiv, denn $a + bx$ ist ein Urbild von $a + b\sqrt{2}$.
Wir müssen nur noch zeigen, dass $\ker \phi = (x^2 - 2)$ gilt, also $f \in \ker \phi$ von $(x^2 - 2)$ geteilt wird.
Sei $f = \sum a_k x^k$ und $f \in \ker \phi$, dann gilt

$$0 = \phi(f) = f(\sqrt{2}) = \sum a_{2k} 2^k + \sqrt{2} \sum a_{2k+1} 2^k$$

Nun gilt $f(-\sqrt{2}) = \sum a_{2k} 2^k - \sqrt{2} \sum a_{2k+1} 2^k$, womit gilt

$$f(-\sqrt{2}) = f(-\sqrt{2}) + f(\sqrt{2}) = 2 \cdot \sum a_{2k} 2^k \in \mathbb{Q}$$

Somit gilt

$$\mathbb{Q} \ni f(-\sqrt{2}) = f(-\sqrt{2}) - f(\sqrt{2}) = -2\sqrt{2} \sum a_{2k+1} 2^k$$

Da $f(-\sqrt{2})$ rational ist, geht dies nur, wenn $\sum a_{2k+1} 2^k = 0$ ist. Es folgt also, dass $f(-\sqrt{2}) = 0$ gilt.
Nun wissen wir, dass f aufgefasst als Polynom über $\mathbb{R}$ durch das Polynom $(x - \sqrt{2})(x + \sqrt{2}) = x^2 - 2$ teilbar ist. Da $x^2 - 2 \in \mathbb{Q}[x]$ ist, ist auch $f/(x^2 - 2) \in \mathbb{Q}[x]$, also f durch $x^2 - 2$ teilbar.

3.4 Aufgabe 4

Sei $M_\ell = \{(m,n) \in \mathbb{Z}^2 \mid m \geq 0, m + \ell n \geq 0\}$. M_ℓ wird als Monoid erzeugt von den drei M_ℓ-Elementen $e_1 := (0,1)$, $e_2 = (1,0)$ und $e_3 := (\ell, -1)$ (d.h. $M_\ell = \sum_i \mathbb{N} e_i$). Diese sind nicht unabhängig, sondern genügen der Relation

$$e_1 + e_3 = \ell e_2 \quad (*)$$

Die Zuordnungen

$$(1,0,0) \mapsto e_1, \quad (0,1,0) \mapsto e_2, \quad (0,0,1) \mapsto e_3$$

definieren einen surjektiven Monoidmorphismus

$$\alpha : \mathbb{N}^3 \to M_\ell.$$

Sei nun M eines dieser beiden Monoide und

$$k[M] = \{ \sum_{m \in M_\ell} c_m X^m | \; c_m \in k, \text{ nur endlich viele } c_m \neq 0\}$$

der zu M gehörige Monoidring. Der Monoidmorphismsmus α induziert dann einen Ringmorphismus

$$\varphi : k[\mathbb{N}^3] \to k[M_\ell], \quad \sum c_m X^m \mapsto \sum c_m \tilde{X}^{\alpha(m)},$$

dessen Kern von der Relation $(*)$ induziert wird:

$$\ker \varphi = (X^{e_1} X^{e_3} - X^{\ell e_2}) = (X_1 X_3 - X_2^\ell).$$

Das definiert den gesuchten Isomorphismus $\phi : k[\mathbb{N}^3]/\ker\varphi \to k[M_\ell]$, $[p] \mapsto \varphi(p)$. In der Tat überprüft man, dass durch

$$\tilde{X}^{(n,m)} \mapsto \begin{cases} X_1^n X_2^m & n \geq 0 \\ X_3^{-n} X_1^{m+\ell n} & n < 0 \end{cases}$$

ein zu ϕ inverser Isomorphismus definiert wird.