uns Nullteiler in R liefert. Dies beweist die Äquivalenz b).
Ist R Integritätsring, so gilt nach a) und b) für alle Einheiten $f = \sum_{i=1}^{n} a_i t^i, g = \sum_{i=1}^{m} b_i t^i \in R[t]$ mit $a_n \neq 0 \neq b_m$ und $f \cdot g = 1_R$:

$$0 = \deg(1_r) = \deg(f \cdot g) = n + m,$$

und damit $n = m = 0$. Ausserdem muss gelten $a_0 \cdot b_0 = 1$, weswegen a_0 und b_0 bereits Einheiten in R sein müssen, was den Beweis abschließt.

□

Ist K ein Körper, so besagt Aussage c) des obigen Lemmas gerade, dass die Einheiten des Polynomrings in einer Variable über K genau die von Null verschiedenen Körperelemente sind.

Ein Analogon zur Aussage a) des vorigen Lemmas macht im Potenzreihenring keinen Sinn. Aussage b) des vorigen Lemmas gilt auch für Potenzreihenringe, jedoch gibt es einen kleinen, aber wichtigen Unterschied im Beweis. (Achten Sie mal darauf, wenn Sie das hier nacharbeiten.) Aussage c) gilt nicht wie oben, sondern es gibt nur eine strikte Inklusion der Einheitengruppen, was zeigt, dass der Potenzreihenring mehr Einheiten besitzt als der Polynomring.

Lemma 2.5.10 *Sei R kommutativer Ring mit 1. Dann gilt:*

a) $R[[t]]$ ist genau dann nullteilerfrei, wenn R nullteilerfrei ist.

b) $(R[[t]])^* = \{f = \sum_{i=0}^{\infty} a_i t^i \in R[[t]] \mid a_0 \in R^*\}$.

Beweis: Besitzt R Nullteiler, so sind diese mittels des injektiven Ringhomomorphismus φ aus Bemerkung 2.5.4 und der Inklusion von Ringen $R[t] \leq R[[t]]$ auch Nullteiler in $R[[t]]$. Besitzt andererseits $R[[t]]$ Nullteiler $f = \sum_{i=0}^{\infty} a_i t^i$ und $g = \sum_{i=0}^{\infty} b_i t^i$ mit $f \cdot g = 0$, so gibt es wegen $f \neq 0 \neq g$ kleinste Indices[2] m, n mit $a_n \neq 0 \neq b_m$. Der $(n+m)$-te Koeffizient von $f \cdot g$ ist dann gerade $a_n \cdot b_m$ und muss wegen $f \cdot g = 0_{R[[t]}$ Null sein, was uns Nullteiler in R liefert. Dies beweist die Äquivalenz a).
Ist $f = \sum_{i=1}^{\infty} a_i t^i \in (R[[t]])^*$ und $g = \sum_{i=1}^{\infty} b_i t^i$ das zugehörige inverse Element, so gilt $f \cdot_{R[[t]]} g = 1_{R[[t]}$ und damit insbesondere $a_0 \cdot_R b_0 = 1_R$, weswegen a_0 eine Einheit sein muss. Ist andererseits $f = \sum_{i=0}^{\infty} a_i t^i$ und $a_0 \in R^*$, so gibt

[2] Das Wohlordnungsaxiom läßt hier grüßen.

es ein $b_0 \in R$ mit $a_0 \cdot b_0 = 1$. Nun machen wir einen Ansatz für ein mögliches Inverses zu f, nämlich eine Potenzreihe $g = \sum_{i=0}^{\infty} b_i t^i$, die bei diesem b_0 beginnt und deren weitere Koeffizienten noch unbekannt sind. Induktiv muss nun aber bei bereits bestimmten Koeffizienten $b_0, \ldots, b_{n-1}$ für den n-ten Koeffizienten von g gelten:

$$a_0 b_n + \sum_{j=1}^{n} a_j b_{n-j} = 0.$$

Dies bestimmt aber eindeutig den Koeffizienten b_n durch

$$b_n = -\sum_{j=1}^{n} \frac{a_j}{a_0} b_{n-j},$$

was die gesuchte Inverse g liefert.

□

Ihnen ist sicher aufgefallen, dass ich auf den letzten Seiten peinlich genau darauf geachtet habe, von *einem neuen Symbol t* zu sprechen und dieses nicht als eine Element eines geeigneten Ringes aufzufassen. Das hat einen guten Grund: Das Einsetzen eines Elements eines geeigneten Ringes in ein Polynom stellt selbst eine Abbildung vom Polynomring in den Ring dar. Diese muss aber nicht injektiv sein, was sie umso interessanter macht.

Definition 2.5.11 *(Einsetzungshomomorphismus) Sei S ein (nicht notwendigerweise kommutativer) Ring und R ein kommutativer Unterring von S. Ein Element $\alpha \in S$ heißt* **einsetzbar** *in Polynome über R, falls es mit jedem Element aus R kommutiert, d.h.*

$$r\alpha = \alpha r \quad \forall r \in R.$$

In diesem Fall definieren wir die Einsetzungsabbildung von α in Polynome über R als

$$\begin{array}{rcl} E_\alpha : R[t] & \longrightarrow & S \\ f = \sum_{i=0}^{n} a_i t^i & \longmapsto & f(\alpha) = \sum_{i=0}^{n} a_i \alpha^i \end{array}$$

Bitte beachten Sie, dass wegen der Kommutativität des Ringes R, alle Elemente aus R stets einsetzbar sind. Dennoch sind das meist nicht die einzigen Elemente aus S, die einsetzbar sind in Polynome über $R[t]$. Denken Sie etwa an das Einsetzen von reellen oder komplexen Zahlen in Polynome mit ganzzahligen Koeffizenten.

Satz 2.5.12 *Seien R, S und α wie in der vorigen Definition. Dann gilt:*

a) E_α *ist ein Ringhomomorphismus.*

b) $R[\alpha] := \mathrm{Im}(E_\alpha) = \{f(\alpha) \mid f \in R[t]\}$ *ist ein kommutativer Unterring von S.*

c) $\ker(E_\alpha) = \{f \in R[t] \mid f(\alpha) = 0\}$.

Beweis:

a) Zum Nachweis, dass E_α ein Ringhomomorphismus ist, sind drei Eigenschaften zu zeigen: Verträglichkeit mit Addition und Multiplikation sowie Abbildung des 1-Elements auf das 1-Element. Diese rechnen wir nun nach. Dazu seien $f = \sum_{i=0}^{n} a_i t^i$ und $g = \sum_{i=0}^{m} b_i t^i$ beliebige Elemente von $R[t]$. (Denken Sie daran, dass auch Koeffizienten jenseits des Grades definiert sind und den Wert 0 haben):

$$\begin{aligned} E_\alpha(f+g) &= E_\alpha\left(\sum_{i=0}^{\max\{n,m\}} (a_i + b_i)t^i\right) \\ &= \sum_{i=0}^{\max\{n,m\}} (a_i + b_i)\alpha^i \\ &= \left(\sum_{i=0}^{\max\{n,m\}} a_i\alpha^i\right) + \left(\sum_{i=0}^{\max\{n,m\}} b_i\alpha^i\right) \\ &= E_\alpha(f) + E_\alpha(g) \end{aligned}$$

$$\begin{aligned} E_\alpha(f \cdot g) &= E_\alpha\left(\sum_{i=0}^{n+m}\left(\sum_{j+k=i} a_j b_k\right) t^i\right) \\ &= \sum_{i=0}^{n+m}\left(\sum_{j+k=i} a_j b_k\right)\alpha^i \\ &\overset{\alpha r = r\alpha}{=} \left(\sum_{i=0}^{n} a_i \alpha^i\right)\cdot\left(\sum_{i=0}^{m} b_i \alpha^i\right) \\ &= E_\alpha(f)\cdot E_\alpha(g) \end{aligned}$$

$$\begin{aligned} E_\alpha(1_{R[t]}) &= E_\alpha(1_R) \\ &= 1_R \end{aligned}$$

b) Diese Aussage ist eine direkte Anwendung von 2.3.7,a) sowie für die Kommutativität von 2.3.7,d).

c) Diese Aussage ist die direkte Anwendung der Definition des Kerns.

□

Die obige Definition und der eben bewiesen Satz rechtfertigen das Einsetzen von Werten in Polynome, wie wir es schon zu Schulzeiten gemacht haben, ohne damals darüber nachzudenken. Mehr noch: die Überlegungen erlauben ein entsprechendes Vorgehen auch für Polynome über Ringen und klären, was einsetzbar ist. Schlampigerweise werden wir oft auch statt $E_\alpha(f)$ einfach wieder $f(\alpha)$ schreiben. Da Einsetzen ein Homomorphismus ist, gilt dann auch $(f+g)(\alpha) = f(\alpha) + g(\alpha)$ sowie $(f \cdot g)(\alpha) = f(\alpha) \cdot g(\alpha)$.

Die genauere Beschreibung des Kerns des Einsetzungshomomorphismus hat sie in anderer Sprechweise bereits in der Schule beschäftigt: Es ist die Frage nach Nullstellen von Polynomen. Ehe wir uns damit jedoch genauer beschäftigen können, müssen wir noch einen weiteren Begriff einführen, die Teilbarkeit von Polynomen:

Satz 2.5.13 *Sei R ein kommutativer Ring. Seien $f, g \in R[t]$ mit $LC(g) \in R^*$. Dann existieren eindeutige Polynome $q, r \in R[t]$, so daß*

$$f = q \cdot g + r \quad \textit{und} \ \deg(r) < \deg(g).$$

Beweis: Siehe Videoschnippsel DivMitRestPolynome.

□

Vergleichen sie die Struktur dieser Division mit Rest mit der in 1.1.1. Die verblüffende Ähnlichkeit ist kein Zufall, sondern beruht auf tieferen Gemeinsamkeiten der beiden Ringe, die wir in Abschnitt 2.7 noch allgemeiner untersuchen werden.

Bemerkung 2.5.14 *Die Zusatzbedingung $LC(g) \in R^*$ sichert im allgemeinen Fall auch, daß $g \neq 0$ gilt. Ist R ein Körper, so ist jedes Element außer Null eine Einheit und die Bedingung ist sogar äquivalent zu $g \neq 0$.*

Definition 2.5.15 *Sei R kommutativer Ring und seien $f, g \in R[t]$. f heißt teilbar durch g, falls es ein $q \in R[t]$ gibt mit $f = q \cdot g$.*
Sei S ein Ring, für den R ein Unterring ist. Ein einsetzbares $\alpha \in S$ heißt Nullstelle eines $f \in R[t]$, falls $f(\alpha) = 0$.

Blättern Sie einmal zurück zur Division mit Rest in den ganzen Zahlen. Bei der Definition der Teilbarkeit konnten wir dort auf die Division mit Rest zurückgreifen. Hier ist das schwieriger, weil auch ein Polynom f mit $LC(f) \notin R^*$ ein Teiler eines anderen Polynoms sein kann, dies aber vom Satz über die Division mit Rest nicht abgedeckt ist.

Proposition 2.5.16 *Sei R kommutativer Ring, $f \in R[t]$ und $\alpha \in R$. Dann existiert ein eindeutiges $q \in R[t]$ mit*

$$f = q \cdot (t - \alpha) + f(\alpha),$$

wobei $\deg(q) = \deg(f) - 1$.

Beweis:
Fall 1: $f_1 = a_n t^n$
Da $LC(t - \alpha) = 1_R$, können stets geeignete Vielfache von $t - \alpha$ von f_1 abziehen, so dass der Grad der Differenz kleiner als n ist. Dies werden wir nun induktiv für n ausführen: Ist $n = 0$, so ist f_1 konstant, $q = 0$ und $f_1(\alpha) = f_1(t)$, was den Induktionsanfang bildet. Sei nun als Induktionsvoraussetzung die Behauptung für Monome (d.h. Polynome mit nur einem von

Null verschiedenen Summanden) bis zum Grad n bewiesen. Im Induktionsschritt sei $f_1 = a_{n+1}t^{n+1}$ und wir rechnen:

$$f_1 = a_{n+1}t^{n+1} = a_{n+1}t^n(t-\alpha) + a_{n+1}\alpha t^n$$

Dann gibt es nach Induktionsvoraussetzung $q_1 \in R[t]$ mit $t^n = q_1(t-\alpha)+\alpha^n$, das wir in f_1 einsetzen können:

$$\begin{aligned} f_1 &= a_{n+1}(q_1(t-\alpha)+\alpha^n)(t-\alpha) + a_{n+1}\alpha(q_1(t-\alpha)+\alpha^n) \\ &= \underbrace{(a_{n+1}(q_1(t-\alpha)+\alpha^n) + a_{n+1}\alpha q_1)}_{:=q}(t-\alpha) + a_{n+1}\alpha^{n+1}, \end{aligned}$$

womit wir die gesuchte Darstellung gefunden haben.

Fall 2: $f \in R[t]$ beliebig
Auch diesen Fall behandeln wir mittels Induktion und verwenden dabei die Vorüberlegung aus Fall 1: Der Induktionsanfang bleibt derselbe wie im anderen Fall, da Polynome vom Grad Null Monome sind. Als Induktionsvoraussetzung sei die Behauptung bewiesen für $\deg(f) \leq n$. Im Induktionsschritt zerlegen wir f in seinen Leitterm und die anderen Terme $f = a_{n+1}t^{n+1}+f_2$, dann wissen wir nach Induktionsvoraussetzung und Fall 1, dass es $q_1, q_2 \in R[t]$ gibt mit

$$\begin{aligned} f_2 &= q_2(t-\alpha) + f_2(\alpha) \\ a_{n+1}t^{n+1} &= q_1(t-\alpha) + a_{n+1}\alpha^{n+1} \text{ und damit} \\ f &= q_1(t-\alpha) + a_{n+1}\alpha^{n+1} + q_2(t-\alpha) + f_2(\alpha) \\ &= \underbrace{(q_1+q_2)}_{:=q}(t-\alpha) + \underbrace{(a_{n+1}\alpha^{n+1} + f_2(\alpha))}_{=f(\alpha)}. \end{aligned}$$

Damit ist die Existenz gezeigt.
Für die Eindeutigkeit nehmen wir an, dass $q, s \in R[t]$ beide die Behauptung erfüllen:

$$q \cdot (t-\alpha) = f = s \cdot (t-\alpha).$$

Damit gilt:

$$(q-s)(t-\alpha) = 0.$$

Da aber $LC(t-\alpha) = 1$ und damit $(t-\alpha)$ kein Nullteiler sein kann, muss $q-s=0$ gelten, weswegen $q=s$ und damit die Eindeutigkeit gezeigt ist.

□

Korollar 2.5.17 *Sei R ein kommutativer Ring, $f \in R[t]$ und $\alpha \in R$. Dann gilt*

$$\alpha \text{ ist Nullstelle von } f \iff (t-\alpha) \mid f.$$

Beweis: α ist Nullstelle von f, genau dann wenn $f(\alpha) = 0$. Das bedeutet aber nach Proposition 2.5.16 genau, dass $f = q \cdot (t-\alpha)$, was nach Definition gerade $(t-\alpha) \mid f$ bedeutet.

□

Aus der Analysis sind wir darauf gepägt, nach mehrfachen Nullstellen zu suchen, indem wir die gemeinsamen Nullstellen einer Polynomfunktion und ihrer Ableitung zu betrachten. So würden wir natürlich auch für allgemeine Polynome vorgehen wollen, haben aber leider keine Ableitung, wie sie in der Analysis mittels einer Limes-Betrachtung definiert wurde, zur Verfügung. Stattdessen betrachten wir die Konstruktion, mit der die Ableitung eines Polynoms in der Analysis bestimmt werden konnte als Definition einer formalen Ableitung.

Definition 2.5.18 *Sei R ein Integritätsring und $f = \sum_{i=0}^{n} a_i t^i \in R[t]$. Dann ist die* **formale Ableitung** *von f das Polynom*

$$f' = \sum_{i=1}^{n} i a_i t^{i-1} \in R[t].$$

Proposition 2.5.19 *Sei R ein Integritätsring, seien $f, g \in R[t]$ und $\alpha \in R$. Dann gilt:*

a) $(\alpha f)' = \alpha f'$

b) $(f+g)' = f' + g'$

c) $(f \cdot g)' = f' \cdot g + f \cdot g'$

Beweis: Alle drei Eigenschaften lassen sich direkt mit der Definition nachrechnen. Die explizite Ausführung bleibt den Lesern überlassen.

□

Definition 2.5.20 *Sei R ein Integritätsring, $f \in R[t]$ und $\alpha \in R$ eine Nullstelle von f. α heißt m-**fache Nullstelle** von f, falls*

$$\exists g \in R[t] : f = (t-\alpha)^m \cdot g \quad \text{und} \quad g(\alpha) \neq 0$$

Proposition 2.5.21 *Seien $R \leq S$ Integritätsringe, $f \in R[t]$ und $\alpha \in S$ in f einsetzbar. Dann gilt:*

$$\alpha \text{ mehrfache Nullstelle von } f \iff f(\alpha) = 0 = f'(\alpha).$$

Bei diesem Beweis sollten Sie sich die Bedeutung einer mehrfachen Nullstelle nochmals vor Augen führen und an das obige Korollar zurückdenken. Der Beweis bleibt als Aufgabe für Übungsblatt 3.

Zum Abschluss dieses Abschnitts wenden wir uns nun einer Konstruktion zu, die Sie bereits für die ganzen Zahlen gesehen haben: Wir betrachten die Restklassen bzgl. eines Elements. Wie dort auch kann man zwei Zugänge wählen, die wir hier beide kurz skizzieren – vergleichen Sie beim Nacharbeiten mit der Konstruktion von $\mathbb{Z}_m$ bzw. $\mathbb{Z}/m\mathbb{Z}$ aus der Linearen Algebra und füllen Sie die fehlenden Details selbst.

Konstruktion 2.5.22 *Sei R ein kommutativer Ring und sei $d \in \mathbb{N}$.*

Variante 1: $R[t]_{\leq d}$
Wir setzen als Menge:

$$R[t]_{\leq d} := \{f \in R[t] \mid \deg(f) \leq d\} \subseteq R[t].$$

Sei $h \in R[t]$ mit $LC(h) \in R^*$ und $\deg(h) = d+1$. Dann ist Division mit Rest durch h definiert und wir können $R[t]_{\leq d}$ auch als die Reste der Division durch h auffassen und damit Rechenoperationen darauf definieren:

$$R[t]_{\leq d} = \{f \in R[t] \mid \deg(f) < \deg(h)\}$$

mit den Operationen

$$\begin{aligned} + : R[t]_{\leq d} \times R[t]_{\leq d} &\longrightarrow R[t]_{\leq d} \\ (f,g) &\longmapsto (f+g) \bmod h \\ \cdot : R[t]_{\leq d} \times R[t]_{\leq d} &\longrightarrow R[t]_{\leq d} \\ (f,g) &\longmapsto (f \cdot g) \bmod h \end{aligned}$$

Dann läßt sich analog zu $\mathbb{Z}_m$ *zeigen, dass* $(R[t]_{\leq d}, +, \cdot)$ *ein kommutativer Ring mit* 1 *ist und dass*

$$\begin{array}{rcl} \rho_h : R[t] & \longrightarrow & R[t]_{\leq d} \\ f & \longmapsto & f \bmod h \end{array}$$

ein Ringepimorphismus ist.

Variante 2: $R[t]/ < h >$
Sei $h \in R[t]$ *mit* $LC(h) \in R^*$ *und* $\deg(h) = d + 1$. *Definiere*

$$< h >:= \{ah \mid a \in R[t]\}.$$

Dann definiert $f \sim_h g :\Longleftrightarrow f - g \in < h >$ *eine Äquivalenzrelation auf* $R[t]$. *Die Menge* $R[t]/ < h >$ *ist ein kommutativer Ring mit* 1 *bzgl. der induzierten Addition und Multiplikation und*

$$\begin{array}{rcl} \rho_h : R[t] & \longrightarrow & R[t]/ < h > \\ f & \longmapsto & [f]_h \end{array}$$

ist ein Ringepimorphismus. In dieser Variante sind alle Konstruktionen analog zu $\mathbb{Z}/m\mathbb{Z}$.

2.6 Ideale

Der Begriff eines Ideals ist uns bereits für Ideale in $\mathbb{Z}$ bekannt, wo er half, sehr knapp und präzise Aussagen wie die Bezout-Identität zu formulieren. Diese Begriffsbildung würden wir gerne auch in beliebigen Ringen mit 1 vornehmen, müssen dabei allerdings etwas genauer auf Details achten, wie die folgende Definition im Vergleich zu Definition 1.2.1 zeigt.

Definition 2.6.1 *Sei R ein Ring. Eine Teilmenge $\emptyset \neq I \subseteq R$ heißt* **Linksideal** *in R, falls gilt:*

a) $\forall a, b \in I : \quad a + b \in I$

b) $\forall a \in I, \forall r \in R : \quad ra \in I$

Analog heißt eine Teilmenge $\emptyset \neq I \subseteq R$ heißt **Rechtsideal** *in R, falls gilt:*

a) $\forall a, b \in I : \quad a + b \in I$

b) $\forall a \in I, \forall r \in R : \quad ar \in I$

I heißt ein **Ideal** *(oder präziser* **zweiseitiges Ideal***) in R, falls es Rechts- und Linksideal ist.*

Bemerkung 2.6.2 *Wegen Bedingung b) enthält jedes Ideal das Element 0_R.*

Bemerkung 2.6.3 *Ist R ein kommutativer Ring, dann fallen die Begriffe Rechts- und Linksideal zusammen mit dem Begriff eines Ideals. Damit ist der Begriff eines Ideals in $\mathbb{Z}$, wie wir ihn aus Abschnitt 1.1 kennen, lediglich ein Spezialfall der allgemeinen Definition.*

Bemerkung 2.6.4 *Die beiden Bedingungen an ein Linksideal kann man zusammenfassen als*

$$\forall a, b \in I, \forall r, s \in R : \quad ra + sb \in I.$$

Ein Linksideal enthält also jede linksseitige R-Linearkombination von Elementen aus I. Für Rechtsideale und zweiseitige Ideale können die entsprechenden Bedingungen analog zusammengefasst werden.

Notation 2.6.5 *Wie schon im Fall des Ringes der ganzen Zahlen, so schreiben wir auch im allgemeinen Fall:*

$$\begin{aligned}\langle a_1,\dots,a_n\rangle_\ell &:= \{\sum_{i=1}^{n} r_i a_i \mid r_1,\dots,r_n \in R\}\\ \langle a_1,\dots,a_n\rangle_r &:= \{\sum_{i=1}^{n} a_i r_i \mid r_1,\dots,r_n \in R\}\\ \langle a_1,\dots,a_n\rangle &:= \{\sum_{i=1}^{n} r_i a_i s_i \mid r_1,\dots,r_n,s_1,\dots,s_n \in R\}\end{aligned}$$

für das Links- und Rechtsideal, das von $a_1,\dots,a_n \in R$ erzeugt wird. Analog schreiben wir im kommutativen Fall:

$$\langle a_1,\dots,a_n\rangle := \{\sum_{i=1}^{n} r_i a_i \mid r_1,\dots,r_n \in R\}$$

für das von $a_1,\dots,a_n \in R$ erzeugte Ideal.
Für unendliche Mengen $\emptyset \neq A \subseteq R$ schreiben wir:

$$\langle A\rangle_\ell := \{\sum_{i=1}^{n} r_i a_i \mid n \in \mathbb{N}, a_1,\dots,a_n \in A, r_1,\dots,r_n \in R\}$$

sowie die analogen Notationen für Rechtsideale und zweiseitige Ideale

Nicht jedes Ideal kann von endlich vielen Elementen erzeugt werden. Ein Ring, in dem jedes Ideal endlich erzeugt ist, heißt noetherscher Ring. Diesen Begriff werden wir in der Kommutativen Algebra näher studieren. In der Algebra I fehlt uns dafür die Zeit.

Notation 2.6.6 *Jeder Ring R enthält die Ideale $\langle 0_R\rangle = \{0_R\}$, das* **Nullideal**, *und $\langle 1_R\rangle = R$, das* **Einsideal** . *Wir bezeichnen diese beiden Ideale auch als die* **trivialen Ideale** *in R. Ein Ideal $I \subset R$ mit $\{0\} \subsetneq I \subsetneq R$ heißt ein* **echtes Ideal** *in R.*

Denken Sie an die Generalvoraussetzung, dass ab 2.3 alle Ringe eine $1 \neq 0$ haben.

Lemma 2.6.7 *Sei K kommutativer Ring. K ist genau dann ein Körper, wenn $\langle 0_K\rangle = \{0_K\}$ und $\langle 1_K\rangle = K$ die einzigen Ideale in K sind.*

Beweis: " $\Longrightarrow$ ":
Sei $I \subseteq K$ ein Ideal, das mindestens ein von Null verschiedenes Element a enthält. Dann existiert, da K Körper ist, auch ein multiplikatives Inverses a^{-1} zu a in K. Damit muss gelten, dass $1_K = a^{-1}a \in K$. Also ist I bereits der Körper K.
" $\Longleftarrow$ ":
Ist K kein Körper, so gibt es ein $a \in K \setminus \{0\}$, welches kein multiplikatives Inverses besitzt. Damit kann 1_K kein Vielfaches von a sein und es gilt:

$$\langle 0_K \rangle \subsetneq \langle a \rangle \subsetneq \langle 1_K \rangle,$$

was zu zeigen war.

□

Satz 2.6.8 *Seien R, S Ringe und sei $\varphi : R \longrightarrow S$ ein Ringhomomorphismus. Dann ist* $\ker(\varphi) \trianglelefteq R$ *ein Ideal in R. Da nach Generalvoraussetzung $1_R \neq 0_R$ ist* $\ker(\varphi)$ *eine echte Teilmenge von R.*

Beweis: Wir wissen, dass $\ker(\varphi) \neq \emptyset$, da $\varphi(0_R) = 0_S$ für jeden Gruppenhomomorphismus, als den sich die Abbildung φ bzgl. der zugrunde liegenden additiven Gruppen von R und S auffassen läßt.
Sind nun $a_1, a_2 \in \ker(\varphi)$ und $r_1, r_2 \in R$ beliebig. Dann gilt:

$$\begin{aligned} \varphi(r_1 a_1 + r_2 a_2) &= \varphi(r_1)\underbrace{\varphi(a_1)}_{=0_S} + \varphi(r_2)\underbrace{\varphi(a_2)}_{=0_S} = 0_S \\ \varphi(a_1 r_1 + a_2 r_2) &= \underbrace{\varphi(a_1)}_{=0_S}\varphi(r_1) + \underbrace{\varphi(a_2)}_{=0_S}\varphi(r_2) = 0_S. \end{aligned}$$

Somit liegt mit auch jede linksseitige und jede rechtsseitige R-Linearkombination von a_1 und a_2 in $\ker(\varphi)$, was damit ein Ideal in R ist.
Da wir mit Ringen mit $1 \neq 0$ arbeiten, ist eine der Bedingungen an den Ringhomomorphismus, dass $\varphi(1_R) = 1_S \neq 0_S$, weswegen $1_R \notin \ker(\varphi)$.

□

Korollar 2.6.9 *Sei R ein Ring mit $1 \neq 0$ und sei K ein Körper. Ist $\varphi : K \longrightarrow R$ ein Ringhomomorphismus, so ist φ injektiv.*

Beweis: Den Beweis finden Sie als Übungsaufgabe wieder.

□

Lemma 2.6.10 *Seien I, J Linksideale (bzw. Rechtsideale bzw. Ideale) in einem Ring R. Dann sind auch*

$$\begin{aligned} I + J &:= \{a + b \mid a \in I, b \in J\} \\ I \cap J &:= \{a \in R \mid a \in I \text{ und } a \in J\} \end{aligned}$$

Linksideale in R.

Der Beweis dieser Aussage besteht im Nachrechnen der Idealeigenschaften und bleibt den Studierenden überlassen.

Lemma 2.6.11 *Sei R ein Ring und $a \in R$. Dann gilt*

$$\langle a \rangle = \bigcap_{\substack{I \trianglelefteq R \\ a \in I}} I \trianglelefteq R.$$

Analoge Aussagen kann man für Links- bzw. Rechtsideal formulieren und beweisen, was im Vergleich zu zweiseitigen Idealen nur die offensichtlichen Änderungen erfordert.

Beweis: Offensichtlich ist $\langle a \rangle$ ein Ideal in R, das a enthält und damit ist die rechte Seite in der linken enthalten. Zu zeigen ist also nur die andere Inklusion.
Ist aber $a \in I$ für ein zweiseitiges Ideal I, so ist auch $ras \in I$ für alle $r, s \in R$ und damit $\langle a \rangle \subseteq I$. Damit ist $\langle a \rangle$ im Durchschnitt aller a enthaltenden Ideale enthalten.

□

Definition 2.6.12 *Sei R ein Ring und $I \trianglelefteq R$ ein Ideal (oder Linksideal oder Rechtsideal). Existiert ein $a \in I$, so dass $I = \langle a \rangle$ (bzw. $I = \langle a \rangle_\ell$ bzw. $I = \langle a \rangle_r$) , so heißt I* **Hauptideal** *(bzw.* **Linkshauptideal** *bzw.* **Rechtshauptideal***). Ist R ein Integritätsring und ist jedes Ideal in R ein Hauptideal, so heißt R* **Hauptidealring**.

Bemerkung 2.6.13 *Auch ein Ideal, das durch ein Erzeugersystem mit mehr als einem Erzeuger spezifiziert ist, kann ein Hauptideal sein. Man denke an $\langle 12, 15 \rangle \subseteq \mathbb{Z}$, was das von 3 erzeugte Hauptideal ist, oder an $\langle x^2 - 2x + 1, x^2 - 1 \rangle \subseteq \mathbb{Q}[x]$, welches von $x - 1$ erzeugt wird.*
Zwei Hauptideale $\langle a \rangle$ und $\langle b \rangle$ in einem Integritätsring R sind genau dann gleich, wenn es eine Einheit $c \in R^*$ gibt mit $a = cb$. Welches Argument brauchen Sie dafür?

Proposition 2.6.14 *$\mathbb{Z}[t]$ ist ein Integritätsring, jedoch kein Hauptidealring.*

Beweis: Da $\mathbb{Z}$ ein Integritätsring ist, ist nach 2.5.9,b) $\mathbb{Z}[t]$ ein Integritätsring. Betrachte andererseits $\langle 2, t\rangle \trianglelefteq \mathbb{Z}[t]$. Angenommen dieses Ideal ist ein Hauptideal $\langle a\rangle$. Dann gilt $a \neq 0$, $a \mid 2$ und $a \mid t$. Aus $a \neq 0$ und $a \mid 2$ können wir nach 2.5.9,a) schließen, dass $0 \leq \deg(a) \leq \deg(2) = 0$ gilt und damit $a \in \mathbb{Z}$. Wegen $a \mid t$ muss gelten $a = LC(a) \mid LC(t) = 1$, weswegen $a \in (\mathbb{Z}[t])^*$, das nach 2.5.9,c) gerade $\mathbb{Z}^* = \{1, -1\}$ ist. Andererseits gilt $1 \notin \langle 2, t\rangle$, was den gesuchten Widerspruch liefert. Also ist $\mathbb{Z}[t]$ kein Hauptidealring.

□

Proposition 2.6.15 *Sei R ein Integritätsring, aber kein Körper, so ist $R[t]$ kein Hauptidealring.*

Beweis: Dies finden Sie als Übungsaufgabe wieder.

□