KAPITEL 3

Ringe, Algebren und Körper

Wir kommen nun zu Strukturen mit zwei verträglichen Operationen, wobei wir etwas Hintergrund aus der linearen Algebra voraussetzen werden. Wir werden oft auf die Analogie zu Gruppen verweisen und dadurch die grundlegenden Resultate relativ schnell erhalten.

Grundlagen

3.1. Die grundlegenden Definition in diesem Bereich orientieren sich eng an den bekannten Zahlbereichen:

Definition 3.1. (1) Ein *Ring* $(R, +, \cdot)$ ist eine Menge R zusammen mit zwei Operationen $+, \cdot : R \times R \to R$ sodass gilt

- (i) $(R, +)$ ist eine kommutative Gruppe.
- (ii) Die Multiplikation $\cdot$ ist assoziativ.
- (iii) Für alle $a, b, c \in R$ gilt $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ und $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ ("Distributivität").

(2) Ein Ring $(R, +, \cdot)$ heißt *kommutativ*, wenn die Multiplikation $\cdot$ kommutativ ist.

(3) Existiert ein neutrales Element 1 für die Multiplikation, (das ungleich dem neutralen Element 0 der Addition ist), dann sagt man "R ist ein *Ring mit Eins(element)*".

(4) Ein *Nullteiler* in einem kommutativen Ring R ist ein Element $x \in R \setminus \{0\}$ sodass es ein $y \in R \setminus \{0\}$ mit $x \cdot y = 0$ gibt. Gibt es keine Nullteiler in R, dann heißt R *nullteilerfrei*. Ein *Integritätsbereich* ist ein nullteilerfreier, kommutativer Ring mit Einselement.

(5) Sei $(R, +, \cdot)$ ein Ring mit Einselement. Ein Element $x \in R$ heißt eine *Einheit*, wenn es ein Element $y \in R$ gibt, sodass $x \cdot y = y \cdot x = 1$ gilt. Ein *Körper* ist ein kommutativer Ring mit Einselement, in dem jedes Element $x \in R \setminus \{0\}$ eine Einheit ist.

(6) Sind $(R, +, \cdot)$ und $(S, \oplus, \odot)$ Ringe, dann ist ein *Ringhomomorphismus* $\varphi : R \to S$ eine Funktion, die mit beiden Operationen verträglich ist, d.h. $\varphi(x + y) = \varphi(x) \oplus \varphi(y)$ und $\varphi(x \cdot y) = \varphi(x) \odot \varphi(y)$ erfüllt. Bei Ringen mit Eins verlangt man zusätzlich, dass φ das Einselement von R auf das Einselement von S abbildet.

(7) Ein *Ringisomorphismus* ist ein bijektiver Ringhomomorphismus. Zwei Ringe heißen *isomorph* wenn es einen Ringisomorphismus zwischen ihnen gibt. In diesem Fall schreibt man $R \cong S$.

Bemerkung 3.1. (1) Ähnlich wie im Fall von Gruppen werden wir ab sofort die Addition auf jedem Ring mit $+$ bezeichnen und die Multiplikation einfach nur durch hinter einander schreiben der Elemente. Außerdem werden wir die übliche Konvention verwenden, dass die Multiplikation stärker bindet als die Addition ("Punktrechnung geht vor Strichrechnung") um Ausdrücke wie $ab + c$ zu interpretieren.

(2) Da $(R, +)$ und $(R, \cdot)$ Halbgruppen sind, können wir die Resultate aus Kapitel 2 anwenden. So ist etwa das neutrale Element für $(R, +)$ eindeutig bestimmt und wir werden dieses Element für jeden Ring mit 0 bezeichnen. Das additiv inverse Element

zur $x \in R$ werden wir immer mit $-x$ bezeichnen. Analog ist ein Einselement eindeutig bestimmt (wenn es existiert) und wir schreiben 1 dafür.

(3) Ein Ringhomomorphismus von $(R, +, \cdot)$ nach $(S, +, \cdot)$ ist nach Definition eine Funktion, die zugleich ein Homomorphismus der additiven Gruppen und der multiplikativen Halbgruppen ist. Damit können wir die Resultate über Homomorphismen aus Kapitel 2 auf Ringhomomorphismen anwenden. Insbesondere hat jeder Ringhomomorphismus φ einen Kern $\mathrm{Ker}(\varphi) = \{x \in R : \varphi(x) = 0\}$, der eine Untergruppe von $(R, +)$ und eine Unterhalbgruppe von $(R, \cdot)$ (und damit ein Teilring – siehe später) ist. Außerdem sehen wir aus den Resultaten aus 2.1 sofort, dass die Komposition von zwei Ringhomomorphismen wieder ein Ringhomomorphismus ist und dass für einen Ringisomorphismus φ auch die inverse Funktion φ^{-1} ein Ringhomomorphismus ist. Damit ist Isomorphie von Ringen eine Äquivalenzrelation. Aus 2.2 sehen wir, dass φ genau dann injektiv ist, wenn $\mathrm{Ker}(\varphi) = \{0\}$ gilt.

Beispiel 3.1. (1) $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring mit Einselement. Es gibt keine Nullteiler in $\mathbb{Z}$ (und dieses Beispiel motiviert den Namen "Integritätsbereich") aber die einzigen Einheiten in $\mathbb{Z}$ sind 1 und -1.

Die anderen Zahlbereiche $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +\cdot)$ sind Körper. Für jedes $n \geq 2$ bildet die Menge $\mathbb{Z}_n$ der Restklassen modulo n einen kommutativen Ring mit Einselement mit den üblichen Operationen. Ist n eine Primzahl, dann ist $\mathbb{Z}_n$ sogar ein Körper.

(2) Es gibt ganz natürliche Beispiele von kommutativen Ringen mit Einselement, die viele Nullteiler haben. Betrachten wir etwa die Menge $\mathcal{F}(\mathbb{R}, \mathbb{R})$ aller Funktionen von $\mathbb{R}$ nach $\mathbb{R}$ mit den punktweisen Operationen, also $(f + g)(t) = f(t) + g(t)$ und $(fg)(t) = f(t)g(t)$. Man verifiziert sofort, dass diese Operationen $\mathcal{F}(\mathbb{R}, \mathbb{R})$ zu einem kommutativen Ring mit Eins machen, wobei das Nullelement und das Einselement die konstanten Funktionen 0 und 1 sind. Damit gilt aber $f \neq 0$ genau dann, wenn es ein Element $t \in \mathbb{R}$ gibt, sodass $f(t) \neq 0$ gilt. Gibt es zusätzlich auch ein $s \in \mathbb{R}$ sodass $f(s) = 0$ gilt, dann ist f ein Nullteiler. Definiert man nämlich $g : \mathbb{R} \to \mathbb{R}$ durch $g(s) = 1$ und $g(x) = 0$ für $x \neq s$, dann gilt offensichtlich $(fg)(x) = f(x)g(x) = 0$ für alle $x \in \mathbb{R}$. Damit sind die Nullteiler in $\mathcal{F}(\mathbb{R}, \mathbb{R})$ genau die Funktionen, die mindestens eine Nullstelle besitzen.

Ist andererseits $f(x) \neq 0$ für alle $x \in \mathbb{R}$, dann ist f eine Einheit in $\mathcal{F}(\mathbb{R}, \mathbb{R})$, denn dann kann man eine multiplikativ inverse Funktion durch $g(x) := 1/(f(x))$ definieren.

(3) Wie aus der linearen Algebra bekannt ist, ist ein Vektorraum über einem Körper K eine kommutative Gruppe $(V, +)$ zusammen mit einer Skalarmultiplikation $K \times V \to V$, die gewisse Verträglichkeitsbedingungen erfüllt. Betrachtet man nun eine Multiplikation $\cdot : V \times V \to V$, dann ist die natürliche Verträglichkeitsbedingung mit der Vektorraumstruktur, dass $\cdot$ *bilinear* ist. Das bedeutet, dass für jedes fixe $v_0 \in V$, die Abbildungen $V \to V$, die durch $v \mapsto v \cdot v_0$ und $v \mapsto v_0 \cdot v$ gegeben sind, linear sind. Das bedeute insbesondere, dass die Distributivgesetze gelten, also $(V, +, \cdot)$ ein Ring ist. Man sagt dann, $(V, +, \cdot)$ ist eine *K–Algebra*. Außerdem gilt dann $\lambda(v \cdot w) = (\lambda v) \cdot w = v \cdot (\lambda w)$ für $\lambda \in K$ und $v, w \in V$. Ein *Algebrahomomorphismus* zwischen zwei K–Algebren ist eine K–lineare Abbildung, die zugleich ein Ringhomomorphismus ist.

Da man auf $\mathcal{F}(\mathbb{R}, \mathbb{R})$ auch eine Skalarmultiplikation punktweise definieren kann, die dann $\mathcal{F}(\mathbb{R}, \mathbb{R})$ zu einem $\mathbb{R}$–Vektorraum macht, liefert uns Beispiel (2) von oben sogar ein Beispiel einer $\mathbb{R}$–Algebra. Analog ist für $X \subset \mathbb{R}$ die Menge $\mathcal{F}(X, \mathbb{R})$ eine $\mathbb{R}$–Algebra unter den punktweisen Operationen. Für eine Funktion $f : \mathbb{R} \to \mathbb{R}$ kann man dann die Einschränkung $f|_X : X \to \mathbb{R}$ betrachten. Man verifiziert sofort, dass $\varphi(f) := f|_X$ einen Algebrahomomorphismus $\varphi : \mathcal{F}(\mathbb{R}, \mathbb{R}) \to \mathcal{F}(X, \mathbb{R})$ definiert.

(4) Die lineare Algebra liefert weitere wichtige Beispiele von, insbesondere auch nicht–kommutativen, Algebren. Betrachten wir nämlich für einen K–Vektorraum V den Raum $L(V,V)$ aller linearen Abbildungen $f : V \to V$. Dann ist $L(V,V)$ ein Vektorraum unter punktweisen Operationen und die Komposition $\circ$ macht $L(V,V)$ zu einer K–Algebra (siehe Übungen). Natürlich ist diese Algebra nicht kommutativ, falls $\dim(V) > 1$ gilt.

Spezialisiert man auf $V = K^n$, dann kann man $L(V,V)$ mit dem Raum $M_n(K)$ aller $n \times n$–Matrizen über K identifizieren. Die (punktweise) Vektorraumstruktur auf $L(V,V)$ entspricht der komponentenweisen Addition und Skalarmultiplikation auf $M_n(K)$. Die Komposition linearer Abbildungen entspricht genau der üblichen Matrizenmultiplikation. Damit ist $M_n(K)$ eine (für $n > 1$ nicht–kommutative) K–Algebra unter der Matrizenmultiplikation.

Wir können nun einige elementare Eigenschaften sofort abklären:

Lemma 3.1. *Sei $(R, +, \cdot)$ ein Ring.*

(1) Für jedes Element $x \in R$ gilt $0 \cdot x = x \cdot 0 = 0$.

(2) Für $x, y \in R$ gilt $(-x)y = x(-y) = -(xy)$. Hat insbesondere R ein Einselement, dann ist $(-1)x = -x$ für alle $x \in R$.

(3) Eine Einheit x in einem kommutativen Ring mit Einselement ist kein Nullteiler und das multiplikativ inverse Element zu x ist eindeutig bestimmt. Insbesondere ist jeder Körper automatisch ein Integritätsbereich. Umgekehrt ist ein endlicher Integritätsbereich automatisch ein Körper.

Beweis. (1) Es gilt $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x$, und das Resultat folgt, indem man von beiden Seiten $0 \cdot x$ subtrahiert. Die zweite Gleichung folgt analog.

(2) Wir rechnen $(-x)y + xy = ((-x) + x) \cdot y = 0 \cdot y$, was nach Teil (1) gleich 0 ist. Damit ist aber $(-x)y$ das additiv inverse Element zu xy. Der Beweise für $x(-y)$ geht analog.

(3) Nach Voraussetzung gibt es ein Element $y \in R$ sodass $yx = 1$ gilt. Ist nun $z \in R$ so, dass $xz = 0$ gilt, dann ist $0 = y(xz) = (yx)z = 1 \cdot z = z$. Damit ist x kein Nullteiler und die Aussage, dass jeder Körper ein Integritätsbereich ist, ist klar.

Für Elemente $x, y, \tilde{y}$ in einem Ring R folgt aus $xy = x\tilde{y}$ natürlich $0 = xy - x\tilde{y} = x(y - \tilde{y})$ und falls x kein Nullteiler ist, dann ist das nur für $y - \tilde{y} = 0$, also $y = \tilde{y}$ möglich. Mit dem obigen Argument folgt daraus einerseits, dass das multiplikativ inverse Element eindeutig bestimmt ist. Andererseits sehen wir, dass die Funktion $\ell_x : R \to R$, die definiert ist durch $\ell_x(y) := xy$ injektiv ist. Ist R endlich, dann ist $\ell_x(R) \subset R$ eine Teilmenge, die (wegen der Injektivität) gleich viele Elemente hat wie R selbst, also $\ell_x(R) = R$. Insbesondere gibt es ein Element $y \in R$ sodass $xy = \ell_x(y) = 1$ gilt. □

3.2. Teilringe, Ideale und Quotienten. Das Konzept des Teilringes wirft keinerlei Probleme auf. Man betrachtet einfach eine Untergruppe S von $(R, +)$ sodass für $x, y \in S$ auch $xy \in S$ gilt, also S zugleich eine Unterhalbgruppe von $(R, \cdot)$ ist. Ist $S \subset R$ ein Teilring, dann schreibt man $S \leq R$. Daraus folgt einerseits sofort, dass der Durchschnitt über eine beliebige Familie von Teilringen wieder ein Teilring ist. Insbesondere gibt es zu jeder Teilmenge $A \subset R$ einen kleinsten Teilring von R, der A enthält, den *von A erzeugten Teilring*. Damit macht auch der Begriff eines Erzeugendensystems für einen Ring R Sinn.

Andererseits sehen wir aus den Resultaten für Gruppen aus 2.2 sofort, dass Bilder und Urbilder von Teilringen unter Ringhomomorphismen automatisch wieder Teilringe sind. Insbesondere sind für einen Ringhomomorphismus $\varphi : R \to S$ der Kern $\mathrm{Ker}(\varphi) \subset$

R und das Bild $\mathrm{Im}(\varphi) \subset S$ wieder Teilringe. Außerdem sieht man wieder leicht, dass ein Ringhomomorphismus φ durch seine Einschränkung auf ein Erzeugendensystem E eindeutig bestimmt ist und dass $\varphi(E)$ ein Erzeugendensystem für $\mathrm{Im}(\varphi)$ ist.

Als nächstes wollen wir überlegen, was wir brauchen um Quotienten von Ringen zu bilden. Wir betrachten also eine Äquivalenzrelation $\sim$ auf einem Ring R. Um die Operationen auf die Menge $R/\sim$ der Äquivalenzklassen übertragen zu können müssen wir verlangen, dass aus $x \sim \tilde{x}$ und $y \sim \tilde{y}$ immer $x+y \sim \tilde{x}+\tilde{y}$ und $xy \sim \tilde{x}\tilde{y}$ folgen. Aus der Diskussion in 2.4 und 2.5 wissen wir bereits, dass die erste Bedingung impliziert, dass die Äquivalenzklasse $[0] =: I \subset R$ eine Untergruppe von $(R,+)$ sein muss und dass $x \sim y$ genau dann gilt, wenn die Nebenklassen $x+I$ und $y+I$ gleich sind. (Wegen der Kommutativität der Addition ist I ja automatisch ein Normalteiler.) Ist nun aber $x \sim 0$ und $y \in R$ beliebig, dann folgt wegen $y \sim y$ auch $xy \sim 0y = 0$ und $yx \sim y0 = 0$. Das motiviert die folgende Definition:

Definition 3.2. Sei $(R,+,\cdot)$ ein Ring. Ein *Ideal* in R ist eine Teilmenge $I \subset R$, sodass

(*i*) $(I,+)$ ist eine Untergruppe von $(R,+)$.
(*ii*) Für beliebige Elemente $x \in I$ und $y \in R$ gilt $xy \in I$ und $yx \in I$.

Ist I ein Ideal in R, dann schreibt man $I \lhd R$.

Wir werden hauptsächlich Ideale in kommutativen Ringen betrachten, wo die Reihenfolge im Produkt keine Rolle spielt. In nicht–kommutativen Ringen kann man detaillierter *Linksideale*, *Rechtsideale* und *beidseitige Ideale* betrachten, wir werden das aber nicht tun.

Bevor wir uns der Frage der Quotientenbildung widmen, betrachten wir die strukturellen Eigenschaften von Idealen. Hier zeigt sich, dass man mit Idealen sehr gut rechnen kann. Daher kommt auch der Name, der sich von "ideale Zahlen" ableitet.

Proposition 3.2. *Sei $(R,+,\cdot)$ ein Ring.*

(1) Für eine beliebige Familie $\{I_a : a \in A\}$ von Idealen in R ist auch der Durchschnitt $I := \cap_{a\in A} I_a$ ein Ideal in R.

(2) Ist $\varphi : R \to S$ ein Ringhomomorphismus und $I \lhd S$ ein Ideal, dann ist $\varphi^{-1}(I)$ ein Ideal in R.

(3) Sind $I, J \lhd R$ Ideale in R, dann sind auch $I+J := \{x+y : x \in I, y \in J\}$ und IJ, die von $\{xy : x \in I, y \in J\}$ erzeugte Untergruppe von $(R,+)$, Ideale in R.

Beweis. (1) Beweist man ganz analog wie für Untergruppen, Normalteiler und Teilringe.

(2) Wir wissen bereits aus 2.2, dass $\varphi^{-1}(I)$ eine Untergruppe von $(R,+)$ ist. Für $x \in \varphi^{-1}(I)$ und $y \in R$ ist $\varphi(xy) = \varphi(x)\varphi(y)$ und $\varphi(yx) = \varphi(y)\varphi(x)$. Nach Voraussetzung gilt $\varphi(x) \in I$ und weil I ein Ideal ist, folgt $\varphi(xy), \varphi(yx) \in I$, also $xy, yx \in \varphi^{-1}(I)$.

(3) Da I und J Untergruppen von $(R,+)$ sind, ist $0 \in I$ und $0 \in J$, also $0 = 0+0 \in I+J$. Für $x+y \in I+J$ gilt natürlich $-(x+y) = (-x)+(-y) \in I+J$, weil $-x \in I$ und $-y \in J$ gilt. Für $x_1, x_2 \in I$ und $y_1, y_2 \in J$ ist schließlich $(x_1+y_1)+(x_2+y_2) = (x_1+x_2)+(y_2+y_2) \in I+J$. Damit ist $I+J$ eine Untergruppe von $(R,+)$, was für IJ nach Definition gilt.

Für $x \in I$, $y \in J$ und $z \in R$ gilt nach Voraussetzung $zx, xz \in I$ und $zy, yz \in J$. Damit liegen aber $z(x+y) = zx+zy$ und $(x+y)z = xz+yz$ in $I+J$, also ist $I+J$ ein Ideal. Außerdem liegen $z(xy) = (zx)y$ und $(xy)z = x(yz)$ in IJ und daraus folgt leicht, dass das auch für alle Elemente der von solchen Produkten erzeugten Untergruppe gilt. □

Nach Teil (1) gibt es wieder für jede Teilmenge $A \subset R$ ein kleinstes Ideal $I \lhd R$ für das $A \subset I$ gilt. Man nennt dieses *das von A erzeugte Ideal in R.*

Beispiel 3.2. (1) Sei $\varphi : R \to S$ ein Ringhomomorphismus. Dann ist $\mathrm{Ker}(\varphi)$ ein Ideal in R. Wir habe oben schon bemerkt, dass $\mathrm{Ker}(\varphi)$ eine Untergruppe von $(R, +)$ ist. Für $x \in \mathrm{Ker}(\varphi)$ und $y \in R$ gilt aber $\varphi(xy) = \varphi(x)\varphi(y) = 0 \cdot \varphi(y) = 0$ und analog ist $\varphi(yx) = 0$.

(2) Ist R ein kommutativer Ring und $a \in R$ ein beliebiges Element. Dann behaupten wir, dass $aR := \{ax : x \in R\}$ ein Ideal ist. Wegen $a \cdot 0 = 0$, $a \cdot (-x) = -ax$ und $ax + ay = a(x + y)$ ist aR eine Untergruppe von $(R, +)$. Für $x, y \in R$ ist weiters $(ax)y = a(xy)$, und wegen der Kommutativität genügt, dass um die Behauptung zu beweisen. Das Ideal $aR \lhd R$ heißt das *von a erzeugte Hauptideal* von R.

(3) Ist R ein Ring mit Einselement und $I \lhd R$ ein Ideal, das eine Einheit enthält, dann ist $I = R$. Ist nämlich $x \in I$ eine Einheit in R, dann ist $xx^{-1} = 1 \in I$ und damit für jedes Element $y \in R$ auch $y = y \cdot 1 \in I$. Damit folgt insbesondere, dass es in einem Körper K nur die trivialen Ideale $\{0\}$ und K gibt.

Wir wissen nun also, dass eine Äquivalenzrelation $\sim$ auf einem Ring R genau dann zwei wohldefinierte Operationen auf der Menge $R/\sim$ aller Äquivalenzklassen liefert, wenn aus $x \sim \tilde{x}$ und $y \sim \tilde{y}$ sowohl $x + y \sim \tilde{x} + \tilde{y}$ als auch $xy \sim \tilde{x}\tilde{y}$ folgt. Wir haben auch schon überlegt, dass dann die Relation durch $x \sim y \Leftrightarrow x + I = y + I$ für ein Ideal $I \lhd R$ sein muss. Wir schreiben wieder R/I für die Menge der Nebenklassen, die ja nach Satz 2.5 eine (offensichtlich kommutative) Gruppe ist und $\pi : R \to R/I$ für den kanonischen Quotientenhomomorphismus (von Gruppen).

Satz 3.2. *Sei R ein Ring und $I \lhd R$ ein Ideal. Dann gilt:*

(1) Die Multiplikation auf R induziert eine wohldefinierte Multiplikation auf R/I, die diese Menge zu einem Ring und $\pi : R \to R/I$ zu einem Ringhomomorphismus mit $\mathrm{Ker}(\pi) = I$ macht.

(2) Ist $\varphi : R \to S$ ein Ringhomomorphismus mit $I \subset \mathrm{Ker}(\varphi)$, dann gibt es einen eindeutigen Ringhomomorphismus $\underline{\varphi} : R/I \to S$, sodass $\varphi = \underline{\varphi} \circ \pi$ gilt. Insbesondere induziert φ einen Isomorphismus $\overline{R/}\,\mathrm{Ker}(\varphi) \to \mathrm{Im}(\varphi)$ von Ringen.

Beweis. (1) Wir wissen bereits aus Kapitel (2), dass man auf R/I eine eindeutige Addition erhält, die R/I zu einer kommutativen Gruppe und π zu einem Gruppenhomomorphismus macht. Diese ist explizit durch $(x + I) + (y + I) = (x + y) + I$ gegeben. Natürlich wollen wir $(x+I)(y+I) := xy+I$ definieren, was ja gerade $\pi(x)\pi(y) = \pi(xy)$ bedeutet. Um zu zeigen, dass das wohldefiniert ist, bedenken wir, dass ein Element $\tilde{x}$ mit $x + I = \tilde{x} + I$ von der Form $\tilde{x} = x + z$ mit $z \in I$ sein muss. Ist analog $\tilde{y} = y + w$ mit $w \in I$, dann ist

$$\tilde{x}\tilde{y} = (x + z)(y + w) = xy + xw + zy + yw,$$

und weil I ein Ideal ist, gilt $xw + zy + zw \in I$, also $\tilde{x}\tilde{y} + I = xy + I$. Damit ist die Multiplikation auf R/I wohldefiniert. Die Assoziativität der Multiplikation und die Distributivität in R/I folgen sofort aus den entsprechenden Eigenschaften für R. Damit ist R/I ein Ring und nach Konstruktion ist π ein Ringhomomorphismus.

(2) Aus Satz 2.6 wissen wir, dass wir durch $\underline{\varphi}(x + I) := \varphi(x)$ einen wohldefinierten Gruppenhomomorphismus $(R, +) \to (S, +)$ erhalten, der $\varphi = \underline{\varphi} \circ \pi$ erfüllt und durch diese Eigenschaft eindeutig bestimmt ist. Nach Konstruktion ist weiters

$$\underline{\varphi}((x + I)(y + I)) = \underline{\varphi}(xy + I) = \varphi(xy) = \varphi(x)\varphi(y) = \underline{\varphi}(x + I)\underline{\varphi}(x + I),$$

also ist $\underline{\varphi}$ ein Ringhomomorphismus. Aus Korollar 2.6 wissen wir weiters, dass der induzierte Homomorphismus für $I = \mathrm{Ker}(\varphi)$ eine Bijektion auf $\mathrm{Im}(\varphi)$ definiert damit einen Ringisomorphismus $R/\mathrm{Ker}(\varphi) \to \mathrm{Im}(\varphi)$ liefert. □

Polynome

3.3. Polynomringe. Neben den Zahlbereichen liefern Polynomringe ganz zentrale Beispiele von kommutativen Ringen mit Einselement. Wie wir später sehen werden, kann man auch relativ einfach Körper als Quotienten von Polynomringen konstruieren. Die Analogie zwischen dem Polynomring über einem Körper und den ganzen Zahlen ist ein sehr schönes Beispiel für die verbindenden Rolle von allgemeinen algebraischen Ideen.

Die aus der Schule bekannte Idee, Polynome als spezielle Funktionen zu definieren ist für die allgemeine Behandlung von Polynomringen nicht geeignet. Betrachten wir zum Beispiel den endlichen Körper $\mathbb{Z}_2 = \{0, 1\}$. Dann macht natürlich für jedes $k \in \mathbb{N}$, $t^k = 1 \cdot t^k$ als Polynom über $\mathbb{Z}_2$ Sinn, also gibt es unendlich viele Polynome über $\mathbb{Z}_2$. Zugleich gibt es aber nur 4 Funktionen von der zweielementigen Menge $\mathbb{Z}_2$ auf sich selbst. Man kann leicht sehen, dass das Polynom $t^2 + t = t(t + 1)$ als Funktion $\mathbb{Z}_2 \to \mathbb{Z}_2$ interpretiert die Nullfunktion liefert. Daher definieren wir Polynome als formale Ausdrücke.

Definition 3.3. Sei R ein kommutativer Ring mit Einselement.

(1) Ein *Polynom* über R ist ein formaler Ausdruck p, den man entweder als $a_0 + a_1t + a_2t^2 + \cdots + a_Nt^N$ oder als $\sum_{i=0}^N a_it^i$ schreibt, wobei die *Koeffizienten* a_i von p Elemente von R sind und die *Variable* t bzw. t^i nur als Symbol betrachtet wird. (Man kann die Variable auch problemlos mit x oder y bezeichnen.) Die Menge aller Polynome über R wird mit $R[t]$ bezeichnet.

(2) Ist $p \neq 0$ (d.h. mindestens ein $a_i \neq 0$), dann heißt der größte Index n, für den $a_n \neq 0$ gilt, der *Grad* des Polynoms p. Man schreibt $\deg(p) \in \mathbb{N}$ dafür. Wir folgen der Konvention, dass die Koeffizienten a_i von p immer für alle $i \in \mathbb{N}$ definiert sind, indem wir $a_i = 0$ für alle $i > \deg(p)$ setzen.

(3) Für $p = \sum_{i=0}^N a_it^i$ und $q = \sum_{j=0}^M b_jt^j$ definiert man $p+q := \sum_{k=0}^{\max(N,M)}(a_k+b_k)t^k$ und $pq := \sum_{\ell=0}^{M+N} c_\ell t^\ell$, wobei $c_k := \sum_{i+j=k} a_ib_j$.

Bemerkung 3.3. Die Definition von Polynomen als "formale Ausdrücke" ist nicht die mathematisch saubere Version. Für diese betrachtet man die Menge aller endlichen Folgen in R d.h. aller jener Funktionen $a : \mathbb{N} \to R$ sodass es ein $N \in \mathbb{N}$ gibt, sodass $a(n) = 0$ für alle $n > N$ gilt. Dann schreibt man, wie bei Folgen üblich, einfach $a_n \in R$ für den Funktionswert $a(n)$ und schreibt die Folge (a_n) als $\sum_n a_nt^n$. In diesem Bild entspricht die Summe von Polynomen genau der üblichen (punktweisen) Summe von Funktionen, aber das Produkt von Polynomen ist nicht als das punktweise Produkt von Funktionen definiert, sondern als $(a * b)(k) := \sum_{i+j=k} a(i)b(j)$. Diese Operation findet auch in anderen Bereichen der Mathematik Verwendung und wird üblicherweise als *Faltung* bezeichnet.

Die Schreibweise $\sum_n a_nt^n$ hat einerseits den Vorteil, dass die Multiplikation in dieser Schreibweise einfach aussieht: Es gilt einfach $t^it^j = t^{i+j}$ und Distributivität bezüglich der Addition.

Die grundlegenden Eigenschaften von Polynomen sind:

Proposition 3.3. *Sei R ein kommutativer Ring mit Eins, $\mathbb{K}$ ein Körper und seien $R[t]$ und $\mathbb{K}[t]$ die zugehörige Menge von Polynomen. Dann gilt:*

(1) Die Operationen aus Teil (2) von Definition 3.3 machen $R[t]$ zu einem kommutativen Ring mit Einselement und $\mathbb{K}[t]$ zu einer $\mathbb{K}$–Algebra.

(2) Für $p, q \in R[t]$ mit $p, q, p+q \neq 0$ gilt $\deg(p+q) \leq \max(\deg(p), \deg(q))$.

(3) Ist R ein Integritätsbereich, dann ist auch $R[t]$ ein Integritätsbereich und für $p, q \in R[t]$ mit $p, q \neq 0$ gilt $\deg(pq) = \deg(p) + \deg(q)$. *Die Einheiten im Ring $\mathbb{K}[t]$ sind genau die konstanten Polynome ungleich Null, also jene $p \neq 0$, die* $\deg(p) = 0$ *erfüllen.*

Beweis. (1) Man muss die definierenden Eigenschaften einfach direkt verifizieren, wobei man die Eigenschaften der Operationen in R benutzt. Die Tatsache, dass $(R[t], +)$ eine kommutative Gruppe ist, folgt sofort aus den entsprechenden Eigenschaften von $(R, +)$. Insbesondere ist das neutrale Element das Nullpolynom, dessen Koeffizienten alle 0 sind und für $p \in R[t]$ mit Koeffizienten a_i sind die Koeffizienten von $-p$ gerade $-a_i$ für alle $i \in \mathbb{N}$. Die Kommutativität der Multiplikation ist aus der Definition und der Kommutativität der Multiplikation auf R offensichtlich. Das Einselement 1 hat Koeffizienten $a_0 = 1$ und $a_i = 0$ für alle $i > 0$. Um die Assoziativität der Multiplikation zu verifizieren zeigt man, dass für drei Polynome $p, q, r \in R[t]$ mit Koeffizienten a_i, b_j und c_k der ℓ–te Koeffizient von $(pq)r$ durch $\sum_{i+j+k=\ell}(a_i b_j)c_k$ gegeben ist, während man für $p(qr)$ durch $\sum_{i+j+k=\ell} a_i(b_j c_k)$ erhält. Die Distributivität folgt einfach aus

$$\sum_{i+j=k} a_i(b_j + c_j) = \sum_{i+j=k} (a_i b_j + a_i c_j) = \sum_{i+j=k} a_i b_j + \sum_{i+j=k} a_i c_j.$$

Im Fall eines Körpers $\mathbb{K}$ verifiziert man leicht, dass die koeffizientenweise Skalarmultiplikation $\mathbb{K}[t]$ zu einem $\mathbb{K}$–Vektorraum macht. Dass das Produkt mit der Skalarmultiplikation in jedem der beiden Faktoren verträglich ist, ist offensichtlich.

(2) Haben p und q die Koeffizienten a_i bzw. b_j und gilt $k > \deg(p)$ und $k > \deg(q)$, dann ist $a_k = b_k = 0$, also auch $a_k + b_k = 0$.

(3) Seien $p, q \neq 0$ mit $\deg(p) = n$ und $\deg(q) = m$ und Koeffizienten a_i und b_j. Bezeichnen wir die Koeffizienten von pq mit c_k, dann gilt nach Definition $c_k = \sum_{i+j=k} a_i b_j$. Ist $k > n+m$ und $i+j = k$, dann muss entweder $i > n$ und damit $a_i = 0$ oder $j > m$ und damit $b_j = 0$ gelten, also ist jedenfalls $a_i b_j = 0$ und damit folgt $c_k = 0$. Ist andererseits $k = n + m$ und $i + j = k$, dann ist $i \leq n$ und $j \leq m$ nur für $i = n$ und $j = m$ möglich. Damit gilt aber $c_{n+m} = a_n b_m$. Nach Voraussetzung ist $a_n \neq 0$ und $b_m \neq 0$ und da R ein Integritätsbereich ist, folgt $c_{n+m} \neq 0$, also $pq \neq 0$ und $\deg(pq) = \deg(p) + \deg(q)$.

Ist $p \in \mathbb{K}[t]$ ein Einheit, dann muss $p \neq 0$ gelten. Wegen $\deg(1) = 0$ und $\deg(pp^{-1}) = \deg(p) + \deg(p^{-1})$ sehen wir, dass $\deg(p) = 0$ gelten muss. Sind a_i die Koeffizienten von p, dann gilt also $a_0 \neq 0$ und $a_i = 0$ für alle $i > 0$. Damit ist aber das konstante Polynom $(a_0)^{-1}$ multiplikativ invers zu p. □

3.4. Polynomfunktionen. Einer der Gründe für die Wichtigkeit von Polynomringen ist, dass man in einem Polynom für die Variable t "einsetzen" und damit Polynome "auswerten" kann. Damit kann man einerseits Polynome als Funktionen auf anderen Mengen betrachten (was in dem Fall, wo man für einen Körper $\mathbb{K}$ Polynome in $\mathbb{K}[t]$ als Funktionen auf $\mathbb{K}$ interpretiert, zurück zu der aus der Schule bekannten Sichtweise von Polynomen führt). Wichtiger ist aber, dass diese Konstruktion, ähnlich wie in 2.3 für Gruppen besprochen, zu einer Beschreibung des von einem Element erzeugten Teilringes führt.

Sei R ein Ring mit Einselement 1 und $r \in R$ ein Element. Dann definieren wir $r^0 := 1$, $r^1 := r$ und induktiv $r^{k+1} := r^k r$ für $k \geq 1$. Aus 2.3 und 2.13 wissen wir auch schon, dass wir Elemente der kommutativen Gruppe $(R, +)$ mit Elementen von $\mathbb{Z}$

multiplizieren können, indem wir $0 \cdot r = 0$, und für $k > 0$, $k \cdot r = r + r + \cdots + r$ mit k Summanden und $(-k) \cdot r := -(k \cdot r)$ setzen. Ist nun $p := \sum_{i=0}^{N} a_i t^i \in \mathbb{Z}[t]$ ein Polynom mit Koeffizienten in $\mathbb{Z}$, dann definieren wir $p(r) := \sum_{i=0}^{n} a_i \cdot r^i \in R$, wobei wir die Summe in R interpretieren. Anders gesagt, können wir p auch als Funktion $p : R \to R$ interpretieren.

Ist R nicht nur ein Ring sondern eine Algebra über einem Körper $\mathbb{K}$, dann können wir völlig analog $p(r)$ für jedes $p \in \mathbb{K}[t]$ und jedes $r \in R$ bilden, wobei wir jetzt $a_i \cdot r^i$ als die Skalarmultiplikation interpretieren. (Es gilt ja $a_i \in \mathbb{K}$ und $r^i \in R$.)

Ist R ein Ring, dann gilt natürlich $(a + b) \cdot r = a \cdot r + b \cdot r$ für alle $a, b \in \mathbb{Z}$ und $r \in R$. Wenden wir das auf Potenzen von r und die Koeffizienten von Polynomen und benutzen die Kommutativität der Addition, dann folgt sofort, dass

$$(\sum_i a_i \cdot r^i) + (\sum_j b_j \cdot r^j) = \sum_k (a_k + b_k) r^k$$

gilt. Das zeigt aber, dass $(p+q)(r) = p(r) + q(r)$ gilt. Aus der Distributivität in R folgt auch, dass für $a \in \mathbb{Z}$ und $r, s \in R$ die Gleichung $(a \cdot r)s = r(a \cdot s) = a \cdot (rs)$ gilt und daraus folgt für $b \in \mathbb{Z}$ auch $(a \cdot r)(b \cdot s) = ab \cdot (rs)$. Zusammen mit $r^i r^j = r^{i+j}$ und der Distributivität in R folgt daraus, dass

$$(\sum_i a_i \cdot r^i)(\sum_j b_j \cdot r^j) = \sum_{i,j} a_i b_j r^{i+j}$$

gilt. Fasst man in dieser Summe die Terme, in denen r mit der gleichen Potenz auftritt zusammen, dann erhält man $\sum_k (\sum_{i+j=k} a_i b_j) r^k$, also folgt $p(r)q(r) = (pq)(r)$ für alle $p, q \in \mathbb{Z}[t]$. Ist R eine Algebra über einem Körper $\mathbb{K}$, dann erhalten wir die analogen Aussagen auch für $p, q \in \mathbb{K}[t]$. Damit erhalten wir:

Proposition 3.4. *Sei R ein Ring mit Einselement. Dann definiert $\varphi(p) := p(r)$ für jedes Element $r \in R$ einen Ringhomomorphismus $\varphi : \mathbb{Z}[t] \to R$, dessen Bild genau der von r erzeugte Teilring von R ist.*

Ist R eine Algebra über einem Körper $\mathbb{K}$, dann erhält man analog einen Algebrahomomorphismus $\varphi : \mathbb{K}[t] \to R$, dessen Bild die von r erzeugte Teilalgebra von R ist.

Beweis. Nach Definition ist $\varphi(p+q) = (p+q)(r)$, und wir haben gerade verifiziert, dass das gleich $p(r) + q(r) = \varphi(p) + \varphi(q)$ ist. Analog sagt $(pq)(r) = p(r)q(r)$ genau, dass $\varphi(pq) = \varphi(p)\varphi(q)$ gilt, also ist φ ein Ring bzw. Algebrahomomorphismus. Damit ist $\mathrm{Im}(\varphi) \subset R$ ein Teilring. Das Polynom $t = 0 + 1t + 0t^2 + \ldots$ wird unter φ auf $r \in R$ abgebildet, also enthält $\mathrm{Im}(\varphi)$ den von r erzeugten Teilring von R. Andererseits muss dieser natürlich mit r auch $r^2 = rr$ und damit induktiv r^i für $i \in \mathbb{N}$ und somit $a_i r^i$ für jedes $a_i \in \mathbb{Z}$ enthalten. Addiert man solche Elemente auf, dann sieht man, dass für jedes $p \in \mathbb{Z}[t]$ auch $p(r)$ in dem von R erzeugten Teilring liegen muss. Im Fall einer Algebra geht der Beweis ganz analog. □

In Anbetracht dieses Resultats bezeichnet man für einen Ring R und ein Element $r \in R$ den von r erzeugten Teilring oft mit $\mathbb{Z}[r] \subset R$, weil er ja genau aus den Elementen von R besteht, die man als "Polynom mit ganzzahligen Koeffizienten in r" schreiben kann. Analog bezeichnet man für eine $\mathbb{K}$–Algebra R und ein Element $r \in R$ die von r erzeugte Teilalgebra von R mit $\mathbb{K}[r] \subset R$.

Bemerkung 3.4. Man kann dieses Resultat auch so lesen, dass man für einen Ring R jedem $p \in \mathbb{Z}[t]$ eine Funktion $R \to R$ zuordnen kann, die wir der Einfachheit halber ebenfalls mit p bezeichnen. Die Menge $\mathcal{F}(R, R)$ aller Funktionen $R \to R$ ist ein Ring unter den punktweisen Operationen (vergleiche mit Beispiel (2) von 3.1). Unsere obigen

Beobachtungen sagen auch, das diese Zuordnung ein Ringhomomorphismus ist. Analog ist für eine $\mathbb{K}$–Algebra R die Menge $\mathcal{F}(R,R)$ eine $\mathbb{K}$–Algebra unter den punktweisen Operationen, und wir erhalten einen Homomorphismus $\mathbb{K}[t] \to \mathcal{F}(R,R)$ von Algebren. Wendet man das auf die $\mathbb{K}$–Algebra $\mathbb{K}$ an, dann ist der resultierende Homomorphismus für unendliche Körper injektiv und man kommt (für $\mathbb{K} = \mathbb{R}$) zurück zum aus der Schule bekannten Begriff von Polynomen.

Euklidische Ringe, Hauptidealbereiche und eindeutige Primfaktorzerlegung

Wir werden nun einige spezielle Klassen von Integritätsbereichen betrachten. In diesem Abschnitt sind also alle Ringe kommutativ und nullteilerfrei und haben ein Einselement. Nachdem allgemeine Elemente in so einem Ring keine multiplikativ Inversen besitzen, macht der Begriff der Teilbarkeit Sinn. Dieser hängt eng mit Idealen zusammen. Für $x, y \in R$ bedeutet "x teilt y" ja gerade, dass es ein Element $z \in R$ gibt, sodass $y = xz$ gilt. Das ist aber genau äquivalent dazu, dass y im von x erzeugten Hauptideal xR liegt. Im Beispiel von $\mathbb{Z}$ ist der Schlüssel zur Analyse von Teilbarkeitsfragen die Division mit Rest. Dieses Konzept lässt sich im Begriff des Euklidischen Ringes abstrahieren. Das führt zu einer sehr schönen Analogie zwischen $\mathbb{Z}$ und dem Polynomring $\mathbb{K}[t]$ über einem Körper $\mathbb{K}$.

3.5. Euklidische Ringe. Wenn man eine Division mit Rest betrachten möchte, dann braucht man einen Weg um auszudrücken, dass der Rest kleiner ist als der Divisor. Im Fall von $\mathbb{Z}$ geht das einfach durch den üblichen Absolutbetrag, im Allgemeinen muss man verlangen, dass man eine geeignete Funktion zum Messen der Größe gegeben hat.

Definition 3.5. Ein *Euklidischer Ring* ist ein Integritätsbereich R zusammen mit einer Funktion $\delta : R \setminus \{0\} \to \mathbb{N}$ sodass

(*i*) $\delta(ab) \geq \delta(a)$ für alle $a, b \in R \setminus \{0\}$
(*ii*) Zu beliebigen Elementen $p_1, p_2 \in R \setminus \{0\}$ gibt es immer Elemente $q, r \in R$, sodass $p_1 = qp_2 + r$ und $r = 0$ oder $\delta(r) < \delta(p_2)$ gilt.

Wie schon gesagt ist das motivierende Beispiel $\mathbb{Z}$ mit $\delta(m) = |m|$, dem üblichen Absolutbetrag. Dann gilt (*i*) offensichtlich und für (*ii*) verwendet man die übliche Division mit Rest. Das zweite Beispiel von entscheidender Bedeutung ist:

Lemma 3.5. *Sei $\mathbb{K}$ ein Körper. Dann ist der Polynomring $\mathbb{K}[t]$ ein Euklidischer Ring, wobei man für $p \neq 0$ $\delta(p) := \deg(p)$ setzt.*

Beweis. Eigenschaft (*i*) gilt wegen $\deg(pq) = \deg(p) + \deg(q)$ und $\deg(q) \geq 0$. Für (*ii*) verwendet man die Polynomdivision, die ebenfalls bereits aus der Schule bekannt ist: Ist $\deg(p_2) = 0$, dann ist p_2 ein konstantes Polynom $\neq 0$, also $p_2 = b_0$. Dann können wir für beliebiges p_1 einfach $q = \frac{1}{b_0}p_1$ und $r = 0$ setzen. Nehmen wir als $\deg(p_2) = n > 0$ an und bezeichnen die Koeffizienten von p_2 mit b_i. Dann beweisen wir die Existenz von q und r durch Induktion nach $\deg(p_1)$. Ist $\deg(p_1) < n$, dann können wir $q = 0$, $r = p_1$ wählten. Nehmen wir also an, dass $\deg(p_1) = k \geq n$ gilt, und die Behauptung für Polynome vom Grad $< k$ bereits bewiesen ist. Sind a_i die Koeffizienten von p_1, dann können wir wegen $b_n \neq 0$ das Polynom $\tilde{p}_1 := p_1 + (\frac{-a_k}{b_n}t^{k-n})p_2$ bilden. Das zweite Polynom in dieser Summe hat Grad $(k-n)+n = k$ und der Koeffizient von t^k ist $\frac{-a_k}{b_n} \cdot b_n = -a_k$. Damit sehen wir aber, dass $\deg(\tilde{p}_1) \leq k$ gilt und der Koeffizient von t^k in $\tilde{p}_1$ ist $a_k - a_k = 0$, also ist $\deg(\tilde{p}_1) < k$. Damit gibt es nach Induktionsvoraussetzung Polynome $\tilde{q}, \tilde{r} \in \mathbb{K}[t]$, sodass $\tilde{p}_1 = \tilde{q}p_2 + \tilde{r}$ sowie $r = 0$ oder $\deg(r) < n$ gilt. Setzen wir

nun $q := \tilde{q} + \frac{a_k}{b_n} t^{k-n}$ und $r := \tilde{r}$. Dann ist

$$qp_2 + r = \tilde{q}p_2 + \tfrac{a_k}{b_n} t^{k-n} p_2 + \tilde{r} = \tilde{p}_1 + \tfrac{a_k}{b_n} t^{k-n} p_2 = p_1$$

und $r = 0$ oder $\deg(r) < n$. □

Das erste fundamentale Resultat über Euklidische Ringe ist der sogenannte *Hauptidealsatz*.

Proposition 3.5. *Sei (R, δ) ein Euklidischer Ring und $I \triangleleft R$ ein Ideal. Dann gibt es ein Element $a \in R$, sodass $I = aR$ gilt. Das Element a ist eindeutig bis auf Multiplikation mit einer Einheit, d.h. ist $\tilde{a} \in R$ so, dass $I = \tilde{a}R$ gilt, dann gibt es eine Einheit $e \in R$ mit $\tilde{a} = ea$.*

Beweis. Ist $I = \{0\}$, dann ist $I = 0 \cdot R$. Für $I \neq \{0\}$ gibt es Elemente $r \in I$ mit $r \neq 0$. Damit ist $\{\delta(r) : r \in I\}$ eine nichtleere Teilmenge von $\mathbb{N}$, also findet man ein Element $a \in I$ sodass $\delta(a)$ minimal ist. Da $a \in I$ gilt, ist $ar \in I$ für alle $r \in R$ und damit $aR \subset I$. Sei nun $b \in I$ beliebig. Da R Euklidisch ist, finden wir $q, r \in R$ mit $b = qa + r$ und $r = 0$ oder $\delta(r) < \delta(a)$. Wegen $b \in I$ ist auch $b - qa = r \in I$. Wäre $r \neq 0$, dann wäre $\delta(r) < \delta(a)$, ein Widerspruch zur Definition von a. Also muss $r = 0$ und damit $b = aq \in aR$ gelten.

Ist $\tilde{a}R = aR$, dann gibt es Elemente $r, s \in R$, sodass $\tilde{a} = ar$ und $a = \tilde{a}s$ und damit $a = ars$ gilt, und wir müssen nur zeigen, dass r eine Einheit ist. Nun ist aber $0 = a - ars = a(1 - rs)$. Nach Voraussetzung ist $a \neq 0$ und R nullteilerfrei, also $1 - rs = 0$, also $rs = 1$. □

Bemerkung 3.5. (1) Die "Eindeutigkeit bis auf Multiplikation mit Einheiten" wird uns noch öfters unterkommen. Im Allgemeinen kann man sie nicht vermeiden, aber in den beiden Hauptbeispielen von Euklidischen Ringen kann man ganz leicht damit umgehen. In $\mathbb{Z}$ sind die beiden Einheiten gerade ± 1, also erhalten wir gerade Eindeutigkeit bis auf das Vorzeichen. Die Elemente werden damit eindeutig, indem man zusätzlich verlangt, dass sie positiv sind.

Im Fall von $\mathbb{K}[t]$ sind die Einheiten genau die konstanten Polynome $\neq 0$. Hier kann man benutzen, dass ein Polynom $p \neq 0$ einen Grad $\deg(p) =: n$ hat und nach Definition der Koeffizient a_n, der sogenannte *Leitkoeffizient* ungleich Null ist. Durch Multiplikation mit $(a_n)^{-1}$ kann man erreichen, dass der Leitkoeffizient 1 ist und damit die Freiheit der Multiplikation mit einer Einheit eliminieren. Man nennt Polynome mit Leitkoeffizient 1 *monisch*.

(2) Mit diesem Satz haben wir das in 2.3 angekündigte konzeptuelle Verständnis der Beschreibung der Untergruppen von $(\mathbb{Z}, +)$ erreicht. Aus 2.13 wissen wir ja schon, dass jede solche Untergruppe ein Ideal im Ring $\mathbb{Z}$ sein muss. Nach dem Hauptidealsatz und (1) ist jedes solche Ideal von der Form $n\mathbb{Z}$ für eine Zahl $n \in \mathbb{N}$.

Wir können sofort eine schöne Anwendung der bisher entwickelten Ideen ableiten, nämlich die Existenz eines *Minimalpolynoms* für Elemente einer $\mathbb{K}$–Algebra.

Korollar 3.5. *Sei R eine $\mathbb{K}$–Algebra und sei $r \in R$ ein Element. Ist R nicht endlichdimensional als $\mathbb{K}$–Vektorraum, dann nehmen wir zusätzlich an, dass es ein Polynom $p \in \mathbb{K}[t]$ gibt, sodass $p(r) = 0$ gilt.*

Dann gibt es ein eindeutig bestimmtes, monisches Polynom $m \in \mathbb{K}[t]$ minimalen Grades, sodass $m(r) = 0$ gilt und ein Polynom $p \in \mathbb{K}[t]$ erfüllt genau dann $p(r) = 0$, wenn es von der Form mq für $q \in \mathbb{K}[t]$ ist.

BEWEIS. Aus Proposition 3.4 wissen wir, dass $\varphi(p) := p(r)$ einen Homomorphismus $\varphi : \mathbb{K}[t] \to R$ von $\mathbb{K}$–Algebren definiert, und nach Proposition 3.2 ist $\mathrm{Ker}(\varphi)$ ein Ideal in $\mathbb{K}[t]$. Hat R als $\mathbb{K}$–Vektorraum Dimension n, dann sind die $n+1$ Elemente $1, r, r^2, \ldots, r^n \in R$ auf jeden Fall linear abhängig, also gibt es $a_0, \ldots, a_n \in \mathbb{K}$, sodass $0 = a_0 1 + a_1 r + a_2 r^2 + \cdots + a_n r^n$ gilt. Das sagt aber gerade, dass das Polynom $p = \sum a_i t^i$ die Gleichung $p(r) = 0$ erfüllt. Somit sehen wir, dass $\mathrm{Ker}(\varphi) \neq \{0\}$ ist. Nach dem Hauptidealsatz und seinem Beweis ist $\mathrm{Ker}(\varphi) = qR$, wobei $q \in \mathrm{Ker}(\varphi)$ ein Polynom mit minimalem Grad ist. Insbesondere gibt es nach Bemerkung (1) von oben ein eindeutige monisches Polynom m mit dieser Eigenschaft. Nachdem $\mathrm{Ker}(\varphi) = \{p \in \mathbb{K}[t] : p(r) = 0\}$ folgen alle Behauptungen. □

Im Prinzip sollte dieses Resultat für den Spezialfall der Algebra $L(V, V)$ der linearen Abbildungen auf einem $\mathbb{K}$–Vektorraum V schon aus der linearen Algebra bekannt sein. Dort weiß man zusätzliche, dass nach dem Satz von Cayley–Hamilton das charakteristische Polynom p_f von f die Gleichung $p_f(f) = 0$ erfüllt und damit das Minimalpolynom ein Teiler des charakteristischen Polynoms sein muss.

3.6. Eindeutige Primfaktorzerlegung. Der Hauptidealsatz ist so nützlich, dass er einen eigenen Begriff motiviert. Man nennt einen Integritätsbereich R einen *Hauptidealbereich*, wenn jedes Ideal in R ein Hauptideal ist. Es gibt Beispiele (aber keine einfachen) von Hauptidealbereichen, die keine Euklidischen Ringe sind. Andererseits ist zum Beispiel leicht einzusehen, dass $\mathbb{Z}[t]$ kein Hauptidealbereich ist.

In einem Hauptidealbereich R machen nun einige der grundlegenden Begriffe aus der Zahlentheorie Sinn. Für $a, b \in R$ können wir die Hauptideale aR und bR betrachten. Nach Proposition 3.2 sind dann auch $(aR) \cap (bR)$ und $aR + bR$ Ideale in R. Nach Definition besteht $(aR) \cap (bR)$ aus allen Elementen, die sowohl als Vielfaches von a als auch als Vielfaches von b geschrieben werden kann. Da R ein Hauptidealbereich ist, gibt es ein Element $p := \mathrm{kgV}(a, b) \in R$, sodass $pR = (aR) \cap (bR)$ und das ist natürlich tatsächlich das kleinste gemeinsame Vielfache von a und b. Analog gibt es $q := \mathrm{ggT}(a, b) \in R$ sodass $qR = (aR + bR)$ und man überlegt leicht, dass q tatsächlich der größte gemeinsame Teiler von a und b ist. Die Elemente $\mathrm{kgV}(a, b)$ und $\mathrm{ggT}(a, b)$ sind jeweils bis auf Multiplikation mit Einheiten eindeutig bestimmt und für $\mathbb{Z}$ und $\mathbb{K}[t]$ macht man sie eindeutig indem man verlangt, dass sie positiv bzw. monisch sind.

Als nächsten Schritt in der Analogie zur Zahlentheorie definiert man Analoga von Primzahlen. Dazu nennt man für einen Ring R ein Element $p \in R$ *irreduzibel*, wenn p keine Einheit ist und für $a, b \in R$ mit $p = ab$ entweder a oder b eine Einheit in R sein muss. Man zeigt dann, dass es für jedes Element $r \in R$ eine eindeutige Zahl k, (bis auf die Reihenfolge und Multiplikation mit Einheiten) eindeutige irreduzible Elemente $p_1, \ldots, p_k \in R$ gibt, sodass $r = p_1 \cdots p_k$. Man hat also in jedem Hauptidealbereich eine *eindeutige Primfaktorzerlegung*. Wiederum ist dieses Resultat so wichtig, dass es einen eigenen Begriff motiviert. Man nennt einen Integritätsbereich einen *EZ–Bereich*, wenn es in ihm eine eindeutige Primfaktorzerlegung gibt. Eine der schönen Eigenschaften dieses Begriffs ist, dass für einen EZ–Bereich R auch der Polynomring $R[t]$ ein EZ–Bereich ist. Insbesondere gibt es also in $\mathbb{Z}[x]$ eine eindeutige Primfaktorzerlegung, obwohl $\mathbb{Z}[x]$ kein Hauptidealbereich ist.

Die eindeutige Primfaktorzerlegung in $\mathbb{K}[t]$ ist ein entscheidender Schritt zum Verständnis der linearen Abbildungen auf einem endlichdimensionalen $\mathbb{K}$–Vektorraum V. Dazu betrachtet man für eine lineare Abbildung $f : V \to V$ das Minimalpolynom m_f und zerlegt es in Primfaktoren $p_1^{a_1} \cdots p_k^{a_k}$ (wobei man Primfaktoren, die öfters auftreten, zusammenfasst). Dann kann man für $i = 1, \ldots, k$ natürlich die lineare Abbildung $p_i^{a_i}(f)$

auf V betrachten. Die Kerne dieser Abbildungen liefern die sogenannte Primärzerlegung von V. Für $\mathbb{K} = \mathbb{C}$ führt das dann zur Jordan'schen Normalform für lineare Abbildungen.

Körpererweiterungen

In diesem letzten Abschnitt wollen wir kurz beschreiben, wie man Körper (insbesondere $\mathbb{Q}$) vergrößern kann, indem man Nullstellen von Polynomen "dazu fügt". Damit kann man dann einem Polynom eine Gruppe zuordnen, was uns einen Bezug zurück zur Gruppentheorie liefert.

3.7. Nullstellen von Polynomen. Wir wissen schon, dass wir einem Polynom $p \in \mathbb{K}[t]$ mit Koeffizienten in einem Körper $\mathbb{K}$ eine Funktion $p : \mathbb{K} \to \mathbb{K}$ zuordnen können, indem wir für die Variable t Elemente von $\mathbb{K}$ einsetzen. Eine *Nullstelle* von P ist dann ein Element $\lambda \in \mathbb{K}$, sodass $p(\lambda) = 0$ gilt. Wir können nun Nullstellen schön mit der algebraischen Struktur auf $\mathbb{K}[t]$ in Verbindung bringen:

Proposition 3.7. *Sei $\mathbb{K}$ ein Körper und $p \in \mathbb{K}[t]$ ein Polynom. Dann ist $\lambda \in \mathbb{K}$ genau dann eine Nullstelle von p, wenn das Polynom $t - \lambda$ das Polynom p teilt, also wenn $p \in (t-\lambda)\mathbb{K}[t]$ gilt. Insbesondere hat ein Polynom vom Grad n höchsten n verschiedene Nullstellen in $\mathbb{K}$.*

Beweis. Nach Lemma 3.5 gibt es zu p und $t - \lambda$ eindeutige Polynome $q, r \in \mathbb{K}[t]$ sodass $p = (t - \lambda)q + r$ und $r = 0$ oder $\deg(r) < \deg(t - \lambda) = 1$ gilt. Somit ist aber r ein konstantes Polynom. Setzen wir λ ein, dann gilt nach Proposition 3.4

$$p(\lambda) = (t - \lambda)(\lambda) + r(\lambda) = 0 + r,$$

also $r = p(\lambda)$ und die erste Behauptung folgt.

Als nächsten Schritt behaupten wir, dass man für verschiedene Nullstellen $\lambda_1, \dots, \lambda_k$ von p, das Polynom p als $(t - \lambda_1) \cdots (t - \lambda_k)q$ für ein $q \in \mathbb{K}[t]$ schreiben kann. Daraus folgt natürlich die zweite Behauptung, weil $\deg(p) = k + \deg(q)$ und $\deg(q) \geq 0$ gilt. Aus dem ersten Schritt erhalten wir $p = (t-\lambda_1)q_1$. Setzen wir λ_2 ein, dann erhalten wir $0 = p(\lambda_2) = (\lambda_2 - \lambda_1)q_1(\lambda_2)$ und da der erste Faktor ungleich Null ist, muss $q_1(\lambda_2) = 0$ gelten. Nach dem ersten Schritt ist $q_1 = (t - \lambda_2)q_2$, also $p = (t - \lambda_1)(t - \lambda_2)q_2$ und die Behauptung folgt mit Induktion. □

Aus den Grundvorlesungen ist bereits eine Fülle von Resultaten über Polynome und ihre Nullstellen bekannt. Die Tatsache, dass $\sqrt{2}$ eine irrationale Zahl ist, kann man etwa so interpretieren, dass das Polynom $t^2 - 2 \in \mathbb{Z}[t] \subset \mathbb{Q}[t]$ keine Nullstellen im Körper $\mathbb{Q}$ der rationalen Zahlen hat. Daraus folgt sofort, dass $p = t^2 - 2 \in \mathbb{Q}[t]$ ein irreduzibles Polynom ist. Kann man nämlich $p = q\tilde{q}$ für $q, \tilde{q} \in \mathbb{Q}[t]$ schreiben, dann ist $\deg(q) + \deg(\tilde{q}) = \deg(p) = 2$. Wäre weder q noch $\tilde{q}$ eine Einheit, dann müsste $\deg(q) = \deg(\tilde{q}) = 1$ gelten. Schreibt man dann $q = a_1 t + a_0$, dann ist $a_1 \neq 0$ und $\frac{1}{a_1}q = t - \lambda$ für $\lambda = \frac{-a_0}{a_1}$ und $p = (\frac{1}{a_1}q)(a_1\tilde{q})$ und damit wäre λ eine Nullstelle von p. Analog sehen wir, dass ein Polynom $p \in \mathbb{K}[t]$ vom Grad 2 oder 3 genau dann irreduzibel ist, wenn p kein Nullstelle in $\mathbb{K}$ hat. Für Polynome höheren Grades ist die Situation komplizierter, aber da die Nullstellen eines Produkts von Polynomen immer Nullstellen eines Faktors sind, kann man sich bei der Betrachtung von Nullstellen meist auf den Fall irreduzibler Polynome beschränken.

Viele Polynome in $\mathbb{Q}[t]$ (oder sogar in $\mathbb{Z}[t]$) haben keine Nullstellen in $\mathbb{Q}$. In $\mathbb{R}$ ist die Situation wesentlich besser, aber etwa das Polynom $t^2 + 1 \in \mathbb{Z}[t]$ hat auch in $\mathbb{R}$ keine Nullstelle. Möchte man auch für dieses Polynom eine Nullstelle haben, dann muss

man zum Körper $\mathbb{C}$ der komplexen Zahlen übergehen. Der Fundamentalsatz der Algebra sagt dann, dass jedes Polynom in $\mathbb{C}[t]$ eine Nullstelle in $\mathbb{C}$ hat, woraus folgt, dass jedes Polynom über $\mathbb{C}$ in ein Produkt von Polynomen vom Grad 1 zerfällt. Insbesondere sind die irreduziblen Polynome in $\mathbb{C}[t]$ genau die Polynome vom Grad 1. Daraus kann man dann leicht ableiten, dass die irreduziblen Polynome in $\mathbb{R}[t]$ genau die Polynome vom Grad 1 sowie die Polynome vom Grad 2 ohne reelle Nullstellen sind.

Wie wir schon in 1.1 bemerkt haben, ist der Übergang von $\mathbb{Q}$ zu $\mathbb{R}$ nicht von algebraischer Natur und man gibt dabei zu $\mathbb{Q}$ viel mehr dazu als nur Nullstellen von Polynomen, nämlich transzendente Zahlen wie π oder e. Es stellt sich damit die Frage, ob es auch algebraische Konstruktionen gibt, um zu einem Körper Nullstellen von Polynomen "hinzuzufügen" (ohne etwa $\mathbb{C}$ als Hilfsmittel zu verwenden).

3.8. Körpererweiterungen. Um das "Vergrößern eines Körpers" formulieren zu können betrachten wir für einen gegeben Körper $\mathbb{K}$ eine sogenannte *Körpererweiterung* von $\mathbb{K}$, also einen Körper $\mathbb{L}$, der $\mathbb{K}$ als Teilkörper enthält. (Allgemeiner kann man auch verlangen, dass es einen Homomorphismus $\varphi : \mathbb{K} \to \mathbb{L}$ von Körpern mit $\varphi \neq 0$ gibt. Dann ist nämlich $\mathrm{Ker}(\varphi) \subset \mathbb{K}$ ein Ideal $\neq \mathbb{K}$ und aus Beispiel (3) von 3.2 sehen wir, dass daraus $\mathrm{Ker}(\varphi) = \{0\}$ folgt. Somit ist φ injektiv und man kann $\mathbb{K}$ mit dem Teilkörper $\varphi(\mathbb{K}) \cong \mathbb{K}$ identifizieren.)

Haben wir so eine Körpererweiterung $\mathbb{K} \subset \mathbb{L}$ gegeben, dann können wir die kommutative Gruppe $(\mathbb{L}, +)$ betrachten und die Multiplikation auf $\mathbb{L}$ zu einer Abbildung $\mathbb{K} \times \mathbb{L} \to \mathbb{L}$ einschränken. Aus den definierenden Eigenschaften eines Körpers folgt sofort, dass diese Operationen $\mathbb{L}$ zu einem $\mathbb{K}$–Vektorraum machen. Man spricht von einer *endlichen Erweiterung* wenn dieser Vektorraum endlichdimensional ist, dann heißt diese Dimension der *Grad der Körpererweiterung*.

Da $\mathbb{K} \subset \mathbb{L}$ gilt, kann man jedes Polynom $p \in \mathbb{K}[t]$ auch als Element des Polynomrings $\mathbb{L}[t]$ auffassen. Damit macht es Sinn zu fragen, ob ein Polynom p in $\mathbb{K}[t]$ eine Nullstellen in $\mathbb{L}$ besitzt.

Wir können nun relativ leicht für gegebenes $\mathbb{K}$ und $p \in \mathbb{K}[t]$ eine Körpererweiterung konstruieren, in der p mindestens eine Nullstelle hat. Dazu brauchen wir zunächst zwei kleine, allgemeine Resultate:

Lemma 3.8. *(1) Sei R ein Hauptidealbereich und $r \in R$ ein irreduzibles Element. Dann ist $I := rR \triangleleft R$ ein* maximales Ideal*, d.h. ist $J \triangleleft R$ ein Ideal mit $I \subset J$, dann ist $J = I$ oder $J = R$.*

(2) Sei R ein kommutativer Ring mit Einselement und $I \triangleleft R$ ein maximales Ideal. Dann ist der Quotientenring R/I ein Körper.

Beweis. (1) Sei $J \triangleleft R$ mit $I \subset J$ gegeben. Da R ein Hauptidealbereich ist, gibt es ein Element $a \in R$ mit $J = aR$ und wegen $r \in I \subset J$ finden wir ein Element $b \in R$ mit $r = ab$. Da r irreduzibel ist, muss entweder a oder b eine Einheit in R sein. Ist a eine Einheit, dann ist $1 = aa^{-1} \in aR$ und damit $s = s1 \in aR$ für alle $s \in R$, also $J = aR = R$. Ist b eine Einheit, dann ist $a = rb^{-1} \in rR = I$ und damit $J = aR \subset I$, also $J = I$.

(2) Offensichtlich ist R/I ein kommutativer Ring mit Einselement $\pi(1)$, wobei $\pi : R \to R/I$ der kanonische Quotientenhomomorphismus ist. Jedes Element $\neq 0$ in R/I kann als $\pi(a)$ für eine $a \in R \setminus I$ geschrieben werden. Ist nun a so ein Element, dann betrachten wir das zugehörige Hauptideal aR. Nach Proposition 3.2 ist $J := I + aR$ ein Ideal in R. Offensichtlich gilt $I \subset J$ und $a \in J$ aber $a \notin I$, also folgt aus der Maximalität von I, dass $J = R$ gilt. Das bedeutet aber, dass es Elemente $x \in I$ und $b \in R$ gibt,

sodass $1 = x + ab$ gilt. Damit ist aber

$$\pi(1) = \pi(x + ab) = \pi(x) + \pi(ab) = 0 + \pi(a)\pi(b),$$

also ist $\pi(b)$ ein multiplikativ inverses Element zu $\pi(a)$. □

Damit können wir nun unsere Körpererweiterung konstruieren, wobei wir uns der Einfachheit halber auf irreduzible Polynome beschränken.

Satz 3.8. *Sei $\mathbb{K}$ ein Körper und $p \in \mathbb{K}[t]$ ein irreduzibles Polynom vom Grad $n = \deg(p)$. Dann ist der Quotientenring $\mathbb{L} = \mathbb{K}[t]/p\mathbb{K}[t]$ eine Körpererweiterung von $\mathbb{K}$. Ist $\pi : \mathbb{K}[t] \to \mathbb{L}$ der kanonische Quotientenhomomorphismus, dann bilden die Elemente $\{\pi(1), \pi(t), \dots, \pi(t^{n-1})\}$ eine Basis für $\mathbb{L}$ über $\mathbb{K}$, also ist der Grad der Körpererweiterung $\deg(p)$. Außerdem ist $\pi(t) \in \mathbb{L}$ eine Nullstelle von p in $\mathbb{L}$.*

Beweis. Aus dem Lemma wissen wir, dass $\mathbb{L}$ ein Körper ist und natürlich können wir $\mathbb{K}$ als Teilkörper auffassen, indem wir $r \in \mathbb{K}$ als konstantes Polynom auffassen und dann $\pi(r) \in \mathbb{L}$ betrachten.

Ist $q = \sum_{j=0}^{N} b_j t^j \in \mathbb{K}[t]$, dann kann man das auch als Gleichung in $\mathbb{K}[t]$ auffassen, indem man die b_j als konstante Polynome und jedes t^j als Polynom betrachtet. Insbesondere ist daher $\pi(q) = \sum_{j=0}^{N} \pi(b_j)\pi(t^j)$. Schreiben wir $p = \sum_{i=0}^{n} a_i t^i$, dann ist $a_n \neq 0$. Dann ist $\frac{1}{a_n} p = t^n + \sum_{i=0}^{n-1} \frac{a_i}{a_n} t^i \in I$, also gilt $0 = \pi(t^n) + \sum_{i=0}^{n-1} \pi(\frac{a_i}{a_n})\pi(t^i)$. Das sagt aber gerade, dass man $\pi(t^n)$ als Linearkombination der $\pi(t^i)$ für $i = 0, \dots, n-1$ schreiben kann. Dann kann man $\pi(t^{n+1}) = \pi(t^n)\pi(t)$ als Linearkombination von $\pi(t)\pi(t^i) = \pi(t^{i+1})$ für $i = 0, \dots, n-1$ schreiben. Setzt man für $\pi(t^n)$ nochmals ein, dann sieht man, dass auch $\pi(t^{n+1})$ als Linearkombination der $\pi(t^i)$ für $i = 0, \dots, n-1$ schreiben kann. Induktiv folgt das analoge Resultat für $\pi(t^k)$ für alle $k \geq n$, also bildet die angegebene Menge ein Erzeugendensystem für den $\mathbb{K}$–Vektorraum $\mathbb{L}$.

Sind $r_0, \dots, r_{n-1} \in \mathbb{K}$ so, dass $0 = \sum_{i=0}^{n-1} r_i \pi(t^i)$ gilt, dann rechnen wir

$$0 = \sum_{i=0}^{n-1} r_i \pi(t^i) = \sum_{i=0}^{n-1} \pi(r_i t^i) = \pi(\sum_{i=0}^{n-1} r_i t^i),$$

also liegt das Polynom $\sum_{i=0}^{n-1} r_i t^i$, das höchstens Grad $n-1$ hat, in $\mathrm{Ker}(\pi) = p\mathbb{K}[t]$, kann also als pq für $q \in \mathbb{K}[t]$ geschrieben werden. Wäre $q \neq 0$, dann wäre $\deg(pq) = \deg(p) + \deg(q) \geq n$, ein Widerspruch. Damit gilt aber $0 = \sum_{i=0}^{n-1} r_i t^i$ und damit $r_i = 0$ für alle i. Damit ist die Menge $\{\pi(1), \pi(t), \dots, \pi(t^{n-1})\}$ linear unabhängig, also eine Basis für den $\mathbb{K}$–Vektorraum $\mathbb{L}$.

Da π ein Ringhomomorphismus ist, gilt schließlich $\pi(t)^i = \pi(t^i)$ für alle $i \in \mathbb{N}$. Bildet man $p(\lambda)$ für $\lambda := \pi(t) \in \mathbb{L}$, dann erhält man damit

$$p(\lambda) = \sum_{i=0}^{n} a_i \lambda^i = \sum_{i=0}^{n} a_i \pi(t^i) = \pi(\sum_{i=0}^{n} a_i t^i) = \pi(p) = 0.$$

□

Wendet man das auf $\mathbb{R}$ und das irreduzible Polynom $t^2 + 1$ an und setzt $\pi(t) =: i$, dann ist das genau die übliche Konstruktion von $\mathbb{C}$ aus $\mathbb{R}$.

Mit Satz 3.8 findet man also zu $p \in \mathbb{K}[t]$ eine Körpererweiterung $\mathbb{L} \supset \mathbb{K}$, in der p ein Nullstelle $\lambda \in \mathbb{L}$ hat. Nach Proposition 3.7 gibt es ein Polynom $q \in \mathbb{L}[t]$ sodass $p = (t - \lambda)q$ gilt. Hat q Nullstellen in $\mathbb{L}$, dann kann man weitere Polynome ersten Grades abspalten. Geht das nicht mehr, dann kann man die Konstruktion von Satz 3.8 auf das resultierende Polynom (bzw. einen Primfaktor davon) anwenden. Dieses

Polynom hat kleineren Grad als p. Damit muss man in endlich vielen Schritten zu einer Körpererweiterung gelangen, über der das Polynom p in ein Produkt von Polynomen ersten Grades zerfällt. Die minimale Körpererweiterung mit dieser Eigenschaft heißt der *Zerfällungskörper* $\mathbb{L}_p$ des Polynoms p.

Anfang des 19. Jahrhunderts hatte der französische Mathematiker E. Galois die Idee, einem Polynomen $p \in \mathbb{K}[t]$ eine Gruppe zuzuordnen. Die Idee war, geeignete Permutationen der Nullstellen von p (in einer Körpererweiterung) zu betrachten. Die moderne Formulierung dieser Theorie benutzt Körpererweiterungen. Zu so einer Erweiterung $\mathbb{L} \supset \mathbb{K}$ betrachtet man die Gruppe G aller Ringisomorphismen $\varphi : \mathbb{L} \to \mathbb{L}$, die $\varphi|_{\mathbb{K}} = \mathrm{id}_{\mathbb{K}}$ erfüllen. Da Kompositionen und inverse von Ringhomomorphismen wieder Ringhomomorphismen sind, bilden die Ringisomorphismen eine Untergruppe der Bijektionsgruppe $\mathrm{Bij}(\mathbb{L})$. Da auch die Bedingung $\varphi|_{\mathbb{K}} = \mathrm{id}_{\mathbb{K}}$ stabil unter Komposition und Inversion ist, erhalten wir so tatsächlich eine Untergruppe von $\mathrm{Bij}(\mathbb{L})$, die *Galoisgruppe* der Körpererweiterung. Betrachtet man den Zerfällungskörper $\mathbb{L}_p$ eines Polynoms $p \in \mathbb{K}[t]$, dann erhält man die Galoisgruppe von p. Es zeigt sich, dass für $\deg(p) = n$ die Galoisgruppe als Untergruppe von $\mathfrak{S}_n$ realisiert werden kann (das entspricht der Idee der Permutation der Nullstellen von oben) und insbesondere endlich ist.

Die aus der Schule bekannte Lösungsformel für quadratische Gleichungen zeigt, dass sich für Polynome zweiten Grades die Nullstellen immer durch Wurzeln ausdrücken kann. Um eine Nullstelle von $t^2 + at + b$ zu finden, braucht man nur eine Nullstelle von $t^2 = (\frac{a^2}{4} - b)$ (d.h. $\pm\sqrt{\frac{a^2}{4} - b}$) zu finden. Über die Galoisgruppen kann man nun die Frage beantworten, ob das analog auch für Polynome höheren Grades funktioniert. Dazu zeigt man zunächst, dass Erweiterungen um Wurzeln immer kommutative Galoisgruppen liefern. Dann zeigt man, dass beim schrittweisen Aufbau von Erweiterungen (unter gewissen Bedingungen) die Galoisgruppe schrittweise mit aufgebaut wird. Damit haben aber Körpererweiterungen, die schrittweise durch Hinzufügen von Wurzeln aufgebaut werden, immer Galoisgruppen, die im Sinn von 2.16 auflösbar sind. (Das ist der Ursprung des Namens "auflösbar".) Man kann sogar zeigen, dass die Auflösbarkeit der Galoisgruppe eines Polynoms p äquivalent dazu ist, dass die Nullstellen von p durch Wurzeln beschrieben werden können.

Nun können wir aber die Tatsachen über auflösbare Gruppen aus 2.16 verwenden. Dort haben wir gesehen, dass die Permutationsgruppe $\mathfrak{S}_n$ für $n \leq 4$ und damit auch jede ihrer Untergruppen auflösbar ist. Insbesondere lassen sich die Nullstellen von Polynomen bis zum Grad 4 immer in Termen von Wurzeln schreiben, und es gibt dafür sogar universelle Formeln (analog wie im quadratischen Fall). Ab $n = 5$ ist aber $\mathfrak{S}_n$ nicht auflösbar und $\mathfrak{A}_n$ sogar einfach. Es zeigt sich nun, dass für ganz einfache Polynome, etwa $t^5 - t - 1 \in \mathbb{Q}[t]$, als Galoisgruppe die volle Permutationsgruppe $\mathfrak{S}_5$ haben. Damit können schon für dieses einfach Polynom die Nullstellen nicht in Termen von Wurzeln geschrieben werden.

Eine weitere sehr schönen Anwendung von Körpererweiterungen betrifft die Frage der Konstruierbarkeit mit Zirkel und Lineal. Man kann offensichtlich mit Zirkel und Lineal aus einer Einheitsstrecke eine Strecke mit Länge $\sqrt{2}$ konstruieren, etwa als Länge der Diagonale eines Einheitsquadrats. Betrachtet man von $\mathbb{Q}$ ausgehend, die Längen aller Strecken, die Schritt für Schritt mit Zirkel und Lineal konstruiert werden können, dann bilden diese ein Körpererweiterung von $\mathbb{Q}$. Man kann nun zeigen, dass man diese Körpererweiterung schrittweise durch hinzufügen von Quadratwurzeln aufbauen kann. Damit kann man nun die Unlösbarkeit der klassischen Probleme über Konstruktionen mit Zirkel und Lineal (Quadratur des Kreises, Würfelverdopplung, Winkeldreiteilung und Konstruktion des regelmäßigen n–Ecks) beweisen. Dazu muss man im wesentlichen

nur zeigen, dass so eine Körpererweiterung keine irrationalen Zahlen (wie die Seitenlänge $\sqrt{\pi}$ des zum Einheitskreis flächengleichen Quadrats) und keine dritten Wurzeln (wie die Seitenlänge $2^{1/3}$ des Würfels mit Volumen 2) enthalten kann. Für die Winkeldreiteilung kann man leicht zeigen, dass die Zahl $u = \cos(20°)$ Nullstelle eines Polynoms dritten Grades ist, das im Körper der konstruierbaren Zahlen keine Nullstelle haben kann. Das zeigt dann etwa auch, dass das regelmäßige 9–Eck nicht mit Zirkel und Lineal konstruiert werden kann.