KAPITEL 1

Der Polynomring $K[X]$

Wir beginnen mit etwas Allgemeinbildung, dem Polynomring über einem Körper. Später betrachten wir gewissen Polynome, das charakteristische Polynom einer linearen Abbildung oder Matrix beziehungsweise das Minimalpolynom einer linearen Abbildung oder Matrix. Diese wollen wir faktorisieren, um Nullstellen zu bestimmen. In diesem Kapitel wollen wir verstehen, dass das Faktorisieren von Polynomen in einem Polynomring über einem Körper eindeutig ist, sich also die Nullstellen eines Polynoms auf diese Art und Weise eindeutig bestimmen lassen. Sei K ein Körper, seien R und S kommutative Ringe mit Einselement 1.

DEFINITION 1.1. Ein *Ringhomomorphismus*, kurz *Homomorphismus*, zwischen Ringen R und S ist eine Abbildung $\varphi : R \to S$ mit

(R1) $\varphi(1_R) = 1_S$
(R2) $\varphi(a+b) = \varphi(a) + \varphi(b)$
(R3) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

für alle $a, b \in R$. Abbildung φ heißt *Isomorphismus*, falls φ zusätzlich bijektiv ist. Zwei Ringe R und S heißen *isomorph*, geschrieben $R \simeq S$, falls es einen Isomorphismus $\varphi : R \to S$ gibt.

BEISPIEL 1.2.

(a) Sei $n \in \mathbb{N}$. Dann ist $\mathbb{Z} \to \mathbb{Z}_n, a \mapsto a + n\mathbb{Z}$ ein Ringhomomorphismus. Das Einselement von $\mathbb{Z}$ ist 1. Das Einselement von $\mathbb{Z}_n$ ist $1 + n\mathbb{Z}$. Es gilt $\varphi(1) = 1 + n\mathbb{Z}$, also gilt $(R1)$. Weiterhin gelten $(R2)$ und $(R3)$: Für alle $a, b \in R$ gilt:

$$\varphi(a+b) = (a+b) + n\mathbb{Z} = (a + \mathbb{Z}) + (b + n\mathbb{Z}) = \varphi(a) + \varphi(b);$$

und genauso gilt:

$$\varphi(a \cdot b) = (a \cdot b) + n\mathbb{Z} = (a + \mathbb{Z}) \cdot (b + n\mathbb{Z}) = \varphi(a) \cdot \varphi(b).$$

Also ist φ Ringhomomorphismus. Es ist $\varphi(n+1) = n + 1 + n\mathbb{Z} = 1 + n\mathbb{Z} = \varphi(1)$, also ist φ nicht injektiv. Die Abbildung φ ist aber surjektiv: Zu $a + n\mathbb{Z}$ mit $a \in \mathbb{Z}$ gilt $\varphi(a) = a + n\mathbb{Z}$.

(b) Inklusion von Ringen ist ein Ringhomomorphismus, zB. $\mathbb{Z} \overset{\varphi}{\hookrightarrow} \mathbb{Q}, a \mapsto a$ ist Ringhomomorphismus. Die Inklusion ist injektiv.

(c) Ist die Abbildung $\varphi : \mathbb{R} \times \mathbb{R} \to \mathbb{C}, (x, y) \mapsto x + yi$ ein Ringisomorphismus? Nein, das Einselement in $\mathbb{R} \times \mathbb{R}$ ist $(1, 1)$ und das in $\mathbb{C}$ ist 1. Hier gilt aber $\varphi(1, 1) = 1 + i \neq 1$. Also ist φ kein Ringhomomorphismus, und damit kein Ringisomorphismus.

(d) Sei $\varphi : R \to S$ ein Ringisomorphimus. Dann ist φ bijektiv, also existiert eine Abbildung $\varphi^{-1} : S \to R$, (die natürlich auch bijektiv ist, nach Lineare Algebra I). Die Abbildung φ^{-1} ist ein Homomorphismus: Seien $a, b \in S$. Dann ist

$$\begin{aligned}
\varphi^{-1}(a+b) &= \varphi^{-1}\left(\varphi(\varphi^{-1}(a)) + \varphi(\varphi^{-1}(b))\right) \\
&= \varphi^{-1}\left(\varphi(\varphi^{-1}(a) + \varphi^{-1}(b))\right), \text{ da } \varphi \text{ Homomorphismus ist,} \\
&= (\varphi^{-1} \circ \varphi)(\varphi^{-1}(a) + \varphi^{-1}(b)) \\
&= \varphi^{-1}(a) + \varphi^{-1}(b),
\end{aligned}$$

da $\varphi^{-1} \circ \varphi = \mathrm{id}_R$ ist; analog gilt $\varphi^{-1}(a \cdot b) = \varphi^{-1}(a) \cdot \varphi^{-1}(b)$. Damit ist die inverse Abbildung eines Ringisomorphismus wieder ein Ringisomorphismus.

BEMERKUNG 1.3. Ein Element $a \in R$ heißt *invertierbar* oder *Einheit in R*, falls es $b \in R$ gibt mit $ab = 1 = ba$. Definiere $R^\times = \{r \in R \mid r \text{ invertierbar }\}$. Dann ist $(R^\times, \cdot)$ eine Gruppe, die Einheitengruppe von *Ring R*. Siehe Lineare Algebra I.

BEISPIEL 1.4. Es ist $\mathbb{Z}^\times = \{+1, -1\}$, oder $\mathbb{R}^\times = \mathbb{R}\backslash\{0\}$. Allgemeiner gilt für einen Körper K, dass $K^\times = K\backslash\{0\}$ ist, da nach Definition jedes Element ungleich Null invertierbar ist bezüglich der Multiplikation. Im Restklassenring $\mathbb{Z}_n$ haben wir die Einheiten bereits in Lineare Algebra I charakterisiert. Es ist $\bar{a} \in \mathbb{Z}_n^\times$ genau dann, wenn $\mathrm{ggt}(a, n) = 1$ ist. Beispielsweise ist also $\mathbb{Z}_{15}^\times = \{\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \bar{11}, \bar{13}, \bar{14}\}$.

Aus der Schule und aus Analysis kennen wir Polynomfunktionen vom Typ $\mathbb{R} \to \mathbb{R}$ oder $\mathbb{C} \to \mathbb{C}$. Wir lassen auch andere Grundkörper zu:

DEFINITION 1.5. Sei R ein Ring oder Körper. Der Polynomring $R[X]$ in einer Variablen X besteht aus formalen Summen $p := \sum_{i=0}^{n} a_i X^i$, mit $n \in \mathbb{N}_0$ und $a_i \in R$, für $0 \le i \le n$. Wir nennen p ein *Polynom* und schreiben $p = \sum_{i \ge 0} a_i X^i$ mit $a_i = 0$ für $i \ge n + 1$. Definiere Addition und Multiplikation von Polynomen durch:

$$\sum_{i \ge 0} a_i X^i + \sum_{i \ge 0} b_i X^i := \sum_{i \ge 0} (a_i + b_i) X^i$$

und

$$\Big(\sum_{i \ge 0} a_i X^i\Big) \cdot \Big(\sum_{i \ge 0} b_i X^i\Big) = \sum_{i \ge 0} c_i X^i$$

mit

$$c_i := \sum_{t=0}^{i} a_t b_{i-t} = \sum_{s+t=i} a_s b_t,$$

beispielsweise $p = (X^3 - 2X)(X^2 + 1) = X^5 + X^3 - 2X^3 - 2X = X^5 - X^3 - 2X$, wie wir das aus der Schule gewohnt sind.

BEMERKUNG 1.6.

(a) Die Ringaxiome von R implizieren die Ringaxiome von $R[X]$, beispielsweise:

(i) das Kommutativgesetz für die Addition gilt, denn:

$$\begin{aligned} \sum_{i \ge 0} a_i X^i + \sum b_i X^i &= \sum_{i \ge 0} (a_i + b_i) X^i \\ &= \sum_{i \ge 0} (b_i + a_i) X^i, \text{ da Addition in } R \text{ kommutativ,} \\ &= \sum_{i \ge 0} b_i X^i + \sum_{i \ge 0} a_i X^i; \end{aligned}$$

(ii) das Assoziativgesetz für die Multiplikation gilt: Seien $f = \sum a_i X^i$ und $g = \sum b_i X^i$ und $h = \sum d_i X^i$ in $R[X]$. Dann ist der Koeffizient des i-ten Summanden von $(f \cdot g) \cdot h$ gegeben durch:

$$\begin{aligned} \sum_{p=0}^{i} c_p d_{i-p} &\overset{Def \text{ von } c_p \text{ wie in 1.5}}{=} \sum_{p=0}^{i} \Big(\sum_{q=0}^{p} a_q b_{p-q}\Big) d_{i-p} \\ &= \sum_{p=0}^{i} \sum_{q=0}^{p} a_q b_{p-q} d_{i-p} \qquad (1) \\ &= \sum_{r+s+t=i} a_r b_s d_t \qquad (2) \end{aligned}$$

und dies entspricht auch dem Koeffizienten des i-ten Summanden von $f(g \cdot h)$. Bei (1) benutzen wir das Assoziativgesetz für die Multiplikation in R sowie das Distributivgesetz in R; bei (2) benutzen wir das Assoziativgesetz und das Kommutativgesetz für die Addition in R.

Die anderen Ringaxiome prüft man ganz analog.

(b) Formal gesehen sind Polynome Folgen $(a_i)_{i \in \mathbb{N}_0}$ mit $a_i \in R$, wobei nur endlich viele a_i ungleich Null sind. Setze $X := (0, 1, 0, 0, \dots)$. Dann folgt mit obiger Multiplikationsformel

$$X^2 = X \cdot X = (0, 1, 0, 0, \dots) \cdot (0, 1, 0, 0, \dots) = (0, 0, 1, 0, \dots), \text{ etc.}$$

Induktiv ist also $X^j = (b_i)$ mit

$$b_i = \begin{cases} 1 \text{ für } i = j \\ 0 \text{ für } i \neq j \end{cases} .$$

Für $a \in R$, definiere $a \cdot (b_i) := (a \cdot b_i)$. Dann entspricht die Folge (a_i) genau der formalen Summe $\sum\limits_{i \geq 0} a_i X^i$ aus Definition 1.5.

(c) Sei $n \geq 2$. Definiere induktiv $R[X_1, \dots, X_n] := R[X_1, \dots, X_{n-1}][X_n]$, den Polynomring über R in n Unbestimmten $X_1, X_2, \dots, X_n$.

Einfachheitshalber spezialisieren wir und arbeiten ab jetzt mit $R = K$ Körper.

Bemerkung 1.7. Der Polynomring $K[X]$ ist auch ein K-Vektorraum. Eine Basis von $K[X]$ ist durch die Potenzen von X gegeben: $1, X, X^2, \dots$. Nach Bemerkung 1.6 (b) ist $K[X]$ auch ein Untervektorraum des K-Vektorraumes der Folgen.

Definition 1.8. Wir definieren die Auswertungsabbildung für $x \in K$ als die Abbildung $F_x : K[X] \longrightarrow K$, gegeben durch $p = \sum\limits_{i \geq 0} a_i X^i \mapsto \sum\limits_{i \geq 0} a_i x^i$.

Beachten Sie die Notation: X Großbuchstabe bedeutet X ist Variable; x Kleinbuchstabe bedeutet x ist Element aus Körper K.

Proposition 1.9. *Sei K ein Körper und $x \in K$. Die Auswertungsabbildung für $x \in K$ ist ein Ringhomomorphismus.*

Beweis. Es ist $F_x(1_{K[X]}) = 1_K$, damit gilt also (R1). Seien $f, g \in K[X]$ mit $f = \sum a_i X^i$ und $g = \sum b_i X^i$. Dann folgt:

$$\begin{aligned} F_x(f+g) &= F_x(\sum (a_i + b_i) X^i) = \sum (a_i + b_i) x^i = \sum a_i x^i + \sum b_i x^i = F_x(f) + F_x(g), \\ F_x(f \cdot g) &= F_x(\sum_i (\sum_{t=0}^{i} a_t b_{i-t}) X^i) = (\sum_i (\sum_{t=0}^{i} a_t b_{i-t}) x^i) = (\sum_i a_i x^i)(\sum_j b_j x^j) = F_x(f) \cdot F_x(g). \end{aligned}$$

Also gelten (R2) und (R3).

Bemerkung 1.10. (Polynom versus Polynomfunktion)

(a) Die Menge $\mathrm{Abb}(K, K) = \{f : K \to K\}$ aller Abbildungen von K nach K ist ein K-Vektorraum und trägt auch die Struktur eines Ringes. Die Operation Addition, Skalarmultiplikation bzw. Multiplikation (im Ring) sind gegeben durch

$$\begin{aligned} (f+g)(x) &:= f(x) + g(x) \\ (\lambda f)(x) &:= \lambda \cdot f(x) \\ (f \cdot g)(x) &:= f(x) \cdot g(x), \end{aligned}$$

für alle $f, g \in \mathrm{Abb}\,(K, K)$ und $\lambda \in K$.

(b) (i) Wir unterscheiden zwischen Polynomen und ihren zugehörigen Polynomfunktionen: Jedes Polynom $p = \sum a_i X^i \in K[X]$ definiert eine *Polynomfunktion* f_p durch $f_p : K \longrightarrow K, x \mapsto \sum a_i x^i =: f_p(x)$. Statt $f_p(x)$ schreiben wir üblicherweise $p(x)$.

(ii) Die resultierende Abbildung $f : K[X] \to \mathrm{Abb}(K,K), p \mapsto f_p$ die einem Polynom p die zugehörige Polynomfunktion f_p zuordnet ist ein Ringhomomorphismus, sowie eine K-lineare Abbildung (dh. ein Vektorraumhomomorphismus). Das Bild von f, also $\mathrm{im}(f)$, entspricht dem Unterraum der Polynomfunktionen im Vektorraum $\mathrm{Abb}(K,K)$. Abbildung f ist im Allgemeinen also nicht surjektiv.

(c) Ein Ring R, der gleichzeitig ein K-Vektorraum ist, so daß Skalare mit allem kommutieren, nennt man eine *K-Algebra*. Sowohl $K[X]$ als auch $\mathrm{Abb}(K,K)$ sind Beispiele von K-Algebren. Die in (b) erwähnte Abbildung ist ein K-Algebrenhomomorphismus.

(d) Aus der formalen Definition von Polynomen in Definition1.6 (b) folgt: zwei Polynome $p = \sum a_i X^i$ und $q = \sum b_i X^i$ sind gleich, genau dann, wenn $a_i = b_i$ für alle i. Insbesondere sind dann auch die zugehörigen Polynomfunktionen f_p und f_q gleich. Die Umkehrung gilt im Allgemeinen nicht: Sei zum Beispiel $K = \mathbb{Z}_2$, sei p das Nullpolynom und sei $q = X^2 + X$ in $\mathbb{Z}_2[X]$. Dann ist $p \neq q$ als Polynom. Die zugehörigen Polynomfunktionen sind aber gleich: $f_p = f_q$, denn $q(0) = 0$, $q(1) = 0$. Insbesondere ist der Homomorphismus f aus (b) nicht notwendigerweise injektiv.

LEMMA 1.11. *Sei $a, b \in K\backslash\{0\}$. Dann ist $ab \neq 0$.*

BEWEIS. Angenommen $a \cdot b = 0$ mit $a \neq 0$. Dann existiert $a^{-1} \in K$, und es folgt: $0 = a^{-1} \cdot 0 = a^{-1}(ab) = (a^{-1}a) \cdot b = 1 \cdot b = b$.

BEMERKUNG/BEISPIEL 1.12. Sei R kommutativer Ring mit 1.

(a) Ein Element $a \in R$ heißt *Nullteiler*, falls $a \neq 0$ und es existiert $b \in R\backslash\{0\}$ mit $ab = 0$ (oder $ba = 0$). Beispielsweise: $\bar{2}, \bar{3}$ sind Nullteiler in $\mathbb{Z}_6$, denn $\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$. Ein kommutativer Ring mit 1 ohne Nullteiler ist ein *Integritätsbereich* (kurz IB).

(b) (i) Lemma 1.11 besagt, daß jeder Körper ein Integritätsbereich ist.

(ii) Sei $a \in R^\times$ eine Einheit. Dann ist a kein Nullteiler. Der Beweis hierzu ist wie der Beweis zu Lemma 1.11.

(iii) Der Ring $M_n(K)$ hat viele Nullteiler, beispielsweise ist $E_{ij} \cdot E_{kl} = 0$ für $j \neq k$.

(iv) Seien R, S Ringe. Dann ist $R \times S = \{(r,s) \mid r \in R, s \in S\}$ ein Ring mit komponentenweise Addition und Multiplikation $(r,s) \dot{+} (a,b) := (r + a, s \dot{+} b)$ für alle $r, a \in R$ und $s, b \in S$. Dieser Ring $R \times S$ hat Nullteiler; beispielsweise alle Elemente $(a,0)$ oder $(0,b)$ sind Nullteiler.

(v) Sei $n \geq 2$ und $R = \mathbb{Z}_n$. Dann ist $a + n\mathbb{Z} \neq 0 + n\mathbb{Z}$ ein Nullteiler genau dann, wenn $ggt(a,n) > 1$.

DEFINITION 1.13. Der *Grad* eines Polynoms $p = \sum a_i X^i \in K[X]$ ist definiert als

$$deg(p) := \begin{cases} max\{i \mid a_i \neq 0\} \text{ falls } p \neq 0, \\ -\infty \text{ falls } p = 0. \end{cases}$$

Ist $d := deg(p) \neq -\infty$, so heißt der Koeffizient a_d auch *Leitkoeffizient* von p, der Summand $a_d X^d$ heißt *Leitsummand*. Polynom p heißt *normiert*, falls der Leitkoeffizient Eins ist.

BEISPIEL 1.14.

(a) Es gilt $deg(X - a) = 1$, für alle $a \in K$, oder $deg(2X^3 - 7X + 5) = 3$; Polynom $p \in K[X]$ ist konstant $\Leftrightarrow deg\ p < 1$.

(b) Definiere $p = 2X + 1, q = 3X^2$. Dann ist $p \cdot q = 6X^3 + 3X^2$. In $\mathbb{R}[X]$ ist $deg(p \cdot q) = 3$. In $\mathbb{Z}_6[X]$ ist $deg(p \cdot q) = 2$, da hier gilt $p \cdot q = 3X^2$.

PROPOSITION 1.15 (Gradformel). *Für alle $p, q \in K[X]$ gilt:*

(a) $deg(p \cdot q) = deg(p) + deg(q)$,
(b) $deg(p+q) \leq max\{deg\ p, deg\ q\}$, *und hierbei gilt Gleichheit, falls $deg\ p \neq deg\ q$ ist.*

BEWEIS.

(a) Sei $p = 0$ oder $q = 0$. Dann ist $deg(p \cdot q) = deg(0) = -\infty = deg(p) + deg(q)$. Sei also $p \neq 0$ und $q \neq 0$ mit $p = \sum_{i=0}^{n} a_i X^i$, $q = \sum_{i=0}^{m} b_i X^i$ mit $a_n \neq 0, b_m \neq 0$, also $deg\ p = n, deg\ q = m$. Sei $p \cdot q = (\sum a_i X^i)(\sum b_i X^i) =: \sum c_k X^k$. Dann ist $c_k = 0$ für alle $k > n+m$. Der Koeffizient $c_{n+m} = a_n \cdot b_m \neq 0$ nach Lemma 1.11. Also ist $deg(p \cdot q) = n + m = deg(p) + deg(q)$.
(b) Übung.

ÜBUNG. Zeigen Sie $K[X]^\times = K^\times = K \backslash \{0\}$, wobei Elemente aus K hierbei mit der entsprechenden konstanten Funktion identifiziert werden.

KOROLLAR 1.16. *Seien $p, q, r \in K[X]$.*

(a) *Ist $pq = 0$, so ist $p = 0$ oder $q = 0$, dh. $K[X]$ ist Nullteiler-frei, dh. $K[X]$ ist Integritätsbereich.*
(b) *Ist $pq = pr$ und $p \neq 0$, so ist $q = r$, das heisst die Küerzungsregel gilt.*

BEWEIS.

(a) Ist $p \neq 0, q \neq 0$, so ist $deg(p \cdot q) \overset{1.15}{=} deg\, p + deg\, q \geq 0$. Also ist $pq \neq 0$.
(b) Ist $pq = pr$ mit $p \neq 0$, so ist $p(q - r) = 0$. Da $p \neq 0$ nach Voraussetzung, folgt aus (a), dass $q - r = 0$ ist, also $q = r$.

THEOREM 1.17. *(Division mit Rest für Polynome) Sei K ein Körper. Im Polynomring $K[X]$ gilt Division mit Rest bezüglich der Gradfunktion: Zu $f, g \in K[X], g \neq 0$, existierten $q, r \in K[X]$ mit $f = q \cdot g + r$ mit $deg(r) < deg(g)$. Die Polynome q, r sind hierbei eindeutig durch f und g bestimmt.*

BEWEIS.

(a) *Existenz*: Wir machen Induktion nach $deg(f) =: n$. Ist $deg(f) < deg(g)$, wähle $q = 0$ und $r = f$, und die Behauptung folgt. Sei nun $deg(f) \geq deg(g)$. Sei

$$f = \sum_{i=0}^{n} a_i x^i$$
$$g = \sum_{j=0}^{m} b_j x^j$$

Sei $f_1 := f - a_n b_m^{-1} X^{n-m} g$ Dann ist $deg(f_1) < deg(f)$. Nach Induktionsvoraussetzung existieren also $q_1, r_1 \in K[X]$ mit $f_1 = q_1 g + r_1$ und $deg(r_1) < deg(g) = m$. Es folgt:

$$\begin{aligned} f &= f_1 + a_n b_m^{-1} X^{n-m} g = (q_1 \cdot g + r_1) + a_n b_m^{-1} X^{n-m} g \\ &= \underbrace{\left(q_1 + a_n b_m^{-1} X^{n-m}\right)}_{=:q} g + r_1 \end{aligned}$$

mit $deg(r_1) < m = deg(g)$.

(b) *Eindeutigkeit*: Angenommen $q \cdot g + r = \tilde{q} \cdot g + \tilde{r}$ mit $deg(r)$, $deg(\tilde{r}) < m = deg(g)$. Dann ist $(q - \tilde{q})g = \tilde{r} - r$, und mit Proposition 1.15 gilt

$$m = deg(g) > deg(r - \tilde{r}) = deg((q - \tilde{q}) \cdot g) = deg(q - \tilde{q}) + \underbrace{deg(g)}_{=m}.$$

Also ist $deg(q - \tilde{q}) < 0$, dh. $q - \tilde{q} = 0$, also $q = \tilde{q}$. Einsetzen ergibt auch $r = \tilde{r}$.

Bemerkung: Der Beweis von Theorem 1.17 liefert einen Algorithmus zur Bestimmung von q und r: Solange $deg(f) \geq deg(g)$ ist:

- *Bestimme $c_{n-m} := a_n b_m^{-1}$ aus Leitkoeffizient a_n bzw. b_m von f bzw. g, und notiere den Summanden $c_{n-m}X^{n-m}$.*
- *Starte erneut mit f_1 als f wobei $f_1 = f - c_{n-m}X^{n-m}g$.*

Wenn $deg(f) < deg(g)$ ist:

- *Dann ist $r = f$ und q die Summe der notierten Summanden.*

Der Algorithmus endet dann.

Beispiel 1.18. Der Algorithmus für $f = 2X^4 + 1, g = X^2 + 1$ liefert:

(a) Sei $f = 2X^4 + 1, g = X^2 + 1$. Dann ist
- $c_{4-2} = c_2 = 2 \cdot 1^{-1} = 2$. Notiere $2X^2$.
- $f_1 = f - c_2X^2g = 2X^4 + 1 - 2(X^4 + X^2) = -2X^2 + 1$.

(b) Sei $f = -2X^2 + 1, g = X^2 + 1$. Es ist
- $c_{2-2} = c_0 = -2$. Notiere $-2X^0 = -2$.
- $f_1 = f - c_0X^0g = -2X^2 + 1 + 2(X^2 + 1) = 3$.

(c) Sei $f = 3, g = X^2 + 1$. Es ist $deg\, f < deg\, g$. Dann ist $r = 3$ und $q = 2X^2 - 2$.
Also $f = 2X^4 + 1 = (2X^2 - 2) \cdot g + 3$.

Die Kurznotation für diesen Algorithmus in der Schule ist
$2X^4 + 1 = (X^2 + 1)(2X^2 - 2X^0) + 3$
$\frac{-(2X^4+2X^2)}{-2X^2+1}$
$\frac{-(2X^2-2)}{3}$

Übung. Bestimmen Sie $q, r \in \mathbb{Z}_3[X]$ mit $X^5 + X^4 + X^3 + 2X^2 + X - 1 = (2X^2 + 1)q + r$.

Für die Anwendungen von Polynomen in Lineare Algebra müssen wir Nullstellen von Polynomen verstehen.

Definition 1.19. Eine Nullstelle (kurz NS) von $p \in K[X]$ ist ein Element $a \in K$ mit $p(a) = 0$.

Beispiel 1.20.

(a) Sei $p = X^2 + 1$. Für alle $a \in \mathbb{R}$ gilt $a^2 + 1 > 0$. Also hat p keine Nullstelle als Polynom in $\mathbb{R}[X]$. Als Polynom in $\mathbb{C}[X]$ gilt $p = (X + i)(X - i)$. Damit sind i und $-i$ jeweils Nullstelle von $p \in \mathbb{C}[X]$. Sei $z \in \mathbb{C}\backslash\{\pm i\}$. Dann ist $z + i \neq 0$, $z - i \neq 0$. Nach Lemma 1.11 ist damit $p(z) = (z + i)(z - i) \neq 0$. Also sind $\pm i$ die einzigen Nullstellen von $p \in \mathbb{C}[X]$.

(b) Sei $f = X^2 - 7X + 12$. In $\mathbb{R}[X]$ faktorisiert das Polynom f durch: $f = (X - 4)(X - 3)$. Analog wie in (a) folgt: Polynom $f \in \mathbb{R}[X]$ hat die Nullstelle: $a_1 = 4$ $a_2 = 3$.

(c) Sei $h = X^4 - 7X^2 + 12$. In $\mathbb{R}[X]$ hat h die Nullstelle: $2, -2, \sqrt{3}$ und $-\sqrt{3}$. Es gibt also vier verschiedene Nullstellen. In $\mathbb{Q}[X]$ hat h genau zwei Nullstellen, nämlich $2, -2$.

Proposition 1.21. *Sei K Körper und $p \in K[X]$. Es sind äquivalent:*

(a) *Element $a \in K$ ist Nullstelle von p, also $p(a) = 0$.*
(b) *$X - a$ ist ein Faktor von p, das heisst, es existiert $q \in K[X]$ mit $p = (X - a) \cdot q$.*

Beweis. "$(b) \Rightarrow (a)$": Sei $X-a$ ein Faktor von p. Dann existiert also $q \in K[X]$ mit $p = (X-a)\cdot q$. Einsetzen von a liefert: $p(a) = ((X - a) \cdot q)(a) = (a - a)q(a) = 0 \cdot q(a) = 0$.
"$(a) \Rightarrow (b)$": Sei $a \in K$ Nullstelle von $p \in K[X]$. Nach Theorem 1.17 existiert $q, r \in K[X]$ mit $p = (X - a) \cdot q + r$, wobei $deg(r) < deg(X - a) = 1$ ist. Also ist r ein konstantes Polynom mit

$$r(a) = (p - (X - a) \cdot q)(a) = p(a) - \underbrace{(a - a)}_{=0} \cdot q(a) = p(a) \overset{Vor.}{=} 0.$$

Also ist $p = (X - a) \cdot q$.

Beispiel 1.22. Sei $g = X^3 - 6X^2 + 5X + 12 \in \mathbb{R}[X]$. Durch Raten/Einsetzen kleiner Werte findet man die Nullstelle $a_1 = 3$ Polynomdivision liefert $X^3 - 6X^2 + 5X + 12 = (X-3)\cdot(X^2 - 3X - 4) = (X-3)(X+1)(X-4)$. Also hat g die drei Nullstellen: $-1, 3, 4$.

Theorem 1.23. *Sei $0 \neq p \in K[X]$. Dann gilt*

(a) *Das Polynom p hat eine Darstellung*

$$p = (X - a_1)^{n_1} \cdot \ldots \cdot (X - a_r)^{n_r} \cdot q \tag{3}$$

mit $r \in \mathbb{N}_0$ und paarweise verschiedenen $a_1, \ldots, a_r \in K$, sowie Exponenten $n_1, \ldots, n_r \in \mathbb{N}$ und einem Polynom $q \in K[X]$ ohne Nullstelle in K.

(b) *Die Nullstellen von p sind genau $a_1, \ldots, a_r$.*

(c) *Darstellung (3) von p ist eindeutig bis auf Permutation der Faktoren.*

Bemerkung: Wir nennen den Exponenten n_i die Vielfachheit der Nullstelle a_i.

Beweis.

(a) Wir machen Induktion nach $deg(p)$

(i) Hat p keine Nullstelle, so ist $r = 0$ und $q = p$. Dies gilt zum Beispiel für Polynome vom Grad Null, und liefert damit den Induktionsanfang.

(ii) Wir nehmen an, die Behauptung gilt für Polynome vom Grad $< deg(p)$ und p habe eine Nullstelle $a \in K$. Nach Proposition 1.21 existiert $\tilde{p} \in K[X]$ mit $p = (X-a)\tilde{p}$. Nach Proposition 1.15 folgt:

$$\begin{aligned} deg(\tilde{p}) &= deg(p) - deg(X - a) \\ &= deg(p) - 1 \underset{\neq}{<} deg(p). \end{aligned}$$

Nach Induktion Voraussetzung hat dann $\tilde{p}$ eine Darstellung wie in (3). Die Darstellung von p ergibt sich hieraus durch Multiplikation mit $(X - a)$.

(b) Sei $b \in K$ mit $p(b) = 0$. So folgt: $0 = p(b) \overset{(3)}{=} (b-a_1)^{n_1} \cdot \ldots \cdot (b-a_r)^{n_r} q(b)$. Nach Lemma 1.11 ist einer der Faktoren Null. Da q keine Nullstelle hat (nach Voraussetzung), existiert $1 \leq i \leq r$ mit $b = a_i$. Umgekehrt ist nach Proposition 1.21 jedes $a_i, 1 \leq i \leq r$, eine Nullstelle von p.

(c) Wir machen Induktion nach $deg(p)$.

(i) Angenommen $p \in K[X]$ hat keine Nullstelle in K. Dann ist $q = p$ in (3) und $r = 0$ – andernfalls wäre $a_1 \in K$ eine Nullstelle von p. Widerspruch. Also ist die Darstellung in (3) eindeutig in diesem Fall. Dies gilt zum Beispiel für Polynome vom Grad Null, und liefert also den Induktionsanfang.

(ii) Sei $p \in K[X]$ mit mindestens einer Nullstelle. Seien

$$\prod_{i=0}^{r} (X - a_i)^{n_i} q = p = \prod_{i=0}^{s} (X - b_1)^{m_i} u$$

zwei Darstellungen von p. Da p nach Voraussetzung eine Nullstelle hat, ist $r \geq 1$. Nach Voraussetzung hat u keine Nullstelle, also ist $u(a_1) \neq 0$. Also ist

$$0 = p(a_1) = \prod_{i=0}^{s} (a_1 - b_i) \underbrace{u(a_1)}_{\neq 0}.$$

Mit Lemma 1.11 folgt, dass $0 = \prod_{i=0}^{s} (a_1 - b_i)$ ist, und es existiert $1 \leq i \leq s$ mit $a_1 = b_i$. Nach Anwendung einer Permutation der Faktoren, sei ohne Einschränkung $a_1 = b_1$. Nach Korollar 1.16 dürfen wir kürzen (um den Faktor $(X - a_1)$), und erhalten

$$(X - a_1)^{n_1 - 1} \cdot \ldots \cdot (X - a_r)^{n_r} q = (X - b_1)^{m_1 - 1} \cdot \ldots \cdot (X - b_s)^{m_s} u, \tag{4}$$

ein Polynom vom Grad $deg(p) - 1$. Nach Induktionsvoraussetzung folgt (bis auf Permuation der Faktoren) die Eindeutigkeit für die Darstellung (4), und damit auch für die Darstellung von p.

KOROLLAR 1.24. *Sei* $0 \neq p \in K[X]$.

(a) *Polynom p hat höchstens $deg(p)$ viele paarweise verschiedene Nullstellen.*
(b) *Polynom p hat höchstens $deg(p)$ viele Nullstellen, wenn man diese mit ihrer Vielfachheit zählt.*

BEWEIS. Benutze Notation aus Theorem 1.23.

(a) *Nach Theorem 1.23 hat p genau r paarweise verschiedene Nullstellen mit*

$$deg(p) \overset{1.15}{\underset{(*)}{=}} deg(q) + \sum_{i=0}^{r} n_i \geq 0 + \sum_{i=0}^{r} 1 = r.$$

(b) *Nach Proposition 1.15 und Theorem 1.23 hat p genau $\sum_{i=0}^{r} n_i$ viele Nullstellen, mit Vielfachheit gezählt, wobei*

$$\sum_{i=1}^{r} n_i \underset{(q\neq 0)}{\leq} deg(q) + \sum_{i=1}^{r} n_1 \overset{1.15}{\underset{(3)}{=}} deg(p).$$

BEISPIEL 1.25. Sei $p = X^2 + 1$. Siehe auch Beispiel 1.20(a).

(a) In $\mathbb{C}[X]$ hat $p = (X + i)(X - i)$ zwei verschiedene Nullstellen, nämlich i und $-i$, beide mit Vielfachheit Eins.
(b) In $\mathbb{R}[X]$ hat p keine Nullstelle.
(c) In $\mathbb{Z}_5[X]$ ist $X^2 + 1 = (X - 2)(X + 2)$ mit $+2 = -3$ in $\mathbb{Z}_5$. Also hat p die Nullstelle 2 und 3, jeweils mit Vielfachheit Eins.
(d) In $\mathbb{Z}_2[X]$ ist $X^2 + 1 = (X - 1)^2$ In diesem Fall hat p genau eine Nullstelle, nämlich 1, mit Vielfachheit Zwei.

DEFINITION 1.26. Ein Polynom $0 \neq f \in K[X]$ heißt *unzerlegbar* oder *irreduzibel*, falls f nicht konstant ist und wenn $f = g \cdot h$ ist für $g, h \in K[X]$, dann ist entweder g konstant oder h konstant.

BEMERKUNG/BEISPIEL 1.27.

(a) Irreduzible Polynome in $K[X]$ sind das Analogon zu Primzahlen in $\mathbb{Z}$. Die Primfaktorzerlegung in $\mathbb{Z}$ ist eindeutig bis auf Reihenfolge und Einheiten (also bis auf ein Vorzeichen). Die Primfaktorzerlegung in $K[X]$, also die Faktorisierung von $f \in K[X]$ als Produkt irreduzibler Polynome ist ebenfalls eindeutig, bis auf Reihenfolge und Einheiten in $K[X]$ (also bis auf konstante Faktoren). Bewiesen wird dies in der Algebravorlesung.
(b) Sei $f = X^2 + 1 \in \mathbb{Z}_3[X]$. Angenommen $f = g \cdot h$ mit $g, h \in K[X] \backslash K[X]^*$ mit $K[X]^* = K$. Nach Proposition 1.15 ist $2 = deg\, f = deg(gh) = deg\, g + deg\, h$. Da g, h nicht konstant, ist $deg\, g = deg\, h = 1$. Mit Proposition 1.21 folgt, dass f eine Nullstelle in $\mathbb{Z}_3[X]$ hat. Es ist aber $f(0) = 1$, $f(1) = 2$, $f(2) = 2^2 + 1 = 5 = 2$. Widerspruch. Also ist f irreduzibel in $\mathbb{Z}_3[X]$. Es gibt neun Polynome $f \in \mathbb{Z}_3[X]$ mit f normiert und $deg\, f = 2$. Polynome mit konstanten Koeffizienten Null sind reduzibel, sie haben Faktor X. Es bleiben also sechs Polynome über, für die wir durch Einsetzen von $\{0, 1, 2\}$ prüfen müssen, ob sie eine Nullstelle haben und damit zerfallen oder nicht. Die irreduziblen Polynome $f \in \mathbb{Z}_3[X]$ mit f normiert und $deg\, f = 2$ sind: $X^2 + 1$, $X^2 + X + 2$, $X^2 + 2X + 2$.
(c) Sei $f \in K[X]$ mit $deg \in \{2, 3\}$. Dann ist f irreduzibel, genau dann wenn f keine Nullstelle hat.

(d) Ein Polynom $f \in \mathbb{Z}_2[X]$ mit $deg(f) = 4$, derart, dass f keine Nullstelle in $\mathbb{Z}_2$ hat, ist aber dennoch nicht notwendigerweise irreduzibel. Zum Beispiel ist das Polynom $X^2 + X + 1 \in \mathbb{Z}_2[X]$ irreduzibel, aber das Polynom $X^4 + X^2 + 1 = (X^2 + X + 1)^2$ ist reduzibel, ohne eine Nullstelle in $\mathbb{Z}_2$ zu haben. Das Polynom $f = X^4 + X + 1$ ist hingegen irreduzibel: Weder Null noch Eins sind Nullstelle dieses Polynoms. Wenn es reduzibel wäre, so existiert ein irreduzibles Polynom zweiten Grades, dass das Polynom f teilt. Irreduzible Polynome vom Grad zwei in $\mathbb{Z}_2[X]$ gibt es nur eines: $g := X^2 + X + 1$. Es ist aber $g^2 \neq f$, also ist f irreduzibel.

THEOREM 1.28. *(Fundamentalsatz der Algebra)*
Jedes Polynom in $\mathbb{C}[X]$ vom Grad mindestens Eins hat mindestens eine Nullstelle in $\mathbb{C}$.

BEWEIS. Funktionentheorie- oder Topologievorlesung (oder Algebravorlesung).

KOROLLAR 1.29. *Ein Polynom $p \in \mathbb{C}[X]$ hat genau $deg(p)$ viele Nullstellen in $\mathbb{C}$, mit Vielfachheiten gezählt, dh. p zerfällt über $\mathbb{C}$ vollständig in Linearfaktoren:*

$$p = c \cdot \prod_{i=0}^{deg\, p} (X - a_i), \text{ mit } a_i \in \mathbb{C},\ c \in \mathbb{C}.$$

Die Elemente a_i müssen nicht notwendigerweise paarweise verschieden sein.

BEWEIS. Folgt aus Theorem 1.28 und mit Induktion.

ÜBUNG. Sei $f \in \mathbb{C}[X]$ und seien alle Koeffizienten von f aus $\mathbb{R}$.

(a) Zeigen Sie: Ist $z \in \mathbb{C}$ Nullstelle von f, dann ist auch $\bar{z} \in \mathbb{C}$ Nullstelle von f.
(b) Folgern Sie, daß die unzerlegbaren Elemente in $\mathbb{R}[X]$ entweder lineare Polynome (mit Koeffizienten in $\mathbb{R}$) sind oder quadratische Polynome f in $\mathbb{R}[X]$ sind (also $deg = 2$) mit negativer Diskriminante $D = b^2 - 4ac$, wobei $f = aX^2 + bX + c$ ist.

Allgemeiner definiert man:

DEFINITION. Ein Körper $\bar{K}$ heißt *algebraisch abgeschlossen*, falls jedes nicht-konstante Polynom in $\bar{K}[X]$ eine Nullstelle in $\bar{K}$ hat.

BEISPIEL 1.30. Nach Theorem 1.28 ist $\mathbb{C}$ algebraisch abgeschlossen.

BEMERKUNG. In der Algebra-Vorlesung können Sie lernen, daß es zu jedem Körper K einen Körper $\bar{K}$ gibt mit $K \leq \bar{K}$ Teilkörper (also Teilring) mit $\bar{K}$ ist algebraisch abgeschlossen. Gilt zusätzlich, daß es keinen algebraisch abgeschlossenen Körper L gibt mit $K \underset{\neq}{<} L \underset{\neq}{<} \bar{K}$, dann heißt $\bar{K}$ *algebraischer Abschluß* von K. Die Standardnotation für den algebraischen Abschluß von K ist $\bar{K}$. Beispielsweise ist $\bar{\mathbb{R}} = \mathbb{C}$. Man kann zeigen, daß jeder Körper einen algebraischen Abschluß hat, und daß dieser in einem gewissen Sinne (bis auf sogenannte K-Isomorphie) eindeutig ist.

ÜBUNG. Sei K algebraisch abgeschlossen. Dann hat K unendlich viele Elemente.

BEWEIS. Angenommen $K = \{a_1, \ldots, a_n\}$ endlich. Definiere Polynom $f := 1 + \prod_i (X - a_i) \in K[X]$. Dann ist $f(a_i) = 1 \neq 0$. Also hat f keine Nullstelle in K. Widerspruch. Also ist K nicht endlich.