Teil 3

Körper

KAPITEL 10

Körperkonstruktionen

1. Körper aus irreduziblen Polynomen

DEFINITION 10.1. Eine algebraische Struktur R ist ein *Körper*, wenn R ein kommutativer Ring mit Eins ist, R zumindest zwei Elemente hat, und alle Elemente $x \in R \setminus \{0\}$ invertierbar sind.

SATZ 10.2. *Sei R ein Hauptidealbereich, und sei f ein irreduzibles Element von R. Dann ist $R/(f)$ ein Körper.*

Beweis: Sei $x \in R$ so, dass $x+(f) \neq 0+(f)$. Wir zeigen, dass $x+(f)$ invertierbar in $R/(f)$ ist. Sei dazu I das von $\{x, f\}$ erzeugte Ideal, und sei $z \in R$ so, dass $(z) = I$. Dann gilt $z \mid f$, also ist z entweder assoziiert zu f oder invertierbar. Wenn z assoziiert zu f ist, so gilt wegen $z \mid x$ auch $f \mid x$. Dann gilt aber $x \in (f)$, und somit $x+(f) = 0+(f)$. Folglich ist z invertierbar. Dann gilt $1 \in I$, und es gibt somit $u, v \in R$, sodass $ux+vf = 1$. Dann gilt $(u+(f))(x+(f)) + (v+(f))(f+(f)) = 1+(f)$, also $(u+(f))(x+(f)) = 1+(f)$. Folglich ist $x+(f)$ invertierbar. □

KOROLLAR 10.3. *Sei p eine Primzahl. Dann ist $\mathbb{Z}_p$ ein Körper.*

KOROLLAR 10.4. *Sei K ein Körper und sei f ein irreduzibles Element aus dem Polynomring $K[t]$. Dann ist $K[t]/(f)$ ein Körper.*

Wir definieren den Grad des Nullpolynoms als -1.

LEMMA 10.5. *Sei K ein Körper, und sei $f \in K[t]$. Das Polynom f ist ein invertierbares Element von $K[t]$, wenn* $\deg(f) = 0$. *Das Polynom f ist ein irreduzibles Element von $K[t]$, wenn* $\deg(f) \geq 1$ *und für alle $g, h \in K[t]$ mit $f = g \cdot h$ gilt* $\deg(g) = 0$ *oder* $\deg(h) = 0$.

Für einen Körper K nennen wir ein irreduzibles Element von $K[t]$ auch ein *über K irreduzibles Polynom*.

2. Irreduzible Polynome über $\mathbb{Q}$

DEFINITION 10.6. Sei R ein kommutativer Ring mit Eins, sei $n \in \mathbb{N}_0$, und sei $f = \sum_{i=0}^{n} f_i\, t^i \in R[t]$. Das Polynom f ist *primitiv*, wenn es kein primes $p \in R$ gibt, das alle Koeffizienten f_i $(i = 0, \ldots, n)$ teilt.

LEMMA 10.7 (Gaußsches Lemma). *Sei R ein kommutativer Ring mit Eins, und seien $f, g \in R[t]$ primitiv. Dann ist $f \cdot g$ ebenfalls primitiv.*

Beweis: Wir nehmen an, dass $f \cdot g$ nicht primitiv ist. Dann gibt es ein primes $p \in R$, das alle Koeffizienten von $f \cdot g$ teilt. Da f und g primitiv sind, teilt p weder alle Koeffizienten von f noch alle Koeffizienten von g. Sei k maximal, sodass $p \nmid f_k$, und sei l maximal, sodass $p \nmid g_l$. Wir berechnen den Koeffizienten von t^{k+l} von $f \cdot g$ und erhalten $(f \cdot g)_{k+l} = \sum_{i=0}^{k+l} f_{(k+l)-i} g_i$. Für $i < l$ gilt $p \mid f_{(k+l)-i}$, und für $i > l$ gilt $p \mid g_i$. Da $p \mid (f \cdot g)_{k+l}$, gilt also $p \mid f_k g_l$. Da p prim ist, teilt es daher einen der beiden Faktoren, im Widerspruch zur Wahl von k und l. □

DEFINITION 10.8. Sei $a = \sum_{i=1}^{n} a_i t^i \in \mathbb{Z}[t]$, $a \neq 0$. Wir definieren den *Inhalt von a* durch $\mathrm{c}(a) := \mathrm{ggT}(a_0, a_1, \ldots, a_n)$.

SATZ 10.9. *Sei $f \in \mathbb{Z}[t] \setminus \{0\}$, seien $g, h \in \mathbb{Q}[t]$ so, dass $f = g \cdot h$, und seien $\alpha, \beta \in \mathbb{Z} \setminus \{0\}$ so, dass $\alpha\, g \in \mathbb{Z}[t]$ und $\beta\, h \in \mathbb{Z}[t]$. Wir setzen:*

$$\begin{aligned} \gamma &:= \tfrac{1}{\alpha\,\beta} \cdot \mathrm{c}(\alpha\, g) \cdot \mathrm{c}(\beta\, h), \\ g' &:= \tfrac{1}{\mathrm{c}(\alpha\, g)}\, \alpha\, g, \\ h' &:= \tfrac{1}{\mathrm{c}(\beta\, h)}\, \beta\, h. \end{aligned}$$

Dann gilt $f = \gamma\,(g' \cdot h')$ und $\gamma \in \mathbb{Z}$, $g' \in \mathbb{Z}[t]$, $h' \in \mathbb{Z}[t]$.

Beweis: Die Gleichung $f = \gamma\,(g' \cdot h')$ erhält man unmittelbar durch Nachrechnen. Wir zeigen nun, dass $\gamma \in \mathbb{Z}$. Seien $\delta, \varepsilon \in \mathbb{Z} \setminus \{0\}$ so, dass $\gamma = \frac{\delta}{\varepsilon}$ und $\mathrm{ggT}(\delta, \varepsilon) = 1$. Dann gilt $\varepsilon\, f = \delta\,(g' \cdot h')$. Da $f \in \mathbb{Z}[t]$, teilt ε alle Koeffizienten von $\delta\,(g' \cdot h')$. Wegen $\mathrm{ggT}(\delta, \varepsilon) = 1$ teilt ε alle Koeffizienten von $g' \cdot h'$. Nun sind g' und h' primitiv. Wegen des Gaußschen Lemmas (Lemma 10.7) ist $g' \cdot h'$ ebenfalls primitiv, also gilt $\varepsilon \in \{1, -1\}$. Folglich gilt $\gamma \in \mathbb{Z}$. □

SATZ 10.10 (Eisenstein-Kriterium). *Seien $n \in \mathbb{N}$, p Primzahl, $a = \sum_{i=0}^{n} a_i\, t^i \in \mathbb{Z}[t]$ so, dass*

(1) $p \mid a_0, \ldots, p \mid a_{n-1}$,
(2) $p \nmid a_n$,
(3) $p^2 \nmid a_0$.

Dann ist a ein irreduzibles Element von $\mathbb{Q}[t]$ (also ein über $\mathbb{Q}$ irreduzibles Polynom).

Beweis: Wenn a nicht irreduzibel ist, gibt es $b, c \in \mathbb{Q}[t]$ vom Grad ≥ 1, sodass $a = b\,c$. Wegen Satz 10.9 gibt es dann auch $r, s \in \mathbb{Z}[t]$ sodass $a = r\,s$ und $\deg(r) \geq 1$, $\deg(s) \geq 1$. Sei $k := \deg(r)$, $l := \deg(s)$. Dann gilt $k + l = n$. Wegen $p \nmid a_n$ gilt $p \nmid r_k$ und $p \nmid s_l$. Wir zeigen nun, dass für alle $k_1 \in \mathbb{N}_0$ mit $k_1 < k$ und für alle $l_1 \in \mathbb{N}_0$ mit $l_1 < l$ gilt, dass $p \mid r_{k_1}$ und $p \mid s_{l_1}$. Sei dazu k_2 minimal mit $p \nmid r_{k_2}$, und sei l_2 minimal mit $p \nmid s_{l_2}$. Dann ist der Koeffizient von $t^{k_2+l_2}$ des Polynoms a nicht durch p teilbar. Somit gilt $k_2 + l_2 = n$, und somit $k_2 = k$, $l_2 = l$. Also gibt es Polynome $u, v \in \mathbb{Z}[t]$, sodass $r = r_k\,t^k + p\,u$ und $s = s_l\,t^l + p\,v$. Somit gilt $a_0 = (r \cdot s)_0 = \overline{r}(0) \cdot \overline{s}(0) = p \cdot \overline{u}(0) \cdot p \cdot \overline{v}(0)$. Folglich ist a_0 ein Vielfaches von p^2, im Widerspruch zur Annahme. □

Übungsaufgaben 10.11.

(1) Seien $f, g \in \mathbb{Z}[t] \setminus \{0\}$. Zeigen Sie, dass $\mathrm{c}(f \cdot g) = \mathrm{c}(f) \cdot \mathrm{c}(g)$.
(2) Sei $a \in \mathbb{Z}[t]$, $n := \deg a$, und sei r eine rationale Nullstelle von $a = a_0 t^0 + \cdots + a_n t^n$. Zeigen Sie, dass es $p, q \in \mathbb{Z}$ gibt, sodass $r = \frac{p}{q}$ und $p \mid a_0$, $q \mid a_n$.

3. Quotientenkörper

Wir verallgemeinern jetzt die Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$.

Sei dazu D ein Integritätsbereich. Auf der Menge $\{(a, b) \in D^2 \mid b \neq 0\}$ definieren wir eine Relation durch $(a, b) \sim (c, d) :\Leftrightarrow ad = bc$. Diese Relation ist eine Äquivalenzrelation, und wir kürzen die Klasse $(a, b)/\!\sim$ mit $\frac{a}{b}$ ab. Mit $Q(D)$ bezeichnen wir die Faktormenge $\{(a, b) \in D^2 \mid b \neq 0\}/\!\sim$. Auf $Q(D)$ definieren wir $+$ durch $\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}$, $-$ durch $-\frac{a}{b} := \frac{-a}{b}$, und $\cdot$ durch $\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$.

Satz und Definition 10.12. *Sei D ein Integritätsbereich. Dann ist $(Q(D), +, -, \cdot, \frac{0}{1}, \frac{1}{1})$ ein Körper. Er heißt der* Quotientenkörper *von D.*

Satz 10.13. *Sei D ein Integritätsbereich, sei K ein Körper, und sei φ ein Ring-mit-Eins-Monomorphismus von D nach K. Dann ist $\psi : Q(D) \to K$, $\psi(\frac{a}{b}) := \varphi(a) \cdot (\varphi(b))^{-1}$ wohldefiniert und ein Ring-mit-Eins-Monomorphismus vom Quotientenkörper von D nach K.*

Sei K ein Körper. Den Quotientenkörper des Polynomrings $K[t_1, \ldots, t_n]$ bezeichnet man als den Körper der *rationalen Funktionen vom Transzendenzgrad n über K*, und kürzt ihn mit $K(t_1, \ldots, t_n)$ ab.

KAPITEL 11

Körpererweiterungen

1. Unterkörper und Primkörper

DEFINITION 11.1. Sei $E = (E, +, -, \cdot, 0, 1)$ ein Körper, und sei $K \subseteq E$. Die Menge K ist dann ein *Unterkörper* von E, wenn

(1) $0 \in K$, $1 \in K$,
(2) für alle $x, y \in K$ gilt $x + y \in K$, $x - y \in K$, $x \cdot y \in K$,
(3) für alle $x \in K$ gilt $x^{-1} \in K$.

Wenn K ein Unterkörper von E ist, so ist $(K, +|_{K\times K}, -|_K, \cdot|_{K\times K}, 0, 1)$ selbst ein Körper. Wir bezeichnen dann E als *Erweiterung* von K.

ÜBUNGSAUFGABEN 11.2.

(1) Zeigen Sie: Der Durchschnitt beliebig vieler Trägermengen von Unterkörpern eines Körpers ist wieder Trägermenge eines Unterkörpers.
(2) Sei E ein endlicher Körper, und sei $K \subseteq E$ mit $|K| \geq 2$ so, dass für alle $x, y \in K$ auch $x + y$ und $x \cdot y$ in K liegen. Zeigen Sie, dass K ein Unterkörper von E ist.

Der Durchschnitt aller Unterkörper eines Körpers E ist wieder ein Körper, er heißt *Primkörper* von E.

SATZ 11.3. *Sei E ein Körper. Dann ist sein Primkörper entweder isomorph zu $\mathbb{Q}$ oder zu $\mathbb{Z}_p$ mit einer Primzahl p.*

BEWEIS. Offensichtlich sind alle $a * 1$ mit $a \in \mathbb{Z}$ in jedem Unterkörper von E enthalten. Die Abbildung

$$\begin{array}{rccc} \Phi & : & \mathbb{Z} & \longrightarrow & E \\ & & z & \longmapsto & z * 1 \end{array}$$

ist ein Ring mit Eins-Homomorphismus. Da E ein Integritätsbereich ist, ist $\mathrm{im}(\Phi)$ auch ein Integritätsbereich und das Ideal $I = \ker(\Phi)$ daher prim. Falls $I = 0$, so ist Φ ein Monomorphismus. Wegen Satz 10.13 kann daher auch der Quotientenkörper von $\mathbb{Z}$, also $\mathbb{Q}$, in E eingebettet werden. Somit enthält E einen zu $\mathbb{Q}$ isomorphen Unterkörper Q. Da $\mathbb{Q}$ keinen echten Unterkörper enthält, ist Q der Primkörper von E.

Falls $I \neq 0$, so gibt es eine Primzahl p mit $\ker(\Phi) = (p)$. Dann ist $\mathrm{im}(\Phi)$ isomorph zu $\mathbb{Z}_p$. Also enthält E einen zu $\mathbb{Z}_p$ isomorphen Unterkörper P. Da P keinen echten Unterkörper enthält, ist P der Primkörper von E. □

Sei E ein Körper. Das kleinste $p \in \mathbb{N}$ mit $p * 1 = 0$ heißt *Charakteristik* von E. Wenn es kein solches $p \in \mathbb{N}$ gibt, dann definieren wir die Charakteristik von E als 0.

2. Algebraische und Transzendente Elemente in Körpern

Für Körper schreiben wir $K \leq L$, um auszudrücken, dass L eine Erweiterung von K ist.

Definition 11.4. Seien $K \leq L$ Körper, und sei $a \in L$. Dann ist a *algebraisch* über K, wenn es $f \in K[t] \setminus \{0\}$ gibt, sodass $f(a) = 0$. Wenn a nicht algebraisch ist, so ist es *transzendent* über K.

Beispiel: 2, $\sqrt{2}$ und $\frac{1}{\sqrt[3]{2}}$ sind algebraisch über $\mathbb{Q}$, $l = \sum_{i=1}^{10^{-i!}}$ ist transzendent (Liouville 1844), e ist transzendent (Hermite 1873), in $\mathbb{R}$ gibt es überabzählbar viele Zahlen, die transzendent über $\mathbb{Q}$ sind (Cantor 1874), π ist transzendent (Lindemann 1882).

Definition 11.5. Seien $K \leq L$ Körper, und sei $S \subseteq L$. Die Körpererweiterung $K(S)$ ist der Durchschnitt aller Unterkörper K' von L mit $K \cup S \subseteq K'$.

Es gilt dann

$$K(S) = \{\frac{f(s_1, \ldots, s_n)}{g(s_1, \ldots, s_n)} \mid n \in \mathbb{N}_0, f, g \in K[x_1, \ldots, x_n], s_1, \ldots, s_n \in S, g(s_1, \ldots, s_n) \neq 0\}.$$

Wenn $S = \{a\}$, so schreiben wir $K(a)$ für $K(\{a\})$ und nennen $K(\{a\})$ eine *einfache* Körpererweiterung von K.

Satz 11.6. *Seien $K \leq L$ Körper und sei $a \in L$. Dann gilt genau eine der folgenden Alternativen:*

1. *a ist algebraisch über K und es gibt ein Polynom irreduzibles Polynom $m_a \in K[x]$, sodass $K(a)$ isomorph zu $K[x]/(m_a)$ ist und $\dim_K(K(a)) = \deg(m_a)$.*
2. *a ist transzendent über K, $K(a)$ ist isomorph zum rationalen Funktionenkörper $K(x)$ und $\dim_K(K(a))$ ist nicht endlich.*

Definition 11.7. Sei $K \leq L$. Der *Grad* der Körpererweiterung $[L : K]$ ist $\dim_K(L)$. Die Körpererweiterung ist *endlich*, wenn $[L : K]$ endlich ist. L ist *algebraisch* über K, wenn jedes $a \in L$ algebraisch über K ist.

Satz 11.8. *Sei $K \leq L$. Wenn $[L : K]$ endlich ist, so ist L algebraisch über K.*

Satz 11.9. *Seien $K \leq L$ und $L \leq M$. Dann gilt $[M : K] = [M : L] \cdot [L : K]$.*

SATZ 11.10. *Sei $K \leq L$, und sei $\overline{K}$ die Menge der Elemente von L, die algebraisch über K sind. Dann ist $\overline{K}$ ein Unterkörper von L.*

Beweis: Seien $a, b \in \overline{K}$. Da a algebraisch über K ist, ist $[K(a) : K]$ endlich. Da b algebraisch über K ist, ist b algebraisch über $K(a)$, und daher ist $[K(a)(b) : K(a)]$ endlich. Also erhalten wir, dass $[K(a, b) : K] = [K(a)(b) : K] = [K(a)(b) : K(a)] \cdot [K(a) : K]$ endlich ist. Somit ist $K(a, b)$ eine endliche Erweiterung von K, und folglich gilt $K(a, b) \subseteq \overline{K}$. Also gilt $ab, a + b \in \overline{K}$ und wenn $a \neq 0$ auch $a^{-1} \in \overline{K}$. □

KAPITEL 12

Endliche Körper

1. Grundlegende Eigenschaften endlicher Körper

Ein Körper E ist *endlich*, wenn er nur endlich viele Elemente hat.

SATZ 12.1. *Sei E ein endlicher Körper. Dann gibt es eine Primzahl p, sodass der Primkörper von E isomorph zu $\mathbb{Z}_p$ ist.*

SATZ 12.2. *Die Anzahl der Elemente eines endlichen Körpers ist eine Primzahlpotenz.*

Wir beweisen folgende stärkere Aussage:

SATZ 12.3. *Sei K ein Unterkörper des endlichen Körpers E. Dann gibt es ein $n \in \mathbb{N}$, sodass $|E| = |K|^n$.*

Beweis: Durch die skalare Multiplikation $* : K \times E \to E$, $k * e := k \cdot e$ wird $(E, +, -, 0; *)$ zu einem Vektorraum über K. Wegen der Endlichkeit von K hat K eine endliche Basis $B = (b_1, \ldots, b_n)$. Die Abbildung, die jedem $e \in E$ sein Koordinatentupel $(e)_B$ zuordnet, ist eine Bijektion von E nach K^n. □

Satz 12.3 folgt nun, wenn man als K den Primkörper von E wählt.

SATZ 12.4. *Sei E ein Körper der Charakteristik p mit $q = p^m$ Elementen. Dann gilt für alle $x, y \in E$:*

(1) $(x + y)^p = x^p + y^p$.
(2) $x^q = x$.

Beweis: (1): Nach dem binomischen Lehrsatz gilt

$$(x + y)^p = x^p + \sum_{i=1}^{p-1} \binom{p}{i} * x^i y^{p-i} + y^p.$$

Da $\binom{p}{i}$ für alle $i \in \{1, 2, \ldots, p-1\}$ Vielfache von p sind, gilt $(x + y)^p = x^p + y^p$.

(2): Wir verwenden den Satz von Fermat für die Gruppe $(E^*, \cdot)$ und erhalten, dass alle $x \neq 0$ die Gleichung $x^{q-1} = 1$ erfüllen. □

ÜBUNGSAUFGABEN 12.5.

(1) Sei K ein Körper der Charakteristik p, sei $m \in \mathbb{N}$, und seien $x, y \in K$. Zeigen Sie: $(x+y)^{p^m} = x^{p^m} + y^{p^m}$.
(2) Sei K ein Körper, und sei $f \in K[x]$. Seien $\alpha_1, \alpha_2, \ldots, \alpha_k \in K$ paarweise verschiedene Nullstellen von f. Zeigen Sie, dass $\prod(x - \alpha_i)$ ein Teiler von f in $K[x]$ ist.
(3) Zeigen Sie, dass ein Polynom in $K[x]$ vom Grad $\leq n$, das $n+1$ verschiedene Nullstellen hat, automatisch das Nullpolynom sein muss.
(4) Sei K ein Körper der Charakteristik p und sei $\xi \in K$.
   (a) Zeigen Sie mithilfe des Satzes, dass für alle $z \in \mathbb{Z}$ die Kongruenz $z^p \equiv z \pmod{p}$ gilt, dass das Polynom
   $$f(x) := (x+\xi)^p - x^p - \xi^p$$
   zumindest p Nullstellen hat (probieren Sie $n * \xi$ mit $n \in \mathbb{Z}$).
   (b) Bestimmen Sie den Grad dieses Polynoms.
   (c) Schließen Sie daraus, dass $p \mid \binom{p}{i}$ für alle $i \in \{1, 2, \ldots, p-1\}$, und dass für alle $\alpha, \beta \in K$ gilt: $(\alpha + \beta)^p = \alpha^p + \beta^p$.

Aus dem Hauptsatz über endlich erzeugte abelsche Gruppen erhalten wir (Korollar 7.11):

SATZ 12.6. *Die multiplikative Gruppe eines endlichen Körpers ist zyklisch.*

Wenn man nicht auf den Hauptsatz zurückgreifen will, so kann man diesen Satz auch aus folgender Beobachtung beweisen:

SATZ 12.7. *Sei $A = (A, \cdot)$ eine abelsche Gruppe mit neutralem Element 1. Wenn es für jedes $n \in \mathbb{N}$ höchstens n Elemente in A mit $x^n = 1$ gibt, dann ist A zyklisch.*

Beweis: Sei $h := |A|$. Falls $h = 1$, ist A klarerweise zyklisch. Wir nehmen also nun $h \geq 2$ an. Wir bilden die Primfaktorzerlegung von h und finden also $N \in \mathbb{N}$, Primzahlen $p_1, p_2, \ldots, p_N$ und $r_1, r_2, \ldots, r_N \in \mathbb{N}$ sodass

$$h = \prod_{m=1}^{N} {p_m}^{r_m}.$$

Wir werden nun für jedes $i \in \{1, 2, \ldots, N\}$ ein Element a_i und ein Element $b_i \in A$ wählen: Da $\frac{h}{p_i} < h$, gibt es ein Element $a_i \in A$, sodass ${a_i}^{\frac{h}{p_i}} \neq 1$. Wir setzen

$$b_i := {a_i}^{\frac{h}{{p_i}^{r_i}}}.$$

Es gilt dann (Satz von Fermat)

$${b_i}^{{p_i}^{r_i}} = 1. \tag{12.1}$$

Sei nun k die Ordnung von b_i, also das kleinste $n \in \mathbb{N}$, sodass $(b_i)^n = 1$. Da $k \mid {p_i}^{r_i}$ gibt es ein $s_i \in \{0, 1, \ldots, r_i\}$, sodass $k = {p_i}^{s_i}$. Wir zeigen nun

$$s_i = r_i. \tag{12.2}$$

Nehmen wir an $s_i \leq r_i - 1$. Dann gilt

$$b_i^{p_i^{r_i-1}} = 1,$$

also

$$a_i^{\frac{h}{p_i}} = 1.$$

Das widerspricht der Wahl von a_i; dieser Widerspruch beweist (12.2). Die Ordnung von b_i ist also ${p_i}^{r_i}$. Wir bilden nun

$$c = \prod_{i=1}^{N} b_i.$$

Klarerweise gilt $c^h = 1$. Wir zeigen nun, dass c wirklich Ordnung h hat. Wenn c kleinere Ordnung hätte, dann gibt es ein $j \in \{1, \ldots, N\}$, sodass $c^{\frac{h}{p_j}} = 1$. Daher gilt

$$\prod_{i=1}^{N} b_i^{\frac{h}{p_j}} = 1. \tag{12.3}$$

Falls $i \neq j$, so gilt ${p_i}^{r_i} \mid \frac{h}{p_j}$. Wegen (12.1) sind also Faktoren in (12.3) mit $i \neq j$ gleich 1. Wir erhalten also

$$b_j^{\frac{h}{p_j}} = 1.$$

Da b_j wegen (12.2) die Ordnung ${p_j}^{r_j}$ hat, gilt ${p_j}^{r_j} \mid \frac{h}{p_j}$. Daher gilt ${p_j}^{r_j+1} \mid h$, was im Widerspruch zur Primfaktorzerlegung von h steht. Das Element c hat also wirklich Ordnung h, und ist somit ein erzeugendes Element für die Gruppe A. □

Aus dem Satz 12.7 folgt nun direkt der Satz 12.6, da in jedem Körper und für jedes n das Polynom $x^n - 1$ höchstens n Nullstellen hat.

Übungsaufgaben 12.8.

(1) Sei $(A, \cdot)$ eine Gruppe, und sei $a \in A$ und $n \in \mathbb{N}$ so, dass $a^n = 1$. Zeigen Sie, dass n ein Vielfaches der Ordnung von a ist.

2. Irreduzible Polynome

Wenn K ein endlicher Körper mit q Elementen ist, und f ein über K irreduzibles Polynom vom Grad n, dann ist $K[x]/(f)$ ein Körper mit q^n Elementen. Wir brauchen also zunächst irreduzible Polynome.

Satz 12.9. *Sei K ein endlicher Körper mit q Elementen, und sei f ein irreduzibles Polynom vom Grad n. Dann gilt $f \mid x^{q^n} - x$.*

Wir betrachten den Körper $K[x]/(f)$. Dieser Körper hat q^n Elemente. Es gilt also wegen Satz 12.4 (2) $(x + (f))^{q^n} = x + (f)$. Das bedeutet $f \mid x^{q^n} - x$. □

Satz 12.10. *Sei K ein Körper mit q Elementen. Dann gilt $\prod_{\nu \in K}(x - \nu) = x^q - x$.*

Beweis: Beide Polynome haben q Nullstellen: für das linke Polynom ist das offensichtlich; für das rechte eine Konsequenz aus dem Satz von Fermat bzw. aus Satz 12.4. Die Differenz dieser beiden Polynome hat also mindestens q Nullstellen, und einen Grad $\leq q-1$. Die Differenz ist also das Nullpolynom. □

LEMMA 12.11. *Sei K ein endlicher Körper mit q Elementen, sei $m \in \mathbb{N}$, und sei f ein über K irreduzibles Polynom vom Grad m. Sei E ein Erweiterungskörper von K mit q^m Elementen. Dann zerfällt f in $E[x]$ in ein Produkt lauter linearer Polynome.*

Beweis: Da $\deg f = m$, gilt nach Satz 12.9, dass f das Polynom $x^{q^m} - x$ teilt. Nach Satz 12.10 gilt

$$\prod_{a \in E}(x-a) = x^{q^m} - x.$$

Das Polynom f ist auch ein Polynom in $E[x]$. Jeder über E irreduzible Teiler von f in $E[x]$ teilt also eines der Polynome in $\{x-b \,|\, b \in E\}$. Das bedeutet, dass f in $E[x]$ vollständig in Linearfaktoren zerfällt. □

Wir bezeichnen ein Polynom f als *normiert*, wenn sein führender Koeffizient (also der Koeffizient von $x^{\deg(f)}$) gleich 1 ist.

SATZ 12.12. *Sei p eine Primzahl, sei $m \in \mathbb{N}$, und sei $q = p^m$. Sei f ein normiertes, über $\mathbb{Z}_p$ irreduzibles Polynom in $\mathbb{Z}_p[x]$ vom Grad m. Dann ist jeder Körper mit q Elementen zu $\mathbb{Z}_p[x]/(f)$ isomorph.*

Beweis: Sei E ein Körper mit q Elementen. Wegen Lemma 12.11 wissen wir, f eine Nullstelle in $E[x]$ hat. Sei $b \in E$ so, dass $\overline{f}(b) = 0$. Wir bilden nun die Abbildung

$$\begin{array}{rccc} \Phi & : & \mathbb{Z}_p[x] & \longrightarrow & E \\ & & g & \longmapsto & g(b). \end{array}$$

Die Abbildung Φ ist ein Ring mit Eins-Homomorphismus. Ihr Kern ist $\{g \in \mathbb{Z}_p[x] \,|\, g(b) = 0\}$. Sei h der normierte Erzeuger des Ideals $\ker \Phi$. Da $f \in \ker \Phi$, gilt $h \mid f$. Da f irreduzibel über $\mathbb{Z}_p$ ist, ist h entweder von Grad 0 oder gleich f. Im Fall, dass h vom Grad 0 ist, gilt wegen $h(b) = 0$, dass h das Nullpolynom ist, was $h \mid f$ widerspricht. Also ist $h = f$. Es gilt also nach dem Homomorphiesatz, dass $\mathbb{Z}_p[x]/(f)$ isomorph zu E ist. □

3. Existenz irreduzibler Polynome

Wir geben im folgenden einen Beweis dafür, dass es für jedes n und für jeden endlichen Körper K ein irreduzibles Polynom vom Grad n über K gibt.

SATZ 12.13. *Sei K ein Körper, und sei f ein normiertes Polynom in $K[x]$ vom Grad n. Dann gibt es einen Erweiterungskörper E von K, sodass jeder in $E[x]$ irreduzible Teiler von f Grad 1 hat.*

Wir beweisen folgende Aussage durch Induktion nach n:

> Für jeden Körper K und jedes Polynom $f \in K[x]$ vom Grad n gibt es einen Erweiterungskörper E von K, sodass jeder in $E[x]$ irreduzible Teiler von f Grad 1 hat.

Für $n = 1$ ist die Aussage klar. Wir fixieren nun einen Körper K und ein Polynom $f \in K[x]$ mit $\deg f = n > 1$. Wir zerlegen f in ein Produkt von normierten, über K irreduziblen Polynomen in $K[x]$. Sei g einer der irreduziblen Faktoren. Wir bilden den Körper $L := K[x]/(g)$. Wir zeigen nun, dass $x + (g)$ eine Nullstelle von f ist. Dazu berechnen wir $\overline{f}(x+(g)) = \sum_{i=0}^{\deg f} f_i \cdot (x+(g))^i$. Wir wissen, wie man in Quotienten, also in $K[x]/(g)$ rechnet, und erhalten $\sum_{i=0}^{\deg f} f_i \cdot (x+(g))^i = (\sum_{i=0}^{\deg f} f_i \cdot x^i) + (g)$. Wir wissen, das jedes Polynom $f = (f_0, f_1, f_2, \ldots, f_{\deg f}, 0, 0, \ldots)$ die Eigenschaft $f = \sum_{i=0}^{\deg f} f_i \cdot x^i$ erfüllt, da ja $x^0 = (1, 0, 0, \ldots)$, $x^1 = (0, 1, 0, 0, \ldots)$, $x^2 = (0, 0, 1, 0, 0, \ldots), \ldots$. Also gilt $(\sum_{i=0}^{\deg f} f_i \cdot x^i) + (g) = f + (g)$. Da $g \mid f$, gilt $f + (g) = 0 + (g)$. Also ist $x + (g)$ eine Nullstelle von f in L. Da f eine Nullstelle l in L hat, gibt es $h \in L[x]$, sodass $f = (x-l) \cdot h$. Da h kleineren Grad als f hat, gibt es nach nach Induktionsvorraussetzung einen Erweiterungskörper M von L, sodass jeder in $M[x]$ irreduzible Teiler des Polynoms h Grad 1 hat. In $M[x]$ hat jeder irreduzible Teiler von f also Grad 1. □

Satz 12.14. *Sei K ein endlicher Körper, und sei $n \in \mathbb{N}$. Dann gibt es ein über K irreduzibles Polynom vom Grad n in $K[x]$.*

Beweis: Sei $q := K$. Es gibt einen Erweiterungskörper E von K, in dem $x^{q^n} - x$ in lauter Linearfaktoren zerfällt. Wir bilden

$$L := \{e \in E \mid e^{q^n} - e = 0\}.$$

Mit Satz 12.4 (1) erhalten wir, dass L ein Unterkörper von E ist; mit mit Satz 12.4 (2), dass L ein Erweiterungskörper von K ist. Da $x^{q^n} - x$ über E in lauter Linearfaktoren zerfällt, gibt es $e_1, e_2, \ldots, e_{q_n} \in E$, sodass

$$x^{q^n} - x = \prod_{r}^{q^n} (x - e_r).$$

Mithilfe der Ableitung zeigt man wieder, dass $x^{q^n} - x$ quadratfrei ist, und dass daher alle e_i verschieden sind. Alle e_i liegen in L. Der Körper L hat daher mindestens q^n Elemente. Da $x^{q^n} - x$ in E höchstens q^n Nullstellen haben kann, hat L höchstens q^n Elemente.

Sei nun α ein erzeugendes Element der multiplikativen Gruppe $(L^*, \cdot)$ von L, und sei $f \in K[x]$ ein normiertes, erzeugendes Element des Ideals

$$I = \{g \in K[x] \mid \overline{g}(\alpha) = 0\}.$$

Wegen $x^{q^n} - x \in I$ gilt $I \neq \{0\}$. Wir zeigen nun:

$$f \text{ ist ein irreduzibles Element von } K[x]. \tag{12.4}$$

Wir nehmen an, es gibt normierte $f_1, f_2 \in K[x]$ sodass $f = f_1 \cdot f_2$. Dann gilt $\overline{f_1}(\alpha) \cdot \overline{f_2}(\alpha) = 0$. Wenn nun $\overline{f_1}(\alpha) = 0$, so gilt $f \mid f_1$, und somit $f_2 = 1$. Das beweist (12.4).

Die Abbildung

$$\begin{array}{rccc} \Phi & : & K[x] & \longrightarrow & L \\ & & g & \longmapsto & g(\alpha) \end{array}$$

ist surjektiv ($\Phi(x^k) = \alpha^k$ für alle k); ihr Kern ist I. Wir wissen, das L genau q^n Elemente hat. $K[x]/I$ hat daher ebenfalls genau q^n Elemente, und somit gilt $\deg f = n$. Das Polynom f ist also irreduzibel vom Grad n. □

Definition 12.15 (Möbiusfunktion). Wir definieren $\mu : \mathbb{N} \to \{-1, 0, 1\}$ durch

$$\mu(n) = \begin{cases} (-1)^k, \text{ falls } n = p_1 \cdot p_2 \cdots p_k \text{ mit } p_i \neq p_j \text{ für } i \neq j, \\ 1 \text{ falls } n = 1, \\ 0 \text{ sonst.} \end{cases}$$

Satz 12.16. *Die Anzahl N der irreduziblen Polynome vom Grad n über einem Körper mit q Elementen ist gegeben durch*

$$N = \frac{1}{n} \sum_{d \mid n} \mu(d) q^{\frac{n}{d}}.$$

Beweis: [**Wil99**, p.49].

Übungsaufgaben 12.17.

(1) Leiten Sie aus diesem Satz her, dass es über jedem endlichen Körper für jedes n ein irreduzibles Polynom vom Grad k gibt.

Für Polynome $f, g \in K[x]$ bezeichnen wir mit $f \circ g$ das Polynom, das man erhält, wenn man g in f einsetzt.

Satz 12.18. *Sei K ein Körper mit q Elementen, sei $n \in \mathbb{N}$, und sei $f \in K[x]$. Dann gilt*

$$f \circ x^{q^n} = x^{q^n} \circ f.$$

Beweis: Sei p die Charakteristik von K. Es gibt dann ein m, sodass $q = p^m$. Es gilt dann

$$\begin{aligned} x^{q^n} \circ f &= f^{q^n} \\ &= (\sum_{i=0}^{\deg f} f_i x^i)^{(q^n)} \\ &= (\sum_{i=0}^{\deg f} f_i x^i)^{(p^{mn})} \\ &= \sum_{i=0}^{\deg f} f_i^{p^{mn}} (x^i)^{(p^{mn})} \\ &= \sum_{i=0}^{\deg g} f_i^{q^n} (x^i)^{(q^n)} \\ &= \sum_{i=0}^{\deg f} f_i (x^{(q^n)})^i \\ &= f \circ x^{(q^n)}. \quad \square \end{aligned}$$

In einem Euklidischen Bereich kann man einen größten gemeinsamen Teiler von a, b definieren, zum Beispiel als einen Erzeuger des von a und b erzeugten Ideals. Wenn wir aus jeder Klasse konjugierter Elemente einen Repräsentanten auswählen, so können wir ggT sogar als Funktion definieren.

Satz 12.19. *Sei E ein Euklidischer Bereich, und sei $f \in E$, f nicht invertierbar, und seien $n, m \in \mathbb{N}_0$, nicht beide 0. Dann gilt* $\mathrm{ggT}(f^m - 1, f^n - 1) = f^{\mathrm{ggT}(n,m)} - 1$.

Beweis: Wir beweisen den Satz durch Induktion nach $\max(m, n)$. Wenn $m = n = 1$, dann gilt der Satz offensichtlich. Sei nun $\max(m, n) > 1$.

- *Fall* $m = 0$ oder $n = 0$: offensichtlich.
- *Fall* $m > n \geq 1$: Es gilt $\mathrm{ggT}(f^m - 1, f^n - 1) = \mathrm{ggT}(f^m - 1 - f^{m-n} \cdot (f^n - 1), f^n - 1)$, da beide Polynompaare die gleichen gemeinsamen Teiler haben. Durch ausrechnen erhalten wir $\mathrm{ggT}(f^m - 1, f^n - 1) = \mathrm{ggT}(f^{m-n} - 1, f^n - 1)$. Da $m > n$, gilt $\max(m - n, n) < \max(m, n)$. Nach Induktionsannahme gilt also $\mathrm{ggT}(f^{m-n} - 1, f^n - 1) = f^{\mathrm{ggT}(m-n,n)} - 1 = f^{\mathrm{ggT}(m,n)} - 1$.
- *Fall* $n > m \geq 1$: analog.
- *Fall* $m = n$: offensichtlich. $\square$

Korollar 12.20.

(1) *Sei K ein Körper, sei f ein normiertes Polynom in $K[x]$ mit* $\deg(f) \geq 1$, *und seien $m, n \in \mathbb{N}$. Dann gilt* $\mathrm{ggT}(f^m - 1, f^n - 1) = f^{\mathrm{ggT}(n,m)} - 1$.

(2) *Seien* $f, m, n \in \mathbb{N}$ *mit* $f \geq 2$. *Dann gilt* $\mathrm{ggT}(f^m - 1, f^n - 1) = f^{\mathrm{ggT}(n,m)} - 1$.

SATZ 12.21. *Sei* K *ein endlicher Körper mit* q *Elementen, und sei* $n \in \mathbb{N}$. *Sei* F *die Menge aller über* K *irreduziblen, normierten Polynome in* $K[x]$, *deren Grad ein Teiler von* n *ist. Dann gilt*

$$\prod_{f \in F} f = x^{q^n} - x.$$

Beweis: Wir zerlegen $x^{q^n} - x$ in ein Produkt normierter, über K irreduzibler Polynome; wir finden also $k \in \mathbb{N}$ und normierte irreduzible Polynome $g_1, g_2, \ldots, g_k$, sodass

$$x^{q^n} - x = \prod_{i=1}^{k} g_i \,.$$

Als erstes zeigen wir, dass alle g_i verschieden sind. Nehmen wir an, dass es ein Polynom h mit $\deg h \geq 1$ gibt, sodass $h^2 \mid x^{q^n} - x$. Dann gibt es $a \in K[x]$, sodass

$$h^2 \cdot a = x^{q^n} - x.$$

Durch Differenzieren erhalten wir

$$2hh'a + h^2a' = q^n * x^{q^n - 1} - 1,$$

und da q^n ein Vielfaches der Charakteristik von K ist, gilt

$$h(2h'a + ha') = -1.$$

Das ist aber nicht möglich, weil $\deg h \geq 1$. Sei also $G = \{g_i \,|\, i \in \{1, 2, \ldots, k\}\}$. Dann gilt, weil alle g_i verschieden sind, $x^{q^n} - x = \prod_{g \in G} g$. Wir zeigen nun noch

$$F = G. \tag{12.5}$$

$\subseteq$: Sei also $f \in F$ ein normiertes, über $K[x]$ irreduzibles Polynom, dessen Grad (=: d) ein Teiler von n ist. Wir müssen zeigen, dass f das Polynom $x^{q^n} - x$ teilt. Dazu betrachten wir den Körper $K[x]/(f)$. Dieser Körper hat q^d Elemente. Es gilt also wegen Satz 12.4 (2) $(x + (f))^{q^d} = x + (f)$. Das bedeutet

$$f \mid x^{q^d} - x.$$

Wir zeigen nun

$$x^{q^d} - x \mid x^{q^n} - x. \tag{12.6}$$

Dazu zeigen wir $x^{q^d - 1} - 1 \mid x^{q^n - 1} - 1$. Wir berechnen $\mathrm{ggT}(x^{q^d-1} - 1, x^{q^n-1} - 1)$. Nach Lemma 12.20 gilt $\mathrm{ggT}(x^{q^d-1} - 1, x^{q^n-1} - 1) = x^{\mathrm{ggT}(q^d-1, q^n-1)} - 1 = x^{(q^{\mathrm{ggT}(d,n)})} - 1 = x^{q^d} - 1$; das impliziert (12.6). Wir erhalten also $f \mid x^{q^n} - x$. Somit (Fundamentallemma) liegt $f \in G$. $\supseteq$: Sei g ein normiertes irreduzibles Polynom, das $x^{q^n} - x$ teilt. Wir müssen zeigen, dass $d := \deg g$ ein Teiler von n ist. Der Körper $K[x]/(g)$ hat q^d Elemente. Es gilt also $g \mid x^{q^d} - x$. Falls $g \neq x$, gilt $g \mid \mathrm{ggT}(x^{q^d-1} - 1, x^{q^n-1} - 1) = x^{\mathrm{ggT}(g^d-1, q^n-1)} - 1 = x^{(q^{\mathrm{ggT}(n,d)} - 1)} - 1$. Sei $r := \mathrm{ggT}(n, d)$. Es gilt also $g \mid x^{q^r} - x$. Wir zeigen nun, dass jedes

Element von $K[x]/(g)$ eine Nullstelle von $x^{q^r} - x$ ist. Sei dazu $h \in K[x]$. Wir berechnen $(h + (g))^{(q^r)}$. Es gilt

$$\begin{aligned}(h + (g))^{(q^r)} &= h^{(q^r)} + (g) \\ &= (x^{(q^r)} \circ h) + (g) \\ &= (h \circ x^{(q^r)}) + (g) \\ &= (\sum_{i=0}^{\deg h} h_i x^{i \cdot q^r}) + (g).\end{aligned}$$

Es gilt $x^{(q^r)} \equiv x \pmod g$, also für alle $i \in \mathbb{N}_0$ auch $x^{i \cdot q^r} \equiv x^i \pmod g$. Insgesamt erhalten wir also

$$(h + (g))^{(q^r)} = h + (g),$$

und somit ist jedes Element aus $K[x]/(g)$ eine Nullstelle von $x^{q^r} - x$. Da $r \geq 1$, ist $x^{q^r} - x$ nicht das Nullpolynom. Es hat also höchstens q^r Nullstellen. Der Körper $K[x]/(g)$ hat q^d Elemente. Es gilt also $d \leq r$, also $d \leq \mathrm{ggT}(n, d)$. Das bedeutet, dass d ein Teiler von n ist. Das Polynom g liegt also in der Menge F. □

4. Test auf Irreduzibilität

Der folgende Satz liefert einen Test, ob ein Polynom irreduzibel über einem endlichen Körper mit q Elementen ist.

Satz 12.22. *Sei K ein Körper mit q Elementen, sei $n \in \mathbb{N}$ und sei $f \in K[x]$ mit $\deg(f) = n$. Äquivalent sind:*

(1) *Für alle $i \in \{1, 2, \ldots, \lfloor \frac{n}{2} \rfloor\}$ gilt:*

$$\mathrm{ggT}(f, x^{q^i} - x) = 1.$$

(2) *f ist irreduzibel über K.*

Beweis: (1)⇒(2): Wenn f nicht irreduzibel über K ist, so gibt es ein über K irreduzibles Polynom $g \in K[t]$ mit $g \mid f$, $1 \leq \deg(g) \leq \lfloor \frac{n}{2} \rfloor$. Sei $i := \deg(g)$. Dann gilt wegen Satz 12.9 $g \mid (x^{q^i} - x)$,und somit $g \mid \mathrm{ggT}(f, x^{q^i} - x)$, im Widerspruch zu $\mathrm{ggT}(f, x^{q^i} - x) = 1$. (2)⇒(1): Wenn f über K irreduzibel ist, $i \in \{1, \ldots, \lfloor \frac{n}{2} \rfloor\}$, und $\mathrm{ggT}(f, x^{q^i} - x) \neq 1$, so gilt $f \mid x^{q^i} - x$. Wegen Satz 12.21 ist der Grad von f dann ein Teiler von i; somit gilt $n \leq i$, im Widerspruch zu $i \leq \lfloor \frac{n}{2} \rfloor$. □

Satz 12.23. *Sei K ein Körper mit q Elementen, sei $n \in \mathbb{N}$ und sei $f \in K[x]$ mit $\deg(f) = n$, $\mathrm{ggT}(f, f') = 1$, und seien $f_1, \ldots, f_r$ über K irreduzible Polynome mit $\prod_{i=1}^r f_i = f$. Sei Q die $n \times n$-Matrix, an deren (i, j)-ter Stelle der Koeffizient von x^{i-1} des Polynoms $x^{q \cdot (j-1)} \bmod f$ steht. Dann ist die Dimension des Nullraums von $Q - I$ gleich r.*

Es gilt $(Q - I) \cdot \begin{pmatrix} a_0 \\ \vdots \\ a_n \end{pmatrix} = 0$ genau dann, wenn für das Polynom $a := \sum_{j=0}^{n-1} a_j x^{q^j}$ gilt, dass $a(x^q) - a(x)$ ein Vielfaches von f ist. Wegen Satz 12.18 gilt $a(x^q) = a(x)^q$.

Wir zeigen nun, dass $f \mid a(x)^q - a(x)$ genau dann gilt, wenn es $\alpha_1, \ldots, \alpha_r \in K$ gibt, sodass für alle $i \in \{1, \ldots, r\}$ gilt, dass $f_i \mid (a(x) - \alpha_i)$. Wenn es $(\alpha_1, \ldots, \alpha_r) \in K^r$ mit dieser Eigenschaft gibt, so gilt für jedes i, dass $f_i \mid (a(x) - \alpha_i) \mid \prod_{\beta \in K}(a(x) - \beta)$. Wegen Satz 12.10 gilt also $f_i \mid (a(x)^q - a(x)$. Da alle f_i irreduzibel und paarweise verschieden sind (wegen $\mathrm{ggT}(f, f') = 1$), gilt also $f \mid a(x)^q - a(x)$. Sei nun umgekehrt a so, dass $f \mid a(x)^q - a(x)$, und $i \in \{1, \ldots, r\}$. Dann gilt $f_i \mid \prod_{\beta \in K}(a(x) - \beta)$. Da f_i irreduzibel über K ist, teilt es einen der Faktoren.

Wegen des Chinesischen Restsatzes gibt es für jedes r-Tupel $(\alpha_1, \ldots, \alpha_r) \in K^r$ genau ein Polynom a vom Grad $\leq n-1$, sodass $f_i \mid a(x) - \alpha_i$ für alle $i \in \{1, \ldots, r\}$. Folglich hat das Gleichungssystem $(Q - I) \cdot a = 0$ genau q^r Lösungen, die Dimension des Nullraums ist also r. □

Literaturverzeichnis

[Buc82] B. Buchberger, *Algebraic simplification*, Computer algebra – symbolic and algebraic computation (B. Buchberger, G.E. Collins, and R. Loos, eds.), Springer-Verlag Wien, 1982, pp. 11–43.

[Cam99] P. J. Cameron, *Permutation groups*, London Mathematical Society Student Texts, vol. 45, Cambridge University Press, Cambridge, 1999.

[GAP12] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.5.6*, 2012.

[Kau23] M. Kauers, *Lineare Algebra und Analytische Geometrie*, Lecture notes for a course at Johannes Kepler University Linz, Austria, September 2023.

[KB70] D. E. Knuth and P. B. Bendix, *Simple word problems in universal algebras*, Computational Problems in Abstract Algebra (Proc. Conf., Oxford, 1967), Pergamon, Oxford, 1970, pp. 263–297.

[LP98] R. Lidl and G. F. Pilz, *Applied abstract algebra*, second ed., Springer-Verlag, New York, 1998.

[Rob03] D. J. S. Robinson, *An introduction to abstract algebra*, Walter de Gruyter, Berlin – New York, www.deGruyter.com, 2003.

[RU87] R. Remmert and P. Ullrich, *Elementare Zahlentheorie*, Birkhäuser Verlag, Basel, 1987.

[Wil99] W. Willems, *Codierungstheorie*, de Gruyter, Berlin, New York, 1999.