KAPITEL 3

Ausgewählte Kapitel der Diskreten Mathematik

1. Graphen

1.1. Definition eines Graphen.

DEFINITION 3.1. Ein *Graph* ist ein Tripel (V, E, I), wobei V, E endliche Mengen sind, $V \neq \emptyset$, $I \subseteq V \times E$, und für alle $e \in E$ die Menge $\{v \in V \mid (v, e) \in I\}$ zweielementig ist. Die Elemente aus V sind die *Knoten*, die Elemente aus E die *Kanten* des Graphen.

Falls $(v, e) \in I$, dann sagen wir, dass die Kante e mit dem Knoten v inzidiert. Falls $x, y \in V$ so sind, dass es ein $e \in E$ gibt, sodass $(x, e) \in I$ und $(y, e) \in I$, dann sagen wir, dass xy eine Kante des Graphen ist.

Ein Graph heißt *einfach*, wenn zwischen zwei Knoten immer höchstens eine Kante verläuft. Unsere Definition eines Graphen lässt keine Schleifen, also Kanten mit dem gleichen Anfangs- und Endpunkt zu.

DEFINITION 3.2. Sei (V, E, I) ein Graph, und sei v ein Knoten des Graphen. Dann ist der *Grad* von v definiert als die Anzahl der Kanten, die mit v inzidieren.

ÜBUNGSAUFGABEN 3.3.

(1) Sei (V, E, I) ein Graph. Zeigen Sie:
$$|I| = \sum_{v \in V} \text{Grad}\,(v).$$
(2) Sei (V, E, I) ein Graph. Zeigen Sie:
$$|I| = 2 \cdot |E|.$$
(3) Zeigen Sie, dass ein Graph eine gerade Anzahl von Knoten ungeraden Grades hat.
(4) Geben Sie eine Definition von Graphen, die Schleifen zulässt. Definieren Sie den Grad eines Knoten so, dass $\sum_{v \in V} \text{Grad}\,(v)$ das Doppelte der Kantenanzahl ist.
(5) Geben Sie eine Definition von Graphen, die Schleifen zulässt, und die es erlaubt, dass zwischen zwei Knoten mehr als eine Kante verläuft. Definieren Sie den Grad eines Knoten so, dass $\sum_{v \in V} \text{Grad}\,(v)$ das Doppelte der Kantenanzahl ist.

1.2. Eulersche Wege.

DEFINITION 3.4. Sei $k \in \mathbb{N}_0$. Eine Folge $(x_0, e_1, x_1, e_2, x_2, \ldots, e_k, x_k)$ heißt *Verbindung der Länge k*, wenn alle x_i Knoten und alle e_k Kanten des Graphen sind, und außerdem für alle $i \in \{1, 2, \ldots, k\}$ die Knoten x_{i-1} und x_i genau die Knoten sind, die mit e_i inzidieren. Eine Verbindung heißt *Weg*, wenn alle e_i voneinander verschieden sind. Ein Weg ist *geschlossen*, wenn $x_k = x_0$.

Zwei Knoten eines Graphen sind *verbunden*, wenn es eine Verbindung mit Anfang x_0 und Ende x_k gibt. Die Relation "verbunden sein" ist eine Äquivalenzrelation auf den Knoten. Ihre Äquivalenzklassen heißen *Zusammenhangskomponenten* des Graphen. Ein Graph mit nur einer Zusammenhangskomponente heißt *zusammenhängend*.

DEFINITION 3.5. Ein geschlossener Weg in einem Graphen heißt *Eulerscher Kreis*, wenn er jede Kante des Graphen genau einmal enthält.

Der Name kommt daher, dass sich Euler überlegt hat, ob es einen Spaziergang über die sieben Brücken Königsbergs gibt, bei dem man über jede Brücke genau einmal geht.

SATZ 3.6. *Ein Graph enthält genau dann einen Eulerschen Kreis, wenn nur höchstens eine Zusammenhangskomponente Kanten enthält, und jeder Knoten geraden Grad hat.*

Beweis: Wir zeigen zunächst, dass die Bedingung, dass jeder Knoten geraden Grad hat, notwendig ist. Sei k die Länge des Weges, sei v ein Knoten, und sei

$$I(v) := \{i \in \{0, \ldots, k-1\} \mid x_i = v\}.$$

Dann inzidiert v mit allen Kanten in $\{e_i \mid i \in I(v)\} \cup \{e_{i+1} \mid i \in I(v)\}$. Der Knoten v inzidiert nur mit Kanten in dieser Menge: Wenn v mit einer Kante e inzidiert, muss e irgendwo im Eulerschen Kreis vorkommen, und somit gleich irgendeinem e_i sein. Dann ist aber entweder x_{i-1} oder x_i gleich v. Außerdem sind für $i, j \in I(v)$ mit $i \neq j$ die Mengen $\{e_i, e_{i+1}\}$ und $\{e_j, e_{j+1}\}$ disjunkt: wenn $e_i = e_{j+1}$, dann gilt auch $i = j + 1$. Somit ist $x_j e_i x_i$ ein Teil des Kreises. Da $x_i = x_j = v$, inzidiert e_i nur mit v – ein Widerspruch zur Schleifenfreiheit des Graphen. Somit inzidiert v mit einer geraden Anzahl von Knoten.

Da ein Eulerscher Kreis nur Knoten der gleichen Zusammenhangskomponente enthält, müssen alle Kanten zwischen Knoten in der gleichen Zusammenhangskomponente verlaufen.

Wir zeigen nun, dass die Bedingung, dass jeder Knoten geraden Grad hat, hinreichend ist. Wir gehen mit Induktion nach der Anzahl der Kanten vor. Wenn der Graph keine Kanten enthält, so sei v ein Knoten. Die Folge (v) ist ein Eulerscher Kreis der Länge 0. Wenn der Graph eine Kante e_1 von x_0 nach x_1 enthält, so

verlängern wir diesen Weg, bis wieder nicht mehr weiter können. Da alle Knoten geraden Grad haben, kann das erst passieren, wenn wir ein k mit $x_k = x_0$ gefunden haben. Wir haben also einen Weg $x_0e_1x_1 \dots e_kx_k$ mit $k \in \mathbb{N}$ gefunden. Wir bilden nun einen neuen Graphen G', indem wir aus G die Kanten $e_1, \dots, e_k$ entfernen. Jeder Knoten von G' hat geraden Grad. Wir können nach Induktionsvoraussetzung in jeder Zusammenhangskomponente Z von G', die zumindest eine Kante enthält, einen Eulerschen Kreis $C(Z)$ finden. Jede dieser Komponenten enthält zumindest ein x_i, und dann auch eine damit inzidierende Kante. Also können wir jeden Kreis $C(Z)$ an den Kreis $x_0e_1 \cdots x_k$ anhängen. □

1.3. Planare Graphen.

DEFINITION 3.7. Ein Graph ist *planar*, wenn er sich in $\mathbb{R}^2$ "überschneidungsfrei zeichnen lässt".

DEFINITION 3.8. Ein ebener Graph ist ein Paar (G, Z), wobei G ein planarer Graph und Z eine überschneidungsfreie Zeichnung von G in $\mathbb{R}^2$ ist.

SATZ 3.9 (Euler). *Sei G ein zusammenhängender, ebener Graph mit v Knoten und e Kanten, der die Ebene in f Flächen unterteilt. Dann gilt*

$$v - e + f = 2.$$

Beweisskizze: Wir zeigen, dass für jeden ebenen Graphen mit z Zusammenhangskomponenten die Gleichung $v - e + f = 1 + z$ gilt. Das kann man durch Induktion nach der Kantenanzahl zeigen. □

SATZ 3.10. *Sei G ein einfacher planarer Graph. Dann hat G einen Knoten, dessen Grad höchstens 5 ist.*

Beweis: ([**Aigner and Ziegler, 1998**]) Sei G ein einfacher ebener Graph, und seien v, e, f die Anzahl der Knoten, Kanten, Flächen. Wir nehmen $v \geq 3$ an. Wir bilden die Menge

$$F = \{(x, y, a) \mid x \in V, y \in V, xy \text{ ist Kante von } V, \\ a \text{ liegt rechts von } xy, \text{ wenn man von } x \text{ nach } y \text{geht.}\}$$

Für jede Fläche a definieren wir die Menge seiner Begrenzungsseiten als

$$\{(x, y) \in V^2 \mid (x, y, a) \in F\}.$$

Für jedes $i \in \mathbb{N}$ sei f_i die Anzahl der Flächen mit genau i Begrenzungsseiten. Es gilt

$$f = \sum_{i \in \mathbb{N}} f_i,$$

$$|F| = 2e,$$

und

$$|F| = \sum_{i \in \mathbb{N}} f_i \cdot i.$$

Da G einfach ist, gilt $f_1 = f_2 = 0$, und somit

$$2e - 3f \geq 0.$$

Für jedes $i \in \mathbb{N}$ sei v_i die Anzahl der Knoten vom Grad i. Für die Inzidenzrelation I zwischen Knoten und Kanten gilt

$$|I| = 2e$$

und

$$|I| = \sum_{i \in \mathbb{N}} v_i \cdot i.$$

Ausserdem gilt

$$\sum_{i \in \mathbb{N}} v_i = v.$$

Wenn wir annehmen, dass alle Knoten Grad ≥ 6 haben, so gilt $v_1 = v_2 = \cdots = v_5 = 0$. Also gilt $2e - 6v \geq 0$. Also gilt $(2e - 6v) + 2(2e - 3f) \geq 0$, somit $v - e + f \leq 0$ im Widerspruch zur Eulerschen Flächenformel. □

Übungsaufgaben 3.11.

(1) [**Aigner and Ziegler, 1998**, p.59] Sei G ein einfacher planarer Graph mit $v \geq 3$ Knoten und e Kanten. Dann gilt $e \leq 3v - 6$.
(2) [**Aigner and Ziegler, 1998**, p.59] Zeigen Sie, dass die Graphen K_5 (der vollständige Graph mit 5 Knoten) und $K_{3,3}$ (der vollständige bipartite Graph mit 2 mal 3 Knoten) nicht planar sind.

Satz 3.12. *Sei G ein einfacher planarer Graph. Dann kann man die Knoten von G so mit 6 Farben färben, dass keine zwei Knoten, zwischen denen eine Kante verläuft, die gleiche Farbe haben.*

Es reichen sogar 4 (statt 6) Farben (*Vierfarbensatz*).

2. Der Satz von Ramsey

Für eine Menge X und eine Zahl $p \in \mathbb{N}$ bezeichnen wir mit $\binom{X}{p}$ die Menge aller p-elementigen Teilmengen von X. Eine *Partition* einer Menge U in t Teilmengen ist (in diesem Kapitel) eine Folge $(A_1, A_2, \ldots, A_t)$ von Teilmengen von U, sodass $A_1 \cup A_2 \cup \cdots \cup A_t = U$ ist, und für alle $i, j \in \{1, 2, \ldots, t\}$ mit $i \neq j$ die Menge $A_i \cap A_j$ leer ist.

Satz 3.13. *Seien $p, t, n \in \mathbb{N}$. Dann gibt es eine Zahl $N \in \mathbb{N}$, sodass folgendes erfüllt ist:*

Für jede Menge X mit $|X| \geq N$ und jede Partition von $\binom{X}{p}$ in t Teilmengen der Form

$$\binom{X}{p} = A_1 \cup A_2 \cup \cdots \cup A_t$$

gibt es eine n-elementige Teilmenge Y von X und ein $j \in \{1, 2, \ldots, t\}$, sodass $\binom{Y}{p} \subseteq A_j$. (Das heißt, dass alle alle p-elementigen Teilmengen von Y in der gleichen Klasse der Partition sind).

Äquivalent ist:

SATZ 3.14. *Seien $p, t, n \in \mathbb{N}$. Dann gibt es eine Zahl $N \in \mathbb{N}$, sodass folgendes erfüllt ist:*

Sei X eine Menge mit N Elementen. Wir färben jede p-elementige Teilmenge von X mit einer von t Farben. Dann gibt es eine Menge $Y \subseteq X$ mit n Elementen, sodass alle p-elementigen Teilmengen von Y die gleiche Farbe haben.

Das kleinste N, für das die Aussage erfüllt ist, bezeichnen wir mit $r(p, t, n)$ (Ramsey-Zahl).

Wir betrachten Spezialfälle:

- $p = 1, n = 2$: Es gibt ein N, sodass für jede Menge X mit N Elementen folgendes gilt: Wenn man die Elemente von X in t Klassen aufteilt, so gibt es zwei Elemente, die in der gleichen Klasse liegen. Daraus sehen wir $r(1, t, 2) = t + 1$. (Schubfachprinzip)

ÜBUNGSAUFGABEN 3.15.

(1) Berechnen Sie $r(1, t, n)$ für alle $t, n \in \mathbb{N}$.

Weitere Spezialfälle:

- $p = 2, t = 2, n = 3$: Man weiß, dass $r(2, 2, 3) = 6$ ist. Das heißt:
  Wenn man jede 2-elementige Teilmengen einer 6-elementigen Menge entweder rot oder blau färbt, dann gibt es drei Elemente a, b, c, sodass $\{a, b\}$, $\{a, c\}$ und $\{b, c\}$ die gleiche Farbe haben.

  Das kann man auch so formulieren:
  Sei K_6 der vollständige Graph mit 6 Knoten und $\binom{6}{2}$ Kanten. Wir färben jede Kante entweder rot oder blau. Dann enthält der Graph ein einfärbiges Dreieck, also drei Knoten x, y, z, sodass xy, xz und yz die gleiche Farbe haben.

ÜBUNGSAUFGABEN 3.16.

(1) Zeigen Sie $r(2, 2, 3) \leq 6$.

(2) Zeigen Sie $r(2,3,3) \leq 17$.
(3) Zeigen Sie $r(2,k,3) \leq (r(2,k-1,3)-1) \cdot k + 2$.
(4) (Lästiger Spezialfall I) Berechnen Sie $r(p,t,p)$!
(5) (Lästiger Spezialfall II) Sei $p \leq n$. Was ist $r(p,1,n)$?
(6) (Lästiger Spezialfall III) Sei $p > n$. Was ist $r(p,t,n)$?

LEMMA 3.17. *Seien $p,t \in \mathbb{N}$. Dann sind folgende Aussagen äquivalent:*

(1) *Für alle $n \in \mathbb{N}$ gibt es ein $N \in \mathbb{N}$, sodass es für jede Färbung der p-elementigen Teilmengen von $\{1,2,\ldots,N\}$ mit t Farben eine n-elementige Teilmenge Y von $\{1,2,\ldots,N\}$ gibt, sodass alle p-elementigen Teilmengen von Y die gleiche Farbe haben.*
(2) *Für alle $n \in \mathbb{N}$ gibt es ein $M \in \mathbb{N}$, sodass folgendes gilt: für jede M-elementige Teilmenge X der natürlichen Zahlen und für jede Färbung der p-elementigen Teilmengen von X mit t Farben gibt es eine n-elementige Teilmenge Y von X, sodass alle p-elementigen Teilmengen von Y, die das gleiche minimale Element haben, die gleiche Farbe haben.*

Beweis: (2) $\Rightarrow$ (1): Wir fixieren $n \in \mathbb{N}$. Wegen (2) gibt es ein M, sodass es für jede Färbung der p-elementigen Teilmengen von $\{1,2,\ldots,M\}$ mit t Farben eine $t(n-1)+1$-elementige Teilmenge Y von $\{1,2,\ldots,M\}$ gibt, sodass alle p-elementigen Teilmengen von Y, die das gleiche minimale Element haben, die gleiche Farbe haben. Wir behaupten, dass $N := M$ in (1) das Gewünschte leistet. Wir fixieren eine Färbung der p-elementigen Teilmengen von $\{1,2,\ldots,M\}$ mit t Farben, und wählen eine $(t(n-1)+1)$-elementige Teilmenge Y wie oben. Für jede Farbe f der t Farben definieren wir die Menge $M_f := \{x \in Y \mid \text{jede } p\text{-elementige Teilmenge von } Y \text{ mit } x \text{ als minimalem Element hat die Farbe } f\}$. Eine der Mengen M_f hat zumindest n Elemente. Alle p-elementigen Teilmengen von M_f haben dann die gleiche Farbe. □

Beweis des Satzes von Ramsey: Wir definieren ein Prädikat

$$G(p,t,n)$$

dadurch, dass $G(p,t,n)$ wahr ist, wenn der Satz von Ramsey für p,t,n gilt, das heißt, wenn es ein N gibt, sodass für alle N-elementigen Mengen und alle Färbungen der p-elementigen Teilmengen .... Wir wissen, dass z.B. $G(2,2,3)$ wahr ist.

Wir beweisen jetzt, dass $G(p,t,n)$ für alle $p,t,n \in \mathbb{N}$ gilt, durch Induktion nach p.

- $p = 1$: Wir fixieren $t,n \in \mathbb{N}$. Dann leistet $N := t(n-1)+1$ das Gewünschte.
- Wir fixieren $p \geq 2$ und $t \in \mathbb{N}$. Wir zeigen nun, dass die Eigenschaft (2) aus Lemma 3.17 gilt. Wir zeigen diese Eigenschaft durch Induktion nach n.

- Für $n \leq p$ leistet $M := p$ das Gewünschte.
- Wir fixieren $n > p$. Mit der Induktionsvoraussetzung produzieren wir ein M für $n-1$. Wir behaupten nun, dass

$$M' := 1 + r(p-1, t, M)$$

das Gewünschte leistet. Wir fixieren dazu eine Färbung der p-elementigen Teilmengen von $X = \{1, 2, \ldots, M'\}$ mit t Farben.
Wir geben nun jeder $p-1$-elementigen Teilmenge Z von $X \setminus \{1\}$ die Farbe von $\{1\} \cup Z$. Wir finden dann (wegen der Induktionsvoraussetzung der Induktion nach p) eine M-elementige Teilmenge A von $X \setminus \{1\}$, sodass alle $p-1$-elementigen Teilmengen von A die gleiche Farbe haben.
Wir wählen nun nach Induktionsvoraussetzung (der Induktion nach n) eine $(n-1)$-elementige Teilmenge B von A, sodass alle p-elementigen Teilmengen von B mit dem gleichen minimalen Element die gleiche Farbe haben.
Wir behaupten, dass $B \cup \{1\}$ das Gewünschte leistet. Wir wählen dazu zwei p-elementige Teilmengen P_1, P_2 von $B \cup \{1\}$ mit dem gleichen minimalen Element. Ist dieses Element 1, so haben P_1, P_2 die gleiche Farbe, da alle p-elementigen Teilmengen von $A \cup \{1\}$, die 1 enthalten, die gleiche Farbe haben.
Ist dieses Element nicht 1, dann sind P_1, P_2 beide p-elementige Teilmengen von B und haben daher die gleiche Farbe. □

Satz 3.18 (Erdős-Szekeres). *Sei $n \in \mathbb{N}$. Dann gibt es eine Zahl N, sodass jede Menge von N Punkten in der Ebene, von denen keine drei auf einer Geraden liegen, n Punkte enthält, die die Eckpunkte eines konvexen n-Ecks sind.*

Hinweis zum Beweis: Für $n = 4$ funktioniert $N := 5$. Für $n > 4$ kann man $N := r(4, 2, n)$ wählen.

Satz 3.19. *Sei $t \in \mathbb{N}$. Dann gibt es ein N, sodass es für jede Gruppe $\mathbf{G}$ mit mehr als N Elementen und jede Aufteilung von $G \setminus \{1\}$ in t Klassen eine Klasse gibt, die drei verschiedene Elemente x, y, z mit $z = x \cdot y$ enthält.*

Hinweis zum Beweis: $N := r(2, t, 4) + 1$. Sei $G = \{1, x_1, \ldots, x_N\}$ Wir färben die Menge $\{x_i, x_j\}$ mit der Farbe von $x_{\min(i,j)}^{-1} \cdot x_{\max(i,j)}$. □

Übungsaufgaben 3.20.

(1) Sei $t \in \mathbb{N}$. Zeigen Sie, dass es eine Zahl N gibt, sodass für jede Aufteilung der Menge $\{1, 2, \ldots, N\}$ in t Klassen es eine Klasse gibt, die zwei verschiedene Zahlen und deren Summe enthält.
(2) Zeigen Sie den "unendlichen" Satz von Ramsey:

> Sei M eine unendliche Menge. Wir färben jede p-elementige Teilmenge von M mit einer von endlich vielen Farben. Dann gibt es eine unendliche Teilmenge T von M, sodass alle p-elementigen Teilmengen von T die gleiche Farbe haben.

Hinweis: Nehmen Sie an, M sei abzählbar unendlich. Gehen Sie mit Induktion nach p vor. Konstruieren Sie eine Folge $(a_1, a_2, \ldots)$ von Elementen in M, sodass alle Teilmengen von $\{a_i \mid i \in \mathbb{N}\}$, die das gleiche "minimale Element" besitzen, die gleiche Farbe haben. (Der Beweis steht auch im Artikel "Ramsey's Theorem" in `http://en.wikipedia.org/wiki`.)

(3) Verwenden Sie Übung (2), um zu zeigen, dass jede reelle Zahlenfolge eine monoton fallende oder eine streng monoton steigende Teilfolge enthält.

(4) (Dixons Lemma) Für zwei Vektoren $v, w \in \mathbb{N}_0^k$ schreiben wir $v \leq' w$ falls für alle $i \in \{1, \ldots, k\} : v_i \leq w_i$. Sei $(v_1, v_2, \ldots)$ eine Folge von Vektoren in $\mathbb{N}_0^k$. Dann gibt es eine (unendliche) Teilfolge, die bezüglich $\leq'$ schwach monoton aufsteigend ist. *Hinweis:* Verwenden Sie den unendlichen Ramseysatz für eine bestimmte Färbung von Paaren von Vektoren mit 2^k Farben.

KAPITEL 4

Polynome und Körper

1. Körper

DEFINITION 4.1. Ein kommutativer Ring mit Eins $\mathbf{R} = (R, +, -, \cdot, 0, 1)$ ist ein *Körper* wenn

(1) $|R| \geq 2$,
(2) Für alle $x \in R \setminus \{0\}$ gibt es ein $y \in R$ mit $x \cdot y = 1$.

ÜBUNGSAUFGABEN 4.2.

(1) Zeigen Sie, dass es in einem Körper für jedes x höchstens ein y mit $x \cdot y = 1$ geben kann.
(2) Zeigen Sie, dass das Produkt zweier Elemente in einem Körper nur dann 0 ist, wenn einer der Faktoren gleich 0 ist.

In einem Körper hat jedes Element $a \neq 0$ genau ein multiplikativ inverses Element; wir bezeichnen es mit a^{-1}. Für jede Primzahl p ist der Ring $\mathbb{Z}_p$ ein Körper.

DEFINITION 4.3. Sei $\mathbf{E} = (E, +, -, \cdot, 0, 1)$ ein Körper, und sei $K \subseteq E$. Die Menge K ist dann *Trägermenge eines Unterkörpers* von $\mathbf{E}$, 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 $x \in K \setminus \{0\}$ gilt $x^{-1} \in K$.

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

ÜBUNGSAUFGABEN 4.4.

(1) Zeigen Sie: Der Durchschnitt beliebig vieler Trägermengen von Unterkörpern eines Körpers ist wieder Trägermenge eines Unterkörpers.
(2) Sei $\mathbf{E}$ 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 Trägermenge eines Unterkörpers von $\mathbf{E}$ ist.

2. Polynome

DEFINITION 4.5. Sei $\mathbf{K}$ kommutativer Ring mit Eins. Dann ist $K[t] := \{a \in K^{\mathbb{N}_0} \mid \exists i \in \mathbb{N}\ \forall j \in \mathbb{N} : j \geq i \Rightarrow a_j = 0\}$.

DEFINITION 4.6. Addition und Multiplikation auf $K[t]$.

DEFINITION 4.7. Sei $f \in K[t]$. $\deg f := \ldots$, $\deg 0 := -1$.

Mit $t = (0, 1, 0, \ldots)$ gilt $a = (a_0, a_1, \ldots) = \sum_{i=0}^{\deg a} a_i t^i$.

DEFINITION 4.8. Sei $\mathbf{K}$ Körper, und seien $f, g \in K[t]$.

(1) f *teilt* g, wenn es $q \in K[t]$ gibt, sodass $g = q \cdot f$.
(2) f ist *invertierbar*, wenn $\deg f = 0$.
(3) f ist *irreduzibel über* $\mathbf{K}$ (ein irreduzibles Polynom in $K[t]$), wenn $\deg f \geq 1$ und für alle $a, b \in K[t]$ mit $a \cdot b = f$ entweder a oder b Grad 0 hat.
(4) f ist *normiert*, wenn es führenden Koeffizienten 1 hat.

SATZ 4.1. *Sei* $\mathbf{K}$ *Körper, und seien* $f, g \in K[t]$. *Wenn* $f \neq 0$, *so gibt es* $q, r \in K[t]$ *mit* $g = q \cdot f + r$ *und* $\deg r < \deg f$.

DEFINITION 4.9. Sei $(R, +, \cdot)$ ein Ring, und sei $I \subseteq R$. I ist ein *Ideal* von $\mathbf{R}$, wenn für alle $i, j \in I$ und $r \in R$ gilt: $i - j \in I$, $r \cdot i \in I$, $i \cdot r \in I$.

Kongruenzrelationen und Ideale eines Ringes sind einander durch $\alpha \mapsto 0/\alpha$ bijektiv zugeordnet.

SATZ 4.2 ($\mathbf{K}[t]$ ist Hauptidealbereich). *Sei* $\mathbf{K}$ *ein Körper, und sei* I *ein Ideal von* $\mathbf{K}[t]$. *Dann gibt es* $f \in K[t]$ *mit* $I = \{p \cdot f \mid p \in K[t]\} = (f)$.

Wenn $I \neq 0$, *dann gilt für jedes* f *mit* $\deg f = \min\{\deg i \mid i \in I \setminus \{0\}\}$, *dass* $I = (f)$.

SATZ 4.3 (ggT in $\mathbf{K}[t]$). *Sei* $\mathbf{K}$ *ein Körper, und seien* $f, g \in K[t]$, *nicht beide* 0. *Dann gibt es genau ein* $d \in K[t]$, *sodass*

(1) $d|f$, $d|g$.
(2) *Für alle* u *mit* $u|f$ *und* $u|g$ *gilt* $u|d$.
(3) d *ist normiert.*

Dieses d *heißt der* ggT *von* f *und* g. *Es gibt* $u, v \in K[t]$, *sodass* $u \cdot f + v \cdot g = d$.

Beweisskizze: Wir wählen für d einen normierten Erzeuger des Ideals $I = \{u \cdot f + v \cdot g \mid u, v \in K[t]\}$.

SATZ 4.4. *Sei* $\mathbf{K}$ *Körper,* $f \in K[t]$ *irreduzibel über* $\mathbf{K}$. *Dann ist* $\mathbf{K}[t]/(f)$ *ein Körper.*

3. Zerfällungskörper

SATZ 4.5. *Sei* $\mathbf{K}$ *ein Körper, und sei* f *ein normiertes Polynom in* $\mathbf{K}[t]$ *vom Grad* n*. Dann gibt es einen Erweiterungskörper* $\mathbf{E}$ *von* $\mathbf{K}$*, sodass jeder in* $\mathbf{E}[t]$ *irreduzible Teiler von* f *Grad* 1 *hat.*

Beweis: Wir beweisen folgende Aussage durch Induktion nach n:

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

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

DEFINITION 4.10. Sei $\mathbf{F}$ ein Körper, und sei $f \in F[t]$, $n := \deg f \geq 1$, und sei $\mathbf{E}$ ein Körper. $\mathbf{E}$ heißt *Zerfällungskörper* von f über $\mathbf{F}$, wenn er ein Erweiterungskörper von $\mathbf{F}$ ist, und es $a, e_1, \ldots, e_n \in E$ gibt, sodass

$$f = a \prod_{i=1}^{n} (t - e_i),$$

und $\mathbf{E}$ der von F und $\{e_1, e_2, \ldots, e_n\}$ erzeugte Unterkörper von $\mathbf{E}$ ist.

SATZ 4.6. *Für jedes nichtkonstante Polynom* f *über einem Körper* $\mathbf{K}$ *gibt es einen Zerfällungskörper von* f *über* $\mathbf{K}$*.*

[1] $\mathbf{L}$ ist zunächst kein Erweiterungskörper von $\mathbf{K}$, da K keine Teilmenge von L ist. Man kann aber leicht einen Körper $\mathbf{L}'$ angeben, der zu $\mathbf{L}$ isomorph ist, und $\mathbf{K}$ als Unterkörper enthält, indem man in $\mathbf{L}$ jedes konstante Polynom $(k_0, 0, 0, \ldots)$ durch k_0 ersetzt.

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

DEFINITION 4.11. Sei $a = \sum_{i=1}^{n} a_i t^i \in \mathbb{Z}[t]$, $a \neq 0$. Wir definieren den *Inhalt von* a durch $\operatorname{cont}(a) := \operatorname{ggT}(a_0, a_1, \ldots, a_n)$.

LEMMA 4.12. *Seien* $f, g \in \mathbb{Z}[t] \setminus \{0\}$. *Dann gilt* $\operatorname{cont}(f \cdot g) = \operatorname{cont}(f) \cdot \operatorname{cont}(g)$.

SATZ 4.7. *Sei* $f \in \mathbb{Z}[t] \setminus \{0\}$, *seien* $g, h \in \mathbb{Q}[t]$ *so, dass* $f = g \cdot h$, *und seien* $\alpha, \beta \in \mathbb{Z}$ *so, dass* $\alpha\, g \in \mathbb{Z}[t]$ *und* $\beta\, h \in \mathbb{Z}[t]$. *Wir setzen:*

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

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

SATZ 4.8 (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) $p | a_0, \ldots, p | a_{n-1}$,
(2) $p \nmid a_n$,
(3) $p^2 \nmid a_0$.

Dann ist a *ein in* $\mathbb{Q}[t]$ *irreduzibles Polynom.*

SATZ 4.9. *Sei* $a \in \mathbb{Z}[t]$, $n := \deg a$, *und sei* r *eine rationale Nullstelle von* $a = a_0 t^0 + \cdots + a_n t^n$. *Dann gibt es* $p, q \in \mathbb{Z}$, *sodass* $r = \frac{p}{q}$ *und* $p | a_0$, $q | a_n$.

KAPITEL 5

Endliche Körper

1. Primkörper

Der Durchschnitt aller Unterkörper eines Körpers $\mathbf{E}$ ist wieder ein Körper, er heißt *Primkörper* von $\mathbf{E}$.

SATZ 5.1. *Sei* $\mathbf{E}$ *ein endlicher Körper. Dann gibt es eine Primzahl* p*, sodass der Primkörper von* $\mathbf{E}$ *isomorph zu* $\mathbb{Z}_p$ *ist.*

Beweis: Offensichtlich sind alle $a * 1$ mit $a \in \mathbb{Z}$ in jedem Unterkörper von $\mathbf{E}$ enthalten. Da $\mathbf{E}$ endlich ist, gibt es $a, b \in \mathbb{N}$ mit $a > b$ und $a * 1 = b * 1$, also $(a - b) * 1 = 0$. Wir zeigen nun, dass

$$\min\{n \in \mathbb{N} \mid n * 1 = 0\}$$

eine Primzahl ist. Sei p dieses Minimum. Wenn es $c, d < p$ gibt, sodass $cd = p$, dann gilt $(c*1)\cdot(d*1) = 0$, also entweder $c*1 = 0$ oder $d*1 = 0$. Das widerspricht der Minimalität von p. Die Abbildung

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

ist ein Ring mit Eins-Homomorphismus. Sie hat den Primkörper von $\mathbf{E}$ als Bild, ihr Kern ist $p\mathbb{Z}$. Der Primkörper von $\mathbf{E}$ ist also isomorph zu $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$. □

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

ÜBUNGSAUFGABEN 5.2.

(1) Bestimmen Sie den Primkörper des Körpers der komplexen Zahlen.
(2) Zeigen Sie, dass der Primkörper eines beliebigen Körpers entweder isomorph zu $\mathbb{Z}_p$ für irgendeine Primzahl p, oder isomorph zu $\mathbb{Q}$ ist.

SATZ 5.3. *Die Anzahl der Elemente eines endlichen Körpers ist eine Primzahlpotenz.*

Wir beweisen folgende stärkere Aussage:

SATZ 5.4. *Sei* $\mathbf{K}$ *ein Unterkörper des endlichen Körpers* $\mathbf{E}$*. 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 E hat E 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 5.4 folgt nun, wenn man als **K** den Primkörper von **E** wählt.

Satz 5.5. *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 5.6.

(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 $f \in \mathbf{K}[x]$. 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 $\mathbf{K}[x]$ ist.
(3) Zeigen Sie, dass ein Polynom in $\mathbf{K}[x]$ 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: $(\alpha + \beta)^p = \alpha^p + \beta^p$.

2. Die multiplikative Gruppe eines endlichen Körpers

Satz 5.7. *Die multiplikative Gruppe eines endlichen Körpers ist zyklisch.*

Wir zeigen diesen Satz mithilfe des folgenden Satzes.

SATZ 5.8. *Sei* $\mathbf{A} = (A, \cdot)$ *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* $\mathbf{A}$ *zyklisch.*

Beweis: Sei $h := |A|$. Falls $h = 1$, ist $\mathbf{A}$ 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)

$$ {b_i}^{{p_i}^{r_i}} = 1. \tag{2.1}$$

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

$$s_i = r_i. \tag{2.2}$$

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 (2.2). 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

$$\prod_{i=1}^{N} {b_i}^{\frac{h}{p_j}} = 1. \tag{2.3}$$

Falls $i \neq j$, so gilt ${p_i}^{r_i} | \frac{h}{p_j}$. Wegen (2.1) sind also Faktoren in (2.3) mit $i \neq j$ gleich 1. Wir erhalten also

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

Da b_j wegen (2.2) die Ordnung ${p_j}^{r_j}$ hat, gilt ${p_j}^{r_j}|\frac{h}{p_j}$. Daher gilt ${p_j}^{r_j+1}|h$, 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 $\mathbf{A}$. □

Aus dem Satz 5.8 folgt nun direkt der Satz 5.7, da in jedem Körper und für jedes n das Polynom $x^n - 1$ höchstens n Nullstellen hat.

Übungsaufgaben 5.9.

(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.

3. Körper aus irreduziblen Polynomen

Satz 5.10. *Sei* $\mathbf{K}$ *ein Körper, und sei* $f \in \mathbf{K}[x]$ *irreduzibel über* $\mathbf{K}$*. Dann ist* $\mathbf{K}[x]/(f)$ *ein Körper.*

Als Quotient eines kommutativen Ringes mit 1 ist $\mathbf{K}[x]/(f)$ wieder ein kommutativer Ring mit 1. Es reicht also zu zeigen, dass jedes $h \in \mathbf{K}[x]/(f)$ mit $h \neq 0+(f)$ invertierbar ist. Sei $h' \in \mathbf{K}[x]$ so, dass $h = h' + (f)$. Da f irreduzibel ist, und h' kein Vielfaches von f ist, gilt $\mathrm{ggT}\,(h', f) = 1$. Es gibt also $u, v \in \mathbf{K}[x]$, sodass $u \cdot h' + v \cdot f = 1$. Es gilt also $(u+(f)) \cdot (h'+(f)) = u \cdot h' + (f) = (1 - v \cdot f) + (f) = 1 + (f)$. □

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

Satz 5.11. *Sei* $\mathbf{K}$ *ein endlicher Körper mit* q *Elementen, und sei* f *ein irreduzibles Polynom vom Grad* n*. Dann gilt* $f|x^{q^n} - x$*.*

Wir betrachten den Körper $\mathbf{K}[x]/(f)$. Dieser Körper hat q^n Elemente. Es gilt also wegen Satz 5.5 (2) $(x + (f))^{q^n} = x + (f)$. Das bedeutet

$$f|x^{q^n} - x. \quad \square$$

Satz 5.12. *Sei* $\mathbf{K}$ *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 5.5. Die Differenz dieser beiden Polynome hat also mindestens q Nullstellen, und einen Grad $\leq q - 1$. Die Differenz ist also das Nullpolynom. □

Lemma 5.13. *Sei* $\mathbf{K}$ *ein endlicher Körper mit* q *Elementen, sei* $m \in \mathbb{N}$*, und sei* f *ein über* $\mathbf{K}$ *irreduzibles Polynom vom Grad* m*. Sei* $\mathbf{E}$ *ein Erweiterungskörper*

von $\mathbf{K}$ *mit* q^m *Elementen. Dann zerfällt* f *in* $\mathbf{E}[x]$ *in ein Produkt lauter linearer Polynome.*

Beweis: Da $\deg f = m$, gilt nach Satz 5.11, dass f das Polynom $x^{q^m} - x$ teilt. Nach Satz 5.12 gilt

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

Das Polynom f ist auch ein Polynom in $\mathbf{E}[x]$. Jeder über $\mathbf{E}$ irreduzible Teiler von f in $\mathbf{E}[x]$ teilt also eines der Polynome in $\{x - b \mid b \in E\}$. Das bedeutet, dass f in $\mathbf{E}[x]$ 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 5.14. *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 $\mathbf{E}$ ein Körper mit q Elementen. Aus dem Lemma 5.13 wissen wir, dass f eine Nullstelle in $\mathbf{E}$ 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 $\{g \in \mathbb{Z}_p[x] \mid g(b) = 0\}$. Sei h der normierte Erzeuger des Ideals $\ker \Phi$. Da $f \in \ker \Phi$, gilt $h | f$. 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 $h | f$ widerspricht. Also ist $h = f$. Es gilt also nach dem Homomorphiesatz, dass $\mathbb{Z}_p[x]/(f)$ isomorph zu $\mathbf{E}$ ist. □

4. Existenz irreduzibler Polynome

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

Satz 5.15. *Sei* $\mathbf{K}$ *ein Körper, und sei* f *ein normiertes Polynom in* $\mathbf{K}[x]$ *vom Grad* n*. Dann gibt es einen Erweiterungskörper* $\mathbf{E}$ *von* $\mathbf{K}$*, sodass jeder in* $\mathbf{E}[x]$ *irreduzible Teiler von* f *Grad* 1 *hat.*

Wir beweisen folgende Aussage durch Induktion nach n:

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

Für $n = 1$ ist die Aussage klar. Wir fixieren nun einen Körper $\mathbf{K}$ und ein Polynom $f \in \mathbf{K}[x]$ mit $\deg f = n > 1$. Wir zerlegen f in ein Produkt von normierten, über $\mathbf{K}$ irreduziblen Polynomen in $\mathbf{K}[x]$. Sei g einer der irreduziblen Faktoren. Wir bilden den Körper $\mathbf{L} := \mathbf{K}[x]/(g)$. 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 $\mathbf{K}[x]/(g)$ 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 $g | f$, gilt $f + (g) = 0 + (g)$. Also ist $x + (g)$ eine Nullstelle von f un $\mathbf{L}$. Da f eine Nullstelle l in $\mathbf{L}$ hat, gibt es $h \in \mathbf{L}[x]$, sodass $f = (x - l) \cdot h$. Da h kleineren Grad als f hat, gibt es nach nach Induktionsvorraussetzung einen Erweiterungskörper $\mathbf{M}$ von $\mathbf{L}$, sodass jeder in $\mathbf{M}[x]$ irreduzible Teiler des Polynoms h Grad 1 hat. In $\mathbf{M}[x]$ hat jeder irreduzible Teiler von f also Grad 1. □

Satz 5.16. *Sei* $\mathbf{K}$ *ein endlicher Körper, und sei* $n \in \mathbb{N}$. *Dann gibt es ein über* $\mathbf{K}$ *irreduzibles Polynom vom Grad* n *in* $\mathbf{K}[x]$.

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

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

Mit Satz 5.5 (1) erhalten wir, dass $\mathbf{L}$ ein Unterkörper von $\mathbf{E}$ ist; mit mit Satz 5.5 (2), dass $\mathbf{L}$ ein Erweiterungskörper von $\mathbf{K}$ ist. Da $x^{q^n} - x$ über $\mathbf{E}$ in lauter Linearfaktoren zerfällt, gibt es $e_1, e_2, \ldots, e_{q_n} \in E$, sodass

$$x^{q^n} - x = \prod_{r=1}^{q^n} (x - e_r).$$

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

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

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

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

(4.1) f ist ein irreduzibles Element von $\mathbf{K}[x]$.

Wir nehmen an, es gibt normierte $f_1, f_2 \in \mathbf{K}[x]$ 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 $f | f_1$, und somit $f_2 = 1$. Das beweist (4.1).

Die Abbildung

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

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

Literaturverzeichnis

[Aigner and Ziegler, 1998] Aigner, M. and Ziegler, G. M. (1998). *Proofs from THE BOOK*. Springer Berlin-Heidelberg.

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

[Euklid, 1991] Euklid (1991). *Die Elemente*. Wissenschaftliche Buchgesellschaft, Darmstadt. Buch I–XIII. [Book I–XIII], Based on Heiberg's text, Translated from the Greek and edited by Clemens Thaer.

[GAP, 1999] GAP (1999). *GAP – Groups, Algorithms, and Programming, Version 4.1*. The GAP Group, Aachen, St. Andrews. (`http://www-gap.dcs.st-and.ac.uk/~gap`).

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

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

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

[Rivest et al., 1978] Rivest, R. L., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM*, 21(2):120–126.

[Robinson, 2003] Robinson, D. J. S. (2003). *An Introduction to Abstract Algebra*. Walter de Gruyter, Berlin – New York, www.deGruyter.com.

[Rotman, 1998] Rotman, J. J. (1998). *Galois theory*. Springer-Verlag, New York, second edition.