Kapitel 5

Der Euklidische Algorithmus

In diesem Kapitel stellen wir noch einen weiteren wichtigen Algorithmus vor, der sowohl für ganze Zahlen als auch Polynomringe anwendbar ist. Später werden wir sehen, dass er auch in allgemeineren Ringen Anwendung findet.

5.1 Der Ring der ganzen Zahlen

Lernziele

- Lineare Gleichungssysteme über $\mathbb{Z}$,
- Euklidische Algorithmus über $\mathbb{Z}$,
- Invertieren in $\mathbb{Z}/n\mathbb{Z}$.

In dieser Sektion betrachten wir den Ring $\mathbb{Z}$ der ganzen Zahlen. Wir wollen Gleichungen der Form $ax = b$ für gegebene $a, b \in \mathbb{Z}$ über $\mathbb{Z}$ lösen und untersuchen, wann ein Element $a \in \mathbb{Z}_n$ ein Inverses in $\mathbb{Z}_n$ besitzt.

Definition 5.1

Seien $x \in \mathbb{R}$. Wir schreiben

$$|x| := \begin{cases} x, & \text{falls } x \geq 0 \\ -x, & \text{falls } x < 0 \end{cases}$$

für den **Absolutbetrag** von x.

In den ganzen Zahlen können wir eine Zahl durch eine andere mit

Rest dividieren:

Bemerkung 5.2

Seien $a, b \in \mathbb{Z}$. Dann gibt es eindeutige $q, r \in \mathbb{Z}$ mit

$$a = qb + r \text{ und } 0 \leq r < |b|$$

r heißt auch der kleinste nicht negative **Rest** von a modulo b. Abkürzung: $r = a \pmod{b}$. Falls $r = 0$ gilt, sagt man b **teilt** a oder b ist ein **Teiler** von a, kurz $b|a$.

Definition 5.3: ggT

Für zwei ganze Zahlen $a, b \in \mathbb{Z}$ mit $(a, b) \neq (0, 0)$ heißt die positive ganze Zahl t mit

a) $t|a$ und $t|b$,

b) für alle $c \in \mathbb{Z}$ mit $c|a$ und $c|b$ gilt $c|t$.

der **größte gemeinsame Teiler (ggT)** von a und b. Notation: $t = ggT(a, b)$. Ist $t = 1$, so sagt man auch, dass a und b **teilerfremd** oder **relativ prim** sind.

Der EUKLIDische[1] Algorithmus berechnet für zwei ganze Zahlen $a, b \in \mathbb{Z}$ den größten gemeinsamen Teiler t von a und b.

Algorithmus 5.4: EUKLIDischer Algorithmus, 1. Teil

Eingabe: $a, b \in \mathbb{Z}, a \neq 0 \neq b$.
Ausgabe: Der größte gemeinsame Teiler t von a und b.
Algorithmus:

1. Falls $a = 0$ dann gib $|b|$ zurück. Falls $b = 0$ gib $|a|$ zurück.
2. Setze $r_1 := a$; $r_2 := b$; $k := 2$;
3. Solange $r_k \neq 0$ ist definiere $r_{k+1} := r_{k-1} \pmod{r_k}$.
4. Sobald $r_k = 0$ gib r_{k-1} zurück.

Beweis. Wir müssen erstens zeigen, dass der Algorithmus nach endlich vielen Schritten terminiert. Dies ist klar, denn $r_k \in \mathbb{Z}_{\geq 0}$ für $k \geq 3$ und

[1] Euklid von Alexandria, ca. 325-265 v. Chr.

die Folge $(r_k)_{k\in\mathbb{N}}$ ist ab dem dritten Glied streng monoton fallend. Behauptung: $r_{k-1} = \mathrm{ggT}(a, b)$. Zu diesem Zweck mache man sich klar: Für jedes n mit $2 \leq n \leq k-1$ haben r_{n-1}, r_n dieselben gemeinsamen Teiler wie r_n, r_{n+1}: Dies ist klar, da

$$r_{n-1} = q_{n-1}r_n + r_{n+1} \text{ mit } q_{n-1} \in \mathbb{Z}.$$

Schließlich ist r_{k-1} offensichtlich der größte gemeinsame Teiler von r_{k-1} und $r_k = 0$, so dass die Behauptung folgt. q. e. d.

Beispiel 5.5

Sei $a = 558$ und $b = 423$. Setze $r_1 = a$ und $r_2 = b$.

$$\begin{array}{lcll} r_{n-1} & = & q_{n-1} \cdot r_n & + \; r_{n+1} \\ 558 & = & 1 \cdot 423 & + \; 135 \\ 423 & = & 3 \cdot 135 & + \; 18 \\ 135 & = & 7 \cdot 18 & + \; 9 \\ 18 & = & 2 \cdot 9 & + \; 0 \end{array}$$

Also ist $\mathrm{ggT}(a, b) = 9$. Die Folge der Reste ist $(558, 423, 135, 18, 9, 0)$, d.h. $k = 6$ und $r_k = 0$.

Bemerkung 5.6

Sei $E := \{\begin{pmatrix} a \\ b \end{pmatrix} \mid a, b \in \mathbb{Z}, b \neq 0\}$ und

$$\varepsilon : E \to \mathbb{Z}^{2\times 1} : \begin{pmatrix} a \\ b \end{pmatrix} \mapsto \begin{pmatrix} b \\ a \bmod b \end{pmatrix}$$

1) Der Euklidische Algorithmus kann auch so formuliert werden: Iteriere die Anwendung von ε, solange sie definiert ist:

$$\varepsilon^{k-1}(\begin{pmatrix} a \\ b \end{pmatrix}) = \underbrace{\varepsilon \circ \cdots \circ \varepsilon}_{k-1}(\begin{pmatrix} a \\ b \end{pmatrix}) = \begin{pmatrix} t \\ 0 \end{pmatrix}.$$

Dann ist $t = \mathrm{ggT}(a, b)$.

2) Es gilt:

$$\varepsilon\left(\begin{pmatrix} a \\ b \end{pmatrix}\right) = \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} b \\ r \end{pmatrix}$$

wobei

$$a = qb + r \text{ mit } q \in \mathbb{Z}, 0 \leq r < |b|.$$

Mit dieser recht offensichtlichen Bemerkung bekommt man den zweiten Teil des Euklidischen Algorithmus, der den ggT(a, b) als ganzzahlige Linearkombination von a und b darstellt, recht leicht:

Definition 5.7

Seien $a, b \in \mathbb{Z}$. Eine Darstellung $ggT(a, b) = \alpha a + \beta b$ des größten gemeinsamen Teilers von a und b als Linearkombination von a und b mit $\alpha, \beta \in \mathbb{Z}$ wird **Bézout-Identität**[a] und α und β heißen die **Bézout-Koeffizienten**.

[a] Étienne Bézout, 1730 – 1783

Algorithmus 5.8: EUKLIDischer Algorithmus, 2. Teil

Eingabe: $a, b \in \mathbb{Z}, a \neq 0 \neq b$.
Ausgabe: $t = \text{ggT}(a, b)$ und $\alpha, \beta \in \mathbb{Z}$ mit $\alpha a + \beta b = t$.
Algorithmus:

1. Falls $a = 0$, gib $|b|$, $\alpha = 0$ und $\beta = b/|b|$ zurück.
   Falls $b = 0$, gib $|a|$, $\alpha = a/|a|$ und $\beta = 0$ zurück.
2. Berechne für $r_1 := a$; $r_2 := b$; die Folge (r_n) mit Algorithmus 5.18, d.h. $r_{n-1} = q_{n-1}r_n + r_{n+1}$ mit $q_{n-1} \in \mathbb{Z}$ und $r_k = 0$.
3. Definiere

$$A_n := \begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix}$$

für $1 \leq n \leq k - 2$. Dann liefert die erste Zeile von $A_{k-2} \cdots A_1$ das gewünschte Paar (α, β), denn

$$A_{k-2} \cdots A_1 \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} t \\ 0 \end{pmatrix}$$

Beispiel 5.9

Wir setzen Beispiel 5.5 fort und definieren:

$$A_1 := \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}, A_2 := \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix}, A_3 := \begin{pmatrix} 0 & 1 \\ 1 & -7 \end{pmatrix}, A_4 := \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}.$$

Dann ist $A_4 \cdot A_3 \cdot A_2 \cdot A_1 = \begin{pmatrix} 22 & -29 \\ -47 & 62 \end{pmatrix}$ und daher ist

$$9 = 22 \cdot 558 - 29 \cdot 423.$$

Alternativ können wir diese Darstellung auch durch Rückwärtseinsetzen erhalten:

$$\begin{aligned} 9 &= 135 - 7 \cdot 18 \\ &= 135 - 7(423 - 3 \cdot 135) \\ &= 22 \cdot 135 - 7 \cdot 423 \\ &= 22 \cdot (558 - 423) - 7423 \\ &= 22 \cdot 558 - 29 \cdot 423 \end{aligned}$$

Man beachte, dass der Algorithmus so formuliert ist, dass man nur wenige Zwischenergebnisse abspeichern muß. Außerdem ist die erste Zeile von A_{k-1} gleich der zweiten Zeile von A_{k-2}.

Wir erinnern noch einmal an die Konstruktion des Restklassenrings $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ für ein $n \in \mathbb{N}$ in Sektion 3.4. Wir schreiben die Relation $a \sim b$ genau dann, wenn $n \mid (a - b)$ auch als $a \equiv b \pmod{n}$. Dort und in den Übungen hatten wir gesehen, dass $\mathbb{Z}_n$ ein Ring ist. Wir zeigen nun, dass falls $n = p$ eine Primzahl ist, so ist $\mathbb{Z}_p$ sogar ein Körper. Die fehlende Eigenschaft ist, dass jedes Element $a \in \mathbb{Z}_p - \{0\}$ ein multiplikativ Inverses besitzt.

Satz 5.10

Sei $p \in \mathbb{N}$ mit $p > 1$ eine fest vorgegebene Primzahl, also eine natürliche Zahl $p \neq 1$ mit der Eigenschaft $p = nm$ in $\mathbb{N}$ impliziert $n = 1$ oder $m = 1$, so ist $\mathbb{Z}/p\mathbb{Z}$ ist ein Körper, der **Restklassenkörper** von $\mathbb{Z}$ modulo p. Andere Bezeichnung: $\mathbb{F}_p$.

Beweis. Um zu zeigen, dass $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist, fehlt nur noch zu zeigen: Zu $a+p\mathbb{Z} \neq p\mathbb{Z}$ existiert ein $b+p\mathbb{Z}$ mit $(a+p\mathbb{Z})(b+p\mathbb{Z}) = 1+p\mathbb{Z}$, d.h. $a + p\mathbb{Z} \neq p\mathbb{Z}$ hat ein multiplikativ Inverses. Anders ausgedrückt: zu $a \notin p\mathbb{Z}$ existieren $b, n \in \mathbb{Z}$ mit $ba + np = 1$. Dies folgt direkt aus dem EUKLIDischen Algorithmus. q. e. d.

Beispiel 5.11

Bestimme $(25 + 31\mathbb{Z})^{-1}$ in $\mathbb{Z}/31\mathbb{Z} = \mathbb{F}_{31}$.

$$\begin{aligned} 31 &= 1 \cdot 25 + 6 \\ 25 &= 4 \cdot 6 + 1 \\ 6 &= 6 \cdot 1 + 0, \end{aligned}$$

also

$$\begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -6 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ -4 & 5 \end{pmatrix} = \begin{pmatrix} -4 & 5 \\ * & * \end{pmatrix}.$$

Daher ist

$$-4 \cdot 31 + 5 \cdot 25 = 1, \text{ insbesondere } (25 + 31\mathbb{Z})^{-1} = 5 + 31\mathbb{Z}.$$

Abgesehen davon, dass der Euklidische Algorithmus es uns erlaubt die von 0 verschiedenen Elemente in $\mathbb{Z}/p\mathbb{Z}$ zu invertieren und größte gemeinsame Teiler ganzer Zahlen auszurechnen, ohne diese in Primfaktoren zu zerlegen, hat er auch noch theoretische Konsequenzen: Die eindeutige Primfaktorzerlegung.

Korrolar 5.12

Sei $p \in \mathbb{N} - \{1\}$ ist eine Primzahl (d.h. die einzigen Teiler von p sind 1 und p) genau dann, wenn für alle $a, b \in \mathbb{Z}$ gilt:

$$p \mid ab \Rightarrow (p \mid a) \vee (p \mid b).$$

Beweis. "$\Rightarrow$" Sei p Primzahl und $a, b \in \mathbb{Z}$ mit $p \mid ab$. Angenommen $p \nmid a$. Dann existieren $\alpha, \beta \in \mathbb{Z}$ mit $\alpha p + \beta a = 1$. Da $p \mid ab$ folgt, dass $p \mid \alpha pb + \beta ab = (\alpha p + \beta a)b = b$.
"$\Leftarrow$". Sei $c \in N$ ein Teiler von p. Dann existiert ein $d \in \mathbb{N}$ mit $p = cd$. Insbesondere gilt $1 \leq c \leq p$ und $1 \leq d \leq p$ und $p \mid cd$. Aufgrund unserer Annahme folgt dann $p \mid c$ oder $p \mid d$, d.h. $p \leq c$ oder $p \leq d$. Damit ist dann $p = c$ (und $d = 1$) oder $p = d$ (und $c = 1$). q. e. d.

Bemerkung 5.13

a) Hier ist die Konvention, dass das leere Produkt (also ein Produkt ohne Faktoren) gleich 1 ist. Also hat $1 \in \mathbb{N}$ die eindeutige Primfaktorzerlegung ohne Faktoren.

b) In der Primfaktorzerlegung können Faktoren wiederholt auftreten.

c) Man kann den vorherigen Satz leicht auf alle ganzen Zahlen $\mathbb{Z} - \{0\}$ ausser 0 verallgemeinern, indem eine Einheit in $\mathbb{Z}^* = \{1, -1\}$ als einen weiteren Faktor zur Primfaktorzerlegung hinzufügt.

Satz 5.14: Fundamentalsatz der Arithmetik

Jede natürliche Zahl $a \in \mathbb{N}$ hat eine bis auf Reihenfolge eindeutige Produktzerlegung in Primfaktoren.

Beweis. (vollständige Induktion) Sei $n \in \mathbb{N}$. Nach unserer Bemerkung hat 1 eine Primfaktorzerlegung. Angenommen jede natürliche Zahl kleiner n hat eine Primfaktorzerlegung. Falls n selber Primzahl ist, so ist n bereits eine Zerlegung in Primfaktoren. Ansonsten existieren $b, c \in \mathbb{Z}$ mit $n = bc$ und $1 < b, c < n$. Nach Induktionsannahme haben

b und c jeweils eine Primfaktorzerlegung, etwa

$$b = p_1 \cdot p_2 \cdots p_r \text{ und } c = q_1 \cdot q_2 \cdots q_s,$$

mit p_i und p_j für $1 \leq i \leq r$ und $1 \leq j \leq s$ Primzahlen. Dann ist das Produkt dieser ist eine Primfaktorzerlegung von n, d.h.

$$n = p_1 \cdot p_2 \cdots p_r \cdot q_1 \cdot q_2 \cdots q_s.$$

Die Eindeutigkeit dieser Zerlegung folgt mit Korollar 5.12. q. e. d.

Übung 5.15. Seien $a, b \in \mathbb{Z}$ mit $b \neq 0$ und $A \in \mathbb{Z}^{2\times 2}$ mit ganzzahligem Inversen, also $A^{-1} \in \mathbb{Z}^{2\times 2}$. Zeige:
1.) Ist $A \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}$, so ist $d = \mathrm{ggT}(a, b)$.
2.) Für $(\alpha, \beta) \in \mathbb{Z}^{1\times 2}$ gilt genau dann $\alpha a + \beta b = d$, wenn ein $z \in \mathbb{Z}$ existiert mit $(\alpha, \beta) = A_{1,-} + zA_{2,-}$.

5.2 EUKLIDischer Algorithmus in Polynomringen

In dieser Sektion übertragen wir den Euklidischen Algorithmus auf Polynomringe über Körpern. Sei nun K stets ein Körper. Zuerst die Definition eines größten gemeinsamen Teilers in $K[X]$ und eine Bemerkung, die einige Gemeinsamkeiten zwischen $\mathbb{Z}$ und $K[X]$ auflistet.

Definition 5.16: ggT

Für zwei Polynome $f, g \in K[X]$ mit $(f, g) \neq (0, 0)$ heißt ein Polynom $t \in K[X]$ mit

a) $t|f$ und $t|g$,

b) für alle $c \in K[X]$ mit $c|f$ und $c|g$ gilt $c|t$.

ein **größter gemeinsamer Teiler (ggT)** von f und g. Ist $t = 1$, so sagt man auch, dass f und g **teilerfremd** oder **relativ prim** sind.

Bemerkung 5.17

a) In $\mathbb{Z}$ gilt $|ab| = |a||b|$, in $K[X]$ gilt $\text{Grad}(fg) = \text{Grad}(f) + \text{Grad}(g)$.

b) Der ggT zweier Polynome $f, g \in K[X]$ mit $(f, g) \neq (0, 0)$, ist nur eindeutig bis auf Faktoren in $K[X]^*$, also bis auf Faktoren in $K[X]$ vom Grad 0 bestimmt. Notation: $t = \text{ggT}(f, g)$, bezeichnet eigentlich auch jedes Vielfache at mit $a \in K - \{0\}$ als $\text{ggT}(f, g)$.

c) In beiden Ringen gibt es eine Division mit Rest (siehe Satz 3.23) und damit hat $K[X]$ auch einen Euklidischen Algorithmus zur Berechnung des ggT und einen erweiterten Eu- klidischen Algorithmus zur Bestimmung von Bézout-Koeffizienten. Hier ersetzt der Grad eines Polynoms den Absolutbetrag in $\mathbb{Z}$. Wir geben den ersten Teil des Algorithmus nochmal an.

d) Weiter hat man auch das Analogon von Primzahlen in $K[X]$, nämlich irreduzible Polynome, die wir in Definition 5.20 einführen, und entsprechend eine eindeutige Primfaktorzerlegung für Polynome (Korollar 5.21).

Algorithmus 5.18: EUKLIDischer Algorithmus, 1. Teil

Eingabe: $f, g \in K[X], (f, g) \neq (0, 0)$.
Ausgabe: Der größte gemeinsame Teiler t von f und g.
Algorithmus:

1. Falls $f = 0$ dann gib g zurück. Falls $g = 0$ gib f zurück.
2. Setze $r_1 := f$; $r_2 := g$; $k := 2$;
3. Solange $r_k \neq 0$ ist definiere $r_{k+1} := r_{k-1} \pmod{r_k}$.
4. Sobald $\text{Grad}(r_k) = 0$ gib r_{k-1} zurück.

Beispiel 5.19

Sei $K = \mathbb{Z}_5$ und betrachte die folgenden Polynome $f, g \in K[X]$ mit $f(X) = X^3 + X^2 + X + 1$ und $g(X) = X^3 - X^2 - X + 1$. Beachte: in $\mathbb{Z}_5$ ist $-1 = 4$ und oft schreibt man -1 statt 4. Wir setzen $r_1 = f$ und $r_2 = g$ und dividieren r_1 durch r_2 mit Rest:

$$r_1(X) = 1 \cdot r_2(X) + 2X^2 + 2X.$$

Also ist $q_1(X) = 1$ und $r_3(X) = 2X^2 + 2X$. Weiter ist

$$\begin{array}{rl} X^3 - X^2 - X + 1 & \div \; 2X^2 + 2X = 3X - 1 \\ \underline{-(X^3 + X^2)} & \\ 3X^2 - X + 1 & \\ \underline{-(-2X^2 - 2X)} & \\ X + 1 & \end{array}$$

Also ist

$$r_2(X) = q_2(X) r_3(X) + X + 1$$

mit $q_2(X) = 3X - 1$ und $r_4(X) = X + 1$. Schließlich ist $2X^2 + 2X = 2X(X + 1) + 0$ und somit

$$r_3(X) = q_3(X) r_4(X) + 0$$

mit $q_3(X) = 2X$ und $r_5(X) = 0$. Daher erhalten wir

$$\text{ggT}(f(X), g(X)) = X + 1.$$

Um die Bézout Koeffizienten auszurechnen definieren wir

$$A_1 := \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}, \; A_2 := \begin{pmatrix} 0 & 1 \\ 1 & -(3X-1) \end{pmatrix}, \; A_3 := \begin{pmatrix} 0 & 1 \\ 1 & -2X \end{pmatrix}$$

und da

$$A_3 \cdot A_2 \cdot A_1 = \begin{pmatrix} 2X+1 & 3X \\ X^2+3X+1 & -X^2-1 \end{pmatrix}.$$

erhalten wir

$$X + 1 = \mathrm{ggT}(f, g) = (2X + 1) \cdot f(X) + 3X \cdot g(X).$$

Man beachte: Wir haben unsere Matrizen über Ringen definiert, denn auch dort können wir die Matrixmultiplikation definieren. Weiterhin benötigt man nur die erste Zeile von $A_3 \cdot A_2 \cdot A_1$. Wir haben die 2. Zeile nur der Vollständigkeit halber angegeben.

Wir erinnern daran, dass für einen Ring R die Menge R^* die Menge der Einheiten in R ist. Nun ist der Polynomring $K[X]$ über einem Körper K ein kommutativer Ring und die Einheiten in $K[X]$ sind genau die konstanten Polynome, die wir mit K identifizieren können.

Definition 5.20

Es sei K ein Körper.

1. Ein Polynom $p \in K[X] - \{0\}$ heißt **irreduzibel**, wenn p keine Einheit ist (also $p \notin K[X]^*$) und wenn für $f, g \in K[X]$ gilt: $p = f \cdot g \Rightarrow f \in K[X]^* \vee g \in K[X]^*$. Ein Element $h \in K[X] - \{0\}$ für das $h = f \cdot g$ gilt mit $f, g \in K[X] - K[X]^*$, heißt **reduzibel**.
2. Ein Polynom $f \in K[X] - \{0\}$ mit $f = \sum_{i=0}^{n} a_i X^i$ heißt **normiert**, wenn sein Leitkoeffizient, also a_n mit $n = \mathrm{Grad}(f)$, gleich 1 ist.

Analog zu dem Beweis von Satz 5.14 zeigt man jetzt:

Korrolar 5.21

Es sei K ein Körper. Jedes Polynom $f \in K[X] - \{0\}$ hat eine bis auf die Reihenfolge der Faktoren eindeutige multiplikative Zerlegung in normierte irreduzible Polynome und eine Einheit.