48

Sei nun $b \in \mathbb{Z}$, so daß n die Zahl $a \cdot b - 1$ teilt. Es gilt also

$$a \cdot b - 1 = q' \cdot n, \quad \text{oder}$$

$a \cdot b = q' \cdot n + 1$. Sei nun $b = s \cdot n + r$, $0 \leq r \leq n-1$. Division mit Rest. Dann gilt

$[a] \cdot [r] = \text{Rest von } a \cdot r$. Es ist aber

$$a \cdot b = a(s \cdot n + r) = a \cdot s \cdot n + a \cdot r = q' \cdot n + 1.$$

Also gilt: $\quad a \cdot r = (q' - a \cdot s) \cdot n + 1.$

Wegen Eindeutigkeit des Rests und der Zahl $(q' - as)$ folgt $[a][r] = \text{Rest von } a \cdot r = [1]$.

Also hat $[a]$ ein Inverses. $\boxed{w}$

Man kann leicht entscheiden, ob so ein $b \in \mathbb{Z}$ existiert. Dies beruht auf dem euklidischen Algorithmus:

Sei $a, b > 0$ aus $\mathbb{Z}$. Wir setzen $x_0 = a$ und $x_1 = b$. Wir führen sukzessive Division mit Rest durch:

$$x_0 = q_1 x_1 + x_2 \quad , \quad 0 < x_2 < x_1$$
$$x_1 = q_2 x_2 + x_3 \quad , \quad 0 < x_3 < x_2$$
$$\vdots \qquad\qquad\qquad \vdots$$
$$x_{m-2} = q_{m-1} x_{m-1} + x_m \quad , \quad 0 < x_m < x_{m-1}$$
$$x_{m-1} = q_m x_m + 0$$

Da $x_1 > x_2 > x_3 > \dots \geq 0$ endet dieses Verfahren nach endlich vielen Schritten.

Man definiert $x_m = ggT(a,b)$ und nennt diese Zahl den größten gemeinsamen Teiler von a und b.

Nachdem man $x_m = ggT(a,b)$ gefunden hat, kann man das Verfahren „umdrehen".

$$ggT(a,b) = x_m = x_{m-2} - q_{m-1}\, x_{m-1}$$

$$x_{m-1} = x_{m-3} - q_{m-2}\, x_{m-2}$$

$$\vdots$$

$$x_2 = \underset{\substack{\| \\ a}}{x_0} - q_1 \underset{\substack{\| \\ b}}{x_1}$$

Durch sukzessives Einsetzen erhält man

$x_m = ggT(a,b) = ra + sb$, für geeignete $a, b \in \mathbb{Z}$.

Bsp 4.9 $\quad a = 107, \; b = 7$

$$x_0 = a = 107 = 15 \cdot 7 + 2$$
$$7 = 3 \cdot 2 + 1$$
$$2 = 2 \cdot 1 + 0$$

Also $ggT(107, 7) = 1$. Weiter gilt:

$$1 = ggT(107,7) = 7 - 3 \cdot 2 \quad \text{und}$$
$$2 = 107 - 15 \cdot 7$$

Setzen wir ein, so erhalten wir

$$1 = 7 - 3 \cdot (107 - 15 \cdot 7) = 7 - 3 \cdot 107 + 7 \cdot 3 \cdot 15$$

$= -3 \cdot 107 + 7(3 \cdot 15 + 1)$

$= \underbrace{-3}_{r} \cdot \underbrace{107}_{a} + \underbrace{46}_{s} \cdot \underbrace{7}_{b}$

<u>Notation</u> Seien $r, s \in \mathbb{Z}$. Man sagt r teilt s und schreibt $r \mid s$, wenn es ein $t \in \mathbb{Z}$ gibt mit $r \cdot t = s$.

<u>Propo 4.10</u> Sind $a, b > 0$ aus $\mathbb{Z}$ und $g = ggT(a,b)$. Dann gilt:

(i) $g \mid a$ und $g \mid b$

(ii) Für jedes $d \in \mathbb{Z}$ mit $d \mid a$ und $d \mid b$ gilt $d \mid g$.

<u>Beweis</u> (i) Aus euklidischen Algorithmus folgt $g \mid x_m$ und $g \mid x_{m-1}$. Also auch $g \mid x_{m-2}$. Induktiv folgt $g \mid x_i$, $0 \leq i \leq m$. Insbesondere $g \mid x_0$ und $g \mid x_1$. Da $a = x_0$ und $b = x_1$ folgt Behauptung.

(82)

(ii) $d \mid a$ und $d \mid b$. Aus euklidschem Algorithmus folgt induktiv $d \mid x_i$, $0 \le i \le m$. Insbesondere teilt d die Zahl $x_m = g$.

Aus Proposition 4.8 folgt sofort:

Propo. 4.11 Ein Element $[0] \neq [a] \in \mathbb{Z}/n\mathbb{Z}$ besitzt ein Inverses genau dann, wenn $ggT(a,n) = 1$.

Eine ganze Zahl $p > 0$ heißt Primzahl, wenn $p \neq 1$ und die einzigen Teiler d von p nur $d = 1$ und $d = p$ sind. Beispielsweise sind die ersten Primzahlen

$$p = 2, 3, 5, 7, 11, 13, \ldots$$

Propo 4.12 Sei $n > 0$. Der Ring $\mathbb{Z}/n\mathbb{Z}$ ist Körper genau dann, wenn n eine Primzahl ist.

Beweis „⇒" Sei $\mathbb{Z}/_{n\mathbb{Z}}$ ein Körper und $d>0$ ein Teiler von n. Wir müssen zeigen, daß $d=1$ oder $d=n$.
Da $d>0$ Teiler von n, gilt $0<d\leq n$. Wenn $d=n$ brauchen wir nichts zu zeigen. Also $d<n$.
Dann hat $[d]$ ein Inverses.
Aus Proposition 4.11 folgt $ggT(d,n)=1$. Wir schreiben $1=r\cdot d+s\cdot n$. Da $d\mid n$ und $d\mid d$, folgt $d\mid 1$, d.h. $d=1$.
„⇐" Sei $n>0$ Primzahl und $[0]\neq[a]\in\mathbb{Z}/_{n\mathbb{Z}}$. Wir müssen zeigen, daß $[a]$ Inverses besitzt.
D.h. wir müssen zeigen, daß $ggT(a,n)=1$ gemäß Prop. 4.11.
Wäre $g=ggT(a,n)>1$, so folgt aus $g\mid n$ und $g\mid a$, daß $g=n$, da n Primzahl.

Folglich $n \mid a$, was nicht gehen kann, da $a < n$. $\boxtimes$

Man nennt die Körper $\mathbb{Z}/p\mathbb{Z}$ mit p Primzahl endliche Primkörper und schreibt $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Wir haben folgende Körper kennengelernt: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ und $\mathbb{F}_p$, p Primzahl.

§ 5 Vektorräume

Sei K ein Körper, zB $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p$.
Wir haben in der Einführung lineare Gleichungssysteme

$$\begin{matrix} a_{11} X_1 & + & a_{12} X_2 & + \cdots & + & a_{1n} X_n & = 0 \\ a_{21} X_1 & + & a_{22} X_2 & + \cdots & + & a_{2n} X_n & = 0 \\ \vdots & & \vdots & & & \vdots & \vdots \\ a_{m1} X_1 & + & a_{m2} X_2 & + \cdots & + & a_{mn} X_n & = 0 \end{matrix} \qquad (*)$$

betrachtet. Wir haben folgende Kurzschreibweise

$$\sum_{j=1}^{n} a_{ij} X_j = 0, \quad 1 \leq i \leq m.$$

Eine Lösung von $(*)$ ist ein n-Tupel $(\alpha_1, \ldots, \alpha_n) \in K^n$ mit

$$\sum_{j=1}^{n} a_{ij} \alpha_j = 0, \quad 1 \leq i \leq m$$

Die Lösungsmenge ist gegeben durch

$$L = \{ (\alpha_1, \dots, \alpha_n) \in K^n \mid \sum_{j=1}^{n} a_{ij}\alpha_j = 0, \ 1 \le i \le m \}.$$

Diese Menge L hat folgende Eigenschaft: Sind $(\alpha_1, \dots, \alpha_n)$ und $(\alpha_1', \dots, \alpha_n')$ Lösungen und $\lambda \in K$, so ist

$$(\alpha_1 + \lambda \alpha_1', \dots, \alpha_n + \lambda \alpha_n')$$

ebenfalls eine Lösung. Außerdem ist $(0, \dots, 0) \in K^n$ auch eine Lösung. Dies kann man abstrahieren zum Begriff des Vektorraums.

Def 5.1 Sei K ein Körper. Ein *K-Vektorraum* ist eine kommutative Gruppe V, versehen mit einer Verknüpfung

$$K \times V \to V, \ (\lambda, a) \mapsto \lambda \cdot a,$$

so daß

folgende Axiome gelten:

(V1) $(\lambda+\mu)\cdot a = \lambda a + \mu a$, für $a \in V$ und $\lambda, \mu \in K$.

(V2) $(\lambda\cdot\mu)\cdot a = \lambda(\mu\cdot a)$, für $a \in V$ und $\lambda, \mu \in K$.

(V3) $\lambda(a+b) = \lambda a + \lambda b$, für $a, b \in V$ und $\lambda \in K$.

(V4) $1\cdot a = a$ für ~~Einselement~~ $1 \in K$.

Die Elemente $a \in V$ heißen <u>Vektoren</u> und die $\lambda \in K$ werden <u>Skalare</u> genannt.

Die Gruppen-Verknüpfung

$$V \times V \to V, \quad (a,b) \mapsto a+b$$

heißt <u>Vektoraddition</u>. Die Verknüpfung

$$K \times V \to V, \quad (\lambda, a) \mapsto \lambda\cdot a$$

heißt <u>Skalarmultiplikation</u>.

Bsp 5.2 Standardvektorraum

$V = K^n$, $n \geq 0$.

Vektoraddition ist gegeben durch

$$(\alpha_1, \dots, \alpha_n) + (\alpha_1', \dots, \alpha_n') = (\alpha_1 + \alpha_1', \dots, \alpha_n + \alpha_n'),$$

Skalarmultiplikation durch

$$\lambda \cdot (\alpha_1, \dots, \alpha_n) = (\lambda \alpha_1, \dots, \lambda \alpha_n).$$

Bsp 5.3: Die Lösungsmenge $L \subset K^n$ eines LGS $\sum_{j=1}^{n} a_{ij} X_j = 0$, $1 \leq i \leq m$.

Vektoraddition und Skalarmultiplikation ist gegeben wie in Bsp. 5.2.

Bsp 5.4 $K = \mathbb{R}$. Dann ist $V = \mathbb{R}^2$ das bekannte Koordinatensystem