1. Script zur Vorlesung: Lineare Algebra I
Prof. Dr. Salma Kuhlmann, Dr. Merlin Carl
WS 2011/2012: 18. Oktober 2011
(WS 2015/2016: Korrekturen vom 3. November 2015)

Kapitel 1: § 1 Körper

Definition (i) Eine *Verknüpfung* (oder binäre Operation) (auf einer Menge G) ist eine Funktion:

$$* : G \times G \to G.$$

Bezeichnung $*\,(g,h) := g * h$

(ii) Sei $G \neq \emptyset$.

Das Paar $(G,*)$ ist eine *Gruppe*, wenn

Assoziativ	-	$(g*h)*k = g*(h*k) \quad \forall g,h,k, \in G$
Neutrales Element	-	$\exists e \in G$ s.d. $e*g = g = g*e \quad \forall g \in G$
Ex. von Inversen	-	$\forall g \in G \exists h \in G$ s.d. g * h = e = h * g
NB:		Eindeutigkeit von neutralem Element und Inversen; siehe ÜB.
Kommutativ oder abelsch	-	$g*h = h*g \quad \forall h,g$

Bezeichnung $\mathbb{Z} :=$ Menge der ganzen Zahlen, $\mathbb{Q}$ (rationale),
$\mathbb{R} :=$ Menge der reellen Zahlen.

Beispiel I) $(\mathbb{Z},+), (\mathbb{Q},+), (\mathbb{R},+)$
II) $(\mathbb{Q}^\times,\cdot), (\mathbb{R}^\times,\cdot)$

Bezeichnung $\mathbb{Q}^\times = \mathbb{Q}\backslash\{0\}$
$\mathbb{R}^\times = \mathbb{R}\backslash\{0\}$

III) $F := \{f | f : \mathbb{R} \to \mathbb{R}\}$
Verknüpfung: $f,g \in F$ definiere $f+g : \mathbb{R} \to \mathbb{R}$ mit
$(f+g)(r) := f(r) + g(r) \quad \forall r \in \mathbb{R}$.

Neutrales $Z : \mathbb{R} \to \mathbb{R}$
$Z(r) = 0 \quad \forall r \in \mathbb{R}$

Inverse $-f : \mathbb{R} \to \mathbb{R}$
$(-f)(r) := -(f(r)) \quad \forall r \in \mathbb{R}.$

Dies sind abelsche (siehe Übungsblatt für nicht abelsche) und unendliche Gruppen. Wir konstruieren nun Beispiele von endlichen Gruppen.

Bezeichnung $\mathbb{N} := \{1, 2, \ldots\}$ die Menge der natürlichen Zahlen
$\mathbb{N}_0 := \{0, 1, \ldots\} = \{0\} \cup \mathbb{N}.$

$\mathbb{Z} :=$ die Menge der ganzen Zahlen

Divisionsalgorithmus:
Seien $a, b, \in \mathbb{Z};\ b > 0.\ \exists!\ q, r \in \mathbb{Z}$ mit $0 \leq r < b$ und $a = bq + r$.

Beweis Betrachte zunächst den Fall $a > 0$. Falls $0 < a < b$ setze $q := 0$ und $r := a$, sonst $a \geq b$. Betrachte die Menge $S := \{s \in \mathbb{N}; sb \leq a\}$. $1 \in S$ also $S \neq \emptyset$; und S ist endlich. Setze $q := \max S$
$r := a - qb$ (also $r = 0$ gdw $a = qb$)

Behauptung $\underbrace{0 \leq r}_{r \geq 0} < b$
gilt per Definition.

Widerspruchsbeweis:
Wenn $r \geq b$, dann $a - qb \geq b$ i.e. $a \geq qb + b$ i.e. $a \geq (q + 1)b$, also $q + 1 \in S$ aber $q + 1 > q$. - Widerspruch.

Eindeutigkeit
$$\left.\begin{aligned} a &= q_1 b + r_1 \\ a &= q_2 b + r_2 \end{aligned}\right\} \qquad (\dagger).$$

Also von $(\dagger) : 0 = (q_2 - q_1)b + (r_2 - r_1)$.

Widerspruchsbeweis:
Wenn $r_1 > r_2$, dann $(r_1 - r_2) > 0$. Also ergibt sich aus $(\dagger)$:
$$0 < (r_1 - r_2) = \underbrace{(q_2 - q_1)b}_{b>0,} \qquad (*)$$

Also $(q_2 - q_1) > 0$. Also $(q_2 - q_1)b \geq b$.
Andererseits: $r_1 < b$ und $r_2 < b$ also $(r_1 - r_2) < (b - r_2) \leq b$.

Mit $(*)$ erhält man einen Widerspruch: linke Seite in $(*) :< b$; rechte Seite in $(*) :\geq b$. - Widerspruch.

Also $r_1 = r_2$ und mit $(\dagger)$ bekommt man auch $q_1 = q_2$. Sei nun $c \in \mathbb{Z},\ c \leq 0$. Wenn $c = 0$, setze $q := 0$ und $r := c$, $c = 0 = 0b + 0$. Wenn $c < 0$, setze $a := (-c)$, dann ist $a > 0$. Also $\exists! q, r$ mit $0 \leq r < b$ und $a = bq + r$.

$$\begin{aligned}
r = 0 \quad &\Rightarrow \quad c = -a &&= b(-q) \\
r \neq 0 \quad &\Rightarrow \quad c = -a &&= b(-q) + (-r) \\
& &&= b(-q) - b + (b - r) \\
& &&= b(-q - 1) + (b - r) \\
& &&= b[-(q + 1)] + \underbrace{(b - r)}_{0<r<b}
\end{aligned}$$

also $0 > -r > -b$
also $b > (b - r) > 0$. $\square$