Martin Gubisch
Lineare Algebra I
WS 2007/2008

Gruppen, Ringe, Körper

Definition

Eine *Gruppe* G ist eine Menge $X \neq \emptyset$ mit einer Veknüpfung $*$, so dass gelten:

(1) $\forall x, y, z \in X : (x * y) * z = x * (y * z)$.
(2) $\exists e \in X : \forall x \in X : e * x = x = x * e$.
(3) $\forall x \in X : \exists y \in X : x * y = e = y * x$.

G heißt *abelsch*, falls zusätzlich gilt:

(4) $\forall x, y \in X : x * y = y * x$.

Bemerkung

(1) Üblicherweise bezeichnet man mit G sowohl die Gruppe als auch die Grundmenge: $G = (G, *)$.
(2) Das neutrale Element und die Inversen sind eindeutig bestimmt.
(3) Für $x, y \in G$ gilt $(x * y)^{-1} = y^{-1} * x^{-1}$.

Beispiel

Wir betrachten die Menge $\langle S_3 \rangle$ der Symmetrien eines regelmäßigen Dreiecks ABC, genauer: die Menge der Drehung ρ um den Winkel 60° und der Spiegelungen $\sigma_A, \sigma_B, \sigma_C$ an den durch A, B, C verlaufenden Symmetrieachsen.

Bezeichnen wir die Menge aller Kompositionen dieser Symmetrien mit S_3, dann erhalten wir die Menge $S_3 = \{\mathrm{id}, \rho, \rho^2, \sigma_A, \sigma_B, \sigma_C\}$ (beachte: z.B. $\rho \circ \sigma_A = \sigma_C,\ \rho \circ \sigma_B = \sigma_A,\ \rho \circ \sigma_C = \sigma_B$).

$(S_3, \circ)$ erfüllt die Axiome einer Gruppe, ist aber nicht abelsch (denn $\sigma_A \circ \sigma_B = \rho \neq \rho^2 = \sigma_B \circ \sigma_A$).

$A_3 := \{\mathrm{id}, \rho, \rho^2\} \subseteq S_3$ dagegen bildet mit der Komposition $\circ$ sogar eine abelsche Gruppe. Die Gruppe wird von ρ *erzeugt*, d.h. $A_3 = \{\rho^n \mid n \in \mathbb{Z}\}$; man nennt A_3 daher auch *zyklische Gruppe* der *Ordnung* 3 (da $\rho^3 = \mathrm{id}$).

Beispiel

Sei $m \in \mathbb{N},\ m \geq 2$. Dann gibt es für jedes $z \in \mathbb{Z}$ eindeutig bestimmte $q, r \in \mathbb{Z}$ mit $z = qm + r$ und $0 \leq r \leq m - 1$. Wir bezeichnen die Menge der *m-Reste* $\{0, ..., m-1\}$ mit $\mathbb{Z}_m$ und betrachten die Abbildung $\bar{\cdot}: \begin{smallmatrix} \mathbb{Z} \to \mathbb{Z}_m \\ z \mapsto r_z \end{smallmatrix}$ (mit $z = q_z m + r_z$).

$(\mathbb{Z}_m, *)$ bildet eine abelsche Gruppe, wenn man setzt $\forall x, y \in \mathbb{Z}_m : x * y := \overline{x + y}$. Das neutrale Element ist 0; zu $x \in \mathbb{Z}_m$ ist $-x := m - x$ das Inverse.

Es gilt $\forall x, y \in \mathbb{Z}_m : \overline{x + y} = \overline{x} * \overline{y}$, d.h. $\bar{\cdot}$ ist ein „Gruppenhomomorphismus“ zwischen den Gruppen $(\mathbb{Z}, +)$ und $(\mathbb{Z}_m, *)$. Weiter gilt $\forall z \in \mathbb{Z}_m : \overline{z} = z$ und $\forall z \in \mathbb{Z} : \overline{\overline{z}} = \overline{z}$.

Definition

Seien $(G, *)$ und $(H, +)$ Gruppen. Eine Abbildung $\rho : G \to H$ heißt ein *Gruppenhomomorphismus*, falls für alle $f, g \in G$ gilt: $\rho(f * g) = \rho(f) + \rho(g)$.

Bemerkung

(1) Sei $\rho : G \to H$ ein Gruppenhomomorphismus, dann $\rho(1_G) = 1_H$ und $\rho(g^{-1}) = (\rho(g))^{-1}$.
(2) Mit $\rho : G \to H$ und $\varphi : H \to K$ Gruppenhomomorphismen ist auch $\varphi \circ \rho : G \to K$ ein Gruppenhomomorphismus.
(3) id: $\begin{smallmatrix} G \to G \\ g \mapsto g \end{smallmatrix}$ und $\mathbb{1}: \begin{smallmatrix} G \to G \\ g \mapsto 1_G \end{smallmatrix}$ sind stets Gruppenhomomorphismus von G in sich.
(4) Ist G abelsch, dann ist $\cdot^{-1}: \begin{smallmatrix} G \to G \\ g \mapsto g^{-1} \end{smallmatrix}$ ein Gruppenhohomorphismus.

Definition

Ein *Monomorphismus* ist ein injektiver Homomorphismus.
Ein *Epimorphismus* ist ein surjektiver Homomorphismus.
Ein *Isomorphismus* ist ein bijektiver Homomorphismus.
Ein *Endomorphismus* ist ein Homomorphismus in sich selbst.
Ein *Automorphismus* ist ein bijektiver Endomorphismus.

Beispiel

(1) $\mathbb{1}_G$ ist ein Gruppenendomorphismus; id_G ein Gruppenautomorphismus.
(3) Auf $(\mathbb{Z},+)$ ist für jedes $m \in \mathbb{Z}$ die Abbildung $\begin{smallmatrix}\mathbb{Z} \to & \mathbb{Z} \\ z \mapsto & mz\end{smallmatrix}$ ein Endomorphismus.
(4) Auf $(\mathbb{Z},+)$ ist $\begin{smallmatrix}\mathbb{Z} \to & \mathbb{Z} \\ z \mapsto & z+1\end{smallmatrix}$ sogar ein Automorphismus.

Bemerkung

(1) Ist φ ein Isomorphismus, dann auch φ^{-1}.
(2) Mit ρ, φ ist auch $\rho \circ \varphi$ ein Isomorphismus und es gilt $(\rho \circ \varphi)^{-1} = \varphi^{-1} \circ \rho^{-1}$.
(3) Ist G eine Gruppe, dann bildet $\mathrm{Aut}(G) := \{\rho : G \to G \mid G \text{ Automorphismus}\}$ eine Gruppe.

Definition

$(X,+,\cdot)$ heißt ein *Ring*, falls $+$ und $\cdot$ Verknüpfungen auf X sind, so dass gilt:
(1) $(X,+)$ ist eine abelsche Gruppe.
(2) $(X,\cdot)$ ist assoziativ.
(3) Es gelten die Distributivgesetze.

Gibt es ein Element $1 \in X$ mit $\forall x \in X : 1 \cdot x = x = x \cdot 1$, dann heißt $(X,+,\cdot)$ ein *Ring mit Eins*.

Gilt $\forall x, y \in X : x \cdot y = y \cdot x$, dann heißt *kommutativ*.

Gilt $\forall x, y \in X : x \cdot y = 0 \Rightarrow x = 0$ oder $y = 0$, dann heißt X *nullteilerfrei*.

Gibt es zu $x \in X,\ x \neq 0$ ein $n \in \mathbb{N}$ mit $x^n = 0$, dann heißt x *nilpotent*.

Beispiele

(1) $(\mathbb{Z},+,\cdot)$ ist ein kommutativer, nullteilerfreier Ring mit Eins (ein *Integritätsbereich*).
(2) $(\mathbb{Z}_m,+,\cdot)$ mit $\forall a, b \in \mathbb{Z}_m : a + b := \overline{a+b}$ und $a \cdot b := \overline{a \cdot b}$ ist ein kommutativer Ring mit Eins, der *Restklassenring* von m. $\mathbb{Z}_m$ ist i.A. nicht nullteierlfrei.
(3) Ein besonders langweiliger Ring ist der Nullring $(\{0\},+,\cdot)$ (mit $0+0=0\cdot 0=0$).
(4) Alle „Körper“ wie $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind insbesondere Integritätsbereiche.
(5) Die Menge $\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}$ bildet einen Ring, den *Ring der Gaußschen Zahlen*. Dieser ist kanonisch isomorph zu $\mathbb{Z} \times \mathbb{Z}$ via $\begin{smallmatrix}\mathbb{Z}[i] & \to & \mathbb{Z}^2 \\ a+bi & \mapsto & (a,b)\end{smallmatrix}$.
(6) Ist $(G,+)$ eine Gruppe, dann ist $(G,+,\cdot)$ ein Ring, wobei $\forall x, y \in G : x \cdot y := 0$.
(7) Ist $(G,+)$ eine Gruppe, dann ist $(\mathrm{End}(G),+,\circ)$ ein Ring mit Eins, wenn man für $\varphi, \psi \in G$ setzt $\varphi + \psi : \begin{smallmatrix}G \to & G \\ g \mapsto & \varphi(g)+\psi(g)\end{smallmatrix}$ und $\varphi \circ \psi : \begin{smallmatrix}G \to & G \\ g \mapsto & \varphi(\psi(g))\end{smallmatrix}$; dann ist id das Einselement.

Bemerkung

Wir betrachten den Endomorphismenring $(\mathrm{End}(G),+,\circ)$ der Kleinschen Vierergruppe $G = (\{0,a,b,c\},+)$. Man kann zeigen, dass jeder Endomorphismus auf G durch seine Werte auf a und b eindeutig festgelegt ist und dass es für alle $g, h \in G$ ein $\varphi \in \mathrm{End}(G)$ gibt mit $\varphi(a) = g$ und $\varphi(b) = h$, d.h. es gibt eine Bijektion

$$\begin{smallmatrix}\mathrm{End}(G) \to & G \times G \\ \varphi \quad \mapsto & (\varphi(a), \varphi(b))\end{smallmatrix}.$$

Damit besitzt $\mathrm{End}(G)$ genau 16 Elemente.

Definition

Seien $(R,+,\cdot)$ und $(S,*,\circ)$ Ringe. Eine Abbildung $\rho : R \to S$ heißt ein *Ringhomomorphismus*, falls für alle $f,g \in R$ gilt: $\rho(f+g) = \rho(f) * \rho(g)$ und $\rho(f \cdot g) = \rho(f) \circ \rho(g)$.

Sind R, S Ringe mit Eins, dann heißt ρ *unitär*, falls $\rho(1_R) = 1_S$ gilt.

Beispiele

(1) Die *Inklusionsabbildung* $\iota : \begin{smallmatrix}\mathbb{Z} \to \mathbb{Q} \\ z \mapsto z\end{smallmatrix}$ ist ein Ringhomomorphismus.

(2) $\bar{\cdot} : \begin{smallmatrix}\mathbb{Z} \to \mathbb{Z}_m \\ x \mapsto \overline{x}\end{smallmatrix}$ ist ein surjektiver Ringhomomorphismus.

(3) Sind $\rho : R \to S$ und $\varphi : S \to T$ Ringhomomorphismen, dann ist auch $\varphi \circ \rho : R \to T$ ein Ringhomomorphismus.

(4) id: $\begin{smallmatrix}R \to R \\ r \mapsto r\end{smallmatrix}$ und $\mathbb{0}$: $\begin{smallmatrix}R \to R \\ r \mapsto 0\end{smallmatrix}$ sind stets Ringhomomorphismus von R in sich.

(5) Für festes $a \in \mathbb{Z}$ ordnet der *Einsetzungshomomorphismus* $\begin{smallmatrix}\mathbb{Z}[X] \to \mathbb{Z} \\ p \mapsto p(a)\end{smallmatrix}$ jedem Polynom p des Ringes $\mathbb{Z}[X]$ die Einsetzung $p(a) \in \mathbb{Z}$ zu.

Definition

Sei R ein Ring mit Eins. Dann heißt $r \in R$ eine *Einheit* (bzgl. $\cdot$), falls r invertierbar ist, d.h. falls es ein $q \in r$ gibt mit $rq = 1$.

Ist R ein kommutativer Ring mit Eins, in dem jedes von 0 verschiedene Element eine Einheit ist, dann heißt R ein *Körper*.

Bemerkung

(1) Die Einheiten eines Ringes R bilden eine Gruppe, die mit $R^\times$ bezeichnete *Einheitengruppe* von R.

(2) Sei R ein Ring. Dann gilt R Körper $\Leftrightarrow R^\times = R \backslash \{0\}$.

(3) Sind R, S Ringe mit Eins und $\rho : R \to S$ ein unitärer Rindhomomorphismus, dann gelten $\rho(R^\times) \subseteq S^\times$ und $\forall r \in R^\times : \rho(r^{-1}) = (\rho(r))^{-1}$.

Beispiel

$\mathbb{Z}^\times = \{-1, 1\},\ (\mathbb{Z}[i])^\times = \{-1, 1, -i, i\}$.

Definition

Seien $a, b \in \mathbb{N}$. Wir setzen $a|b$ („a teilt b“), wenn es ein $c \in \mathbb{N}$ gibt mit $ac = b$.

$\mathrm{ggT}(a,b)$ bezeichnet das größte $c \in \mathbb{N}$ mit $c|a$ und $c|b$, den *größten gemeinsamen Teiler* von a und b.

$p \in \mathbb{N} \backslash \{1\}$ heißt eine *Primzahl*, wenn $\forall n \in \mathbb{N} : n|p \Rightarrow n = p$ oder $n = 1$.

Bemerkung

Es gilt $\forall a, b, c \in \mathbb{N} : a|a;\ a|b$ und $b|a \Rightarrow a = b$ und $a|b,\ b|c \Rightarrow a|c$.

Lemma

Für $a, m \in \mathbb{N}$ gilt $\mathrm{ggT}(a,m) = \min\{xa + ym \mid x, y \in \mathbb{Z}\} \cap \mathbb{N}$.

Beweis

Setze $t := \min\{xa + ym \mid x, y \in \mathbb{Z}\} \cap \mathbb{N}$, $r, s \in \mathbb{Z}$ derart, dass $t = ra + sm$ und $d := \mathrm{ggT}(a,m)$. Dann $d|a$ und $d|m \Rightarrow d|(ra + sm) = t$. Noch zu zeigen: $t|d$, bzw. $t|a$ und $t|m$.

Seien $q', r' \in \mathbb{N}$ derart, dass $a = q't + r'$ mit $0 \leq r' < t$. Zu zeigen: $r' = 0$. Betrachte dazu

$$0 \leq r' = a - q't = a - q'(ra + sm) = a - q'ra - q'sm = (1 - q'r)a - (q's)m.$$

Dann $r' \in \{xa + ym \mid x, y \in \mathbb{Z}\} \cap \mathbb{N}_0$; wegen der Minimalität von t folgt aus $0 \leq r' < t$ schon $r' = 0$.

Analog argumentiert man für m.

Satz (Einheiten in $\mathbb{Z}_m$)

Es gilt $a \in \mathbb{Z}_m^\times \Leftrightarrow \mathrm{ggT}(a,m) = 1$.

Beweis

$\Rightarrow$: Sei $a \in \mathbb{Z}_m^\times$, d.h. es gibt $b \in \mathbb{Z}_m$ mit $\overline{ab} = 1$. Dann gibt es $q \in \mathbb{Z}$ mit $ab = qm + 1$. Sei $c \in \mathbb{N}$ mit $c|ab = qm + 1$ und $c|m$. Dann auch $c|1 \Rightarrow c = 1 \Rightarrow \mathrm{ggT}(a,m) = 1$.

$\Leftarrow$: Gelte $\mathrm{ggT}(a,m) = 1$. Nach dem Lemma gibt es dann $r, s \in \mathbb{N}$ mit $ra + sm = 1$. Dann gilt aber $1 = \overline{ra + sm} = \overline{ra} + \overline{sm} = \overline{ra} = \overline{r}\,\overline{a}$, d.h. a ist invertierbar.

Satz (Restklassenkörper)

$\mathbb{Z}_m$ ist genau dann ein Körper, wenn m eine Primzahl ist.

Beweis

$\Rightarrow$: Seien $\mathbb{Z}_m$ ein Körper und $a \in \mathbb{N}$ mit $a \leq m$. Dann $a \in \mathbb{Z}_m^\times$, also invertierbar in $\mathbb{Z}_m$. Nach letzten Satz gilt dann $\mathrm{ggT}(a,m) = 1$. Also $\forall a \in \mathbb{N} : a|m \Rightarrow a = m$ oder $a = 1$, d.h. m ist prim.

$\Leftarrow$: Sei umgekehrt m prim, d.h. $\forall a \in \mathbb{Z}_m \backslash \{0\} : \mathrm{ggT}(a,m) = 1 \Rightarrow a \in \mathbb{Z}_m^\times$ (wiederum mit dem letzten Satz) $\Rightarrow \mathbb{Z}_m^\times = \mathbb{Z}_m \backslash \{0\} \Rightarrow \mathbb{Z}_m$ Körper.

Satz (endliche Integritätsbereiche)

Jeder endliche Integritätsbereich ist ein Körper.

Beweis

Sei R ein endlicher Integritätsbereich. Dann gibt es zu $x \in R\backslash\{0\}$ natürliche Zahlen $n, m \in \mathbb{N}$ mit $n < m$ und $x^m = x^n$. Da R Integritätsbereich, gilt die *Kürzungsregel* $\forall a, b, c \in R,\ a \neq 0 : ab = ac \Rightarrow b = c$, denn $ab = ac \Rightarrow a(b-c) = 0 \Rightarrow b - c = 0 \Rightarrow b = c$; mit $a = x^n,\ b = 1$ und $c = x^{m-n}$ erhalten wir $x^{m-n} = 1$, also $xx^{m-n-1} = 1$, d.h. $x \in R^\times$.

Definition

Seien $(K, +, \cdot)$ und $(L, *, \circ)$ Körper. Eine Abbildung $\rho : K \to L$ heißt ein *Körperhomomorphismus*, falls für alle $f, g \in K$ gilt: $\rho(f + g) = \rho(f) * \rho(g),\ \rho(f \cdot g) = \rho(f) \circ \rho(g)$ sowie $\rho(1_K) = 1_L$.

Bemerkung

(1) Die Verkettung von Körperhomomorphismen ist ein Körperhomomorphismus.

(2) Der einzige Körperendomorphismus auf $\mathbb{Q}$ ist die Identität.

(3) $\varkappa : \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ (a+ib) & \mapsto & a - ib \end{array}$ bzw. $\tilde{\varkappa} : \begin{array}{c} \mathbb{R}\times\mathbb{R} \to \mathbb{R}\times\mathbb{R} \\ (a,b) \mapsto (a,-b) \end{array}$ sind Körperhomomorphismen.

(4) $\iota : \begin{array}{c} \mathbb{Q} \to \mathbb{R} \\ q \mapsto q \end{array}$ und $\begin{array}{c} \mathbb{R} \to \mathbb{C} \\ r \mapsto r \end{array}$ sind Körperhomomorphismen.

Satz (Injektivität von Körperhomomorphismen)

Jeder Körperhomomorphismus ist injektiv.

Beweis

Seien $\rho : K \to L$ ein Körperhomomorphismus und $a, b \in K$ mit $\rho(a) = \rho(b)$, d.h. $\rho(a - b) = 0$. Wegen $\rho(K^\times) \subseteq L^\times = L\backslash\{0\}$ folgt $a - b \notin K^\times$, also $a - b = 0$ und damit $a = b$.

Korollar (Körperhomomorphismen zwischen endlichen Körpern)

Seien p, q prim. Gibt es einen Körperhomomorphismus $\rho : \mathbb{Z}_p \to \mathbb{Z}_q$, dann $p = q$ und ρ=id.

Beweis

Angenommen, $p \neq q$. Da ρ injektiv, gibt es keinen Körperhomomorphismus von $\mathbb{F}_q$ nach $\mathbb{F}_p$. Ein Homomorphismus $\rho : \mathbb{F}_p \to \mathbb{F}_q$ dagegen wäre wegen $\rho(1_p) = 1_q$ und $\rho(1_p) = \rho((p+1)1_p) = (p+1)1_q = p+1$ nicht wohldefiniert.

Ist nun $\rho : \mathbb{F}_p \to \mathbb{F}_p$ ein Homomorphismus, dann $\rho(k) = \rho(1 + ... + 1) = \rho(1) + ... + \rho(1) = 1 + ... + 1 = k$ für jedes $k \in \mathbb{F}_p$.

Bemerkung

Sei $d \in \mathbb{Z}\backslash\{0,1\}$ *quadratfrei*, d.h. $d^2 \notin \mathbb{Z}$. Dann ist $\mathbb{Q}(\sqrt{d}) := \mathbb{Q} + \sqrt{d}\mathbb{Q} := \{q + \sqrt{d}r \mid q, r \in \mathbb{Q}\} \subseteq \mathbb{C}$, versehen mit der Addition und Multiplikation von $\mathbb{C}$, ein Körper.

Für $d \in \mathbb{N}$ ist $\mathbb{Q}(\sqrt{d})$ ein Teilkörper von $\mathbb{R}$; für $d < 0$ lässt sich auch $\mathbb{R}$ zu $\mathbb{R}(\sqrt{d}) \subseteq \mathbb{C}$ erweitern.

Speziell ist $\mathbb{C}$ selbst eine *Erweiterung* von $\mathbb{R}$: $\mathbb{C} = \mathbb{R}(i)$.

Definition

Sei $G = (G, +)$ eine Gruppe, $G' \subseteq G$. Dann heißt G' eine *Untergruppe* von G, falls $(G', +)$ Gruppe ist.

Beispiel

(1) Ist $\rho : G \to H$ ein Gruppenhomomorphismus, dann ist das *Bild* $\rho(G) \subseteq H$ eine Untergruppe von H.

(2) Ist $G' \subseteq G$ eine Untergruppe von G, dann ist $\rho(G') \subseteq H$ eine Untergruppe von H.

(3) Analog ist für $H' \subseteq H$ Untergruppe das Urbild $\rho^{-1}(H')$ eine Untergruppe von G.

(4) Speziell ist $\rho^{-1}(1_H)$ eine Untergruppe von G, der *Kern* von ρ.

Bemerkung

Um zu zeigen, dass $G' \subseteq G$, $G' \neq \emptyset$ eine Untergruppe von G ist, genügt es nachzuweisen, dass mit $x, y \in G'$ auch xy^{-1} in G' liegt, denn dann gilt:

(1) $x \in G' \Rightarrow xx^{-1} = 1 \in G'$, d.h. das neutrale Element liegt in G'.
(2) $x, 1 \in G' \Rightarrow 1x^{-1} = x^{-1} \in G'$, d.h. in G' ist jedes Element invertierbar.
(3) $x, y \in G' \Rightarrow y^{-1} \in G' \Rightarrow x(y^{-1})^{-1} = xy \in G'$, d.h. G' ist abgeschlossen.