0 Gruppen, Ringe, Körper

0.1 Algebraische Grundstrukturen

Grundlagen 0.1

Sei ab jetzt X stets eine nicht leere Menge.

(1) $(X, *)$ heißt eine *Magma*, falls $*$ eine *Verknüpfung* auf X ist, d.h. falls $* : X \times X \to X,\ (x, y) \mapsto x * y$ eine Abbildung ist.

Beispiele hierfür sind $(\mathcal{P}(X), \setminus),\ (\mathcal{P}(X), \cap),\ (\mathcal{P}(X), \cup)$. ◊

(2) Eine Magma $(X, *)$ heißt eine *Halbgruppe*, falls $*$ *assoziativ* ist, d.h. falls für alle $x, y, z \in X$ gilt: $(x * y) * z = x * (y * z)$.

Zum Beispiel sind $(\mathbb{N}, +),\ (\{2n \mid n \in \mathbb{N}\}, +),\ (\{2n \mid n \in \mathbb{N}\}, \cdot)$ Halbgruppen. ◊

(3) Eine Halbgruppe $(X, *)$ heißt ein *Monoid*, falls $(X, *)$ ein *neutrales Element* besitzt, d.h. falls ein $e \in X$ existiert, so dass für alle $x \in X$ gilt: $e * x = x = x * e$.

e ist in dem Fall eindeutig bestimmt.

Betrachte $M := \{1, 2, 3\}$ und $A := \{\mathrm{id}, f, g, h\}$ mit $f \equiv 1,\ g \equiv 2$ und $h(1) = 2,\ h(2) = 1,\ h(3) = 3$, wobei $\mathrm{id}, f, g, h : M \to M$. Dann ist $(A, \circ)$ ein Monoid. ◊

(4) Eine Halbgruppe $(X, *)$ heißt eine *Gruppe*, falls jedes Element *invertierbar* ist, d.h. falls zu jedem $x \in X$ ein $y \in X$ existiert mit $x * y = e = y * x$.

Auch die Inversen sind eindeutig bestimmt.

Wichtige Beispiele sind die Gruppe der reellen $(n \times n)$-Matrizen $(\mathbb{R}^{n \times n}, +)$, die *Kleinsche Vierergruppe* und $(\mathbb{Q}^+, \cdot)$. ◊

(5) Eine Gruppe $(X, *)$ heißt *abelsch*, falls $*$ *kommutativ* ist, d.h. falls $\forall x, y \in X : x * y = y * x$.

Beispiele sind neben den zuvor Genannten etwa $(\mathcal{P}, \Delta)$ und $(\{1, -1, i, -i\}, \cdot)$.

Die Menge der *invertierbaren* $(n \times n$-Matrizen bildet mit dem Matrixprodukt eine *nicht* abelsche Gruppe. ◊

(6) $(X, +, \cdot)$ heißt ein *Ring*, falls $+$ und $\cdot$ Verknüpfungen auf X sind, so dass $(X, +)$ eine abelsche Gruppe ist, $(X, \cdot)$ eine Halbgruppe und für alle $x, y, z \in X$ die *Distributivgesetze* $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ und $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$ gelten.

Beispiele: $(\mathbb{Z}, +, \cdot),\ (\mathbb{Z} \times \mathbb{Z}, +, \cdot),\ \mathbb{R}[X] = \{\sum_{i=0}^{n} a_i X^i \mid n \in \mathbb{Z},\ a_i \in \mathbb{R}\},\ (\mathcal{P}(X), \Delta, \cap),\ (\mathbb{Z}[i], +, \cdot)$.

Für gewöhnlich betrachten wir kommutative Ringe mit Einselement, d.h. Ringe $(X, +, \cdot)$, bei denen $(X, \cdot)$ ein kommutativer Monoid ist. Beachte aber: Die Matrizengruppe ist nicht kummutativ. ◊

(7) Sei $(X, +, \cdot)$ ein Ring. $(X, +, \cdot)$ heißt ein *Körper*, falls $(X \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist, d.h. falls $(X, +, \cdot)$ ein kommutativer Ring mit 1 ist, in dem jedes von 0 verschiedene Element bzgl. $\cdot$ invertiervar ist.

Beispiele: $(\mathbb{Q}, +, \cdot),\ (\mathbb{R}, +, \cdot),\ (\mathbb{C}, +, \cdot),\ \mathbb{R}(X) = \{\frac{p}{q} \mid p, q \in \mathbb{R}[X],\ q \neq 0\},\ \mathbb{F}_2 = (\{0, 1\}, +, \cdot)$. ◊

(8) Sei $\mathcal{R}$ ein kommutativer Ring mit 1. $\mathcal{A}$ heißt ein *$\mathcal{R}$-Modul*, falls es eine Verknüpfung $\mathcal{R} \times \mathcal{A} \to \mathcal{A}$, $(r, a) \to ra$ gibt, so dass gelten:

(a) $(\mathcal{A}, +)$ ist eine abelsche Gruppe.
(b) $\forall q, r \in \mathcal{R},\ a, b \in \mathcal{A} : r(a + b) = ra + rb$ und $(q + r)a = qa + ra$.
(c) $\forall q, r \in \mathcal{R},\ a \in \mathcal{A} : (rq)a = r(qa)$.
(d) $\forall a \in \mathcal{A} : 1a = a$.

Ist $\mathcal{R}$ sogar ein Körper, so heißt $\mathcal{A}$ ein *$\mathcal{R}$-Vektorraum*. ◊

(9) Ist $\mathcal{A}$ ein $\mathcal{R}$-Modul, der zusätzlich eine innere Verknüpfung $\mathcal{A} \times \mathcal{A} \to \mathcal{A},\ (a, b) \mapsto ab$ besitzt, so dass gelten

(e) $\forall a, b, c \in \mathcal{A} : a(bc) = (ab)c$,
(f) $\forall a, b, c \in \mathcal{A} : (a + b)c = ac + bc$ und $a(b + c) = ab + ac$,
(g) $\forall r \in \mathcal{R},\ a, b \in \mathcal{A} : r(ab) = (ra)b$,

so heißt $\mathcal{A}$ eine *$\mathcal{R}$-Algebra*. ◊

0.2 Gruppen und Gruppenhomomorphismen

Definition 0.2

Eine *Gruppe* $\mathcal{G}$ 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) $\forall x \in X : \exists y \in X : x * y = e = y * x$.

$\mathcal{G}$ heißt *abelsch*, falls zusätzlich gilt:

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

Bemerkung 0.3

(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 0.4

(1) Wir betrachten die Menge $\langle \mathcal{S}_3 \rangle$ 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 $\mathcal{S}_3$, dann erhalten wir die Menge $\mathcal{S}_3 = \{\mathrm{id}, \rho, \rho^2, \sigma_A, \sigma_B, \sigma_C\}$ (beachte: z.B. $\rho \circ \sigma_A = \sigma_C,\ \rho \circ \sigma_B = \sigma_A,\ \rho \circ \sigma_C = \sigma_B$).

$(\mathcal{S}_3, \circ)$ erfüllt die Axiome einer Gruppe, ist aber nicht abelsch (denn $\sigma_A \circ \sigma_B = \rho \neq \rho^2 = \sigma_B \circ \sigma_A$).

$\mathcal{A}_3 := \{\mathrm{id}, \rho, \rho^2\} \subseteq \mathcal{S}_3$ dagegen bildet mit der Komposition $\circ$ sogar eine abelsche Gruppe. Die Gruppe wird von ρ erzeugt, d.h. $\mathcal{A}_3 = \{\rho^n \mid n \in \mathbb{Z}\}$; man nennt $\mathcal{A}_3$ daher auch zyklische Gruppe Ordnung 3 (da $\rho^3 = \mathrm{id}$). ◊

(2) 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 $\bar{\cdot} : \mathbb{Z} \to \mathbb{Z}_m,\ z \mapsto \overline{z} := r_z$ (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. $\mathbb{Z}_m$ heißt die *Restklassengruppe modulo m*.

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 0.5

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 0.6

(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 $\varphi \circ \rho : G \to K$ einer.

(3) $\mathrm{id} : G \to G,\ g \mapsto g$ und $0 : G \to G,\ g \mapsto 1_G$ sind stets Gruppenhomomorphismus von G in sich.

(4) Auf $(\mathbb{Z}, +)$ ist für jedes $m \in \mathbb{Z}$ die Abbildung $\mathbb{Z} \to \mathbb{Z},\ z \mapsto mz$ ein Homomorphismus.

(5) Ist φ ein bijektiver Homomorphismus (ein *Gruppenisomorphismus*), dann auch φ^{-1}.

(6) Mit ρ, φ ist auch $\rho \circ \varphi$ ein Isomorphismus und es gilt $(\rho \circ \varphi)^{-1} = \varphi^{-1} \circ \rho^{-1}$.

(7) Ist G eine Gruppe, dann bildet $\mathrm{Aut}(G) := \{\rho : G \to G \mid G \text{ ist Isomorphismus}\}$ eine Gruppe.

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

(9) Seien $\rho : G \to H$ ein Gruppenhomomorphismus, $G' \subseteq G$ und $G' \subseteq H$ Untergruppen. Dann sind $\rho(G') \subseteq H$ und $\rho^{-1}(H') \subseteq G$ Untergruppen. Speziell sind das *Bild* $\rho(G)$ und der *Kern* $\rho^{-1}(1_H)$ Untergruppen. ◊

0.3 Ringe und Ringhomomorphismen

Definition 0.7

$\mathcal{R} := (X, +, \cdot)$ 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 $1 \in X$ mit $\forall x \in X : 1 \cdot x = x = x \cdot 1$, dann heißt $(X, +, \cdot)$ Ring mit Eins.

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

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

Beispiele 0.8

(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 $\mathbb{Z}[i] \to \mathbb{Z}^2,\ a + bi \mapsto (a, b)$.

(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 $\varphi + \psi : G \to G,\ g \mapsto \varphi(g) + \psi(g)$ und $\varphi \circ \psi : G \to G,\ g \mapsto \varphi(\psi(g))$; dann ist id das Einselement. ◊

Definition 0.9

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 0.10

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

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

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

(4) $\mathrm{id} : R \to R,\ r \mapsto r$ und $0 : R \to R,\ r \mapsto 0$ sind stets Ringhomomorphismus von R in sich.

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

(6) 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 $rq = 1$.

(7) Die Einheiten eines Ringes R bilden eine Gruppe, die mit $R^\times$ bezeichnete *Einheitengruppe* von R. Beispielsweise ist $\mathbb{Z}^\times = \{-1, 1\},\ (\mathbb{Z}[i])^\times = \{-1, 1, -i, i\}$.

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

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

0.4 Körper und Körperhomomorphismen

Definition 0.11

Ist $\mathcal{K}$ ein kommutativer Ring mit Eins, in dem jedes von 0 verschiedene Element eine Einheit ist, dann heißt $\mathcal{K}$ ein *Körper*.

Bemerkung 0.12

Sei R ein Ring. Dann ist R genau dann ein Körper, wenn $R^\times = R\backslash\{0\}$. ◊

Satz 0.13 (Restklassenkörper)

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

Beweis

⇒: 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 0.10.7 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.

⇐: 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 0.10.7) $\Rightarrow \mathbb{Z}_m^\times = \mathbb{Z}_m\backslash\{0\} \Rightarrow \mathbb{Z}_m$ Körper. □

Bemerkung 0.14

Jeder endliche Integritätsbereich ist ein Körper: 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 0.15

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 0.16

(1) Die Verkettung von Körperhomomorphismen ist ein Körperhomomorphismus.

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

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

(4) $\iota : \mathbb{Q} \to \mathbb{R},\ q \mapsto q$ und $\mathbb{R} \to \mathbb{C},\ r \mapsto r$ sind Körperhomomorphismen, sog. *Einbettungshomomorphismen*.

(5) Jeder Körperhomomorphismus ist injektiv: 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 $a = b$.

(6) Seien p,q prim. Gibt es einen Körperhomomorphismus $\rho : \mathbb{Z}_p \to \mathbb{Z}_q$, dann $p = q$ und ρ=id: 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 $\rho(k) = \rho(1+\ldots+1) = \rho(1)+\ldots+\rho(1) = 1+\ldots+1 = k$ für jedes $k \in \mathbb{F}_p$.

(7) 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 *Körpererweiterung* von $\mathbb{R}$: $\mathbb{C} = \mathbb{R}(i)$. ◊