Halbgruppen, Gruppen, Ringe

Einige Bezeichnungen.

Die Menge $\mathbb{N}_0$ der natürlichen Zahlen $0, 1, 2, \ldots$.
Die Menge $\mathbb{N} = \mathbb{N}_1$ der von Null verschiedenen natürlichen Zahlen.
Die Menge $\mathbb{Z}$ der ganzen Zahlen, also $\ldots, -2, -1, 0, 1, 2, \ldots$.
Die Menge $\mathbb{Q}$ der rationalen Zahlen (eine rationale Zahl hat die Form $\frac{a}{b}$ mit $a, b \in \mathbb{Z}$ und $b \neq 0$.)
Die Menge $\mathbb{R}$ der reellen Zahlen.

Ist R ein Ring (siehe unten), so bezeichnen wir mit R^* die Menge der invertierbaren Elemente in R.

Das Produkt zweier Mengen. Abbildungen.

Seien A, B Mengen. Das *Produkt* $A \times B$ der Mengen A, B ist die Menge aller Paare (a, b) mit $a \in A$, $b \in B$. Eine *Abbildung* $f\colon A \to B$ ist eine Teilmenge $f \subseteq A \times B$ mit folgenden Eigenschaften:

(A1) Zu jedem $a \in A$ gibt es ein $b \in B$ mit $(a, b) \in f$.
(A2) Gehören die Paare (a, b_1) und (a, b_2) zu f, mit $a \in A$ und $b_1, b_2 \in B$, so ist $b_1 = b_2$.

Sei $f\colon A \to B$ eine Abbildung. Meist schreibt man statt $(a, b) \in f$ lieber $f(a) = b$ oder auch $a \mapsto b$.

Halbgruppen.

Sei S eine Menge. Eine *Verknüpfung* auf S ist eine Abbildung $\mu\colon S \times S \to S$, statt $\mu(s_1, s_2)$ schreibt man manchmal $s_1 + s_2$ oder $s_1 s_2$ oder $s_1 * s_2$ oder $s_1 \circ s_2$ oder $\ldots$.

Eine *Halbgruppe* $H = (H, *)$ ist eine Menge H mit einer Verknüpfung (die $(h_1, h_2) \mapsto h_1 * h_2$ geschrieben wird), mit folgenden Eigenschaften:

(H1) Für alle $h_1, h_2, h_3 \in H$ gilt $(h_1 * h_2) * h_3 = h_1 * (h_2 * h_3)$ (Assoziativität).
(H2) Es gibt ein Element $e \in H$ mit $e * h = h = h * e$ für alle $h \in H$. (Einselement).

Lemma. *Eine Halbgruppe H hat nur ein Einselement.* (Beweis: Sind Elemente $e, e' \in H$ gegeben mit $e * h = h = h * e$ und $e' * h = h = h * e'$ für alle $h \in H$, so ist $e = e * e' = e'$.) Dieser Beweis zeigt sogar: Das Einselement einer Halbgruppe ist die einzige "Rechts-Eins" und die einzige "Links-Eins"; dabei ist eine "Rechts-Eins" ein Element r mit $h * r = h$ für alle $h \in H$, eine "Links-Eins" $\ldots$. Man schreibt manchmal 1_H für das Einselement der Halbgruppe H. Ist H eine Halbgruppe, so heißt $h \in H$ *idempotent*, falls $h * h = h$ gilt. Das Einselement einer Halbgruppe ist idempotent, im allgemeinen wird es aber in einer Halbgruppe weitere idempotente Elemente geben.

Eine Halbgruppe H heißt *kommutativ* oder auch *abelsch* falls gilt: $h_1 * h_2 = h_2 * h_1$ für alle $h_1, h_2 \in H$. In abelschen Halbgruppen bezeichnet man oft die Verknüpfung mit dem Symbol $+$ und man spricht dann statt vom Einselement der

Halbgruppe von der Null der Halbgruppe (Rechenregel: $0 + h = h = h + 0$, für alle $h \in H$).

Ist $H = (H, \cdot)$ eine Halbgruppe und U eine Untermenge von H, so sagt man, daß U *unter der Multiplikation abgeschlossen* ist, falls gilt: Sind $u_1, u_2 \in U$, so ist auch $u_1 u_2 \in U$. Eine Untermenge, die unter der Multiplikation abgeschlossen ist und die das Einselement enthält, ist selbst wieder eine Halbgruppe.

BEISPIELKLASSEN VON HALBGRUPPEN:

Um Beispiele von Halbgruppen zu finden, sehe man sich die Beispiele von Gruppen an (jede Gruppe ist eine Halbgruppe), auch sehe man sich die Beispiele von Ringen und von Körpern an (ist R ein Ring, so sind $(R, +)$ und $(R, \cdot)$ Halbgruppen; ist R sogar ein Körper, so ist zusätzlich auch $(R^*, \cdot)$ eine Halbgruppe). Insbesondere ist die Menge $M(n \times n, R)$ für jeden Ring R bezüglich der Multiplikation eine Halbgruppe (natürlich auch bezüglich der Addition). Und $(\mathbb{N}_0, +)$ und $(\mathbb{N}_0, \cdot)$ sind ebenfalls Halbgruppen. Hier einige derartige Halbgruppen:

Zahlbereiche, die Halbgruppen sind:

$(\mathbb{N}_0, +)$,	$(\mathbb{N}_0, \cdot)$,	$(\mathbb{N}_1, \cdot)$,
$(\mathbb{Z}, +)$,	$(\mathbb{Z}, \cdot)$,	$(\mathbb{Z} \setminus \{0\}, \cdot)$,
$(\mathbb{Q}, +)$,	$(\mathbb{Q}, \cdot)$,	$(\mathbb{Q}^*, \cdot)$,
$(\mathbb{R}, +)$,	$(\mathbb{R}, \cdot)$,	$(\mathbb{R}^*, \cdot)$.

Die Potenzmenge als Halbgruppe. Sei M eine Menge und $\mathcal{P}(M)$ die Potenzmenge von M, also die Menge aller Teilmengen von M. Es ist $(\mathcal{P}(M), \cup)$ eine Halbgruppe, jedes Element dieser Halbgruppe ist idempotent, und die leere Menge $\emptyset$ ist Einselement.

Auch $(\mathcal{P}(M), \cap)$ ist eine eine Halbgruppe, jedes Element dieser Halbgruppe ist idempotent, und die Menge M ist Einselement.

Ein Element h einer Halbgruppe $(H, \cdot)$ heißt *invertierbar*, wenn es ein $h' \in H$ mit $hh' = h'h = 1_H$ gibt. Existiert ein derartiges Element h', so ist es eindeutig bestimmt und wird das *zu h inverse* Element genannt, und man schreibt h^{-1} statt h' (die Eindeutigkeit sieht man so: ist auch $hh'' = h''h = 1_H$, so ist $h' = h' \cdot 1_H = h'(hh'') = (h'h)h'' = 1_H \cdot h'' = h''$). Sind die Elemente $h_1, h_2 \in H$ invertierbar, so ist auch $h_1 h_2$ invertierbar und es gilt $(h_1 h_2)^{-1} = h_2^{-1} h_1^{-1}$ (beachte die Reihenfolge).

Gruppen. Eine *Gruppe* $G = (G, *)$ ist eine Halbgruppe, in der zusätzlich gilt:
(G) Zu jedem Element $g \in G$ gibt es ein $g' \in G$ mit $gg' = 1_G$.

Ist G eine Gruppe, und gilt $gg' = 1_G$, so gilt auch $g'g = 1_G$, es ist also $g' = g^{-1}$; jedes Element in G ist also invertierbar. (Beweis: Sei $gg' = 1_G$. Zu g' gibt es ebenfalls ein Element $g'' \in G$ mit $g'g'' = 1_G$. Dann ist aber $g = g \cdot 1_G = g(g'g'') = (gg')g'' = 1_G \cdot g'' = g''$. Also gilt $g'g = g'g'' = 1_G$.)

In einer Gruppe G ist das Einselement e das einzige idempotente Element. (In einer Halbgruppe kann es viele idempotente Elemente geben, wie die Halbgruppe $(\mathcal{P}(M), \Delta)$ des ersten Übungsblatts zeigt.)

Untergruppen. Sei $G = (G; *)$ eine Gruppe. Eine nicht-leere Teilmenge U von G heißt *Untergruppe,* falls U unter der Multiplikation und unter der Inversen-Bildung abgeschlossen ist (es gelten also die beiden Regeln: Sind $u_1, u_2 \in U$, so ist auch $u_1 * u_2 \in U$. Und: Ist $u \in U$, so auch $u^{-1} \in U$. (Man beachte, dass daraus unmittelbar folgt, daß das Einselement 1_G zu U gehört: wir setzen ja voraus, daß U nicht leer ist, sei etwa $u \in U$; dann ist auch $u^{-1} \in U$ und demnach $1_G = u * u^{-1} \in U$.) Natürlich ist eine Untergruppe selbst eine Gruppe.

Sei $G = (G, *)$ eine Gruppe und S eine beliebige Teilmenge. Sei $S' = S \cup \{s^{-1} \mid s \in S\}$ (wir fügen also alle Elemente hinzu, die zu Elementen aus S invers sind; beachte, dass S' abgeschlossen unter Inversen-Bildung ist - denn es ist $(s^{-1})^{-1} = s$). Sei nun S'' die Menge aller Produkte $x_1 * x_2 * \cdots * x_t$ mit $x_i \in S'$, für alle $1 \leq i \leq t$; dabei sei $t \geq 0$. (Hier verwendet man die in der Mathematik übliche Konvention, dass solche Mehrfachprodukte mit t Faktoren auch für $t = 1$ und sogar für $t = 0$ definiert sind: Für $t = 1$ versteht man unter $x_1 * x_2 * \cdots * x_t$ das Element x_1, für $t = 0$ bezeichnet der Ausdruck $x_1 * x_2 * \cdots * x_t$ das Einselement 1_G; dies ist eine vielleicht willkürliche, aber praktische Festsetzung). Beachte: S'' ist offensichtlich unter Multiplikation abgeschlossen (denn gehören die Elemente $x_1 * x_2 * \cdots * x_t$ und $y_1 * y_2 * \cdots * y_{t'}$ zu S'', so auch $x_1 * x_2 * \cdots * x_t * y_1 * y_2 * \cdots * y_{t'}$), aber auch unter Inversen-Bildung (denn gehört $x_1 * x_2 * \cdots * x_t$ zu S'', so auch $(x_1 * x_2 * \cdots * x_t)^{-1} = x_t^{-1} * \cdots * x_1^{-1}$). Da auch 1_G zu S'' gehört, ist S'' nicht leer (selbst wenn S leer sein sollte). Also ist S'' eine Untergruppe, und zwar eine Untergruppe, die S enthält. Und offensichtlich gilt: *S'' ist die kleinste Untergruppe von G, die S enthält* (denn ist U eine Untergruppe von G mit $S \subseteq U$, so gilt $S' \subseteq U$, da U unter Inversen-Bildung abgeschlossen ist, und dann auch $S'' \subseteq U$, da U unter Multiplikation abgeschlossen ist.

Lemma. *Sei H eine endliche Halbgruppe mit folgender Eigenschaft: Sind g, h_1, h_2 Elemente von H mit $gh_1 = gh_2$, so ist $h_1 = h_2$ (Linkskürzungs-Eigenschaft). Dann ist H eine Gruppe.* Beweis: Sei $g \in H$, wir suchen ein Element g' mit $gg' = 1$. Die Halbgruppe H habe n Elemente und $h_1, \ldots, h_n$ sei die Liste aller Elemente von H. Da die Elemente $gh_1, \ldots, gh_n$ paarweise verschieden sind, sind dies wieder alle Elemente, insbesondere ist das Einselement 1_H eines dieser Elemente. Dies zeigt, daß es ein Element h_i mit $gh_i = 1$ gibt.

Gruppen-Homomorphismen. Sind $G = (G, *)$ und $H = (H, \circ)$ Gruppen, und $f\colon G \to H$ eine Abbildung, so nennt man f einen Gruppen-Homomorphismus, falls für alle $g_1, g_2 \in H$ gilt

$$f(g_1 * g_2) = f(g_1) \circ f(g_2).$$

Einen Homomorphismus, der bijektiv ist, nennt man einen *Isomorphismus.*

Ist $f\colon G \to H$ ein Gruppen-Homomorphismus, so ist $f(1_G) = 1_H$ und $f(g^{-1}) = f(g)^{-1}$, für jedes $g \in G$. (Beweis: Es ist $f(1_G)^2 = f(1_G^2) = f(1_G)$. Und $f(g^{-1})f(g) = f(g^{-1}g) = f(1_G) = 1_H$.)

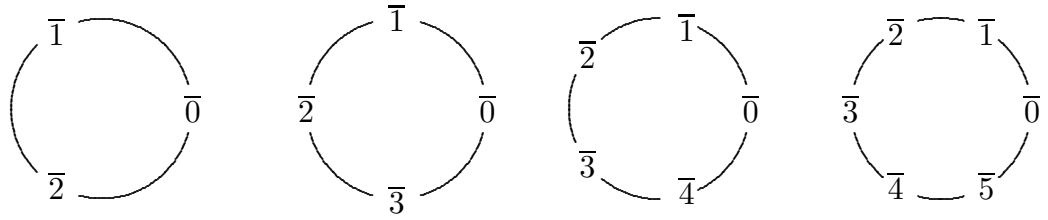
Ist $f\colon G \to H$ ein Gruppen-Homomorphismus, so nennt man $\mathrm{Ker}(f) = \{g \in G \mid f(g) = 1_H\}$ den *Kern* von f. *Dies ist eine Untergruppe von G.*

BEISPIELKLASSEN VON GRUPPEN:

Zahlbereiche, die Gruppen sind: $(\mathbb{Z},+),(\mathbb{Q},+),\mathbb{Q}^*=(\mathbb{Q}\setminus\{0\},\cdot)$, usw.

Geometrisch motivierte Gruppen. Sei $n\geq 3$. Sei E_n ein regelmäßiges n-Eck in der Ebene. Sei D_n die Menge aller Symmetrien der Ebene, die das n-Eck auf sich abbilden (also Drehungen und Spiegelungen). Insgesamt gibt es n Drehungen (nämlich mit den Drehwinkeln $\frac{i}{n}360$ mit $0\leq i<n$) und n Spiegelungen. Es gilt also $|D_n|=2n$. Ist $n\geq 3$, so ist D_n nicht abelsch.

Die zyklischen Gruppen. Sei $n\geq 1$. Sei $n\mathbb{Z}$ die Menge der Vielfachen von n, also die Menge der ganzen Zahlen, die durch n ohne Rest teilbar sind. Für jede ganze Zahl a setze $\overline{a}=a+n\mathbb{Z}$. Beachte: *Es gilt* $\overline{a_1}=\overline{a_2}$ *genau dann, wenn* a_1-a_2 *durch* n *teilbar ist.* Ist $0\leq a<n$, so ist $\overline{a}$ die Menge der ganzen Zahlen, die bei Division durch n den Rest a liefern (man nennt dies eine Restklasse modulo n). Man schreibt $\mathbb{Z}/n\mathbb{Z}$ für die Menge der Restklassen modulo n, und man definiert auf dieser Menge eine Addition vermöge $\overline{a_1}+\overline{a_2}=\overline{a_1+a_2}$. (Zu zeigen: dies ist wohl-definiert). *Mit dieser Addition ist* $\mathbb{Z}/n\mathbb{Z}$ *eine Gruppe,* die zyklische Gruppe der Ordnung n. Für $n\geq 3$ ist dies gerade die Drehgruppe des regulären n-Ecks. Man nennt diese Gruppen $(\mathbb{Z}/n\mathbb{Z},+)$ die *endlichen zyklischen Gruppen.* Zusätzlich nennt man $(\mathbb{Z},+)$ die *unendliche zyklische Gruppe.* Um zu verstehen, warum die endlichen zyklischen Gruppen "zyklisch" heißen, empfiehlt es sich, die Elemente im Kreis anzuorden und die Abbildung $+\overline{1}$ zu betrachten: Hier die Bilder für $n=3,4,5,6$.



Das entsprechende Bild für die unendliche zyklische Gruppe wäre die (ganzzahlige) Zahlengerade, also ein "Zykel mit unendlichem Radius":

$$\cdots \quad — \ -1 — \ 0 \ — \ 1 \ — \ 2 \ — \quad \cdots$$

Die Abbildung $\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}$ mit $z\mapsto\overline{z}$ ist ein Gruppen-Homomorphismus, sein Kern ist $n\mathbb{Z}$.

Ist G eine Gruppe und $g\in G$, so erhält man durch $\phi_g\colon\mathbb{Z}\to G$ mit $\phi_g(z)=g^z$ einen Gruppen-Homomorphismus. Ist ϕ_g injektiv, so erhält man einen Isomorphismus $\mathbb{Z}\to\{g^z\mid z\in\mathbb{Z}\}$ und $\{g^z\mid z\in\mathbb{Z}\}$ ist die von g erzeugte Untergruppe von G. Andernfalls wähle die minimale natürliche Zahl n mit $\phi_g(n)=1_G$. Dann erhalten wir einen Isomorphismus $\mathbb{Z}/n\mathbb{Z}\to\{g^z\mid z\in\mathbb{Z}\}$.

Ringe.

Definition: Ein *Ring* $R = (R, +, \cdot)$ ist eine Menge R mit zwei Verknüpfungen $+$ und $\cdot$, so daß die folgenden Eigenschaften erfüllt sind:

(R1) $(R, +)$ ist eine abelsche Gruppe.

(R2) $(R, \cdot)$ ist eine Halbgruppe.

(R3) Sind r, r_1, r_2 Elemente von R, so gilt $r(r_1 + r_2) = rr_1 + rr_2$ und $(r_1 + r_2)r = r_1r + r_2r$.

Das Einselement von $(R, +)$ bezeichnet man mit 0_R oder einfach mit 0 und nennt es die *Null* des Rings. Das Einselement von $(R, \cdot)$ bezeichnet man mit 1_R oder einfach mit 1 und nennt es die *Eins* von R. Ein Element $r \in R$ heißt *invertierbar,* wenn es als Element der Halbgruppe $(R, \cdot)$ invertierbar ist, wenn es also ein $r' \in R$ mit $rr' = 1_R = r'r$ gibt, und man schreibt dann r^{-1} statt r'. Ist $(R, \cdot)$ abelsch, so nennt man R einen *kommutativen* Ring.

Einfach zu zeigen ist: *Ist R ein Ring, und $r \in R$, so ist $0 \cdot r = 0 = r \cdot 0$.* Beweis: Es ist $0 \cdot r = (0+0) \cdot r = 0 \cdot r + 0 \cdot r$, also ist $0 \cdot r$ ein idempotentes Element der Gruppe $(R, +)$. Das einzige idempotente Element einer Gruppe ist aber ihr Einselement.

Ist R ein Ring und gibt es eine natürliche Zahl $n \geq 1$ mit $\underbrace{1 + 1 + \cdots + 1}_{n} = 0$, so nennt man die kleinste derartige Zahl n die *Charakteristik* des Rings R und man schreibt $\operatorname{char} R = n$. Gibt es keine solche Zahl n, so schreibt man $\operatorname{char} R = 0$.

Sind $R = (R, +, \cdot)$ und $S = (S, +, \cdot)$ Ringe, so ist ein *Ring-Homomorphismus* $f \colon R \to S$ eine Abbildung mit folgenden Eigenschaften:

(1) $f \colon (R, +) \to (S, +)$ ist ein Gruppen-Homomorphismus.

(2) $f(r_1 \cdot r_2) = f(r_1) \cdot f(r_2)$ für alle $r_1, r_2 \in R$.

(3) $f(1_R) = 1_S$.

BEISPIELKLASSEN VON RINGEN.

A) Die Zahlbereiche $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ sind kommutative Ringe

B) Sei $n \geq 1$. Auf der abelschen Gruppe $\mathbb{Z}/n\mathbb{Z}$ definiert man eine Multiplikation durch $\overline{a_1} \cdot \overline{a_2} = \overline{a_1 a_2}$ (wieder ist zu zeigen, daß dies wohl-definiert ist). Auf diese Weise wird $\mathbb{Z}/n\mathbb{Z}$ zu einem kommutativen Ring. Beachte: Im Ring $\mathbb{Z}/n\mathbb{Z}$ gilt:

$$\underbrace{1 + 1 + \cdots + 1}_{n} = 0,$$

$\mathbb{Z}/n\mathbb{Z}$ ist ein Ring der Characteristik n.

Sei nun ein Ring R gegeben. Es gibt eine Vielzahl von Möglichkeiten, um mit Hilfe von R neue Ringe zu konstruieren.

C) Der Matrizenring $M(n \times n, R)$. Sei $n \geq 1$ eine natürliche Zahl. Die Menge der $(n \times n)$-Matrizen mit Koeffizienten in R ist bezüglich der Addition und der Multiplikation von Matrizen wieder ein Ring. Ist $n \geq 2$ und hat R mindestens zwei Elemente, so ist $M(n \times n, R)$ nicht kommutativ.

D) Der Funktionenring $\mathrm{Abb}(S,R)$**.** Sei S eine Menge, sei $\mathrm{Abb}(S,R)$ die Menge der Abbildungen $S \to R$. Definiere auf $\mathrm{Abb}(S,R)$ Addition und Multiplikation komponentenweise (d.h.: sind $f,g\colon S \to R$ Abbildungen, so definiere $f+g$ und fg durch

$$(f+g)(s) = f(s)+g(s), \quad \text{und} \quad (fg)(s) = f(s)g(s) \quad \text{für} \quad s \in S.$$

Mit diesen Verknüpfungen ist $\mathrm{Abb}(S,R)$ ein Ring. Ist R kommutativ, so ist der Ring $\mathrm{Abb}(S,R)$ kommutativ.

Ist $s \in S$, so definiert man $e_s\colon \mathrm{Abb}(S,R) \to R$ durch $e_s(f) = f(s)$ (man nennt dies die Auswertung von f an der Stelle s). Die Abbildung $e_s\colon \mathrm{Abb}(S,R) \to R$ ist ein Ring-Homomorphismus.

E) Der Polynomring $R[T]$**.** Sei $R[T]$ die Menge der Folgen $(a_0,a_1,\dots)$ von Elementen $a_i \in R$ für die $a_i = 0$ für $i \gg 0$ gilt (es gibt also ein $n \in \mathbb{N}_0$ mit $a_i = 0$ falls $i > n$). Wir betrachten auf $R[T]$ die komponentenweise Addition (also $(a_0,a_1,\dots)+(b_0,b_1,\dots) = (a_0+b_0,a_1+b_1,\dots)$. Die Multiplikation ist folgendermaßen definiert:

$$(a_0,a_1,\dots)\cdot(b_0,b_1,\dots) = (c_0,c_1,\dots)$$
$$\text{mit} \quad c_k = a_0b_k + a_1b_{k-1} + \cdots + a_kb_0 = \sum_{i+j=k} a_ib_j.$$

Elemente in $R[T]$ werden üblicherweise in folgenderweise notiert: Statt $(a_0,a_1,\dots)$ schreibt man $\sum_i a_iT^i$ (dabei ist also $1 = T^0 = (1,0,\dots), T = T^1 = (0,1,0,\dots)$ und so weiter).

Die Abbildung $e\colon R[T] \to \mathrm{Abb}(R,R)$ mit $e(f)(r) = f(r)$ für $f = f(T) \in R[T]$ und $r \in R$ ist ein Ring-Homomorphismus.