2. Gruppen und Körper

(2.1) Def. Eine Gruppe ist eine Menge, genannt G, und eine Abbildung ("innere Verknüpfung") von $G \times G$ nach G, hier bezeichnet als

$$\top : G \times G \to G, (a, b) =: ab,$$

so daß folgende Eigenschaften erfüllt sind:

(G_1) Für alle $a, b, c \in G$ gilt: $(a \top b) \top c = a \top (b \top c)$ (Assoziativgesetz)
Es existiert ein Element $e \in G$, so daß gilt:
(G_2) Für alle $a \in G$ gilt $e \top a = a$ (Existenz eines "Linksneutralen")
(G_3) Für alle $a \in G$ existiert ein $b \in G$, so daß gilt: $b \top a = e$. (Ex. eines "Linksinversen")

Eine Gruppe $(G, \top)$ heißt abelsch (oder kommutativ), falls für alle $a, b \in G$ gilt: $a \top b = b \top a$

Die Anzahl der Elemente von G heißt die Ordnung $|G| \in \mathbb{N} \cup \{\infty\}$ einer Gruppe $(G, \top)$. $(G, \top)$ heißt endliche Gruppe, falls $|G| < \infty$ und sonst unendliche Gruppe.

Bem.: Die abelschen Gruppen sind nach dem norwegischen Mathematiker Niels Henrik Abel (1802-1829) benannt.

Beispiele:

1) Einfachste Gruppe: $G = \{e\}$ (mit $e \top e := e$)
2) Zweiteinfachste Gruppe: $G = \{e, a\}$ mit $a \neq e$, wobei $a \top a := e$ (und $e \top a = a \top e = e$)
3) $G := \mathbb{Z}$, $\top := + \rightsquigarrow (\mathbb{Z}, +)$ "unendlich zyklische Gruppe"
   Ebenso: $(\mathbb{Q}, +), (\mathbb{R}, +)$. Hier stets $e := 0$.
   $(\mathbb{N}, +)$ ist keine Gruppe: Es müßte $e = 0$ gelten, aber es existiert zu keinem $n \in \mathbb{N}$ mit $n > 0$ ein additives Inverses. (d.h. (G_3) ist nicht erfüllt).
4) $(\mathbb{Q}_{>0}, \cdot), (\mathbb{R}_{>0}, \cdot), (\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{R} \setminus \{0\}, \cdot)$ sind Gruppen.
   Hier stets $e := 1$.
   $(\mathbb{Z} \setminus \{0\}, \cdot)$ ist keine Gruppe.

Alle Gruppen unter 1) - 4) sind abelsch, die unter 3) und 4) sind unendlich.

5) M Menge: Sei $S_M = \{f : M \to M \mid f \text{ bijektiv}\}$. S_M mit der Hintereinanderausführung $\circ$ als innere Verknüpfung ist Gruppe. $S_n := S_{\{1,\ldots,n\}}$

Zur Motivation: Der Begriff "Gruppe" ist eng verknüpft mit dem Bemühen, die Symmetrien von Figuren (in der Ebene oder im Raum) zu verstehen. Was soll es z.B. bedeuten, daß zwei verschiedene Figuren "die gleiche Symmetrie" besitzen?

Für eine gegebene Figur F betrachtet man die Menge G_F der Kongruenzabbildungen ("Isometrien") der Ebene bzw. des Raumes, die F in sich überführen. G_F mit der inneren Verknüpfung "Hintereinanderausführung" ist eine Gruppe (die "Isometriegruppe" von F)

1) $F =$ gleichseitiges Dreieck $\Rightarrow |G_F| = 6$
   nämlich: G_F besteht aus den Drehungen um $120°$ um den Mittelpunkt und den Spiegelungen an den 3 Höhen.
2) $F =$ regelmäßiges n-Eck $\Rightarrow |G_F| = 2n$
3) $F =$ Kreis $\Rightarrow |G_F| = \infty$
4) Es gibt (außer den aus 1) und 2) abgeleiteten) im Wesentlichen nur 3 endliche Gruppen von Kongruenzabbildungen des Raumes, nämlich die Isometriegruppen von
   a) Regulärem Tetraeder mit $|G| = 24$
   b) Würfel (=Isometriegruppe des regulären Oktaeders) mit $|G| = 48$
   c) Regulärem Dodekaeder (=Isometriegruppe des reg. Ikosaeders) mit $|G| = 120$

   Alle diese Gruppen sind nicht abelsch.

Vorsicht: Es gibt "verschiedene" Gruppen mit der gleichen Ordnung.
Nach jahrzehntelanger Anstrengung vieler Mathematiker hat man einen genauen Überblick über <u>alle</u> endlichen Gruppen (Beweise in Gesamtlänge von über 3000 Seiten)

Beispiel: Die (endliche) zyklische Gruppe $(\mathbb{Z}_p, +)$ (wobei $p \in \mathbb{N}, p \geq 2$). Die Menge $\mathbb{Z}_p$ besteht aus den Restklassen $\pmod p$, d.h.

$$\mathbb{Z}_p = \{[0]_p, [1]_p, \ldots, [p-1]_p\} = \{[m]_p \mid m \in \mathbb{Z}\}$$

Seien $a, b \in \mathbb{Z}_p$. Wir wollen $a \top b$, hier geschrieben $a + b$, definieren. Dazu wählen wir ein $m \in a \subseteq \mathbb{Z}, n \in b \subseteq \mathbb{Z}$, und überlegen, daß die Restklasse $[m+n]_p$ nicht von diesen Wahlen abhängt: Jedes andere $\tilde{m} \in a$ kann nämlich als $\tilde{m} = m + lp$ für ein $l \in \mathbb{Z}$ geschrieben werden und ebenso jedes andere $\tilde{n} \in b$ als $\tilde{n} = n + jp$ für ein $j \in \mathbb{Z}$. Also:

$$\tilde{m} + \tilde{n} = m + n + (j+l)p, \text{ d.h. } [\tilde{m} + \tilde{n}]_p = [m+n]_p$$

Wir können also definieren

$$a + b = [m+n]_p$$

und das ist unabhängig von der Wahl von $m \in a$ und $n \in b$.

Es gilt dann mit $m \in a, n \in b$ und $l \in c \in \mathbb{Z}_p$:

$$\begin{array}{lcll}
(a+b)+c & = & [(m+n)+l]_p = [m+(n+l)]_p = a+(b+c) & \text{Assoziativgesetz} \\
a+b & = & [(m+n)]_p = [n+m]_p = b+a & (\Rightarrow (\mathbb{Z}_p,+) \text{ ist abelsch}) \\
[0]_p + a & = & [(0+m)]_p = [m]_p = a & ([0]_p \text{ ist neutrales Element}) \\
[-m]_p + a & = & [-m+m]_p = [0]_p & ([-m]_p \text{ ist bzgl. + invers zu } [m]_p)
\end{array}$$

$(\mathbb{Z}_p, +)$ heißt zyklisch, weil es ein Element $a \in \mathbb{Z}_p$ gibt, so daß

$$\mathbb{Z}_p = \{[0]_p, a, a+a, \ldots, \underbrace{a + \ldots + a}_{(p-1)-\text{mal}}\}$$

während $\underbrace{a + \ldots + a}_{p-\text{mal}} = [0]_p$ gilt, nämlich $a = [1]_p$.

Die Gruppe $(\mathbb{Z}_p, +)$ verhält sich genau gleich wie die ("ist isomorph zur") Gruppe der Drehungen der Ebene (um einen festen Punkt) um die Winkel $\frac{m}{p} \cdot 360°$, $m \in \{0, \ldots, p-1\}$.

(2.2) Fakt: Sei $(G, \top)$ eine Gruppe. Dann gilt:

(i) Es gibt nur ein Element in G, für das (G_2) gilt (nämlich e).
Für alle $a \in G$ gilt: $a \top e = a$.

(ii) Zu jedem $a \in G$ existiert nur ein $b \in G$, für das $b \top a = e$ gilt.
Für dieses b gilt auch: $a \top b = e$.

Bezeichnung: Das Element $b \in G$ mit $b \top a = a \top b = e$ wird mit a^{-1} (bzw. mit $-a$, falls $\top = +$) bezeichnet.

Beweis: Zeige zunächst:

$(*)$ $\qquad a, b \in G$ und $b \top a = e \Rightarrow a \top b = e \qquad$ ($\Rightarrow$ 2. Behauptung in (ii))

Denn: Nach (G_3) existiert zu $b \in G$ ein $c \in G$ mit $c \top b = e$. Es gilt:

$$a \top b \overset{(G_2)}{=} e \top (a \top b) = (c \top b) \top (a \top b) \overset{!}{=} c \top (\underbrace{(b \top a)}_{=e} \top b) \overset{(G_2)}{=} c \top b = e$$

zu "!": $(c \top b) \top \underbrace{(a \top b)}_{=:d} \overset{(G_1)}{=} c \top (b \top \underbrace{(a \top b)}_{=d}) \overset{(G_1)}{=} c \top ((b \top a) \top b)$ Beweis von (i): Sei $\tilde{e} \in G$ ein Element, so daß (G_2) gilt. Zu zeigen: $e = \tilde{e}$. Es gilt:

$$e \overset{(G_1)\text{für } \tilde{e}}{=} \tilde{e} \top e \overset{(*)}{=} e \top \tilde{e} \overset{(G_2)\text{für } e}{=} \tilde{e}$$

Sei $a \in G$. Wir zeigen $a \top e = a$. Nach (G_3) existiert ein $b \in G$ mit $b \top a = e$ und nach $(*)$ folgt $a \top b = e$. Also

$$a \top e = a \top (b \top a) \overset{(G_1)}{=} (a \top b) \top a = e \top a \overset{(G_2)}{=} a$$

Beweis von (ii): Seien $a, b, \tilde{b} \in G$ und es gelte: $b \top a = e = \tilde{b} \top a$. Zu zeigen: $b = \tilde{b}$

$$\text{Es gilt:} \qquad \tilde{b} \overset{(i)}{=} \tilde{b} \top e \overset{(*)}{=} \tilde{b} \top (a \top b) \overset{(G_1)}{=} (\tilde{b} \top a) \top b = e \top b \overset{(G_2)}{=} b$$

(2.3) Fakt. Sei $(G, \top)$ Gruppe, $a, b \in G$. Dann gilt:

(i) $(a^{-1})^{-1} = a$

(ii) $(a \top b)^{-1} = b^{-1} \top a^{-1}$

Beweis:

(i) Zu zeigen ist: a ist das Inverse von a^{-1}, d.h. $a \top a^{-1} = e$
Nach Definition gilt $a^{-1} \top a = e$, und nach (2.2) (ii) folgt daraus $a \top a^{-1} = e$.

(ii) Zu zeigen ist: $(b^{-1} \top a^{-1}) \top (a \top b) = e$. Wir rechnen:

$$\left(b^{-1} \top a^{-1}\right) \top (a \top b) \overset{(G_1)}{=} b^{-1} \top \left(a^{-1} \top a\right) \top b = b^{-1} \top e \top b \overset{(G_2)}{=} b^{-1} \top b = e$$

(2.4) Def.: Ein Körper ist eine Menge, genannt K, und zwei innere Verknüpfungen $+ : K \times K \to K$, $(a,b) \mapsto a+b$, und $\cdot : K \times K \to K$, $(a,b) \mapsto a \cdot b =: ab$, so daß gilt

(i) $(K,+)$ ist eine abelsche Gruppe mit neutralem Element $e =: 0$
(ii) $(K \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe mit neutralem Element $e =: 1$ (speziell $1 \neq 0$!)
(iii) $\forall a,b,c \in K : (a+b)c = (ac) + (bc)$ (Distributivgesetz)

Schreibweisen: $a + (-b) =: a - b$, $(ab) + c =: ab + c$ "Punkt vor Strich"

$(2.3)(\mathrm{i}) \Rightarrow -(-a) = a$
$(2.3)(\mathrm{ii}) \Rightarrow -(a+b) = (-b) + (-a) = -a - b$

Beispiel: $(\mathbb{R},+,\cdot), (\mathbb{Q},+,\cdot), (\mathbb{C},+,\cdot)$ sind Körper.
$(\mathbb{Z},+,\cdot)$ ist kein Körper (z.B. besitzt 2 in $\mathbb{Z}$ kein multiplikatives Inverses).

Bem.: Verzichtet man in (2.4)(ii) auf die Bedingung der Existenz von multipl. Inversen, so nennt man $(K,+,\cdot)$ einen kommutativen Ring mit 1. Verzichtet man zusätzlich auf die Kommutativität von $(K \setminus \{0\}, \cdot)$ und ergänzt (iii) durch $a(b+c) = ab + ac$, so nennt man $(K,+,\cdot)$ einen Ring mit 1. (Es wird die Existenz von $1 \in K$ mit $1 \cdot a = a \cdot 1 = a$ für alle $a \in K \setminus \{0\}$ gefordert)

Beispiel: $(\mathbb{Z},+,\cdot)$ ist kommutativer Ring mit 1.

(2.5)Rechenregeln: Sei $(K,+,\cdot)$ Körper (es genügt: Ring), $a,b,c \in K$. Dann gilt:

(i) $0 \cdot a = 0$
(ii) $a \cdot (-b) = (-a) \cdot b = -(ab) (=: -ab)$
(iii) $a(bc) = (ab)c$

Beweis:

(i) Es gilt: $0 \cdot a + a = 0 \cdot a + 1 \cdot a \overset{(2.4)(\mathrm{iii})}{=} (0+1)a = 1 \cdot a = a \quad | -a \Rightarrow 0 \cdot a = 0$
(ii) $(-a)b + ab \overset{(2.4)(\mathrm{iii})}{=} ((-a)+a)b = 0 \cdot b \overset{(\mathrm{i})}{=} 0$
(iii) Nach (2.4)(ii), falls $\{a,b,c\} \subseteq K \setminus \{0\}$. Sonst: (i) $\Rightarrow a(bc) = 0 = (ab)c$

Schreibweise: Ist $a \in K \setminus \{0\}$, $b \in K$, so schreibt man auch $a^{-1} =: \frac{1}{a}$ und $a^{-1}b = ba^{-1} =: \frac{b}{a}$.

Der Körper der komplexen Zahlen (Cardano 1501-1576, C.F. Gauß 1777-1855)

$$K = \mathbb{R}^2, \quad \begin{array}{ll} + & : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}^2, (a,b) + (c,d) := (a+c, b+d) \\ \cdot & : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}^2, (a,b) \cdot (c,d) := (ac - bd, ad + bc) \end{array}$$

Eigenschaften:

1) $(\mathbb{R}^2,+)$ ist abelsche Gruppe mit neutralem Element $e = (0,0)$.
2) $(1,0) \cdot (a,b) = (a,b)$, d.h. $(1,0)$ ist neutrales Element bezüglich $\cdot$.
3) $\cdot$ ist kommutativ: $(a,b) \cdot (a',b') = (aa' - bb', ab' + a'b) = (a',b') \cdot (a,b)$

4) Ist $(a,b) \in \mathbb{R}^2 \setminus \{(0,0)\}$, so gilt: $\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2,b^2}\right) \cdot (a,b) = (1,0)$,

d.h. $\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right) = \frac{1}{a^2+b^2}(a,-b)$ ist multiplikatives Inverses zu (a,b).

5) Für alle $(a,b), (a',b'), (a'',b'')$ in $\mathbb{R}^2$ gilt

$$((a,b)\cdot(a',b'))\cdot(a'',b'') = (a,b)\cdot((a',b')\cdot(a'',b''))$$

d.h. $\cdot$ ist assoziativ (Übung)

2)–5) $\Rightarrow$ $(\mathbb{R}^2 \setminus \{(0,0)\}, \cdot)$ ist abelsche Gruppe mit neutralem Element $(1,0)$

6) Distributivgesetz:

$$\begin{aligned}
(a,b)\cdot((a',b')+(a'',b'')) &= (a,b)\cdot(a'+a'', b'+b'') \\
&\overset{\text{Def. von}\ \cdot}{=} (a(a'+a'')-b(b'+b''), a(b'+b'')+b(a'+a'')) \\
(a,b)\cdot(a',b')+(a,b)\cdot(a'',b'') &= (aa'-bb', ab'+ba')+(aa''-bb'', ab''+a''b) \\
&= (a(a'+a'')-b(b'+b''), a(b'+b'')+b(a'+a''))
\end{aligned}$$

Aus 1)–6) folgt, daß $(\mathbb{R}^2,+,\cdot)$ ein Körper ist.

Bem.: Es gilt

$$\begin{array}{rcll}
(0,1)\cdot(0,1) &=& (-1,0) = -(1,0) & \\
(0,1)\cdot(b,0) &=& (0,b) & \forall b \in \mathbb{R} \\
(a,0)\cdot(b,0) &=& (ab,0) & \forall a,b \in \mathbb{R} \\
(a,0)\cdot(0,b) &=& (0,ab) & \forall a,b \in \mathbb{R}
\end{array}$$

Für alle reellen Zahlen a identifiziert man $(a,0)$ mit a und schreibt abkürzend $(0,1) =: i$, $(0,b) = (0,1)\cdot(b,0) =: ib =: bi$, $(a,b) = (a,0)+(0,b) =: a+ib$

Speziell: $(0,0) = 0$, $(1,0) = 1$, $(0,1) = i$ mit:

(2.6) $i^2 = -1$

Mit diesen Bezeichnungen gilt für $a, b, a', b' \in \mathbb{R}$:

(2.7) $(a+ib)+(a'+ib') = a+a'+i(b+b')$

(2.8) $(a+ib)\cdot(a'+ib') = aa'-bb'+i(ab'+ba')$

$\mathbb{C} := \{a+ib \mid a \in \mathbb{R}, b \in \mathbb{R}\}$. Die Veranschaulichung von komplexen Zahlen in der Koordinatenebene $\mathbb{R}^2$ stammt von C.F. Gauß (Gaußsche Zahlenebene).

Ist $z = a+ib \in \mathbb{C}$ mit $a \in \mathbb{R}$, $b \in \mathbb{R}$, so heißen

$$a \text{ der Realteil von } z, a =: \mathrm{Re}(z)$$
$$b \text{ der Imaginärteil von } z, b =: \mathrm{Im}(z)$$

Es gilt $z \neq 0 \Leftrightarrow (a,b) \neq (0,0) \quad (\Leftrightarrow a^2+b^2 > 0)$

4) $\Rightarrow$ Ist $z = a + ib \neq 0$, so ist das multiplikative Inverse z^{-1} von z:

(2.9) $z^{-1} = (a + ib)^{-1} = \frac{1}{a^2+b^2}(a - ib)$

Die Abbildung $z = a + ib \in \mathbb{C} \to \overline{z} = a - ib \in \mathbb{C}$ heißt Konjugation.

Es gilt: $\overline{\overline{z}} = z$, $\overline{z + w} = \overline{z} + \overline{w}$ und $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$

Ist $z = a + ib \in \mathbb{C}$, $a, b \in \mathbb{R}$, eine komplexe Zahl, so heißt $|z| = +\sqrt{a^2 + b^2} \in \mathbb{R}_{\geq 0}$ der Betrag von z. Offensichtlich gilt $z\overline{z} = |z|^2$.

Damit gilt für $z \neq 0$: $z^{-1} = \frac{\overline{z}}{|z|^2}$. Denn: $z^{-1}z = \frac{z\overline{z}}{|z|^2} = 1$.

Existenz von endlichen Körpern

Für $p \in \mathbb{N}$, $p \geq 2$, definieren wir eine Multiplikation auf

$$\mathbb{Z}_p = \{[0]_p, \ldots, [p-1]_p\} = \{[m]_p \mid m \in \mathbb{Z}\}$$

durch: $a = [m]_p, b = [n]_p \to ab = [mn]_p$ unabhängig von der Wahl von $m \in a$, $n \in b$, vgl. Blatt 3, Aufgabe 3.

Es ist leicht nachzuprüfen, daß $(\mathbb{Z}_p, +, \cdot)$ ein kommutativer Ring mit $1 (= [1]_p)$ ist.

(2.10) Satz. *Ist $p \in \mathbb{N}$ Primzahl, so ist $(\mathbb{Z}_p, +, \cdot)$ ein Körper.*

Beweis: Zu zeigen ist die Existenz eines multiplikativen Inversen für jedes $a \in \mathbb{Z}_p \setminus \{0\}$.
$a \in \mathbb{Z}_p \setminus \{0\} \Rightarrow a = [m]_p$ für ein $m \in \{1, \ldots, p-1\}$. Wir zeigen: Die Elemente $[1]_p \cdot [m]_p, [2]_p \cdot [m]_p, \ldots, [p-1]_p \cdot [m]_p$ in $\mathbb{Z}_p$ sind alle ungleich 0.
Denn $[j]_p[m]_p = [0]_p$ ist äquivalent dazu, daß p die Zahl jm teilt. Da p Primzahl ist, teilt p dann j oder m (betrachte die Primfaktorzerlegungen von j, m und jm!), d.h. $[j]_p = 0$ oder $[m]_p = 0$. Dann sind die Elemente $[1]_p \cdot [m]_p, \ldots, [p-1]_p \cdot [m]_p$ alle verschieden, denn aus $[i]_p[m]_p = [j]_p[m]_p$ folgt $[j - i]_p[m]_p = 0$. Also existiert ein $i \in \{1, \ldots, p-1\}$, so daß $[i]_p[m]_p = [1]_p$ gilt, d.h. $[i]_p$ ist multiplikatives Inverses von $a = [m]_p$.

Speziell: $(\mathbb{Z}_2, +, \cdot)$ Körper mit 2 Elementen, $\mathbb{Z}_2 = \{0, 1\}$.

Bem.: Lineare Gleichungssysteme mit Koeffizienten a_{ij} in einem Körper K und "Unbekannten" x_i in K können mit dem Gaußschen Eliminationsverfahren (1.13) gelöst werden.