§1 Algebraische Grundstrukturen

1.1 Definition (Verknüpfung)

Sei M eine Menge. Eine Verknüpfung auf M ist eine Abb. $\circ : M \times M \to M,\ (a,b) \mapsto \circ(a,b)$.
Statt $\circ(a,b)$ benutzen wir die Infixnotation $a \circ b$.
Schreibweise: $(M, \circ)$ für M mit Verknüpfung $\circ$.

Beispiel: $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$. Die Subtraktion ist *keine* Verknüpfung auf $\mathbb{N}$.

Gruppen

1.2 Definition und Satz (Gruppe)

Sei $(G, \circ)$ eine Menge mit einer Verknüpfung $\circ$. $(G, \circ)$ heißt Gruppe, falls gilt:

(a) $\forall a, b, c \in G:\ (a \circ b) \circ c = a \circ (b \circ c)$ (Assoziativgesetz)

(b) $\exists e \in G:\ \forall a \in G:\ a \circ e = e \circ a = a$ (Existenz eines neutralen Elements)

(c) $\forall a \in G\ \exists b \in G:\ a \circ b = b \circ a = e$ (Existenz eines inversen Elements zu a)

Das neutrale Element in (b) ist eindeutig bestimmt.
Ebenso ist zu jedem a in (c) b eindeutig bestimmt und wird mit a^{-1} bezeichnet.
Eine Gruppe heißt kommutativ oder abelsch, wenn zusätzlich gilt

(d) $\forall a, b \in G:\ a \circ b = b \circ a$.

Schreibweise: G anstelle von $(G, \circ)$, wenn die Verknüpfung aus dem Zusammenhang klar hervorgeht.

Beweis:

1. Sei e' ein weiteres neutrales Element. Dann
$$\left.\begin{array}{ll} e' \circ e \overset{\text{(b)}}{=} e \circ e' \overset{\text{(b)}}{=} e' & (e \text{ neutrales Element}) \\ e \circ e' \overset{\text{(b)}}{=} e' \circ e \overset{\text{(b)}}{=} e & (e' \text{ neutrales Element}) \end{array}\right\} e = e'$$

2. Sei b' ein weiteres inverses Element zu a. Dann
$a \circ b' = b' \circ a = e$ $(*)$.
Also: $b \overset{\text{(b)}}{=} b \circ e \overset{(*)}{=} b \circ (a \circ b') \overset{\text{(a)}}{=} (b \circ a) \circ b' \overset{\text{(c)}}{=} e \circ b' \overset{\text{(b)}}{=} b'$

Bemerkung: An Stelle von (b) und (c) reicht es

(b') $\exists e \in G\ \forall a \in G:\ a \circ e = a$ (Existenz eines rechtsneutralen Elements)

(c') $\forall a \in G\ \exists b \in G:\ a \circ b = e$ (Existenz eines rechtsinversen Elements zu a)

zu fordern (oder jeweils die Existenz des linksneutralen und der linksinversen Elemente).

[Denn: Sei $a \in G$. Nach (c') existiert $b \in G$ mit

$$a \circ b = e \qquad (*)$$

und $c \in G$ mit

$$b \circ c = e \qquad (**)$$

1. $e \circ a \overset{(b')}{=} e \circ (a \circ e) \overset{(**)}{=} e \circ (a \circ (b \circ c)) \overset{(a)}{=} e \circ ((a \circ b) \circ c)$
$\overset{(*)}{=} e \circ (e \circ c) \overset{(a)}{=} (e \circ e) \circ c \overset{(b')}{=} e \circ c \overset{(*)}{=} (a \circ b) \circ c$
$\overset{(a)}{=} a \circ (b \circ c) \overset{(**)}{=} a \circ e$
2. $b \circ a \overset{(b')}{=} (b \circ a) \circ e \overset{(**)}{=} (b \circ a) \circ (b \circ c) \overset{(a)}{=} ((b \circ a) \circ b) \circ c$
$\overset{(a)}{=} (b \circ (a \circ b)) \circ c \overset{(*)}{=} (b \circ e) \circ c \overset{(b')}{=} b \circ c \overset{(**)}{=} e$]

Einfache Beispiele für Gruppen:

1. $(\mathbb{Z}, +)$, $(m \cdot \mathbb{Z}, +)$ [$m \in \mathbb{N}$ fest], $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ sind abelsche Gruppen.
Neutrales Element: 0 Inverses Element zu x: $-x$
$(\mathbb{N}, +)$ und $(\mathbb{N}_0, +)$ sind *keine* Gruppen.

2. $(\mathbb{Q}\backslash\{0\}, \cdot)$, $(\mathbb{R}\backslash\{0\}, \cdot)$, $(\mathbb{Q}_+, \cdot)$, $(\mathbb{R}_+, \cdot)$ sind abelsche Gruppen.
Neutrales Element: 1 Inverses Element zu x : $\frac{1}{x}$
$(\mathbb{Z}\backslash\{0\}, \cdot)$ ist **keine** Gruppe.

3. $(\mathbb{R}^n, +)$, $(x_1, \ldots, x_n) + (y_1, \ldots, y_n) \mapsto (x_1 + y_1, \ldots, x_n + y_n)$ ist Gruppe
Neutrales Element: $(0, \ldots, 0)$ Inverses Element zu $(x_1, \ldots, x_n)$: $\underbrace{(-x_1, \ldots, -x_n)}_{=:-x}$

[Analog $(\mathbb{Q}^n, +)$, $(\mathbb{Z}^n, +)$]

1.3 Satz und Definition (Symmetrische Gruppe, Permutation)

Sei X eine nicht leere Menge. $S(X) := \{\varphi : X \to X \text{ bijektiv}\}$ ist mit der Funktionsverkettung als Verknüpfung eine Gruppe. (Sprechweise: Symmetrische Gruppe auf X)
Für $X = \{1, \ldots, n\}$ ($n \in \mathbb{N}$ fest) schreibt man $S_n := S(X)$ und nennt die Elemente von $S(X)$, d.h die bijektiven Abbildungen $\{1, \ldots, n\} \to \{1, \ldots, n\}$, Permutationen. Es gilt $|S_n| = n!$

Bemerkung:
Für Permutationen $\pi \in S_n$ [d.h. $\pi : \{1, \ldots, n\} \to \{1, \ldots, n\}$, $i \mapsto \pi(i)$, bijektiv] verwenden wir zur Vereinfachung von Rechnungen die Schreibweise $\begin{pmatrix} 1 & 2 & \ldots & n \\ \pi(1) & \pi(2) & \ldots & \pi(n) \end{pmatrix}$.

[Die Angabe eines n-Tupels $(\pi(1), \ldots, \pi(n))$ (vgl. Bsp. (d) nach 0.26) würde ebenfalls genügen und ist in Programmen oft eine geeignete Darstellung – für Rechnungen von Hand ist die obige Schreibweise günstiger.]

Beweis zu Satz 1.3:

1. f, g bijektiv auf $X \overset{0.34d}{\Longrightarrow} f \circ g$ bijektiv, d.h. die Funktionsverkettung ist eine Verknüpfung in $S(X)$

2. Das Assoziativgesetz folgt aus Satz 0.30.

3. $f \circ \mathrm{id}_X = \mathrm{id}_X \circ f = f$, d.h. id_X neutrales Element

4. $f : X \to X$ bijektiv $\overset{\text{Satz 0.34a, 0.33}}{\Longrightarrow}$ $f^{-1} : X \to X$ bijektiv $\wedge\ f^{-1} \circ f = \mathrm{id}_X$
$\wedge\ f \circ f^{-1} = \mathrm{id}_X$
Somit ist die Umkehrfunktion f^{-1} inverses Element zu f.

5. Zeige: $|S_n| = n!$
$S_n = \{\pi : \{1, \ldots, n\} \to \{1, \ldots, n\} \text{ bijektiv}\}$
$\overset{\text{Lemma 0.36}}{=} \{\pi : \{1, \ldots, n\} \to \{1, \ldots, n\} \text{ injektiv}\}$
$\overset{\text{Bsp.(d) zu 0.26}}{=} \{(a_1, \ldots, a_n) :\ a_i \in \{1, \ldots, n\} \text{ paarweise verschieden}\}$
Für a_1 bestehen n Möglichkeiten zur Auswahl, für $a_2 \neq a_1$ dann nur noch $n-1$, für $a_3 \neq a_2 \wedge a_3 \neq a_1$ lediglich noch $n-2$ usw.
Insgesamt für $(a_1, \ldots, a_n)$ dann $n(n-1)\cdots 1 = n!$

1.4 Satz

(a) Sei $m \in \mathbb{N}$. $(\mathbb{Z}_m, +)$ ist mit der Verknüpfung $[a]_m + [b]_m := [a+b]_m$ eine abelsche Gruppe mit m Elementen.

(b) Sei p eine Primzahl. $(\mathbb{Z}_p \setminus \{[0]_p\}, \cdot)$ ist mit der Verknüpfung $[a]_p \cdot [b]_p := [a \cdot b]_p$ eine abelsche Gruppe mit $p-1$ Elementen.

Beweis:

(a) $\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\} = \{[a]_m :\ a \in \mathbb{Z}\}$ mit $[a]_m := a + m\mathbb{Z} = \{a + k \cdot m : k \in \mathbb{Z}\}$ (siehe Bsp. 2 zu 0.22)
Es liegt nahe, als Verknüpfung $+ : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m,\ [a]_m + [b]_m := [a+b]_m$ zu wählen.
Dabei ist zu beachten, dass $[a]_m = [a+km]_m$ und $[b]_m = [b+lm]_m$ für $k, l \in \mathbb{Z}$ gilt. Es muss also nachgewiesen werden, dass $[a+b]_m = [a+km+b+lm]_m$ gilt.
Letzteres folgt sofort aus
$[a+b]_m = [a+km+b+lm]_m \Leftrightarrow a+b \sim a+km+b+lm \Leftrightarrow a+km+b+lm \sim a+b \Leftrightarrow m \mid (a+km+b+lm-(a+b)) \Leftrightarrow \underbrace{m \mid (km+lm)}_{\text{wahr}}$.
Nachweis der Gruppenaxiome:
Assoziativgesetz: $([a]_m + [b]_m) + [c]_m = [a+b]_m + [c]_m = [(a+b)+c]_m = [a+(b+c)]_m = [a]_m + [b+c]_m = [a]_m + ([b]_m + [c]_m)$
Neutrales Element: $[0]_m$ $(= m \cdot \mathbb{Z})$
$([a]_m + [0]_m = [a+0]_m = [0+a]_m = [0]_m + [a]_m = [a]_m)$
Inverses Element: $[-a]_m$
$([a]_m + [-a]_m = [a+(-a)]_m = [0]_m = [(-a)+a]_m = [-a]_m + [a]_m)$
Die Gruppe ist kommutativ wegen $[a]_m + [b]_m = [a+b]_m = [b+a]_m = [b]_m + [a]_m$

(b) Analog zu (a) definieren wir $[a]_p \cdot [b]_p := [a \cdot b]_p$ $(a, b \in \mathbb{Z})$
Die Wohldefiniertheit, das Assoziativgesetz, die Kommutativität und $[1]_p$ als neutrales Element ergeben sich auf $\mathbb{Z}_p$ wie in (a).
Für $[a]_p, [b]_p \neq [0]_p$ gilt $[a]_p \cdot [b]_p \neq [0]_p$, weil $[a]_p \neq [0]_p \Leftrightarrow p \nmid a$ und $p \nmid a \wedge p \nmid b \Rightarrow p \nmid a \cdot b$ nach Lemma 0.18. Daher ist die Multiplikation auch eine Verknüpfung auf $\mathbb{Z}_p \setminus \{[0]_p\}$.

Inverses Element: $\exists x \in \mathbb{Z}: \ [a]_p \cdot [x]_p = [1]_p$
$\iff \exists x \in \mathbb{Z}: \ [a \cdot x]_p = [1]_p$
$\iff \exists x \in \mathbb{Z}: \ a \cdot x \sim 1$
$\iff \exists x \in \mathbb{Z}: \ p \,|\, a \cdot x - 1$
$\iff \exists x \in \mathbb{Z}, k \in \mathbb{Z}: \ a \cdot x - 1 = k \cdot p$
$\overset{y:=-k}{\iff} \exists x, y \in \mathbb{Z}: \ a \cdot x + p \cdot y = 1$
$\overset{\text{Satz 0.16+Bem.}}{\Longleftarrow} \operatorname{ggT}(a,p) = 1 \Longleftarrow p \nmid a \iff [a]_p \neq [0]_p$

Es gilt $[x]_p \neq [0]_p$, denn: $[x]_p = [0]_p \Longrightarrow [a]_p \cdot [x]_p = [a]_p \cdot [0]_p = \overbrace{[a \cdot 0]_p}^{[0]_p} \neq [1]_p$

Schreibweise: $\bar{k} := [k]_m$, falls $[k]_m \in \mathbb{Z}_m$ und $k \in \{0, \dots, m-1\}$, d.h. $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$.
[Oft findet man die Schreibweise $\bar{k}$ für $[k]_m$ auch ohne die Einschränkung $k \in \{0, \dots, m-1\}$.]

Beispiele:

(a) $(\mathbb{Z}_4, +)$
Verknüpfungstafel:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

(b) $(\mathbb{Z}_5 \setminus \{\bar{0}\}, \cdot)$
Verknüpfungstafel:

$\cdot$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Frage: Sind beide Gruppen isomorph (=strukturell gleich)?
Umsortieren: $1, 2, 4, 3$

$\cdot$	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{3}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{3}$	$\bar{1}$
$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{1}$	$\bar{2}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{2}$	$\bar{4}$

Zum Begriff der Isomorphie:

$$\underset{G}{\begin{array}{c|ccc} \circ & a & b & \dots \\ \hline a & & a \circ b & \\ b & & & \\ \vdots & & & \end{array}} \quad \xrightarrow[\phi \text{ bijektiv}]{} \quad \underset{H}{\begin{array}{c|ccc} * & \phi(a) & \phi(b) & \dots \\ \hline \phi(a) & & \phi(a) * \phi(b) & \\ \phi(b) & & & \\ \vdots & & & \end{array}}$$

Falls $\phi(a \circ b) = \phi(a) * \phi(b) \ \ (a, b \in G)$, dann stimmen die Verknüpfungstafeln überein.

1.5 Definition (Gruppenhomomorphismus, Gruppenisomorphismus)

Seien $(G, \circ)$ und $(H, *)$ Gruppen und $\phi : G \to H$ eine Abbildung

(a) ϕ heißt Gruppenhomomorphismus, wenn $\forall a, b \in G: \ \phi(a \circ b) = \phi(a) * \phi(b)$

(b) ϕ heißt Gruppenisomorphismus, wenn ϕ ein bijektiver Gruppenhomomorphismus ist. In diesem Fall nennt man $(G, \circ)$ und $(H, *)$ isomorphe Gruppen.

Bemerkung: Die Isomorphie von Gruppen ist eine Äquivalenzrelation auf jeder Menge von Gruppen. (Evtl. ÜA)

Beispiele:

(a) $(\mathbb{R}, +)$ und $(\mathbb{R}_+, \cdot)$ sind isomorph, die Abbildung $\phi : \mathbb{R} \to \mathbb{R}_+, \ a \mapsto 2^a$ ist bijektiv und es gilt $\phi(a + b) = 2^{a+b} = 2^a \cdot 2^b = \phi(a) \cdot \phi(b) \ \ (a, b \in \mathbb{R})$.
[Man hätte als Isomorpismus auch die Funktion $\exp : \mathbb{R} \to \mathbb{R}_+, \, a \mapsto e^a$ wählen können.]

(b) $(\mathbb{Z}_4, +)$ und $(\mathbb{Z}_5 \backslash \{\bar{0}\}, \cdot)$ sind isomorph, z.B. ist $\phi : (\mathbb{Z}_4, +) \to (\mathbb{Z}_5 \backslash \{\bar{0}\}, \cdot), \ \phi([k]_4) = [2^k]_5$ $(k \in \mathbb{N}_0)$ ein wohldefinierter Gruppenisomorphismus.
Wohldefiniertheit: $\phi([k+4m]_4) = [2^{k+4m}]_5 = [2^k \cdot 16^m]_5 = [2^k]_5 \cdot [16^m]_5 = [2^k]_5 \cdot ([16]_5)^m = [2^k]_5 \cdot ([1]_5)^m = [2^k]_5 \quad (k, m \in \mathbb{N}_0)$.
Bijektivität: Wegen $\phi(\bar{0}) = \bar{1}$, $\phi(\bar{1}) = \bar{2}$, $\phi(\bar{2}) = \bar{4}$, $\phi(\bar{3}) = [2^3]_5 = \bar{3}$ sind die Funktionswerte paarweise verschieden, ϕ ist daher injektiv und somit nach Lemma 0.36 bijektiv.
Homomorphie: Für $k, l \in \mathbb{N}_0$ gilt: $\phi([k]_4 + [l]_4) = \phi([k + l]_4) = [2^{k+l}]_5 = [2^k \cdot 2^l]_5 = [2^k]_5 \cdot [2^l]_5 = \phi([k]_4) \cdot \phi([l]_4)$.

1.6 Lemma

Sei $(G, \circ)$ eine Gruppe. Dann gilt:

(a) $\forall a, b \in G: \ (a \circ b)^{-1} = b^{-1} \circ a^{-1}$

(b) $\forall a \in G: \ (a^{-1})^{-1} = a$

(c) $\forall a, b \in G: \ \exists_1 x \in G: \ a \circ x = b$
$\forall a, b \in G: \ \exists_1 y \in G: \ y \circ a = b$
(d.h. die Gleichungen $a \circ x = b$ und $y \circ a = b$ sind für alle $a, b \in G$ eindeutig lösbar)

(d) Sei $a \in G$.
Dann sind die Abbildungen $l_a : G \to G, \ l_a(x) = a \circ x$ und $r_a : G \to G, \ r_a(x) = x \circ a$ jeweils bijektiv.

Beweis: Übung

Schreibweise: $a^n := \underbrace{a \circ \ldots \circ a}_{n-\text{mal}} \qquad (n \in \mathbb{N}), \ a^0 := e$

$$a^{-n} := \underbrace{a^{-1} \circ \ldots \circ a^{-1}}_{n-\text{mal}} \quad (n \in \mathbb{N})$$

Man sieht leicht [Übung], dass

$$\begin{aligned} a^{m+n} &= a^m \circ a^n \quad (m,n \in \mathbb{Z}, a \in G) \\ \text{und } (a^m)^n &= a^{m \cdot n} \quad (m,n \in \mathbb{Z}, a \in G) \end{aligned}$$

Im Falle *additiver abelscher* Gruppen $(G,+)$ schreiben wir 0 für das neutrale Element, $-a$ für das zu a inverse Element, $n \cdot a := \underbrace{a + \cdots + a}_{n-mal}$, $0 \cdot a := 0$ und $(-n) \cdot a := n \cdot (-a)$ $(n \in \mathbb{N})$.

Es gilt dann: $(m+n) \cdot a = m \cdot a + n \cdot a$, $m \cdot (n \cdot a) = (mn) \cdot a \quad (m,n \in \mathbb{Z},\, a \in G)$.

1.7 Satz von Fermat (für endliche Gruppen)

Sei $(G, \circ)$ eine endliche Gruppe, $n = |G|$. Dann gilt für jedes $a \in G: \quad a^n = e$.

Beweis:
Wir zeigen den Satz zunächst nur für den Fall, dass G abelsch ist:
Sei $G = \{x_1, \ldots, x_n\}$ und $a \in G$. Wegen 1.6d gibt es eine Permutation $\pi \in S_n$, so dass

$$(a \circ x_1) \circ (a \circ x_2) \circ \ldots \circ (a \circ x_n) = x_{\pi(1)} \circ x_{\pi(2)} \circ \ldots \circ x_{\pi(n)}$$

Also wegen G abelsch

$$a^n \circ (x_1 \circ x_2 \circ \ldots \circ x_n) = x_1 \circ x_2 \circ \ldots \circ x_n$$

und hieraus

$$a^n = e.$$

1.8 Sätze von Fermat und Euler

(a) Sei p Primzahl, $a \in \mathbb{Z}$, $p \nmid a$. Dann gilt $a^{p-1} \equiv 1 \mod p$.

(b) Sei $n \in \mathbb{N}$, $\varphi(n) := |\{k \in \{0, \ldots, n-1\} : \ \mathrm{ggT}(k,n) = 1\}|$, $a \in \mathbb{Z}$, $\mathrm{ggT}(a,n) = 1$.
Dann gilt $a^{\varphi(n)} \equiv 1 \mod n$.

Bemerkung:

(a) Die Eulersche φ-Funktion gibt für $n \in \mathbb{N}$ (wegen $\mathrm{ggT}(n,n) = \mathrm{ggT}(0,n)$) die Anzahl der zu n teilerfremden natürlichen Zahlen $\leq n$ an. Sie lässt sich für die Primfaktorzerlegung $n = p_1^{k_1} \cdots p_l^{k_l}$ mittels

$$\varphi(n) = p_1^{k_1-1} \cdots p_l^{k_l-1} \cdot (p_1 - 1) \cdots (p_l - 1) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_l})$$

berechnen. ($l \in \mathbb{N}, p_1, \ldots, p_l$ paarweise verschiedene Primzahlen, $k_1, \ldots, k_l \in \mathbb{N}$.)
[Ohne Beweis]

(b) Der Satz von Fermat folgt aus dem Satz von Euler, weil $\varphi(p) = p - 1$.

Beweis:

(a) $G := (\mathbb{Z}_p \setminus \{[0]_p\}, \cdot)$. Dann $|G| = p - 1$ und nach Satz 1.7 $[a]_p^{p-1} = [1]_p$, falls $\underbrace{[a]_p \neq [0]_p}_{\text{d.h. } p \nmid a}$.

Das ist äquivalent zu $[a^{p-1}]_p = [1]_p$ bzw. $a^{p-1} \equiv 1 \mod p$, falls $p \nmid a$.

(b) Beweisskizze: Hier zeigt man analog dem Beweis für die Gruppeneigenschaften von $(\mathbb{Z}_p \setminus \{\bar{0}\}, \cdot)$ wiederum unter Verwendung von Satz 0.17, dass für $n \geq 2$

$\mathbb{Z}_n^* := \{[a]_n \in \mathbb{Z}_n : \overbrace{\mathrm{ggT}(a,n) = 1}^{a,n \text{ teilerfremd}},\ a \in \{0, \dots, n-1\}\}$ mit der Restklassenmultiplikation als Verknüpfung eine Gruppe mit $\varphi(n)$ Elementen bildet und wendet Satz 1.7 an.

Bemerkung:
Der Satz von Euler ist für $n = p \cdot q$ ($p \neq q$ große Primzahlen) die Grundlage der RSA-Verschlüsselung. In diesem Fall gilt $\varphi(n) = (p-1)(q-1)$. Benötigt werden noch die in der Beweisskizze angegebenen Gruppeneigenschaften von $\mathbb{Z}_n^*$ (und von $\mathbb{Z}_{\varphi(n)}^*$).

1.9 Definition (Untergruppe)

Sei $(G, \circ)$ eine Gruppe. Eine nicht leere Teilmenge U von G heißt Untergruppe von G, wenn gilt:

$$\begin{array}{ll} \forall a, b \in U: & a \circ b \in U \\ \forall a \in U: & a^{-1} \in U \end{array}$$

Bemerkung:
Mit der Verknüpfung $U \times U \to U,\ (a,b) \mapsto a \circ b$ ist U eine Gruppe.
[Denn: $U \neq \emptyset$, also $\exists c \in U$.
Dann: $c^{-1} \in U$ und $e = \underbrace{c}_{\in U} \circ \underbrace{c^{-1}}_{\in U} \in U$
Somit: $\forall a \in U: \ a \circ e = e \circ a = a$ (neutrales Element)
Außerdem: $\forall a \in U: \ \underbrace{a}_{\in U} \circ \underbrace{a^{-1}}_{\in U} = \underbrace{a^{-1}}_{\in U} \circ \underbrace{a}_{\in U} = \underbrace{e}_{\in U}$ (inverses Element)]

1.10 Untergruppenkriterium

Sei $(G, \circ)$ eine Gruppe, $\emptyset \neq U \subset G$. Dann gilt:

$$U \text{ Untergruppe von } G \iff \forall a, b \in U: \ a \circ b^{-1} \in U$$

Beweis: Übung

Beispiele:

1. $(m \cdot \mathbb{Z}, +)$ Untergruppe von $(\mathbb{Z}, +)$
   [$a \in m \cdot \mathbb{Z},\ b \in m \cdot \mathbb{Z} \Longrightarrow a + b \in m \cdot \mathbb{Z}$
   $a \in m \cdot \mathbb{Z} \Longrightarrow -a \in m \cdot \mathbb{Z}$]

2. $(\mathbb{Z}, +), (\mathbb{Q}, +)$ Untergruppen von $(\mathbb{R}, +)$

3. $(\{\bar{0}\}, +), (\{\bar{0}, \bar{2}\}, +)$ Untergruppen von $(\mathbb{Z}_4, +)$

$$\left[\begin{array}{c|cc} + & \bar{0} & \bar{2} \\ \hline \bar{0} & \bar{0} & \bar{2} \\ \bar{2} & \bar{2} & \bar{0} \end{array} \qquad \bar{2} + \bar{2} = \bar{0}, \text{ also } \bar{2} \text{ inverses Element von } \bar{2}\right]$$

4. $(\{\bar{1}\},\cdot),(\{\bar{1},\bar{4}\},\cdot)$ Untergruppen von $(\mathbb{Z}_5\backslash\{\bar{0}\},\cdot)$

$$\left[\begin{array}{c|cc} \cdot & \bar{1} & \bar{4} \\ \hline \bar{1} & \bar{1} & \bar{4} \\ \bar{4} & \bar{4} & \bar{1} \end{array} \qquad \bar{4}\cdot\bar{4}=\bar{1}, \text{ also } \bar{4} \text{ inverses Element von } \bar{4}\right]$$

5. $\{\pi : \{1,\dots,n\} \to \{1,\dots,n\} : \ \pi \text{ bijektiv} \wedge \pi(k+1)=k+1,\dots,\pi(n)=n\}$ mit festem $k \in \{1,\dots,n\}$ bildet eine Untergruppe von S_n mit $k!$ Elementen. Diese ist isomorph zu S_k.

[6. Seien G,H Gruppen und $\phi : G \to H$ ein Gruppenhomomorphismus. Dann ist $\phi(G)$ eine Untergruppe von H. (Bew.: Evtl. Übung)]

Bemerkung:
Jede Gruppe mit n Elementen ($n \in \mathbb{N}$) ist isomorph zu einer (n-elementigen) Untergruppe von S_n. (Satz von Cayley)

[*Beweis:*
Betrachte $\Phi : G \to S(G),\ a \mapsto l_a$, wobei $l_a : G \to G,\ l_a(x) = a \circ x$.
Φ ist wohldefiniert, denn nach Satz 1.6 ist l_a bijektiv, also $l_a \in S(G)$.
Φ ist ein Gruppenhomomorphismus, weil $\Phi(a \circ b) = l_{a\circ b} = l_a \circ l_b = \Phi(a) \circ \Phi(b)$.
Nach Bsp. 6 zu 1.10 ist $\Phi(G)$ eine Untergruppe von $S(G)$.
Φ ist injektiv, denn $\Phi(a) = \Phi(b) \Rightarrow l_a = l_b \Rightarrow l_a(e) = l_b(e) \Rightarrow a = b$.
Also ist G isomorph zu $\Phi(G)$ und mittels des Isomorphismus von $S(G)$ und $S_{|G|}$ isomorph zu einer Untergruppe von $S_{|G|}$.]

1.11 Satz und Definition (Erzeugendes Element, zyklische Gruppe)

Sei $(G,\circ)$ eine Gruppe, $a \in G$. Die Untergruppe $\langle a \rangle := \{a^k : k \in \mathbb{Z}\}$ von G heißt von a erzeugte zyklische Untergruppe. Falls G durch ein Element erzeugt wird, nennt man G zyklisch.

Beispiele:

1. $(\mathbb{Z},+)$ wird durch 1 erzeugt
   $(m\cdot\mathbb{Z},+)$ wird durch m erzeugt
2. $(\mathbb{Z}_m,+)$ wird durch $\bar{1}$ erzeugt
3. $(\mathbb{R},+)$ wird *nicht* durch ein $a \in \mathbb{R}$ erzeugt, denn $\langle a \rangle := \{k\cdot a : \ k \in \mathbb{Z}\} \neq \mathbb{R}$

1.12 Satz von Lagrange

Sei $(G,\circ)$ eine endliche Gruppe und U eine Untergruppe. Dann ist $|U|$ ein Teiler von $|G|$.

[*Beweis:*
Für $a \in G$ betrachte $a \circ U := \{a \circ u : \ u \in U\}$.

1. Es gilt: $|a\circ U| = |U| \quad (a \in G)$
   Das folgt sofort aus Lemma 1.6d

2. Es gilt: $a \circ U = b \circ U \;\vee\; (a \circ U) \cap (b \circ U) = \emptyset \quad (a, b \in G)$
   Denn: $x \in (a \circ U) \cap (b \circ U) \Longrightarrow x = a \circ u_1 = b \circ u_2 \quad (u_1, u_2 \in U$ geeignet $)$
   $\Longrightarrow a = b \circ (u_2 \circ u_1^{-1}) \Longrightarrow a \circ u = b \circ \underbrace{(u_2 \circ u_1^{-1} \circ u)}_{\in U}$ $(u \in U)$, d.h. $a \circ U \subset b \circ U \overset{1.}{\Longrightarrow}$ $a \circ U = b \circ U$

3. $\{a \circ U : \; a \in G\} =: \underbrace{\{a_1 \circ U, a_2 \circ U, \ldots, a_m \circ U\}}_{\text{paarweise disjunkt}}$
   Da jedes $x \in G$ genau einer der Teilmengen $a_1 \circ U, \ldots, a_m \circ U$ angehört*, folgt $|G| = m \cdot |U|$.

   $$\text{Zu } *) : \quad \bigcup_{i=1,\ldots,m} a_i \circ U = \bigcup_{a \in G} a \circ U \overset{e \in U}{\supset} \bigcup_{a \in G} \{a \circ e\} = G$$
   $$\bigcup_{i=1,\ldots,m} a_i \circ U \subset \bigcup_{i=1,\ldots,m} G = G$$
   $$\text{Also: } \bigcup_{i=1,\ldots,m} a_i \circ U = G$$
   ]

[*Bemerkung zum Beweis von 1.12:*
Tatsächlich sind $a \circ U$ die Äquivalenzklassen der Äquivalenzrelation $a \sim b :\Leftrightarrow a^{-1} \circ b \in U$
$[a] = \{x \in G : \; x \sim a\} = \{x \in G : \; a \sim x\} = \{x \in G : \; a^{-1} \circ x \in U\}$
$= \{x \in G : \; \exists u \in U : \; a^{-1} \circ x = u\} = \{x \in G : \; \exists u \in U : \; x = a \circ u\} = a \circ U$]

Mit dem Satz von Lagrange können wir auch den nicht kommutativen Fall im Satz von Fermat behandeln:
$U := \{a^k : \; k \in \mathbb{Z}\}$ ist eine abelsche Untergruppe von G ($a \in G$ fest), somit endlich. Also gilt $a^{|U|} = e$ nach dem bereits bewiesenen Teil von Satz 1.7. Mit $|G| = m \cdot |U|$ folgt $a^{|G|} = a^{|U| \cdot m} = (a^{|U|})^m = e^m = e$.

Ringe

1.13 Definition (Ring)

Sei R eine Menge mit zwei Verknüpfungen

$$+ : \; R \times R \to R, \; (a, b) \mapsto a + b \quad (\text{“Addition“})$$
$$\cdot \; : \; R \times R \to R, \; (a, b) \mapsto a \cdot b \quad (\text{“Multiplikation“})$$

. $(R, +, \cdot)$ heißt Ring, wenn gilt:

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

(b) Die Multiplikation $\cdot$ ist assoziativ. [“$(R, \cdot)$ ist Halbgruppe“]

(c) $\forall a, b, c \in R : \quad (a + b) \cdot c = a \cdot c + b \cdot c \qquad$ (Distributivgesetze)
$\qquad c \cdot (a + b) = c \cdot a + c \cdot b$

Das neutrale Element der Addition wird mit 0 bezeichnet und heißt Nullelement. Das inverse Element zu $a \in R$ bezüglich der Addition wird mit $-a$ bezeichnet.
Wir definieren $a - b := a + (-b)$ ("Subtraktion")

1.14 Definition (kommutativer Ring, Einselement, nullteilerfrei)
Sei $(R, +, \cdot)$ ein Ring.

(a) R heißt kommutativ, wenn gilt

$$\forall a, b \in R: \; a \cdot b = b \cdot a$$

(b) Ein Element $1 \in R$ heißt Einselement, wenn gilt

$$\forall a \in R: \; a \cdot 1 = 1 \cdot a = a$$

(c) R heißt nullteilerfrei, wenn gilt

$$\forall a, b \in R: \; a \cdot b = 0 \Longrightarrow a = 0 \;\vee\; b = 0$$

Bemerkung: Das Einselement ist eindeutig bestimmt, wenn es existiert.
[Beweis analog 1.2]

Beispiele:

1. $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer nullteilerfreier Ring mit Einselement.

2. $(m \cdot \mathbb{Z}, +, \cdot)$ ist für $m \in \mathbb{N}$ mit $m \geq 2$ ein kommutativer nullteilerfreier Ring ohne Einselement.

3. $(\mathbb{Z}_m, +, \cdot)$ ist für $m \geq 2$ ein kommutativer Ring mit Einselement. Er ist nullteilerfrei genau dann, wenn m Primzahl ist:

   $(\mathbb{Z}_m, +)$ abelsche Gruppe mit Nullelement $[0]_m$ folgt aus Satz 1.4a.
   $(\mathbb{Z}_m, \cdot)$ Halbgruppe ergibt sich wie im Beweis zu Satz 1.4b.
   Distributivgesetze und Kommutativität der Multiplikation analog.
   $[1]_m$ ist Einselement. (Klar!)

   1.F.: $m \geq 2$ keine Primzahl $\Longrightarrow \exists\, a, b \in \mathbb{N},\; a, b \geq 2: \; m = a \cdot b$
   $\Longrightarrow [a]_m \cdot [b]_m = [a \cdot b]_m = [m]_m = [0]_m$,
   aber $[a]_m \neq [0]_m,\; [b]_m \neq [0]_m$ wegen $m \nmid a$ und $m \nmid b$.

   2.F.: m Primzahl.
   $[a]_m \cdot [b]_m = [0]_m \Longleftrightarrow [a \cdot b]_m = [0]_m \Longleftrightarrow m | ab \overset{\text{Lemma 0.18}}{\Longrightarrow} m|a \;\vee\; m|b$
   $\Longleftrightarrow [a]_m = [0]_m \;\vee\; [b]_m = [0]_m$.

4. $\mathbb{R}^{n \times n}$ (reelle quadratische Matrizen) mit der komponentenweisen Addition und der noch einzuführenden Matrizenmultiplikation ist für $n \geq 2$ ein *nicht kommutativer* Ring mit Einselement, der *nicht* nullteilerfrei ist. (Später!)

1.15 Rechenregeln in Ringen

Sei $(R,+,\cdot)$ ein Ring, $a,b,c \in R$. Dann gilt:

(a) $0 \cdot a = a \cdot 0 = 0$

(b) $-(a \cdot b) = (-a) \cdot b = a \cdot (-b)$

(c) $(-a) \cdot (-b) = a \cdot b$

(d) R hat Einselement $\Longrightarrow -a = (-1) \cdot a = a \cdot (-1)$

(e) R nullteilerfrei $\Longrightarrow \begin{cases} (c \neq 0 \ \wedge \ a \cdot c = b \cdot c) \Longrightarrow \ a = b \\ (c \neq 0 \ \wedge \ c \cdot a = c \cdot b) \Longrightarrow \ a = b \end{cases}$ (Kürzungsregel)

Bemerkung:
Nur im Nullring $(\{0\},+,\cdot)$ stimmen Eins- und Nullelement überein.

$$\left[\left.\begin{array}{ll} \forall a \in R : a \cdot 1 = a & (1.14\text{b}) \\ \forall a \in R : a \cdot 0 = 0 & (1.15\text{a}) \end{array}\right\} \overset{1=0}{\Longrightarrow} a = 0 \right]$$

Beweis:

(a)
$$\begin{array}{ccccccc} 0 \cdot a & + & 0 \cdot a & \overset{\text{Distr.G.}}{=} & (0+0) \cdot a & \overset{\text{Neutr.E.}}{=} & 0 \cdot a \\ 0 \cdot a & + & 0 & = & & & 0 \cdot a \end{array}$$
$\overset{\text{Lemma 1.6c}}{\Longrightarrow} 0 \cdot a = 0$

(b)
$$\begin{array}{lccccc} a \cdot b + (-a) \cdot b & \overset{\text{Distr.G.}}{=} & (a + (-a)) \cdot b & = & 0 \cdot b \overset{(a)}{=} & 0 \\ a \cdot b + (-(a \cdot b)) & & & = & & 0 \end{array}$$
$\overset{\text{Lemma 1.6c}}{\Longrightarrow} -(a \cdot b) = (-a) \cdot b$

Zweite Gleichung analog

(c) $(-a) \cdot (-b) \overset{\text{(b) 1.Gl}}{=} -(a \cdot (-b)) \overset{\text{(b) 2.Gl}}{=} -(-(a \cdot b)) \overset{1.6\text{b}}{=} a \cdot b$

(d) $(-1) \cdot a \overset{(b)}{=} -(1 \cdot a) = -a$

Zweite Gleichung analog

(e) Sei R nullteilerfrei:

$a \cdot c = b \cdot c \Longrightarrow a \cdot c + (-(b \cdot c)) = 0 \overset{(b)}{\Longrightarrow} a \cdot c + (-b) \cdot c = 0$

$\overset{\text{Distr.G.}}{\Longrightarrow} (a + (-b)) \cdot c = 0 \overset{\substack{c \neq 0, \\ R \text{ nullteilerfrei}}}{\Longrightarrow} \underbrace{a + (-b)}_{=:a-b} = 0 \Longrightarrow a = -(-b) \Longleftrightarrow a = b$

Mit der Gaußschen Summenkonvention

$$\sum_{i=1}^{n} a_i := a_1 + \ldots + a_n \qquad (n \in \mathbb{N},\ a_1, \ldots, a_n \in R)$$

gelangt man zu

1.16 Rechenregeln für Summenzeichen

Sei $(R,+,\cdot)$ ein Ring, $m,n\in\mathbb{N}$. Dann gilt

(a) $\sum\limits_{i=1}^{n}(a_i+b_i)=\sum\limits_{i=1}^{n}a_i+\sum\limits_{i=1}^{n}b_i \quad (a_i,b_i\in R \text{ für } i=1,\dots,n)$

(b) $b\cdot\sum\limits_{i=1}^{n}a_i=\sum\limits_{i=1}^{n}b\cdot a_i,\quad \left(\sum\limits_{i=1}^{n}a_i\right)\cdot b=\sum\limits_{i=1}^{n}a_i\cdot b \quad (a_i\in R \text{ für } i=1,\dots,n,\ b\in R)$

(c) $\sum\limits_{i=1}^{m}\left(\sum\limits_{j=1}^{n}a_{ij}\right)=\sum\limits_{j=1}^{n}\left(\sum\limits_{i=1}^{m}a_{ij}\right) \quad (a_{ij}\in R \text{ für } i=1,\dots,m \text{ und } j=1,\dots,n)$

(d) $\left(\sum\limits_{i=1}^{m}a_i\right)\cdot\left(\sum\limits_{j=1}^{n}b_j\right)=\sum\limits_{i=1}^{m}\left(a_i\cdot\sum\limits_{j=1}^{n}b_j\right)=\sum\limits_{i=1}^{m}\left(\sum\limits_{j=1}^{n}a_i\cdot b_j\right)=\sum\limits_{j=1}^{n}\left(\sum\limits_{i=1}^{m}a_i\cdot b_j\right)$
$=\sum\limits_{j=1}^{n}\left(\sum\limits_{i=1}^{m}a_i\right)\cdot b_j \quad (a_i\in R \text{ für } i=1,\dots,m,\ b_j\in R \text{ für } j=1,\dots,n)$

[Verallgemeinerung: $\sum\limits_{i=l}^{n}a_i=a_l+\ldots+a_n \quad (n\in\mathbb{Z},\ l\in\mathbb{Z},\ l\le n,\ a_l,a_{l+1},\dots,a_n\in R)$]

Beweis: [Die Verwendung der Assoziativität wird nicht explizit erwähnt.]

(a) $\sum\limits_{i=1}^{n}(a_i+b_i)=(a_1+b_1)+(a_2+b_2)+\ldots+(a_n+b_n)\overset{\substack{\text{Addition}\\\text{kommutativ}}}{=}a_1+\ldots+a_n+b_1+\ldots+b_n=$
$\sum\limits_{i=1}^{n}a_i+\sum\limits_{i=1}^{n}b_i.$

(b) $b\cdot\sum\limits_{i=1}^{n}a_i=b\cdot(a_1+\ldots+a_n)\overset{\text{Distr.G.}}{=}b\cdot a_1+\ldots+b\cdot a_n=\sum\limits_{i=1}^{n}b\cdot a_i.$
Zweite Gleichung analog.

(c) $\sum\limits_{i=1}^{m}\sum\limits_{j=1}^{n}a_{ij}:=\sum\limits_{i=1}^{m}\underbrace{\left(\sum\limits_{j=1}^{n}a_{ij}\right)}_{\substack{s_i\\\text{hängt nur von } i \text{ ab}}}\overset{\text{s.u.}}{=}\sum\limits_{j=1}^{n}\underbrace{\left(\sum\limits_{i=1}^{m}a_{ij}\right)}_{\substack{t_j\\\text{hängt nur von } j \text{ ab}}}=:\sum\limits_{j=1}^{n}\sum\limits_{i=1}^{m}a_{ij}$

Wegen der Kommutativität der Addition können wir in der folgenden rechteckigen Anordnung die Gesamtsumme sowohl durch Addition der Zeilensummen oder durch Addition der Spaltensummen berechnen.

$$
\begin{array}{cccccccl}
 & a_{11} & +\,a_{12} & +\ldots+\,a_{1n} & = & \sum\limits_{j=1}^{n}a_{1j} & =:s_1 & \\
+ & a_{21} & +\,a_{22} & +\ldots+\,a_{2n} & =+ & \sum\limits_{j=1}^{n}a_{2j} & =:s_2 & \qquad s_i=\sum\limits_{j=1}^{n}a_{ij}\\
 & \vdots & & & & \vdots & & \\
+ & a_{m1} & +\,a_{m2} & +\ldots+\,a_{mn} & =+ & \sum\limits_{j=1}^{n}a_{mj} & \underline{=:s_m} & \\
 & \| & \| & \| & & & & \\
 & \underbrace{\sum\limits_{i=1}^{m}a_{i1}}_{=:t_1} & +\underbrace{\sum\limits_{i=1}^{m}a_{i2}}_{=:t_2} & +\ldots+\underbrace{\sum\limits_{i=1}^{m}a_{in}}_{=:t_n} & & & \sum\limits_{i=1}^{m}\underbrace{\left(\sum\limits_{j=1}^{n}a_{ij}\right)}_{s_i} & \\
 & =\sum\limits_{j=1}^{n}t_j=\sum\limits_{j=1}^{n}\left(\sum\limits_{i=1}^{m}a_{ij}\right) & & & t_j=\sum\limits_{i=1}^{m}a_{ij} & & &
\end{array}
$$

(d) Nach (b) $\left(\sum\limits_{i=1}^{m} a_i\right) \cdot b = \sum\limits_{i=1}^{m} a_i \cdot b$

Setze $b := \sum\limits_{j=1}^{n} b_j$. Dann

$$\left(\sum_{i=1}^{m} a_i\right)\left(\sum_{j=1}^{n} b_j\right) = \sum_{i=1}^{m}\left(a_i \cdot \sum_{j=1}^{n} b_j\right) \stackrel{\text{(b)}}{=} \sum_{i=1}^{m}\left(\sum_{j=1}^{n} a_i b_j\right) \stackrel{\text{(c)}}{=} \sum_{j=1}^{n}\left(\sum_{i=1}^{m} a_i b_j\right) \stackrel{\text{(b)}}{=} \sum_{j=1}^{n}\left(\sum_{i=1}^{m} a_i\right) b_j$$

[*Bemerkung:* Um nicht zu viele Klammern schreiben zu müssen, gehen wir vom folgenden

Operatorenvorrang aus: $\qquad$ *abnehmend* $\left\downarrow \begin{array}{ll} \cdot & \text{Infix} \\ \sum & \text{Präfix} \\ + & \text{Infix} \end{array}\right.$,

d.h. beispielsweise $\sum\limits_{i=1}^{n} a_i \cdot b = \sum\limits_{i=1}^{n}(a_i \cdot b)$ bzw. $\sum\limits_{i=1}^{n} a_i + b = \left(\sum\limits_{i=1}^{n} a_i\right) + b$.]

Die beiden folgenden aus der reellen Analysis bekannten Sätze lassen sich unter bestimmten Zusatzvoraussetzungen auch auf Ringe übertragen.

1.17 Binomischer Satz und geometrische Summenformel

Sei $(R, +, \cdot)$ ein Ring mit Einselement und seien $a, b \in R$ mit $a \cdot b = b \cdot a$. Mit der Definition $r^n := \underbrace{r \cdots r}_{n-mal}$ und $r^0 := 1$ $(r \in R, n \in \mathbb{N})$ gilt:

(a) $(a+b)^n = \sum\limits_{k=0}^{n} \binom{n}{k} \cdot a^k \cdot b^{n-k} = \sum\limits_{k=0}^{n} \binom{n}{k} \cdot a^{n-k} \cdot b^k \quad (n \in \mathbb{N}_0)$

(b) $a^{n+1} - b^{n+1} = (a-b) \cdot \sum\limits_{k=0}^{n} a^k \cdot b^{n-k} = (a-b) \cdot \sum\limits_{k=0}^{n} a^{n-k} \cdot b^k \quad (n \in \mathbb{N}_0)$

Bemerkung:

1. Der Ausdruck $m \cdot r$ $(m \in \mathbb{Z}, r \in R)$ ist entsprechend der nach 1.6 festgelegten Schreibweise für additive abelsche Gruppen zu verstehen.

2. Das Einselement des Rings wird benötigt, damit die Ausdrücke $a^0 \cdot b^n$ und $a^n \cdot b^0$ eine Bedeutung haben.

3. Die Bedingung $a \cdot b = b \cdot a$ ist wesentlich, wie die Identitäten
   $(a+b)^2 = a^2 + a \cdot b + b \cdot a + b^2$
   $(a-b) \cdot (a+b) = a^2 - b \cdot a + a \cdot b - b^2$
   zeigen.

4. (b) ist mit $a = 1$ und $b = q$ (oder umgekehrt mit $a = q$ und $b = 1$) eine Vorstufe zur geometrischen Summenformel.

Beweis: Analog Analysis I.

1.18 Definition und Satz (Einheitengruppe)

Sei $(R, +, \cdot)$ ein Ring mit Einselement. $a \in R$ heißt invertierbar, wenn es ein $b \in R$ gibt mit $a \cdot b = b \cdot a = 1$. Setze $R^* := \{a \in R : a \text{ invertierbar}\}$.
Dann ist $(R^*, \cdot)$ eine Gruppe. (Bezeichnung: Einheitengruppe von R).

Bemerkung: Es gilt $b \in R^*$ und wegen $(R^*, \cdot)$ Gruppe ist b eindeutig bestimmt. (Bez.: a^{-1})

Beweis: Übung

Beispiele:

(a) $\mathbb{Z}^* = \{-1, 1\}$, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$

(b) $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{\bar{0}\}$ (p Primzahl) [Bew. Satz 1.4b]
$\mathbb{Z}_n^* = \{[a]_n : a \in \{0, 1, \dots, n-1\}, \mathrm{ggT}(a, n) = 1\}$ $(n \in \mathbb{N}, n \geq 2)$ [Beweis: Evtl. Übung]

Körper

1.19 Definition (Körper)

$(K, +, \cdot)$ heißt Körper, wenn gilt:

(a) $(K, +, \cdot)$ ist ein Ring,

(b) $(K \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe.

Mit 1 bezeichnen wir das neutrale Element von $K \setminus \{0\}$.
Wir definieren: $\dfrac{a}{b} := a \cdot b^{-1}$ (“Division“)

Bemerkung:

1. Jeder Körper ist ein kommutativer nullteilerfreier Ring mit 1 als Einselement und $1 \neq 0$:

$$\left.\begin{array}{lll} \forall a, b \in K \setminus \{0\}: & a \cdot b = b \cdot a & \text{(wegen (b))} \\ \forall a \in K: & a \cdot 0 = 0 \cdot a & \text{(wegen 1.15a)} \end{array}\right\} \Longrightarrow K \text{ kommutativer Ring}$$

$$\left.\begin{array}{lll} \forall a \in K \setminus \{0\}: & a \cdot 1 = 1 \cdot a = 1 & \text{(wegen (b))} \\ & 0 \cdot 1 = 1 \cdot 0 = 0 & \text{(wegen 1.15a)} \end{array}\right\} \Longrightarrow K \text{ Ring mit 1 als Einselement}$$

Es gilt $1 \neq 0$ nach der Bem. zu 1.15, weil K wegen (b) mindestens 2 Elemente hat.

Sei $a \cdot b = 0$. Zeige $a = 0 \ \vee \ b = 0$:

1.F.: $a = 0$. Fertig.

2.F.: $a \neq 0$. Dann $a^{-1} \cdot (a \cdot b) = 0$, d.h. $b = 0$.

2. *Endliche* nullteilerfreie kommutative Ringe mit $1 \neq 0$ sind Körper. (Ohne Beweis)

Beispiele:

1. $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind Körper, $(\mathbb{Z}, +, \cdot)$ ist *kein* Körper

2. Für p Primzahl ist $(\mathbb{Z}_p, +, \cdot)$ ein Körper. [Beispiel 3 zu 1.14]
Für $m \in \mathbb{N}$, m *keine* Primzahl, ist $(\mathbb{Z}_m, +, \cdot)$ *kein* Körper, weil $(\mathbb{Z}_m, +, \cdot)$ für $m \geq 2$ nicht nullteilerfrei ist [Beispiel 3 zu 1.14] und $\mathbb{Z}_1$ als einelementiger Ring kein Körper sein kann.

Bemerkung:
Es gibt endliche Körper mit p^k Elementen, falls p Primzahl und $k \in \mathbb{N}$. Diese sind bis auf Isomorphie eindeutig bestimmt. Bezeichnung: $\mathrm{GF}(p^k)$ ("Galois-Felder")
Insbesondere sind $\mathbb{Z}_p$ und $\mathrm{GF}(p)$ isomorph. Weitere endliche Körper existieren nicht.
Die Körper $\mathrm{GF}(2^k)$ kommen in der Codierungstheorie zum Einsatz [Fehlerkorrektur bei CD/DVD, DVB, DSL: $\mathrm{GF}(2^8)$].

1.20 Rechenregeln in Körpern (Auszug)

Sei $(K, +, \cdot)$ ein Körper. Zusätzlich zu den Regeln in 1.14, 1.15 und 1.16 gilt:

(a) $a^{-1} = \dfrac{1}{a}, \quad \dfrac{1}{\frac{1}{a}} = a \qquad (a \in K \setminus \{0\})$

(b) $-\dfrac{a}{b} = \dfrac{-a}{b} = \dfrac{a}{-b} \qquad (a \in K,\ b \in K \setminus \{0\})$

(c) $\dfrac{a}{b} \pm \dfrac{c}{d} = \dfrac{a \cdot d \pm b \cdot c}{b \cdot d} \qquad (a, c \in K,\ b, d \in K \setminus \{0\})$

(d) $\dfrac{a}{b} \cdot \dfrac{c}{d} = \dfrac{a \cdot c}{b \cdot d} \qquad (a, c \in K,\ b, d \in K \setminus \{0\})$

(e) $\dfrac{\frac{a}{b}}{\frac{c}{d}} = \dfrac{a \cdot d}{b \cdot c} \qquad (a \in K,\ b, c, d \in K \setminus \{0\})$

Beweis: Übung

Bemerkung:

1. Da $(K, +, \cdot)$ ein kommutativer Ring ist, können in 1.15 und 1.16 in den einzelnen Produkten zusätzlich Faktorvertauschungen durchgeführt werden.

2. Ist K Körper, so gilt die geometrische Summenformel in ihrer üblichen Form
$\sum\limits_{k=0}^{n} q^k = \dfrac{q^{n+1} - 1}{q - 1} = \dfrac{1 - q^{n+1}}{1 - q} \qquad (q \neq 1,\ n \in \mathbb{N}_0)$

3. Auch der binomische Satz gilt mit der nach 1.6 für additive abelsche Gruppen eingeführten Schreibweise des Ausdrucks $m \cdot a \ \ (m \in \mathbb{Z}, a \in K)$.

Komplexe Zahlen

Vorbemerkung:

$$(\mathbb{R}^2, +, \cdot) \text{ mit } \begin{aligned} (x_1, y_1) + (x_2, y_2) &:= (x_1 + x_2, y_1 + y_2) \\ (x_1, y_1) \cdot (x_2, y_2) &:= (x_1 x_2, y_1 y_2) \end{aligned}$$

ist zwar ein kommutativer Ring mit Einselement $(1, 1)$, aber *nicht* nullteilerfrei und somit *kein* Körper. [Denn: $(1, 0) \cdot (0, 1) = (0, 0)$]

Mit einer *anderen* Definition der Multiplikation gelangt man zu den komplexen Zahlen.

1.21 Satz und Definition (komplexe Zahlen)

(a) $\mathbb{R}^2$ ist mit den Verknüpfungen

$$\begin{aligned} + :\ & \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}^2, \ (x_1,y_1)+(x_2,y_2) := (x_1+x_2, y_1+y_2) \\ \cdot :\ & \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}^2, \ (x_1,y_1)\cdot(x_2,y_2) := (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1) \end{aligned}$$

ein Körper. Er heißt Körper der komplexen Zahlen und wird mit $\mathbb{C}$ bezeichnet.

(b) Mit der "imaginären Einheit" $i := (0,1)$ gilt

$$i \cdot i = -(1,0)$$

und

$$(x,y) = (x,0) + i\cdot(y,0) \qquad (x,y \in \mathbb{R})$$

Beweis:

(a) $(\mathbb{R}^2,+,\cdot)$ Ring:

$$\left.\begin{array}{ll} - & (\mathbb{R}^2,+) \text{ abelsche Gruppe} \quad \text{klar!} \\ - & (\mathbb{R}^2,\cdot) \text{ Assoziativgesetz durch Nachrechnen} \\ - & \text{Distributivgesetz durch Nachrechnen} \end{array}\right\} \text{Übung}$$

$(\mathbb{R}^2 \setminus \{(0,0)\},\cdot)$ abelsche Gruppe:

$$\left.\begin{array}{l} \text{Kommutativgesetz durch Nachrechnen} \\ \text{Neutrales Element: } (1,0) \\ \text{Inverses Element zu } (x,y): \left(\dfrac{x}{x^2+y^2}, \dfrac{-y}{x^2+y^2}\right) \end{array}\right\} \text{Übung}$$

(b) $i\cdot i = (0,1)\cdot(0,1) = (0\cdot 0 - 1\cdot 1, 0\cdot 1 + 1\cdot 0) = (-1,0)$
$(x,0)+i\cdot(y,0) = (x,0)+(0,1)\cdot(y,0) = (x,0)+(0\cdot y - 1\cdot 0, 0\cdot 0 + 1\cdot y) = (x,0)+(0,y) = (x,y)$

Schreibweise:
Wir können $\mathbb{R}$ als Teilmenge von $\mathbb{C}$ betrachten, indem wir $x \in \mathbb{R}$ mit $(x,0) \in \mathbb{R}^2$ identifizieren. Damit gelangen wir zu

$$\mathbb{C} = \{x + i\cdot y : \ x,y \in \mathbb{R}\}$$

und den Rechenregeln

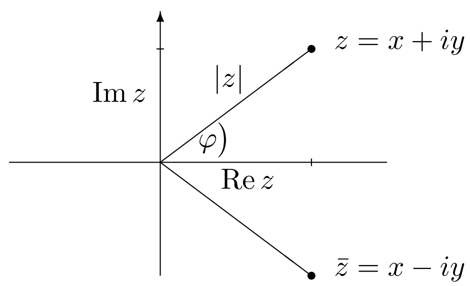
$$\begin{aligned} & i\cdot i = -1 \\ & (x_1 + i\cdot y_1) + (x_2 + i\cdot y_2) &= x_1 + x_2 + i\cdot(y_1+y_2) \\ & (x_1 + i\cdot y_1)\cdot(x_2 + i\cdot y_2) &= x_1x_2 + i\cdot x_2y_1 + i\cdot x_1y_2 + i^2\cdot y_1y_2 \\ & &= x_1x_2 - y_1y_2 + i\cdot(x_2y_1 + x_1y_2) \end{aligned}$$

1.22 Definition (Real- und Imaginärteil, Betrag, konjugiert-komplexe Zahl)

Sei $z = x + iy \in \mathbb{C}$ mit $x,y \in \mathbb{R}$. Dann

$$\begin{array}{lcll} \operatorname{Re} z & := & x & \text{(Realteil von } z) \\ \operatorname{Im} z & := & y & \text{(Imaginärteil von } z) \\ |z| & = & \sqrt{x^2+y^2} & \text{(Betrag von } z) \\ \bar{z} & = & x - iy & \text{(konjugiert-komplexe Zahl)} \end{array}$$

Veranschaulichung in der Gaußschen Zahlenebene:



1.23 Rechenregeln (konjugiert-komplexe Zahlen, Beträge)

Seien $w, z \in \mathbb{C}$. Dann gilt:

(a) $\overline{w+z} = \bar{w} + \bar{z}$

(b) $\overline{w \cdot z} = \bar{w} \cdot \bar{z}$

(c) $|z| = \sqrt{z \cdot \bar{z}}$

(d) $|w \cdot z| = |w| \cdot |z|$

Im folgenden lassen wir den Punkt bei der komplexen Multiplikation in der Regel weg.

Beweis: $w = u + iv$, $z = x + iy \quad (u, v, x, y \in \mathbb{R})$

(a) $\overline{w+z} = \overline{u + iv + x + iy} = \overline{u + x + i(v+y)} = u + x - i(v+y) = u - iv + x - iy = \bar{w} + \bar{z}$

(b) $\overline{wz} = \overline{(u+iv)(x+iy)} = \overline{ux - vy + i(uy + vx)} = ux - vy - i(uy + vx)$
$= (u - iv)(x - iy) = \bar{w}\bar{z}$

(c) $|z|^2 = x^2 + y^2 = x^2 - (iy)^2 = (x + iy)(x - iy) = z\bar{z}$

(d) $|wz|^2 = wz\,\overline{wz} \overset{\text{(b)}}{=} wz\bar{w}\bar{z} = w\bar{w}z\bar{z} = |w|^2|z|^2$

Bemerkungen:

1. Es gilt im allg. *nicht*: $|w+z| = |w|+|z|$, sondern nur $|w+z| \leq |w|+|z|$ (Dreiecksungleichung).
2. Weitere Eigenschaften von $\mathbb{C}$ werden in der Analysis bewiesen, insbesondere die sogenannte Polardarstellung $z = r \cdot e^{i\varphi} = r(\cos\varphi + i \sin\varphi)$ mit $r = |z|$ und $\varphi \in \mathbb{R}$ geeignet. Aus dieser ergibt sich u.a. die Formel von de Moivre
$$(\cos\varphi + i\sin\varphi)^n = \cos(n\varphi) + i\sin(n\varphi) \qquad (\varphi \in \mathbb{R}, n \in \mathbb{N})$$
3. Wir benötigen später neben den Körpereigenschaften von $\mathbb{C}$ im wesentlichen 1.23a,b und den Fundamentalsatz der Algebra:
Jedes Polynom $a_n z^n + a_{n-1}z^{n-1} + \ldots + a_0 \quad (z \in \mathbb{C})$ mit komplexen Koeffizienten $a_0, \ldots, a_n$, wobei $n \in \mathbb{N}$ und $a_n \neq 0$, läßt sich als Produkt $a_n(z - \zeta_1)\cdots(z - \zeta_n)$ schreiben. Dabei sind die komplexen Nullstellen $\zeta_1, \ldots, \zeta_n$ unabhängig von $z \in \mathbb{C}$, jedoch nicht unbedingt paarweise verschieden.
Beispiel: $z^2 + 1 = (z + i)(z - i)$.