technische universität dortmund
Fakultät für Mathematik
Prof. Dr. H. M. Möller

Dortmund, im November 2011

Lineare Algebra für Lehramt Gymnasien und Berufskolleg

Zusammenfassung von Kapitel 3

3. Zahlbereiche und algebraische Strukturen

3.1 Die natürlichen Zahlen

$\mathbb{N} := \{1, 2, 3, \ldots\}$ ist die Menge der natürlichen Zahlen. Mit $\mathbb{N}_0$ wird $\mathbb{N} \cup \{0\}$ bezeichnet.

Mit den *Peano-Axiomen* wird die Menge $\mathbb{N}_0$ und damit auch $\mathbb{N}$ eindeutig definiert. Diese Axiome lauten

(PA1) $0 \in \mathbb{N}_0$.

(PA2) Es gibt eine injektive Abbildung (Nachfolge-Operation) $s : \mathbb{N}_0 \to \mathbb{N}$.

(PA3) Für jede Menge X gilt:
Wenn $0 \in X$ und wenn aus $x \in X \cap \mathbb{N}_0$ folgt, dass auch $s(x) \in X$ gilt, dann gilt $\mathbb{N}_0 \subseteq X$.

Mit Hilfe der Nachfolge-Operation $s : \mathbb{N}_0 \to \mathbb{N}$ kann man die Addition und Multiplikation rekursiv definieren.

$$n + 0 := n, \qquad n + s(m) := s(n + m), \text{ für alle } m, n \in \mathbb{N}_0.$$

$$n \cdot 0 := 0, \qquad n \cdot s(m) := n \cdot m + n, \text{ für alle } m, n \in \mathbb{N}_0.$$

Man macht sich klar, dass Addition und Multiplikation kommutativ und assoziativ sind.

3.2 Die ganzen Zahlen

Zu jeder Zahl $n \in \mathbb{N}$ führt man eine neue Zahl $-n$ ein mit $n + (-n) = 0$. Man erklärt dann die Menge der ganzen Zahlen durch

$$\mathbb{Z} := \mathbb{N}_0 \cup \{-n \mid n \in \mathbb{N}\}$$

und stellt fest, dass man die Addition und Multiplikation in natürlicher Weise auf $\mathbb{Z}$ fortsetzen kann.

Eigenschaften von $\mathbb{Z}$:

(Z1) $\mathbb{N}_0 \subset \mathbb{Z}$.

(Z2) Zu jedem $(a, b) \in \mathbb{Z}$ ist $a + b \in \mathbb{Z}$ definiert und für alle $a, b, c \in \mathbb{Z}$ gilt
(a) $(a + b) + c = a + (b + c)$ (Assoziativgesetz),
(b) $a + b = b + a$ (Kommutativgesetz),
(c) Wenn $a, b \in \mathbb{N}_0$, dann $a + b$ wie in $\mathbb{N}_0$.

(Z3) $a + 0 = a$ für alle $a \in \mathbb{Z}$.

(Z4) Für alle $a \in \mathbb{Z}$ gibt es ein $-a \in \mathbb{Z}$ mit $a + (-a) = 0$.

(Z5) Zu jedem $(a, b) \in \mathbb{Z}$ ist $a \cdot b \in \mathbb{Z}$ definiert und für alle $a, b, c \in \mathbb{Z}$ gilt
(a) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (Assoziativgesetz),
(b) $a \cdot b = b \cdot a$ (Kommutativgesetz),
(c) Wenn $a, b \in \mathbb{N}_0$, dann $a \cdot b$ wie in $\mathbb{N}_0$.

(Z6) Für alle $a, b, c \in \mathbb{Z}$ gilt
$a \cdot (b + c) = a \cdot b + a \cdot c$ (Distributivgesetz).

Satz 3.1 (Teilen mit Rest)
Sei $a \in \mathbb{Z}$ und $m \in \mathbb{N}$. Dann gibt es eindeutig bestimmte Zahlen $q \in \mathbb{Z}$ und $r \in \{0, 1, \ldots, m - 1\}$ mit

$$a = q \cdot m + r.$$

q heißt *Quotient* und r *Rest von a bei Division durch m*. Man schreibt manchmal kurz $a \; div \; m$ für q und $a \; mod \; m$ für r.

Definition 3.2 (Teilbarkeit)
$a \in \mathbb{Z}$ ist durch $m \in \mathbb{N}$ *teilbar*, wenn beim Teilen mit Rest der Rest r Null ist, in Zeichen $m|a$. Mit anderen Worten: $m|a$ gilt genau dann, wenn es ein $q \in \mathbb{Z}$ gibt mit $a = q \cdot m$.

Für $m \in \mathbb{Z} \backslash \mathbb{N}_0$ definiert man $m|a$ falls $-m|a$. Dann gilt auch hier $m|a \Leftrightarrow \exists q \in \mathbb{Z} : a = q \cdot m$.

Definition 3.3 (Primzahl)
$p \in \mathbb{N}$ heißt *Primzahl* wenn $p \neq 1$ und wenn p nicht Produkt zweier kleinerer natürlicher Zahlen ist, also

$$p = a \cdot b, \; a, b \in \mathbb{N} \Rightarrow a = p \vee b = p.$$

Satz 3.4 (Primfaktorzerlegung)
Jede natürliche Zahl n läßt sich als Produkt von Primzahlen schreiben,

$$n = p_1 \cdot p_2 \cdots p_s, \qquad p_i \text{ Primzahl.}$$

Diese Darstellung ist eindeutig, wenn man $p_1, \ldots, p_s$ ordnet, wenn also $p_1 \leq p_2 \leq \ldots \leq p_s$ gilt. D.h., wenn zu n auch Primzahlen $q_1, q_2, \ldots, q_r$ gehören mit $n = q_1 \cdot q_2 \cdots q_r$ und $q_1 \leq q_2 \leq \cdots \leq q_r$, dann folgt $r = s$ und $p_i = q_i$ für $i = 1, \ldots, s$.

Die Primzahlzerlegung bekommt man, indem man n sooft wie möglich durch die erste Primzahl (also durch 2) teilt, den Rest dann sooft wie möglich durch die nächste Primzahl (also durch 3) teilt, dann durch die nächste Primzahl usw. bis endlich der Rest 1 ist oder die nächste Primzahl größer als $\sqrt{n}$ ist. (In der Globalübung wurde gezeigt, dass höchstens ein Primzahlteiler größer als $\sqrt{n}$ ist.) Beispielsweise

$$378 = 2 \cdot 189 = 2 \cdot 3 \cdot 63 = 2 \cdot 3 \cdot 3 \cdot 21 = 2 \cdot 3 \cdot 3 \cdot 3 \cdot 7.$$

Definition und Satz 3.5 (größter gemeinsamer Teiler)
Zu $a, b \in \mathbb{Z}$ gibt es ein $g \in \mathbb{N}$ mit den beiden Eigenschaften
(i) $g|a$ und $g|b$,
(ii) $(d \in \mathbb{Z} \wedge d|a \wedge d|b) \Rightarrow d|g$.
g wird *größter gemeinsamer Teiler von a und b* genannt, in Zeichen $g = ggT(a, b)$. Der $ggT(a, b)$ ist eindeutig durch (i) und (ii) bestimmt.

Wenn $ggT(a, b) = 1$, dann nennt man a und b *teilerfremd.*

Die Berechnung von $ggT(a, b)$ ist dadurch möglich, dass man die Primfaktorzerlegung von a und b bestimmt (wenn a und b natürliche Zahlen sind. Sonst nimmt man $-a$ und/oder $-b$ statt a und/oder b) und mit deren Hilfe die Menge der Teiler von a und die Menge der Teiler von b. Die größte Zahl im Durchschnitt dieser Mengen ist $ggT(a, b)$. Die Berechnung der Primfaktorzerlegung ist für große Zahlen jedoch sehr aufwändig.

Der euklidische Algorithmus
Eingabe: $a \in \mathbb{Z}$ und $b \in \mathbb{N}$.
Ausgabe: $ggT(a, b)$.
Rechnung:($\star$) Teile a durch b mit Rest $r = a \ mod \ b$.
Ersetze a durch b und b durch r.
Wenn $r = 0$, dann gib b als $ggT(a, b)$ zurück,
sonst geh zurück zu ($\star$).

Der Algorithmus endet (man sagt: er terminiert) nach endlich vielen Schritten, weil bei jedem Rücksprung der Rest, d.h., das neue b, echt verkleinert wird, aber immer eine ganze Zahl ≥ 0 ist, so dass nach spätestens b Schritten (b ist das b der Eingabe) der Rest 0 erreicht wird.

Lemma 3.6 Der euklidische Algorithmus gibt für beliebige $a \in \mathbb{Z}$ und $b \in \mathbb{N}$ den $ggT(a, b)$ als Resultat zurück, d.h. er ist *korrekt*.

Beweis: Der Algorithmus führt der Reihe nach die folgenden euklidischen Divisionen durch

$$\begin{array}{ll} a = q_0 b + r_1 & r_1 < b, \\ b = q_1 r_1 + r_2 & r_2 < r_1, \\ r_1 = q_2 r_2 + r_3 & r_3 < r_2, \\ \vdots & \\ r_{s-1} = q_s r_s + r_{s+1} & r_{s+1} < r_s, \\ r_s = q_{s+1} r_{s+1} + 0 \quad . & \end{array}$$

r_{s+1} teilt r_s (s. letzte Zeile). Dann teilt es als Teiler von r_{s+1} und von r_s auch r_{s-1} (s. vorletzte Zeile). Wenn man sich die Zeilen nach oben durcharbeitet, bekommt man dass ein Teiler von r_{i+1} und r_i auch Teiler von r_{i-1} ist, und damit r_{i-1} auch von r_{s+1} geteilt wird. Entsprechend für b und a. Fazit: r_{s+1} ist ein gemeinsamer Teiler von a und b.
Wenn t ein Teiler von a und b ist, dann auch von r_1 (folgt aus Zeile 1). Wenn t ein Teiler von b und r_1 ist, dann auch von r_2 (folgt aus Zeile 2) usw. Aus der vorletzten Zeile folgt dann, dass t auch ein Teiler von r_{s+1} ist. Nach Definition (und Satz) 3.5 ist damit $r_{s+1} = ggT(a, b)$. □

Lemma 3.7 (Lemma von Bezout)
Der größte gemeinsame Teiler zweier Zahlen $a, b \in \mathbb{Z}$, $b \neq 0$, besitzt eine Darstellung

$$ggT(a, b) = s \cdot a + t \cdot b \qquad \text{mit } a, b \in \mathbb{Z}.$$

Beim *erweiterten euklidischen Algorithmus* wird wie beim euklidischen Algorithmus eine Folge von euklidischen Divisionen beginnend mit der Division von a durch b durchgeführt. Zusätzlich wird dabei Buch geführt, wie der jeweilige Divisionsrest von a und b abhängt.

Rechenschema für den erweiterten euklidischen Algorithmus am Beispiel $a = 161$, $b = 91$

s	t	r	$-q$
1	0	161	$-$
0	1	91	-1
1	-1	70	-1
-1	2	21	-3
4	-7	7	-3
-13	23	0	

In der zu r gehörenden Spalte stehen der Reihe nach $a, b, r_1, r_2, \ldots$. Das q ist der jeweilige Quotient bei der euklidischen Division. In jeder Zeile gilt (mit den aktuellen Werten von s, t und r) jeweils $s \cdot 161 + t \cdot 91 = r$. Die ersten zwei Zeilen sind trivial. Die $i+1$-te Zeile entsteht durch Addition der $i-1$-ten und des $-q$-fachen der i-ten. In der **vorletzten** Zeile liest man dann $4 \cdot 161 + (-7) \cdot 91 = 7 = ggT(161, 91)$ ab.

Die letzte Zeile im Rechenschema zeigt Zähler und Nenner des ausgekürzten Bruchs $\frac{91}{161}$,

$$-13 \cdot 161 + 23 \cdot 91 = 0 \Rightarrow \frac{91}{161} = \frac{13}{23}.$$

Man kann zeigen, dass bei beliebigen $a, b \in \mathbb{Z}$, $b \neq 0$, ab der dritten Zeile im Rechenschema die aktuellen Werte von s und t teilerfremd sind, so dass in der letzten Zeile immer $r = 0$ gilt und s und t teilerfremd sind. Damit stehen in der letzten Zeile immer Zähler und Nenner des ausgekürzten Bruches $\frac{a}{b}$.

3.3 Algebraische Strukturen

Definition 3.8 (Verknüpfung)
Sei M eine Menge. Eine Verknüpfung auf M ist eine Vorschrift, die jedem Paar $(x, y) \in M \times M$ ein Element von M zuordnet. Bezeichnet man die Verknüpfung z.B. mit $\circ$, dann wird das Element, welches dem Paar (x, y) zugeordnet ist, mit $x \circ y$ bezeichnet.

Definition 3.9 (assoziativ und kommutativ)
Eine Verknüpfung auf M wird *assoziativ* genannt, wenn für beliebige $x, y, z \in M$ gilt

$$(x \circ y) \circ z = x \circ (y \circ z).$$

Sie heißt *kommutativ*, wenn für beliebige $x, y \in M$

$$x \circ y = y \circ x.$$

Man schreibt $(M, \circ)$ für eine Menge M mit Verknüpfung $\circ$.

Definition 3.10 (neutrales Element)
Sei M eine Menge mit Verknüpfung $\circ$. Wenn es in M ein Element e gibt mit

$$x \circ e = e \circ x = x \qquad \text{für alle } x \in M,$$

dann heißt e *neutrales Element* für die Verknüpfung $\circ$.

Bemerkung. Sind e und e' neutrale Elemente für die Verknüpfung $\circ$, dann gilt $e = e'$. (Zum Beweis betrachte man $e \circ e'$.)

Beispiele. In $(\mathbb{N}, +)$ und $(\mathbb{Z}, +)$ ist die Verknüpfung $+$ jeweils assoziativ und kommutativ. In $\mathbb{Z}$ ist 0 das neutrale Element bzgl. $+$. $(\mathbb{N}, +)$ hat kein neutrales Element. Nimmt man $\mathbb{Z}$ mit dem aus der Schule bekannten "Minus" als Verknüpfung, dann ist diese Verknüpfung weder assoziativ, z.B. gilt $7 - (5 - 1) = 7 - 4 = 3 \neq 1 = 2 - 1 = (7 - 5) - 1$, noch kommutativ, z.B. gilt $7 - 5 \neq 5 - 7$. $(\mathbb{N}, \cdot)$ und $(\mathbb{Z}, \cdot)$ sind ebenfalls assoziativ und kommutativ und haben 1 als neutrales Element.

Definition 3.11 (Gruppe)
Eine *Gruppe* ist eine Menge G mit Verknüpfung $\circ$, so dass die folgenden drei Axiome gelten
(G1) Die Verknüpfung $\circ$ ist assoziativ.
(G2) G besitzt ein neutrales Element e bzgl. $\circ$.
(G3) Zu jedem $a \in G$ gibt es ein $b \in G$ mit

$$a \circ b = b \circ a = e.$$

Ist die Verknüpfung $\circ$ zusätzlich kommutativ, dann heißt die Gruppe *kommutativ* oder *abelsch*.

In (G3) ist das b eindeutig durch a bestimmt. (Zum Beweis betrachte man ein weiteres $b' \in G$ mit $a \circ b' = b' \circ a = e$ und berechne $b \circ a \circ b'$.) Das b in $(G3)$ wird als *invers zu* a bezeichnet. Man schreibt a^{-1} für das zu a inverse Element. Wird die Verknüpfung in der Gruppe G mit $+$ bezeichnet, dann schreibt man für das neutrale Element in der Regel 0 (d.h. Null) und $-a$ für das zu a inverse Element. Im Fall, dass die Verknüpfung eine Multiplikation ist, nennt man das neutrale Element gern *Eins* und schreibt manchmal sogar 1 statt e.

Beispiel $(\mathbb{Z}, +)$ ist eine Gruppe. Dagegen $(\mathbb{Z} \setminus \{0\}, \cdot)$ nicht, weil die inversen Elemente für die Zahlen $\neq \pm 1$ fehlen. Nimmt man die sogenannten *Stammbrüche*) hinzu, das sind die Zahlen $\frac{1}{n}$ für alle $n \in \mathbb{N}$ mit $n \geq 2$), und die

Produkte von ganzen Zahlen $\neq 0$ mit den Stammbrüchen, bekommt man die Menge der rationalen Zahlen ohne Null, $\mathbb{Q} \setminus \{0\}$. Dann ist $(\mathbb{Q} \setminus \{0\}, \cdot)$ eine Gruppe.

Satz 3.12 (Permutationsgruppe)
Sei M eine beliebige Menge. Dann ist ist

$$\text{Per } M := \{f : M \to M \mid f \text{ bijektiv } \}$$

eine Gruppe mit der Komposition als Verknüpfung. Neutrales Element ist id_M. Zu $f \in \text{Per } M$ ist die Umkehrabbildung f^{-1} das inverse Element.

Beweis. Die Komposition zweier bijektiver Abbildungen von M nach M ist wieder eine bijektive Abbildung von M nach M (vgl. Aufgabe 7). Also ist die Komposition eine Verknüpfung im Sinn von Definition 3.8. Die Komposition ist assoziativ, weil $((f \circ g) \circ h)(x) = f(g(h(x))) = (f \circ (g \circ h))(x)$. id_M ist bijektiv mit $(f \circ id_M)(x) = f(x) = (id_M \circ f)(x)$ für alle $x \in M$ und alle $f \in \text{Per } M$, also $f \circ id_M = id_M \circ f$ für alle $f \in$Per M. Und die Umkehrabbildung ist bijektiv und invers zu $f \in \text{Per}M$. □

Ist $M = \{1, 2, \ldots, n\}$ und $f \in \text{Per } M$, dann stellt $(f(1), f(2), \ldots, f(n))$ eine Permutation von $(1, 2, \ldots, n)$ dar. Man bezeichnet Per M dann als *symmetrische Gruppe vom Grad* n und schreibt S_n statt Per M.

Satz 3.14 (Mächtigkeit von S_n)
Für alle $n \in \mathbb{N}$ gilt $|S_n| = n \cdot (n-1) \cdots 2 \cdot 1 = n!$.

Beweis. Für $n = 1$ ist $M = \{1\}$ und $S_1 = \{id_M\}$. Wenn die Behauptung schon für n gilt, dann betrachte $M := \{1, 2, \ldots, n+1\}$. Die bijektiven Abbildungen $f : M \to M$ werden in $n+1$ verschiedenen und elementfremden (disjunkten) Teilmengen eingeordnet,

$$M_k := \{f \in \text{Per } M \mid f(n+1) = k\} \qquad k = 1, \ldots, n+1.$$

Zu $f \in M_k$ betrachte $g : \{1, \ldots, n\} \to M \setminus \{k\}$, $g(i) := f(i)$ für $i = 1, \ldots, n$. Jedes g ist bijektiv. Offenbar gibt es genauso viele derartige g wie es bijektive Abbildungen von $\{1, \ldots, n\}$ auf sich gibt, also nach Induktionsvoraussetzung $|S_n| = n!$. Weil es zu jedem $f \in M_k$ genau ein g gibt, hat die Menge M_k die Mächtigkeit $n!$. Das gilt für $k = 1, \ldots, n+1$. Also $|M| = n! + n! + \ldots + n! = (n+1)n! = (n+1)!$ □

Definition 3.14 (Addition und Multiplikation modulo m)
Sei $m \in \mathbb{N}$. Auf $\mathbb{Z}_m := \{0, 1, \ldots, m-1\}$ wird eine Addition erklärt durch

$$x +_m y = (x + y) \; mod \; m \qquad \text{für alle } x, y \in \mathbb{Z}_m$$

und eine Multiplikation durch

$$x \cdot_m y = (x \cdot y) \; mod \; m \qquad \text{für alle } x, y \in \mathbb{Z}_m.$$

Definition 3.15 (Ring)
Eine Menge R mit Verknüpfungen $+$ und $\cdot$ wird *Ring* genannt, wenn die folgenden drei Axiome gelten,
(R1) $(R, +)$ ist abelsche Gruppe.
(R2) $\cdot$ ist assoziativ.
(R3) Es gelten die Distributivgesetze

$$a(x + y) = ax + ay, \quad (a + b)x = ax + bx \quad \text{für alle } a, b, x, y \in R.$$

Oft verlangt man, dass die Multiplikation im Ring kommutativ ist. In dem Fall spricht man von einem *kommutativen Ring*. Hat der Ring ein neutrales Element bzgl. $\cdot$, also eine "Eins", dann nennt man R einen Ring *mit Eins*.

Beispiele $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring mit Eins. Die Menge der Polynome

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots a_n x^n, \quad a_0, a_1, \ldots, a_n \in \mathbb{R}, \; n \in \mathbb{N}_0,$$

bilden mit der Polynomaddition und -multiplikation einen Ring $(\mathbb{R}[x], +, \cdot)$. Hier ist die Null das Nullpolynom $0 + 0 \cdot x + 0 \cdot x^2 + \cdots$ und die Eins das Polynom $1 + 0 \cdot x + 0 \cdot x^2 + \cdots$.

Definition 3.16 (Körper)
Ein *Körper* ist ein kommutativer Ring mit Eins, bei dem jedes Element $\neq 0$ ein multiplikatives Inverses besitzt.

Beispiele $(\mathbb{Z}, +, \cdot)$ ist kein Körper, weil $(\mathbb{Z} \setminus \{0\}, \cdot)$ keine Gruppe (!) ist. Dagegen ist $(\mathbb{Q}, +, \cdot)$ ein Körper.

Satz 3.17 ($\mathbb{Z}_m$ als Ring)
Für jedes $m \in \mathbb{N}$ ist $(\mathbb{Z}_m, +_m, \cdot_m)$ ein kommutativer Ring mit Eins.

Satz 3.18 (Existenz von Inversen)
Sei $(R, +, \cdot)$ ein kommutativer Ring mit Eins. Ein Element $a \in R$ hat genau dann ein Inverses (bzgl. $\cdot$), wenn die Abbildung $L_a : R \to R, \; x \mapsto a \cdot x$ bijektiv ist.
Beweis.
" $\Leftarrow$ " Sei L_a bijektiv. Dann ist L_a insbesondere surjektiv, d.h., jedes $y \in R$ hat ein Urbild $x \in R$, $L_a(x) = y$, insbesondere $y = 1$:

$$\exists x \in R : \; a \cdot x = L_a(x) = 1.$$

Damit gilt $x = a^{-1}$.
" $\Rightarrow$ " Sei x zu a invers bzgl. $\cdot$, also $x = a^{-1}$. Dann gilt

$$L_a(x_1) = L_a(x_2) \Rightarrow a \cdot x_1 = a \cdot x_2 \Rightarrow x_1 = a^{-1}ax_1 = a^{-1}ax_2 = x_2.$$

Somit ist L_a injektiv. Zu $y \in R$ ist $a^{-1}y \in R$ das Urbild,

$$L_a(a^{-1}y) = aa^{-1}y = y.$$

Das gilt für jedes $y \in R$. Also ist L_a auch surjektiv. □

Satz 3.19 (Existenz von Inversen in $\mathbb{Z}_m$)
Sei $m \in \mathbb{N}$. $a \in \mathbb{Z}_m$ ist genau dann invertierbar, wenn a und m teilerfremd sind.
Beweis.
" $\Leftarrow$ " Sei $ggT(a.m) = 1$. Dann gibt es nach dem Lemma von Bezout $s, t \in \mathbb{Z}$ mit $sa + tm = 1$. Also $sa \equiv 1(mod\ m)$, d.h., $s = a^{-1}$.
" $\Rightarrow$ " Sei $s \cdot_m a = 1$, d.h., s invers zu a. Nach Definition von $\cdot_m$ folgt $sa \equiv 1(mod\ m)$. Das bedeutet $sa + tm = 1$ mit einem $t \in \mathbb{Z}$. Jeder gemeinsame Teiler von a und m ist dann Teiler von 1. Das ist für (positive) Teiler nur möglich, wenn der Teiler 1 ist. Also $ggT(a, m) = 1$. □

Satz 3.20 ($\mathbb{Z}_p$ als Körper)
Für jede Primzahl p ist $(\mathbb{Z}_p, +_p, \cdot_p)$ ein Körper.

Definition 3.21 (Untergruppen)
Sei $(G, *)$ eine Gruppe mit neutralem Element e und sei $H \subseteq G$. $(H, *)$ ist *Untergruppe von* $(G, *)$, wenn die drei folgenden Eigenschaften gelten.
(UG1) Für alle $x, y \in H$ gilt $x * y \in H$.
(UG2) $e \in H$.
(UG3) Für alle $x \in H$ gilt $x^{-1} \in H$.

Beispiele $(\mathbb{Z}, +)$ ist eine Gruppe mit neutralem Element 0. Die Menge $H = 2\mathbb{Z} = \{2m \mid m \in \mathbb{Z}\}$ ist Teilmenge von $\mathbb{Z}$ und $(2\mathbb{Z}, +)$ ist Untergruppe von $(\mathbb{Z}, +)$, weil (UG1), (UG2) und (UG3) erfüllt sind, denn $2m + 2n = 2(m + n) \Rightarrow (UG1)$, $0 \in 2\mathbb{Z}$, $-2m \in 2\mathbb{Z}$ ist (additiv) invers zu $2m$.
S_3, die Menge aller bijektiven Abbildungen von $M := \{1, 2, 3\}$ auf sich, ist mit der Komposition $\circ$ eine Gruppe $(S_3, \circ)$. Betrachte die bijektive Abbildung

$$\varphi : M \to M,\ \varphi(1) = 2, \varphi(2) = 3, \varphi(3) = 1.$$

Dann ist $\varphi^2 := \varphi \circ \varphi$ gegeben durch

$$\varphi^2(1) = 3, \varphi^2(2) = 1, \varphi^2(3) = 2.$$

Die Menge $A_3 := \{id_M, \varphi, \varphi^2\}$ ist Teilmenge von S_3 und es gilt, wie leichte Rechnung zeigt,

$\circ$	id_M	φ	φ^2
id_M	id_M	φ	φ^2
φ	φ	φ^2	id_M
φ^2	φ^2	id_M	φ

Hieraus liest man die Untergruppeneigenschaften (UG1), (UG2), (UG3) für $(A_3, \circ)$ ab.

Definition 3.22 (Unterringe)
Sei $(R, +, \cdot)$ ein Ring und $S \subseteq R$. Dann heißt $(S, +, \cdot)$ *Unterring von* $(R, +, \cdot)$, wenn gilt
(UR1) $(S, +)$ ist Untergruppe von $(R, +)$.
(UR2) Für alle $x, y \in S$ gilt $x \cdot y \in S$.

Beispiel Man definiert $\mathbb{Z}[\sqrt{2}] := \{a + b \cdot \sqrt{2} \mid a, b \in \mathbb{Z}\}$. Offenbar gilt $\mathbb{Z}[\sqrt{2}] \subset \mathbb{R}$. Die Addition in $\mathbb{R}$ beschränkt auf Elemente aus $\mathbb{Z}[\sqrt{2}]$ macht $(\mathbb{Z}[\sqrt{2}], +)$ zu einer Untergruppe von $(\mathbb{R}, +)$, denn es gilt

$$(a + b \cdot \sqrt{2}) + (x + y \cdot \sqrt{2}) = (a + x) + (b + y) \cdot \sqrt{2}.$$

Weil $a + x \in \mathbb{R}$ und $b + y \in \mathbb{R}$, wenn $a, b, x, y \in \mathbb{R}$, gilt (UG1). Das neutrale Element in $(\mathbb{R}, +)$ ist

$$0 = 0 + 0 \cdot \sqrt{2} \in \mathbb{Z}[\sqrt{2}].$$

Damit gilt auch (UG2). Zu $a + b \cdot \sqrt{2}$ ist $-a - b \cdot \sqrt{2}$ sowohl in $(\mathbb{R}, +)$ als auch in $(\mathbb{Z}[\sqrt{2}], +)$ invers. Damit gilt auch (UG3). Insgesamt ist damit (UR1) erfüllt.
Weil für je zwei Elemente aus $\mathbb{Z}[\sqrt{2}]$ gilt

$$(a + b \cdot \sqrt{2}) \cdot (x + y \cdot \sqrt{2}) = (ax + 2by) + (bx + ay) \cdot \sqrt{2} \in \mathbb{Z}[\sqrt{2}]$$

ist auch (UR2) erfüllt und somit $(\mathbb{Z}[\sqrt{2}], +, \cdot)$ ein Unterring von $(\mathbb{R}, +, \cdot)$.

Übrigens ist $(\mathbb{Z}, +, \cdot)$ ein Unterring von $(\mathbb{Z}[\sqrt{2}], +, \cdot)$.

Satz 3.23 (Der Ring $(\mathbb{Z}/m\mathbb{Z}, \oplus, \odot)$)
Auf der Menge aller Restklassen modulo m sind durch

$$[k]_m \oplus [\ell]_m := [k + \ell]_m \quad \text{und} \quad [k]_m \odot [\ell]_m := [k \cdot \ell]_m$$

zwei Verknüpfungen sinnvoll definiert. (Man sagt: sie sind *wohldefiniert*). $(\mathbb{Z}/m\mathbb{Z}, \oplus, \odot)$ ist ein kommutativer Ring mit Eins.

Beweis Jede Äquivalenzklasse wird durch Angabe eines Elements (das dann Repräsentant der Äquivalenzklasse genannt wird) eindeutig bestimmt. Man schreibt $[k]_m$, wenn k das ausgewählte Element ist. Man hätte auch $[k']_m$ für $[k]_m$ schreiben können, wenn $k' \equiv k \; mod \; m$. Das Problem ist also ob auch $k' + \ell' \equiv k + \ell \mod m$ gilt, wenn $k' \equiv k \; mod \; m$ und $\ell' \equiv \ell \; mod \; m$. Die Rechnung zeigt das aber,

$$k' = k + a \cdot m, \; \ell' = \ell + b \cdot m \; \Rightarrow \; k' + \ell' = k + \ell + (a + b) \cdot m.$$

Also ist $\oplus$ wohldefiniert. Entsprechend zeigt man, dass $\odot$ wohldefiniert ist. Weil die Resultate der Zuordnung zweier Elemente aus $\mathbb{Z}/m\mathbb{Z}$ wieder ein Element aus $\mathbb{Z}/m\mathbb{Z}$ ist, sind damit $\oplus$ und $\odot$ Verknüpfungen auf $\mathbb{Z}/m\mathbb{Z}$.
Leichte, aber längliche Rechnung zeigt, dass $(\mathbb{Z}/m\mathbb{Z}, \oplus)$ abelsche Gruppe mit $[0]_m$ als Null und $[-a]_m$ als Inverses zu $[a]_m$ ist, dass $[1]_m$ die Eins ist und dass $\odot$ assoziativ und kommutativ ist und dass auch **das** Distributivgesetz gilt. □

Vergleicht man die Verknüpfungstafeln von $(\mathbb{Z}/m\mathbb{Z}, \oplus, \odot)$ und $(\mathbb{Z}_m, +_m, \cdot_m)$, dann stellt man fest, dass sie im wesentlichen gleich sind. Z.B. gilt für $m = 4$

$\oplus$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\odot$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$
$[1]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[2]_4$	$[0]_4$	$[2]_4$	$[0]_4$	$[2]_4$
$[3]_4$	$[0]_4$	$[3]_4$	$[2]_4$	$[1]_4$

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Definition 3.24 (Isomorphie von Gruppen)
Ein *Isomorphismus* einer Gruppe $(G, \cdot)$ auf eine Gruppe $(H, \odot)$ ist eine Abbildung $\varphi : G \to H$ mit den zwei Eigenschaften
1. φ ist bijektiv,
2. φ ist verknüpfungstreu, d.h.,

$$\varphi(x \cdot y) = \varphi(x) \odot \varphi(y) \quad \text{für alle } x, y \in G.$$

Eine Gruppe $(G, \cdot)$ heißt *isomorph zur* Gruppe $(H, \odot)$, wenn ein Isomorphismus von $(G, \cdot)$ auf $(H, \odot)$ existiert.

Bemerkung Man nennt den in Definition 3.24 eingeführten Isomorphismus manchmal auch *Gruppenisomorphismus,* weil man auch für Ringe und Körper

Isomorphismen definieren kann. Dabei hat man zwei Verknüpfungen auf jeder Menge, sodass die Verknüpfungstreue für beide Verknüpfungen gelten muss. Genauer: Sind $(G, +, \cdot)$ und $(H, \oplus, \odot)$ Ringe (bzw. Körper), und gibt es eine bijektive Abbildung $\varphi : G \to H$ mit

$$\begin{aligned} \varphi(x + y) &= \varphi(x) \oplus \varphi(y) \qquad \text{für alle } x, y \in G, \\ \varphi(x \cdot y) &= \varphi(x) \odot \varphi(y) \qquad \text{für alle } x, y \in G, \end{aligned}$$

dann heißt $(G, +, \cdot)$ *isomorph zu* $(H, \oplus, \odot)$ und φ *(Ring- bzw. Körper-) Isomorphismus.*

Ist eine bijektive Abbildung $\varphi : G \to H$ verknüpfungstreu, dann ist auch die Umkehrabbildung φ^{-1} verknüpfungstreu, denn zu beliebigen $a, b \in H$ gibt es $x, y \in G$ mit $a = \varphi(x),\ b = \varphi(y)$ und

$$\varphi^{-1}(a \odot b) = \varphi^{-1}(\varphi(x) \odot \varphi(y)) = \varphi^{-1}(\varphi(x \cdot y)) = x \cdot y = \varphi^{-1}(a) \cdot \varphi^{-1}(b).$$

Ist also $(G, \cdot)$ isomorph zur Gruppe $(H, \odot)$ (mit Isomorphismus φ), dann ist auch $(H, \odot)$ isomorph zur Gruppe $(G, \cdot)$ (mit Isomorphismus φ^{-1}). Entsprechendes gilt natürlich auch für Ringe und Körper.

Satz 3.25 (Ein Ringisomorphismus)
Für jedes $m \in \mathbb{N}$ sind die Ringe $(\mathbb{Z}_m, +_m, \cdot_m)$ und $(\mathbb{Z}/m\mathbb{Z}, \oplus, \odot)$ isomorph zueinander.

Beweis. Die Abbildung $\varphi : \mathbb{Z}_m \to \mathbb{Z}/m\mathbb{Z},\ r \mapsto [r]_m$ ist bijektiv und verknüpfungstreu. □

Ein Beispiel für isomorphe Körper sind $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{Z} \times \mathbb{N}/_\sim, +, \cdot)$, wobei $\mathbb{Z} \times \mathbb{N}/_\sim$ aus den Äquivalenzklassen $[(z, n)]_\sim := \{(a, b) \in \mathbb{Z} \times \mathbb{N} \mid z \cdot b = n \cdot a\}$ besteht, die Addition in $\mathbb{Z} \times \mathbb{N}/_\sim$ wohldefiniert ist durch

$$[(z_1, n_1)]_\sim + [(z_2, n_2)]_\sim := [(z_1 \cdot n_2 + z_2 \cdot n_1, n_1 \cdot n_2)]_\sim$$

und die Multiplikation durch

$$[(z_1, n_1)]_\sim \cdot [(z_2, n_2)]_\sim := [(z_1 \cdot z_2, n_1 \cdot n_2)]_\sim \ .$$

Die Abbildung $\varphi : \mathbb{Q} \to \mathbb{Z} \times \mathbb{N}/_\sim$ ist gegeben durch $\varphi(\frac{z}{n}) := [(z, n)]_\sim$. (Ohne Beweis!)

Lässt man bei der Definition eines Isomorphismus' $\varphi : G \to H$ nur die Forderung weg, dass φ bijektiv ist, dann hat man einen *Homomorphismus.* Man spricht, jenachdem, ob G und H Gruppen, Ringe oder Körper sind, von Gruppen-, Ring- oder Körperhomomorphismen.

Beispiel Für jedes $m \in \mathbb{N}$ ist die Abbildung

$$\varphi_m : \mathbb{Z} \to \mathbb{Z}_m,\ x \mapsto \varphi_m(x) := x\ mod\ m,$$

ein Ringhomomorphismus von $(\mathbb{Z}, +, \cdot)$ auf $(\mathbb{Z}_m, +_m, \cdot_m)$, denn φ_m ist verknüpfungstreu bezüglich Addition und Multiplikation (aber nicht bijektiv). Man kann nämlich leicht zeigen, dass für alle $a, b \in \mathbb{Z}$ gilt

$$\varphi_m(a+b) = \varphi_m(a) +_m \varphi_m(b) \quad \text{und} \quad \varphi_m(a \cdot b) = \varphi_m(a) \cdot_m \varphi_m(b).$$

Für $m = 9$ und $m = 3$ kann man $\varphi_m(a)$ schnell berechnen. Weil für jedes $k \in \mathbb{N}$ die Zahl $10^k - 1$ durch 9 teilbar ist, gilt für beliebige Ziffern $c_0, c_1, \ldots, c_s \in \{0, 1, 2, \ldots, 9\}$

$$c_0 + c_1 \cdot 10 + c_2 \cdot 10^2 + \ldots + c_s \cdot 10^s \equiv c_0 + c_1 + c_2 + \ldots + c_s\ (mod\ 9).$$

Daher liegt für $m = 9$ und $m = 3$ jedes positive $a \in \mathbb{Z}$, also $a \in \mathbb{N}$, in der selben Äquivalenzklasse modulo m wie seine Quersumme d.h., a und seine Quersumme haben dasselbe Bild unter φ_m. So berechnet man z.B. schnell $\varphi_9(77777) = \varphi_9(35) = \varphi_9(8) = 8$. Speziell folgt die bekannte Regel, dass ein $a \in \mathbb{N}$ genau dann in der Restklasse $[0]_3$ liegt, also durch 3 teilbar ist, wenn dasselbe für seine Quersumme gilt.

3.4 Die komplexen Zahlen

Komplexe Zahlen treten in der Schule erstmals beim Lösen quadratischer Gleichungen auf. Die Gleichung (mit vorgegebenen reellen p und q)

$$x^2 + p \cdot x + q = 0$$

hat im Fall $q > \frac{p^2}{4}$ die nicht-reellen Lösungen

$$x_{1,2} = \frac{-p}{2} \pm \sqrt{q - \frac{p^2}{4}}\sqrt{-1}.$$

Diese zwei nicht-reellen Lösungen sind also vom Typ $a + b \cdot \sqrt{-1}$ mit $a, b \in \mathbb{R}$.

Wenn man mit i eine der beiden Lösungen von $x^2 + 1 = 0$ bezeichnet, kann man die nicht-reellen Lösungen also als $a + b \cdot i$ schreiben mit $a, b \in \mathbb{R}$. Derartige Zahlen nennt man *komplexe Zahlen* und bezeichnet die Menge der komplexen Zahlen als $\mathbb{C}$. Zwei komplexe Zahlen $a_1 + b_1 \cdot i$ und $a_2 + b_2 \cdot i$ sind genau dann verschieden, wenn $a_1 \neq a_2$ oder $b_1 \neq b_2$.

In $\mathbb{C}$ kann man rechnen, als wäre i eine reelle Zahl, also

$$(a + b \cdot i) + (c + d \cdot i) = (a + c) + (b + d) \cdot i$$

und, wenn man ausnutzt, dass $i^2 = -1$ gilt,

$$(a + b \cdot i) \cdot (c + d \cdot i) = (a \cdot c - b \cdot d) + (a \cdot d + b \cdot c) \cdot i.$$

Man kann dann mit (langer und mühevoller) Rechnung zeigen, dass mit dieser Addition und Multiplikation $(\mathbb{C}, +, \cdot)$ ein Körper ist.

Neutrales Element bzgl. $+$ ist hier $0+0\cdot i$, bezüglich der Multiplikation ist es $1+0\cdot i$. Invers zu $a+b\cdot i$ bzgl. $+$ ist $-a+(-b)\cdot i$. Bezüglich der Multiplikation ist $\frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i$ invers zu $a + b \cdot i \neq 0 + 0 \cdot i$, wie man durch Nachrechnen feststellt,

$$(a + b \cdot i) \cdot (\frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2}i) = \frac{a^2 - (-b)b}{a^2 + b^2} + \frac{a(-b) + ba}{a^2 + b^2}i = 1 + 0 \cdot i.$$

Ab sofort schreiben wir a für $a + b \cdot i$, wenn $b = 0$ (und entsprechend $b \cdot i$ für $a + b \cdot i$, wenn $a = 0$). Auf diese Weise können wir die reellen Zahlen als Teilmenge von $\mathbb{C}$ ansehen und wieder 0 für das neutrale Element bzgl. $+$ und 1 für das neutrale Element bzgl. $\cdot$ schreiben.

Satz 3.26 ($(\mathbb{C}, +, \cdot)$ und $(\mathbb{R}^2, +, \cdot)$ sind isomorph)
Auf der Menge $\mathbb{R}^2$ werden zwei Verknüpfungen eingeführt,

$$\begin{aligned}(a, b) + (c, d) &:= (a + c, b + d),\\ (a, b) \cdot (c, d) &:= (a \cdot c - b \cdot d, a \cdot d + b \cdot c).\end{aligned}$$

Dann ist die bijektive Abbildung $\varphi : \mathbb{R}^2 \to \mathbb{C}, (a, b) \mapsto a + b \cdot i$ verknüpfungstreu bzgl. $+$ und $\cdot$, d.h. φ ist ein Isomorphismus von $\mathbb{R}^2$ auf $\mathbb{C}$.

Definition 3.27 (Betrag, Konjugierte, Real- und Imaginärteil)
Zu $z := a + b \cdot i \in \mathbb{C}$ heißt $|z| := \sqrt{a^2 + b^2}$ der *Betrag* von z und $\overline{z} := a - b \cdot i$ die zu z *konjugierte* Zahl. Man nennt $Re(z) := a$ den *Realteil* und $Im(z) := b$ den *Imaginärteil* von $z = a + b \cdot i$.

Satz 3.27 (komplexe Konjugation)
Seien $z, w \in \mathbb{C}$. Dann gelten die folgenden Rechenregeln
1. $\overline{z + w} = \overline{z} + \overline{w}$.
2. $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$.
3. $|z|^2 = z \cdot \overline{z}$.
4. $z^{-1} = \frac{1}{|z|^2}\overline{z}$.

Beweis durch Einsetzen der Definition und Ausrechnen. □

Satz 3.28 (Eigenschaften der Betragsfunktion)
Seien $z, w \in \mathbb{C}$. Dann gelten die folgenden Rechenregeln
1. $|z| \geq 0$.
2. $|z| = 0 \Leftrightarrow z = 0$.
3. $|z \cdot w| = |z| \cdot |w|$.
4. $|z + w| \leq |z| + |w|$ (Dreiecksungleichung)

Beweis Die ersten beiden Regeln folgen aus der Definition. Regel 3 folgt mit Satz 3.27, Regel 3,

$$|z|^2|w|^2 = z\overline{z} \cdot w\overline{w} = zw \cdot \overline{zw} = |z \cdot w|^2.$$

Durch Wurzelziehen bekommt man Regel 3.
Regel 4 ist mühsamer. Mit $z = a + b \cdot i$ und $w = c + d \cdot i$ bekommt man

$$\begin{aligned} z\overline{w} = (a + b \cdot i)(c - d \cdot i) &= ac + bd - (ad - bc)i, \\ \overline{z}w = (a - b \cdot i)(c + d \cdot i) &= ac + bd + (ad - bc)i, \end{aligned}$$

also $z\overline{w} + \overline{z}w = 2(ac + bd)$. Es gelten die Implikationen

$$\begin{aligned} & (ad - bc)^2 \geq 0 \\ \Rightarrow \quad & a^2d^2 + b^2c^2 \geq 2abcd \\ \Rightarrow \quad & a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \geq a^2c^2 + 2abcd + b^2d^2 \\ \Rightarrow \quad & (a^2 + b^2)(c^2 + d^2) \geq (ac + bd)^2 \quad \text{(Cauchy-Schwarz-Ungleichung)} \\ \Rightarrow \quad & |z|^2|w|^2 \geq \tfrac{1}{4}(z\overline{w} + \overline{z}w)^2 \qquad \text{(eben gezeigt)} \\ \Rightarrow \quad & |z| \cdot |w| \geq \tfrac{1}{2}(z\overline{w} + \overline{z}w) \\ \Rightarrow \quad & |z|^2 + 2|z| \cdot |w| + |w|^2 \geq z\overline{z} + z\overline{w} + \overline{z}w + w\overline{w} \\ \Rightarrow \quad & (|z| + |w|)^2 \geq (z + w)\overline{(z + w)} = |z + w|^2 \\ \Rightarrow \quad & |z| + |w| \geq |z + w|. \end{aligned}$$

Weil die erste Aussage $(ad - bc)^2 \geq 0$ wahr ist, gilt auch die letzte Aussage, also Regel 4. □

Zur Veranschaulichung der Multiplikation in der komplexen Zahlenebene benutzt man die *Polarkoordinatendarstellung*: Jedes $z = a + b \cdot i \in \mathbb{C}$ kann man auch als $z = |z|(cos(\varphi) + sin(\varphi) \cdot i)$ schreiben, wobei φ der Winkel zwischen der reellen Achse und der Geraden durch 0 und z ist. Anhand des rechtwinkligen Dreiecks, das die Ecken in 0, z und $a + 0 \cdot i$ hat, erkennt man, dass der Realteil von z, also a, die Ankathete und der Imaginärteil von z, also b die Gegenkathete in diesem Dreieck ist. Daher gilt

$$\cos(\varphi) = \frac{a}{|z|} \quad \text{und} \quad \sin(\varphi) = \frac{b}{|z|}.$$

Satz 3.29 (Multiplikation und Polarkoordinatendarstellung)
Jede komplexe Zahl $z \neq 0$ hat eine Polarkoordinatendarstellung

$$z = |z|(\cos(\varphi) + \sin(\varphi) \cdot i)$$

mit einem (durch z) eindeutig bestimmten Winkel $\varphi \in [0, 2\pi)$. Für die Multiplikation zweier komplexer Zahlen $z = |z|(\cos(\varphi) + \sin(\varphi) \cdot i)$ und $w = |w|(\cos(\psi) + \sin(\psi) \cdot i)$ gilt die Polarkoordinatendarstellung

$$z \cdot w = |z| \cdot |w|(\cos(\varphi + \psi) + \sin(\varphi + \psi) \cdot i).$$

Beweis Die Polarkoordinatendarstellung von $z \cdot w$ erfolgt entweder über die Formel von Euler-deMoivre $\cos(\varphi) + \sin(\varphi) \cdot i = e^{i \cdot \varphi}$ oder mit Hilfe der Additionstheoreme für den Sinus und Cosinus. □

Beispiel Wir betrachten die Zahl $z_1 = i$ und zwei weitere Zahlen z_2 und z_3, die in der komplexen Zahlenebene durch Drehung um $\frac{2\pi}{3}$ bzw. um $\frac{4\pi}{3}$ aus z_1 entstehen. Es gilt $|z_1| = |z_2| = |z_3| = 1$. Rechnung gibt wegen $z_1 = \cos(\frac{\pi}{2}) + \sin(\frac{\pi}{2}) \cdot i$ und wegen $\frac{\pi}{2} + \frac{2\pi}{3} = \frac{7\pi}{6}$, $\frac{\pi}{2} + \frac{4\pi}{3} = \frac{11\pi}{6}$

$$\begin{aligned} z_2 &= \cos(\tfrac{7\pi}{6}) + \sin(\tfrac{7\pi}{6}) \cdot i = \tfrac{-\sqrt{3}}{2} - \tfrac{1}{2}i, \\ z_3 &= \cos(\tfrac{11\pi}{6}) + \sin(\tfrac{11\pi}{6}) \cdot i = \tfrac{\sqrt{3}}{2} - \tfrac{1}{2}i. \end{aligned}$$

Die Multiplikation von z_2 und z_3 kann jetzt auf zwei Weisen erfolgen. Nach der Definition der Multiplikation in $\mathbb{C}$ gilt

$$z_2 \cdot z_3 = \frac{-\sqrt{3}}{2} \cdot \frac{\sqrt{3}}{2} - \frac{1}{2} \cdot \frac{1}{2} + (\frac{-\sqrt{3}}{2} \cdot \frac{-1}{2} + \frac{\sqrt{3}}{2} \cdot \frac{-1}{2}) \cdot i = \ldots = -1.$$

Mit der Polarkoordinatendarstellung bekommt man direkt

$$z_2 \cdot z_3 = \cos(\frac{18\pi}{6}) + \sin(\frac{18\pi}{6}) \cdot i = \cos(3\pi) + \sin(3\pi) = -1.$$

Der folgende Satz ist der Höhepunkt dieses Kapitels. Er besagt im wesentlichen, dass eine Gleichung n-ten Grads,

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$$

bei beliebig vorgegebenen Zahlen $a_{n-1}, \ldots, a_1, a_0$ immer n Lösungen in $\mathbb{C}$ besitzt. Dabei darf es aber sein, dass einige Lösungen mehrfach sind. Für $n = 1$ und $n = 2$ ist dieser Satz bekannt. Für $n > 2$ wurde er erstmal vollständig durch C. F. Gauß in seiner Dissertation 1799 bewiesen. Inzwischen existieren viele alternative Formulierungen dieses Fundamentalsatzes der Algebra und auch viele verschiedene Beweise. Die Beweise erfordern aber Kenntnisse, die

über die von Erstsemestern hinausgehen, so dass der Beweis hier unterbleibt.

Satz 3.20 (Fundamentalsatz der Algebra)
Jedes Polynom

$$f(z) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

mit komplexen Koeffizienten $a_n, a_{n-1}, \ldots, a_1, a_0$ und $a_n \neq 0$, $n \in \mathbb{N}$, hat mindestens eine Nullstelle α in $\mathbb{C}$, d.h., $f(\alpha) = 0,\ \alpha \in \mathbb{C}$.

Dass jetzt ein Polynom vom Grad n wirklich (nicht unbedingt verschiedene) n Nullstellen in $\mathbb{C}$ besitzt, sieht man folgendermaßen ein.

f_n sei Polynom des Grads n mit der nach Satz 3.20 existierenden Nullstelle $\alpha_n \in \mathbb{C}$. Teilt man f_n durch das lineare Polynom $x - \alpha_n$ mit Rest,

$$f_n(x) = f_{n-1}(x)(x - \alpha_n) + r_{n-1}(x),$$

dann hat f_{n-1} den Grad $n-1$ und r_{n-1} den Grad 0 oder $r_{n-1} = 0$. Es gilt

$$r_{n-1}(\alpha_n) = f_n(\alpha_n) - f_{n-1}(\alpha_n)(\alpha_n - \alpha_n) = 0.$$

Daher ist das konstante Polynom r_{n-1} Null, also $f_n(x) = f_{n-1}(x)(x - \alpha_n)$. Wendet man nun den Satz 3.20 auf f_{n-1} an, bekommt man eine Nullstelle α_{n-1} von f_{n-1} und damit entsprechend zur eben gemachten Rechnung $f_{n-1}(x) = f_{n-2}(x)(x - \alpha_{n-1})$. Zusammen also

$$f_n(x) = f_{n-2}(x)(x - \alpha_n)(x - \alpha_{n-1}).$$

Dieses Verfahren setzt man fort bis f_1, das als lineares Polynom die Darstellung

$$f_1(x) = c_1 x + c_0 = c_1(x - \alpha_1) \qquad \text{mit} \quad \alpha_1 = \frac{-c_0}{c_1} \in \mathbb{C}$$

besitzt. Insgesamt also

$$f_n(x) = (x - \alpha_n)(x - \alpha_{n-1}) \cdots (x - \alpha_1) c_1.$$

Hieraus liest man dann ab, dass f_n tatsächlich n (nicht notwendig verschiedene) Nullstellen $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$ besitzt.