4. Algebraische Strukturen: Gruppen, Ringe, Körper

Die bekannten Zahlenmengen besitzen Struktur-Eigenschaften, die wir in abstrakter Form ausdrücken können.

4.1 Definition: Verknüpfung

Eine *Verknüpfung* auf (oder in) einer Menge M ist eine Vorschrift, die je zwei Elementen a und b aus M (unter Beachtung der Reihenfolge) ein weiteres Element c von M zuordnet, also eine Abbildung

$$* : M \times M \to M, \qquad (a, b) \mapsto *(a, b).$$

Anstatt $*(a, b)$ schreiben wir meistens $a * b$.

Notation: Als Symbol für eine Verknüpfung verwendet man auch die üblichen Rechensymbole '$+$', '$\cdot$' (bei Zahlenmengen), oder $\circ$, $\oplus$, $\odot$.
Bei der Multiplikations-Schreibweise $a \cdot b$ lässt man den Punkt oft weg.

4.A Gruppen

4.3 Definition: Gruppe

Eine *Gruppe* ist eine Menge G zusammen mit einer Verknüpfung $\cdot$ auf G, geschrieben $(G, \cdot)$, so dass folgende drei Axiome gelten:

(G1) Die Verknüpfung ist *assoziativ*: Für alle $a, b, c \in G$ gilt

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

(G2) Es gibt ein Element $e \in G$ mit der Eigenschaft

$$e \cdot a = a \quad \text{für alle} \quad a \in G.$$

e heißt *neutrales Element* der Gruppe G.

(G3) Zu jedem Element $a \in G$ gibt es ein $a' \in G$, so dass

$$a' \cdot a = e\,.$$

a' heißt *inverses Element* zu a.

Die Gruppenaxiome lassen weitere Schlüsse zu, z.B. die Eindeutigkeit von neutralem Element e und Inversem a' zu $a \in G$.

4.5 Satz

Es sei $(G, \cdot)$ eine Gruppe.

a) Das neutrale Element $e \in G$ ist eindeutig bestimmt und es gilt

$$e \cdot a = a \cdot e = a \quad \text{für alle} \quad a \in G. \tag{1}$$

b) Das inverse Element a' zu $a \in G$ ist eindeutig bestimmt und es gilt

$$a' \cdot a = a \cdot a' = e. \tag{2}$$

Notation:

- Bei der Verknüpfung '+': Das neutrale Element wird mit 0 bezeichnet, und das inverse Element von a wird mit $(-a)$ bezeichnet und das *Negative* von a genannt. Anstatt $a + (-b)$ schreibt man kurz $a - b$.
- Bei der Verknüpfung '$\cdot$': Das neutrale Element wird oft mit 1 bezeichnet, und das inverse Element von a wird mit a^{-1} bezeichnet.

4.6 Satz: Weitere Rechenregeln

Es sei $(G, \cdot)$ eine Gruppe.

a) Für $a, b \in G$ gilt

$$(a^{-1})^{-1} = a, \qquad (ab)^{-1} = b^{-1}a^{-1}.$$

b) Es gelten die folgenden Kürzungsregeln:

$$ax = ay \;\Rightarrow\; x = y, \qquad xa = ya \;\Rightarrow\; x = y.$$

Bemerkung:

- Man vergleiche die Rechenregel zu $(ab)^{-1}$ mit Satz 2.25.
- Bei einer Gruppe $(G, +)$ bedeuten diese Regeln

$$-(-a) = a, \qquad -(a+b) = (-b) + (-a),$$
$$a + x = a + y \Longrightarrow x = y, \qquad x + a = y + a \Longrightarrow x = y.$$

4.7 Definition

Eine Gruppe $(G, \cdot)$, in der auch das Kommutativgesetz

$$a \cdot b = b \cdot a \quad \text{für alle} \quad a, b \in G$$

gilt, heißt *abelsch* [a] (oder *kommutativ*).

[a] nach Niels Henrik Abel, 1802–1829, norwegischer Mathematiker

Beispiele:

a) Die Gruppen $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ und $(\mathbb{R}, +)$ (mit der üblichen Addition) sind abelsch.

b) Wir setzen $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ und $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$. Die Gruppen $(\mathbb{Q}^*, \cdot)$ und $(\mathbb{R}^*, \cdot)$ (mit der üblichen Multiplikation) sind abelsch.

c) Die symmetrische Gruppe S_n ist für jedes $n \geq 3$ nicht abelsch.

4.8 Definition: Untergruppe

Es sei $(G, \cdot)$ eine Gruppe. Eine nichtleere Teilmenge $H \subseteq G$ heißt *Untergruppe*, wenn mit $a, b \in H$ auch $ab \in H$ sowie $a^{-1} \in H$ gilt.

Insbesondere enthält H dann das neutrale Element von G, und $(H, \cdot)$ ist mit der vorgegebenen Operation selbst eine Gruppe.

Oft betrachten wir die "strukturerhaltenden" Abbildungen zwischen zwei Gruppen.

4.10 Definition: Homomorphismus

Es seien $(G, \cdot)$ und $(H, \odot)$ zwei Gruppen. Eine Abbildung $\phi : G \to H$ heißt *Homomorphismus*, wenn für alle $a, b \in G$

$$\phi(a \cdot b) = \phi(a) \odot \phi(b)$$

gilt. Ein bijektiver Homomorphismus heißt *Isomorphismus*.

4.B Ringe und Körper

4.11 Definition: Ring

Ein *Ring* ist eine Menge R zusammen mit zwei Verknüpfungen $+$ und $\cdot$ (genannt Addition und Multiplikation), für die folgendes gilt:

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

(R2) Die Verknüpfung $\cdot$ ist assoziativ.

(R3) Es gelten die *Distributivgesetze*

$$\left.\begin{aligned} a \cdot (b + c) &= a \cdot b + a \cdot c \\ (a + b) \cdot c &= a \cdot c + b \cdot c \end{aligned}\right\} \quad \text{für alle } a, b, c \in R\,.$$

- Falls auch die Multiplikation das Kommutativgesetz erfüllt, heißt R ein *kommutativer Ring*.
- Eine strukturerhaltende Abbildung $\phi : R_1 \to R_2$ zwischen Ringen $(R_1, +, \cdot)$ und $(R_2, \oplus, \odot)$ heißt *(Ring-)Homomorphismus*:

$$\begin{aligned} \phi(a + b) &= \phi(a) \oplus \phi(b) && \text{für alle } a, b \in R_1, \\ \phi(a \cdot b) &= \phi(a) \odot \phi(b) && \text{für alle } a, b \in R_1. \end{aligned}$$

  Ist ϕ zusätzlich bijektiv, so heißt ϕ *(Ring-)Isomorphismus*.

Wenn man den Begriff eines Ringes benutzt, kann man die Definition eines Körpers (vgl. Analysis I) sehr kurz hinschreiben:

Ein *Körper* K ist ein kommutativer Ring mit Einselement $1 \neq 0$, in dem jedes Element von $K^* := K \setminus \{0\}$ ein Inverses bezüglich der Multiplikation besitzt.

Im Einzelnen bedeutet dies:

4.14 Definition: Körper

Ein *Körper* ist eine Menge K zusammen mit zwei Verknüpfungen $+$ und $\cdot$ (genannt Addition und Multiplikation), für die folgendes gilt:

(K1) $(K, +)$ ist eine abelsche Gruppe. Das neutrale Element wird mit 0 und das Negative von $a \in K$ mit $(-a)$ bezeichnet.

(K2) $(K^* = K \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe. Das neutrale Element wird mit 1 und das Inverse von $a \in K$ mit a^{-1} oder $\frac{1}{a}$ bezeichnet.

(K3) Es gelten die *Distributivgesetze* (R3) in 4.11.

4.C Der Ring $\mathbb{Z}_m$ der Reste modulo m

Den Ring der "Restklassen modulo m" beschreiben wir hier in einer vereinfachten Form, die auch Mittelstufen-Schülern zugänglich ist. Im Abschnitt 5 geben wir eine neue Formulierung an, die sich viel stärker auf das Konzept der Gruppen und Ringe stützt.

4.16 Das Rechnen modulo m (siehe [F; Abschnitt 1.3])

Für ein $m \in \mathbb{N}$ mit $m \geq 2$ fassen wir die Menge

$$\mathbb{Z}_m := \{0, 1, \ldots, m-1\} \subseteq \mathbb{Z}$$

als die Menge der *Reste modulo m* auf (siehe Satz 3.4). Addition und Multiplikation (modulo m) sind definiert durch

$$\begin{aligned} x \oplus_m y &:= (x + y) \bmod m \\ x \odot_m y &:= (x \cdot y) \bmod m \end{aligned}$$

4.17 Beispiel: Addition und Multiplikation in $\mathbb{Z}_6$ geben die folgenden Verknüpfungstafeln an.

$\oplus_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\odot_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

- Den Tabellen entnimmt man, dass 0 neutrales Element der mod-6-Addition und 1 neutrales Element der mod-6-Multiplikation ist.
- Das Negative von 1 ist 5 (siehe Tabelle: $1 \oplus_6 5 = 0$); dies erkennt man auch beim Rechnen in $\mathbb{Z}$, weil -1 und 5 (in $\mathbb{Z}$) den gleichen Rest bei Division durch 6 liefern.
- Man beachte, dass 2, 3 und 4 kein (multiplikatives) Inverses besitzen, denn in der entsprechenden Zeile der Multiplikationstafel tritt die 1 nicht auf.
- Hingegen ist $4 \odot_6 3 = 0$. Man nennt daher die Elemente 4 und 3 *Nullteiler*. Ein weiterer Nullteiler ist 2. Die Existenz von Nullteilern verletzt ein wichtiges Rechengesetz in Körpern.

4.18 Satz

$(\mathbb{Z}_m, \oplus_m, \odot_m)$ ist ein kommutativer Ring, sein Einselement ist 1.

Beweis:

- Das neutrale Element der Addition $\oplus_m$ ist 0, das Negative zu $a \in \mathbb{Z}_m$ ist

$$0 \text{ für } a = 0, \qquad m - a \text{ für } 1 \leq a \leq m - 1.$$

- Das neutrale Element der Multiplikation $\odot_m$ (also das Einselement) ist 1.
- Die Kommutativgesetze sind klar (wie in $\mathbb{Z}$), Assoziativ- und Distributivgesetze folgen aus dem folgenden Lemma.

4.19 Lemma

Für $a, b \in \mathbb{Z}$ gilt

$$\begin{aligned} (a + b) \bmod m &= ((a \bmod m) + (b \bmod m)) \bmod m, \\ (a \cdot b) \bmod m &= ((a \bmod m) \cdot (b \bmod m)) \bmod m. \end{aligned}$$

Gibt es Fälle, in denen $\mathbb{Z}_m$ sogar ein Körper ist, also jedes Element ein multiplikatives Inverses besitzt?

4.20 Beispiel: Verknüpfungstafel für $\mathbb{Z}_5$

$\oplus_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\odot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Alle Elemente (außer 0) besitzen Inverse:

$$1 \odot_5 1 = 1, \quad 2 \odot_5 3 = 3 \odot_5 2 = 1, \quad 4 \odot_5 4 = 1.$$

4.21 Satz

Es sei $p \in \mathbb{N}$ eine Primzahl. Dann ist der Ring $(\mathbb{Z}_p, \oplus_p, \odot_p)$ ein Körper.

Bemerkung: Der endliche Körper $\mathbb{Z}_p$ ganzer Zahlen spielt in der Codierungstheorie eine wichtige Rolle: z.B. ISBN- und EAN-Nummern, Verschlüsselungsverfahren.

In einem Körper K (oder Ring mit Einselement) schreiben wir kurz

$$ma := \underbrace{a + a + \cdots a}_{m-\text{mal}}, \qquad a \in K, \quad m \in \mathbb{N}.$$

4.22 Definition: Charakteristik

Es sei K ein Körper mit Nullelement 0_K und Einselement 1_K. Die Zahl

$$\operatorname{char} K := \begin{cases} 0, & \text{falls } m1_K \neq 0_K \text{ für alle } m \in \mathbb{N}, \\ \min\{m \in \mathbb{N} \mid m1_K = 0_K\}, & \text{sonst,} \end{cases}$$

heißt die *Charakteristik* von K.

Man beachte, dass aus $\operatorname{char} K = 0$ folgt, dass K unendlich viele Elemente besitzt. Das folgende Resultat wird in [F; 1.3.4] bewiesen.

Satz

Es sei K ein Körper. Dann ist entweder $\operatorname{char} K = 0$ oder $\operatorname{char} K$ ist eine Primzahl.

4.D Der Polynomring

Wir verwenden die *Variable* t und definieren Terme der Form t^n mit $n \in \mathbb{N}_0$, die wir mit den üblichen Potenzgesetzen behandeln. Diese Terme werden *formal* betrachtet, sie sind wohlunterschieden. (Wir setzen zunächst keine Zahlen für die Variable t ein.) Eine ausführliche Darstellung ist in [F; 1.3.5–1.3.8] enthalten.

4.23 Definition: Polynom

Ein Term der Form

$$f = \sum_{j=0}^{n} a_j t^j$$

mit $n \in \mathbb{N}_0$ und reellen Zahlen a_j für $0 \leq j \leq n$ heißt *reelles Polynom*. Die Zahlen a_j nennt man die *Koeffizienten* von f.

- Zwei Polynome $f = \sum_{j=0}^{n} a_j t^j, \qquad g = \sum_{j=0}^{m} b_j t^j$ sind *gleich*,

  wenn $a_j = b_j$ für $0 \leq j \leq \min\{m, n\}$ sowie $a_j = 0$ für $j > m$ bzw. $b_j = 0$ für $j > n$ gilt.
- Das Polynom $f = 0$ heißt *Nullpolynom*.
- Für ein Polynom $f = \sum_{j=0}^{n} a_j t^j$, das vom Nullpolynom verschieden ist, heißt

$$\deg f = \max\{j \mid a_j \neq 0\}$$

der Grad (engl. *degree*) von f. Für das Nullpolynom $f = 0$ setzt man $\deg f = -\infty$.

Bemerkung: Das Polynom $p = \sum_{j=0}^{n} a_j t^j$ ist durch die Koeffizientenfolge

$$(a_0, a_1, \ldots, a_n, 0, 0, 0, \ldots)$$

festgelegt. Die Gleichheit von Polynomen $p = \sum_{j=0}^{n} a_j t^j$ und $q = \sum_{j=0}^{m} b_j t^j$ ist genau die Gleichheit der Koeffizientenfolgen

$$(a_0, a_1, \ldots, a_n, 0, 0, 0, \ldots) = (b_0, b_1, \ldots, b_m, 0, 0, 0, \ldots).$$

4.24 Definition: Polynomring

Auf der Menge

$$\mathbb{R}[t] := \left\{ \sum_{j=0}^{n} a_j t^j \;\middle|\; n \in \mathbb{N}_0,\ a_j \in \mathbb{R} \text{ für } 0 \le j \le n \right\}$$

der *reellen Polynome* erklären wir die

- *Addition:* $\displaystyle\sum_{j=0}^{n} a_j t^j + \sum_{j=0}^{m} b_j t^j = \sum_{j=0}^{\max(m,n)} (a_j + b_j) t^j,$
- *Multiplikation:* $\displaystyle\left(\sum_{j=0}^{n} a_j t^j\right) \cdot \left(\sum_{j=0}^{m} b_j t^j\right) = \sum_{j=0}^{m+n} c_j t^j$ mit

$$c_j = \sum_{k=0}^{j} a_k b_{j-k} \quad \text{für} \quad 0 \le j \le m+n.$$

Auf der rechten Seite wird $a_j = 0$ für $j > m$ bzw. $b_j = 0$ für $j > n$ gesetzt.

Bemerkung: Die Multiplikation entspricht dem üblichen Zusammenfassen gleicher Terme unter Berücksichtigung der Regel $t^k \cdot t^{j-k} = t^j$.

Im folgenden Satz fassen wir (ohne Beweis) die Rechenregeln für Polynome zusammen.

4.25 Satz

$(\mathbb{R}[t], +, \cdot)$ ist ein kommutativer Ring mit Einselement. Es gelten also Kommutativ-, Assoziativ- und Distributivgesetze für die Addition und die Multiplikation.

- Sein Nullelement (=neutrales Element der Addition) ist $f = 0$ (das Nullpolynom).
- Sein Einselement (=neutrales Element der Multiplikation) ist $f = 1$.
- Für Polynome $f, g \in \mathbb{R}[t] \setminus \{0\}$ gilt die *Gradformel*

$$\deg(f \cdot g) = \deg f + \deg g.$$

4.26 Erläuterungen

a) Es sei $x \in \mathbb{R}$ fest. Die Abbildung

$$\phi_x : \mathbb{R}[t] \to \mathbb{R}, \quad \phi_x \left(\sum_{j=0}^{n} a_j t^j \right) = \sum_{j=0}^{n} a_j x^j$$

ist ein Ringhomomorphismus von $(\mathbb{R}[t], +, \cdot)$ nach $(\mathbb{R}, +, \cdot)$, der sog. *Einsetz-Homomorphismus*.

b) Die Abbildung

$$\tilde{} : \mathbb{R}[t] \to \mathrm{Abb}(\mathbb{R}, \mathbb{R}), \quad f = \sum_{j=0}^{n} a_j t^j \mapsto \tilde{f} : \mathbb{R} \to \mathbb{R} \text{ mit } \tilde{f}(x) = \sum_{j=0}^{n} a_j x^j$$

ist ein Ringhomomorphismus von $(\mathbb{R}[t], +, \cdot)$ nach $(\mathrm{Abb}(\mathbb{R}, \mathbb{R}), +, \cdot)$.

Dieser Homomorphismus ist injektiv: das Polynom $f \in \mathbb{R}[t]$ und die Abbildung $\tilde{f} : \mathbb{R} \to \mathbb{R}$ werden daher oft identifiziert. Die Schreibweisen $f(x) := \tilde{f}(x) = \phi_x(f)$ für ein $x \in \mathbb{R}$ führen also zu keiner Verwirrung.

c) Die Zahl $\lambda \in \mathbb{R}$ heißt *Nullstelle* des Polynoms $f \in \mathbb{R}[t]$, wenn $\tilde{f}(\lambda) = 0$ gilt; dies ist äquivalent zu $\phi_\lambda(f) = 0$.

d) Für einen beliebigen Körper K ist $K[t]$ die Menge der Polynome mit Koeffizienten in K.
VORSICHT: Für endliche Körper K ist die Abbildung $f \mapsto \tilde{f}$ nicht injektiv: dort muss zwischen dem Polynom $f \in K[t]$ und der (induzierten) Abbildung $\tilde{f} : K \to K$ strikt unterschieden werden. Siehe hierzu Beispiel 1.3.5 in [F].

Die Grad-Abbildung in 4.23 definiert eine "Ordnung" im Polynomring, mit deren Hilfe sich eine *Division mit Rest* ähnlich zu den ganzen Zahlen einführen lässt. Der folgende Satz ist als Analogon zum Satz 3.4 zu verstehen.

4.27 Satz: Division mit Rest im Polynomring

Es seien $f, g \in \mathbb{R}[t]$ Polynome, g sei nicht das Nullpolynom. Dann gibt es eindeutig bestimmte Polynome $q, r \in \mathbb{R}[t]$ derart, dass

$$f = q \cdot g + r \quad \text{und} \quad \deg r < \deg g \tag{3}$$

gilt.

- q heißt der *Quotient* und r heißt der *Rest* von f bei Division durch g.
- f heißt *teilbar durch* g, falls in (3) $r = 0$ gilt, falls also $f = qg$ mit einem Polynom q gilt.

4.28 Satz

Für jedes Polynom $f \in \mathbb{R}[t]$, das vom Nullpolynom verschieden ist, gilt:
$\lambda \in \mathbb{R}$ ist genau dann eine Nullstelle von f, wenn es ein Polynom $g \in \mathbb{R}[t]$ gibt mit

$$f = (t - \lambda) \cdot g \quad \text{und} \quad \deg g = (\deg f) - 1.$$

In diesem Fall ist g eindeutig bestimmt.

Hieraus folgt:

4.29 Korollar

Jedes vom Nullpolynom verschiedene Polynom $f \in \mathbb{R}[t]$ hat höchstens $n := \deg f$ paarweise verschiedene Nullstellen.

Es folgt sogar ein bisschen mehr.

4.30 Definition

Es sei $f \in \mathbb{R}[t]$ verschieden vom Nullpolynom und $\lambda \in \mathbb{R}$. Dann heißt

$$\mu(f,\lambda) := \max\{k \in \mathbb{N}_0 \mid f = (t-\lambda)^k \cdot g_k \text{ mit einem } g_k \in \mathbb{R}[t]\}$$

die *Vielfachheit* von λ. (Hier ist $\mu(f,\lambda) = 0$ zugelassen, also der Fall, dass λ keine Nullstelle von f ist.)

Es gilt die folgende Verschärfung von Korollar 4.29.

4.31 Korollar

Jedes vom Nullpolynom verschiedene Polynom $f \in \mathbb{R}[t]$ hat höchstens $k := \deg f$ paarweise verschiedene Nullstellen unter Berücksichtigung der Vielfachheit; d.h. sind $\lambda_1, \ldots, \lambda_s \in \mathbb{R}$ die paarweise verschiedenen Nullstellen von f, so gilt

$$\mu(f,\lambda_1) + \cdots + \mu(f,\lambda_s) \leq \deg f.$$

5. Äquivalenzrelationen

Das "Rechnen modulo m" wurde in 4.16 in einer Form eingeführt, die für die Mittelstufe geeignet ist. Wir beginnen jetzt mit der neuen Formulierung, die die strukturellen Eigenschaften besser erklärt.

5.1 Der Restklassenring $\mathbb{Z}/m\mathbb{Z}$

Wir betrachten die abelsche Gruppe $(\mathbb{Z}, +)$. Für $m \in \mathbb{N}$ ist $m\mathbb{Z} = \{ma \mid a \in \mathbb{Z}\}$ eine Untergruppe von $\mathbb{Z}$. Wir definieren die *Restklassen*

$$[\ell]_m := \ell + m\mathbb{Z} = \{\ell + ma \mid a \in \mathbb{Z}\}, \qquad \ell = 0, 1, \ldots, m-1.$$

Dies sind m paarweise disjunkte Teilmengen von $\mathbb{Z}$, deren Vereinigung ganz $\mathbb{Z}$ ist,

$$\mathbb{Z} = [0]_m \,\dot\cup\, [1]_m \,\dot\cup \cdots \dot\cup\, [m-1]_m.$$

Der entscheidende Punkt ist nun, dass die Menge der Restklassen

$$\mathbb{Z}/m\mathbb{Z} := \{[0]_m,\ [1]_m, \ldots, [m-1]_m\}$$

selbst wieder eine Gruppe ist, wenn wir als Addition definieren

$$[\ell]_m \oplus [\ell']_m = [(\ell + \ell') \bmod m]_m.$$

Diese Gruppe nennen wir die *Faktorgruppe* oder *Quotientengruppe* $\mathbb{Z}$ *modulo* $m\mathbb{Z}$.

Man beachte:

- Die Addition $\oplus$ verknüpft zwei Restklassen (also Teilmengen von $\mathbb{Z}$) miteinander. Das Ergebnis ist wieder eine Restklasse. Hier wird also eine "mengenwertige" Addition erklärt.

- Die Addition der Restklassen $[\ell]_m \oplus [\ell']_m$ erklärt das eigentliche Wesen der "Addition modulo m": bei der Berechnung

$$(a + b) \bmod m$$

kommt es nicht auf die konkreten **Zahlen** a und b an, sondern nur auf deren **Reste** bei Division modulo m. Daher sollte die "richtige" Definition der Addition eine Verknüpfung von Mengen (den Restklassen $\ell + m\mathbb{Z}$) und nicht von Zahlen sein (wie in 4.16 geschehen).

Für die allgemeine Beschreibung ist ein kurzer Einschub über *Relationen* hilfreich.

5.2 Definition: Relation

a) Es seien X und Y Mengen. Eine Teilmenge $\mathbf{R} \subseteq X \times Y$ heißt *Relation*. Zu einem geordneten Paar $(x, y) \in \mathbf{R}$ sagen wir, dass x in Relation zu y steht und schreiben auch $x\mathbf{R}y$.

b) Es sei X eine Menge. Eine Teilmenge $\mathbf{R} \subseteq X \times X$ heißt *Relation auf* X.

Bemerkung: Der Begriff der Relation ist allgemeiner als der Begriff der Abbildung: Relationen brauchen weder rechts-eindeutig zu sein noch "total" (d.h. nicht jedes $x \in X$ muss 1. Komponente eines Elements von $\mathbf{R}$ sein).

Die letzten Beispiele (4) und (5) illustrieren einen zentralen Begriff der Mathematik. Anstatt die Relation mit **R** zu bezeichnen, verwendet man oft Symbole wie $\equiv$, $\sim$, $\simeq$.

5.4 Definition: Äquivalenzrelation

Eine Relation $\sim$ auf einer Menge M heißt *Äquivalenzrelation*, wenn sie reflexiv, symmetrisch und transitiv ist, d.h.

1. $a \sim a$ für alle $a \in M$ **(Reflexivität)**
2. $(a \sim b) \Longrightarrow (b \sim a)$ für alle $a, b \in M$ **(Symmetrie)**
3. $(a \sim b \ \wedge \ b \sim c) \ \Longrightarrow \ a \sim c$ für alle $a, b, c \in M$ **(Transitivität)**

5.5 Definition: Äquivalenzklasse

Es sei $\mathbf{R}$ eine Äquivalenzrelation auf der Menge M und $a \in M$. Die *Äquivalenzklasse von a bezüglich* $\mathbf{R}$ ist die Teilmenge aller zu a in Relation stehenden Elemente von a:

$$[a]_{\mathbf{R}} := \{x \in M \mid x\mathbf{R}a\}\,.$$

5.6 Satz

Sei $\mathbf{R}$ eine Äquivalenzrelation auf der Menge M.
Die Äquivalenzklassen bezüglich $\mathbf{R}$ bilden eine *Partition* (oder Zerlegung) von M.
Das heißt:

1. Jedes Element von M liegt in einer Äquivalenzklasse.
2. Die Äquivalenzklassen sind paarweise disjunkt.

5.7 Korollar

Sei $\mathbf{R}$ eine Äquivalenzrelation auf der Menge M. Für zwei beliebige Elemente $a, b \in M$ gilt

$$a\mathbf{R}b \text{ genau dann, wenn } [a]_{\mathbf{R}} = [b]_{\mathbf{R}}\,.$$

Bemerkung: Das Korollar begründet die folgende Sprechweise: ein beliebiges Element $b \in [a]_{\mathbf{R}}$ heißt *Repräsentant* der Äquivalenzklasse $[a]_{\mathbf{R}}$.

Wir behandeln nun spezielle Äquivalenzrelationen auf Gruppen (vgl. $\mathbb{Z}/m\mathbb{Z}$).

5.8 Satz: Faktorisierung von Gruppen

Es sei $(G, +)$ eine abelsche Gruppe und $H \subseteq G$ eine Untergruppe.

a) Dann definiert $a \equiv_H b \iff (a - b) \in H$ für $a, b \in G$ eine Äquivalenzrelation auf G.
Die Äquivalenzklassen nennen wir $[a]_H$.

b) Die Addition $[a]_H \oplus_H [b]_H := [a + b]_H$ für $a, b \in G$ ist wohldefiniert, d.h. sie ist unabhängig von der Wahl der Repräsentanten a, b der einzelnen Äquivalenzklassen.

c) Die Menge der Äquivalenzklassen

$$G/H := \{[a]_H \mid a \in G\}$$

ist mit der Addition $\oplus_H$ eine abelsche Gruppe. Sie wird die *Faktorgruppe* (oder *Quotientengruppe*) "G modulo H" genannt.

Bemerkung:

a) Oft schreibt man einfach $+$ für die Addition in H. Man beachte aber den Unterschied zwischen den Operationen in G und in G/H.

b) Die Angabe der Faktorgruppe G/H in Teil c) ist redundant: sie gibt die Äquivalenzklassen mehrmals als Elemente von G/H an. Es genügt, für jede Äquivalenzklasse jeweils nur einen Repräsentanten anzugeben. Wir tun dies am folgenden Beispiel.

c) Für nicht-abelsche Gruppen muss H ein sog. *Normalteiler* von G sein, damit die Addition in G/H wohldefiniert ist. Dies wird in der Vorlesung Algebra I vertieft.

Wohin führt eine solch abstrakte Vorgehensweise der "Faktorisierung"?
Ohne Beweis führen wir den folgenden wichtigen Satz an, der in der Algebra I bewiesen wird. (Der Beweis ist nicht zu schwer, wird aber mangels Anschauungsmaterials erst einmal zurückgestellt.)

5.10 Homomorphie-Satz

Es seien $G, \widetilde{G}$ abelsche Gruppen (mit neutralen Elementen 0_G bzw. $0_{\widetilde{G}}$) und $\phi : G \to \widetilde{G}$ ein Gruppenhomomorphismus.
Dann ist $H = \phi^{-1}(\{0_{\widetilde{G}}\})$ eine Untergruppe von G und $\widetilde{H} = \phi(G)$ eine Untergruppe von $\widetilde{G}$. Weiterhin ist durch

$$\psi : G/H \to \widetilde{H}, \quad [a]_H \mapsto \phi(a),$$

ein **Isomorphismus** von Gruppen definiert.

Wir werden im Kapitel über lineare Gleichungssysteme und lineare Abbildungen zwischen Vektorräumen Beispiele zu diesem Satz finden.

Zwei Ergänzungen zu diesem Abschnitt werden zum Eigenstudium angegeben.

5.11 $\mathbb{Z}/m\mathbb{Z}$ als Ring:

Nicht nur die Addition, auch die Multiplikation lässt sich von $\mathbb{Z}$ auf die Faktorgruppe $\mathbb{Z}/m\mathbb{Z}$ "herunterführen". In Lemma 4.19 wurde für $a, b \in \mathbb{Z}$ gezeigt

$$(a \cdot b) \bmod m = ((a \bmod m) \cdot (b \bmod m)) \bmod m.$$

Daher lässt sich das Produkt zweier Restklassen $[a]_m, [b]_m \in \mathbb{Z}/m\mathbb{Z}$ definieren als

$$[a]_m \odot [b]_m := [a \cdot b]_m.$$

Denn Lemma 4.19 besagt, dass diese Multiplikation wohldefiniert ist, dass also die rechte Seite nicht von der Wahl der Repräsentanten der Restklassen $[a]_m$ und $[b]_m$ abhängt. Somit haben wir gezeigt:

$(\mathbb{Z}/m\mathbb{Z}, \oplus, \odot)$ ist ein Ring, der sog. *Restklassenring modulo m*.

Für jede Primzahl p ist $(\mathbb{Z}/p\mathbb{Z}, \oplus, \odot)$ sogar ein Körper, bezeichnet mit $\mathbb{F}_p$.

Bemerkung: Einordnung in die Ringtheorie

Warum ist auch die Multiplikation von Restklassen "wohldefiniert"?

- $m\mathbb{Z}$ ist ein spezieller Unterring von $\mathbb{Z}$: nicht nur die Produkte $a \cdot b$ von Elementen $a, b \in m\mathbb{Z}$ liegen wieder in diesem Unterring, sondern sogar die Produkte $x \cdot b$ und $b \cdot x$ mit $b \in m\mathbb{Z}$ und $x \in \mathbb{Z}$: wir schreiben kurz

$$\mathbb{Z} \cdot m\mathbb{Z} \subseteq m\mathbb{Z}, \qquad m\mathbb{Z} \cdot \mathbb{Z} \subseteq m\mathbb{Z}.$$

  In der Algebra nennt man $m\mathbb{Z}$ daher ein *Ideal*.

- Diese Eigenschaft von $m\mathbb{Z}$ ist dafür verantwortlich, dass sich das Produkt von $\mathbb{Z}$ auf $\mathbb{Z}/m\mathbb{Z}$ in der angegebenen Weise herunterführen lässt.

Die in Beispiel 5.3 angegebenen Relationen (1)–(3) sind sowohl reflexiv als auch transitiv (aber nicht symmetrisch).

5.12 Definition: Ordnungsrelation

Eine Relation $\leq$ auf einer Menge M heißt *Ordnungsrelation*, , wenn sie reflexiv und transitiv ist.

6 Der Körper der komplexen Zahlen

Das reelle Polynom $f = t^2 + 1$ hat keine reelle Nullstelle, denn für jede reelle Zahl x gilt $x^2 + 1 > 0$.

6.1 Definition von $\mathbb{C}$

Zu den reellen Zahlen fügen wir ähnlich zu Beispiel 4.13(2) eine "neue Zahl" i (="imaginäre Einheit") hinzu, für die gilt $i^2 = -1$.

Dann heißt

$$\mathbb{C} = \mathbb{R}[i] = \{a + b \cdot i \quad \text{mit} \quad a, b \in \mathbb{R}\}$$

Menge der *komplexen Zahlen*. Die Addition und die Multiplikation komplexer Zahlen $z = a + bi$ und $w = c + di$ werden definiert durch

$$z + w = (a + bi) + (c + di) = (a + c) + (b + d)i,$$

$$z \cdot w = (a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i.$$

Bemerkung: Die Multiplikation realisiert das übliche Distributivgesetz und beachtet dabei $i^2 = -1$.

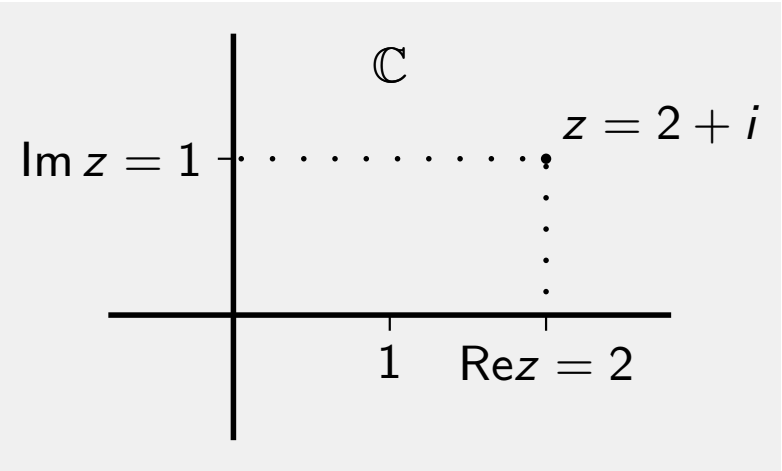
6.2 Die Gaußsche Zahlenebene[a]

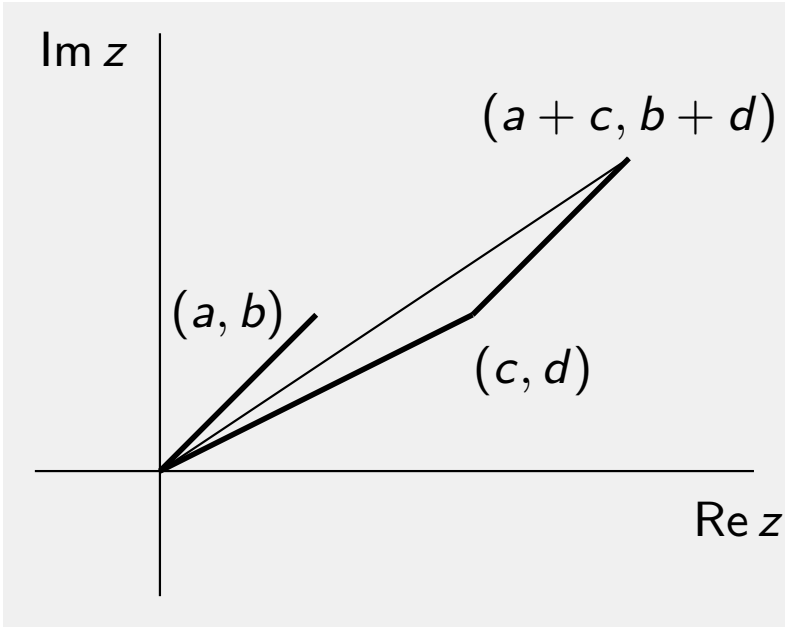
[a] Carl Friedrich Gauß, 1777–1855, deutscher Mathematiker und Astronom

Jede komplexe Zahl $z = a + bi$ entspricht genau einem geordneten Paar (a, b) reeller Zahlen, mit $a = \mathrm{Re}\,(z)$ (*Realteil* von z) und $b = \mathrm{Im}\,(z)$ (*Imaginärteil* von z). Dieses Paar (a, b) wird als Punkt in der Ebene dargestellt. Dabei sind (a, b) die *kartesischen Koordinaten* von $z = a + bi$.

- Die *Addition* $z + w$ komplexer Zahlen entspricht der "Vektoraddition":

$$(a+bi)+(c+di) = (a+c)+(b+d)i \quad \sim \quad (a,b)+(c,d) = (a+c, b+d).$$





- Der *Absolutbetrag* $|z|$ einer komplexen Zahl entspricht dem Abstand vom Nullpunkt:
$$|a + bi| = \sqrt{a^2 + b^2}.$$
- Zu $z = a + bi$ wird die konjugiert komplexe Zahl $\overline{z} = a - bi$ (sprich z-quer) definiert; dies entspricht der Spiegelung von (a, b) an der Realteil-Achse.

6.3 Einfache Rechengesetze:

a) $\mathrm{Re}\,(z) = \frac{1}{2}(z + \overline{z})$, $\quad \mathrm{Im}\,(z) = \frac{1}{2i}(z - \overline{z})$.

b) $|z| = \sqrt{z\overline{z}}$. Weiterhin gilt $|z| = 0 \;\Leftrightarrow\; z = 0$.
Für $r > 0$ ist die Menge $\{z \in \mathbb{C} \mid |z| = r\}$ eine Kreislinie um den Nullpunkt mit Radius r.

c) Für $z \neq 0$ gilt

$$z \cdot \frac{\overline{z}}{|z|^2} = 1 \quad (= 1 + 0i).$$

Dadurch ist der Kehrwert von $z \neq 0$ definiert als $z^{-1} = \frac{1}{z} = \frac{\overline{z}}{|z|^2}$.

Bemerkung: $\mathbb{R} \subseteq \mathbb{C}$ wird durch die Identität $a = a + 0i$ geklärt. Also gilt für beliebiges $z \in \mathbb{C}$:

$$z \in \mathbb{R} \;\Leftrightarrow\; \mathrm{Im}\,(z) = 0 \;\Leftrightarrow\; z = \overline{z}.$$

6.4 Satz: $\mathbb{C}$ ist ein Körper

Die Menge $\mathbb{C}$ der komplexen Zahlen mit der Addition und Multiplikation aus 6.1 ist ein Körper.

Das heißt im Einzelnen:

- es gelten die Kommutativ-, Assoziativ- und Distributivgesetze,
- das neutrale Element der Addition ist $0 = 0 + 0i$, das der Multiplikation ist $1 = 1 + 0i$,
- zu $z = a + bi$ ist $-z = -a - bi$ das negative Element der Addition,
- zu $z = a + bi \neq 0$ ist $z^{-1} = \frac{1}{z} = \frac{\overline{z}}{|z|^2} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i$ das inverse Element der Multiplikation.

6.6 Weitere Rechenregeln in $\mathbb{C}$

Für alle $z, w \in \mathbb{C}$ gilt

(a) $0 \cdot z = z \cdot 0 = 0$ und $(zw = 0 \;\Leftrightarrow\; z = 0 \vee w = 0)$.

(b) $-(-z) = z$ und $(-z) \cdot w = z \cdot (-w) = -(z \cdot w)$.

(c) $\overline{z + w} = \overline{z} + \overline{w}$, $\overline{zw} = \overline{z}\,\overline{w}$, $\overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}}$, falls $w \neq 0$.

(d) $|zw| = |z|\,|w|$, $\left|\frac{z}{w}\right| = \frac{|z|}{|w|}$, falls $w \neq 0$.

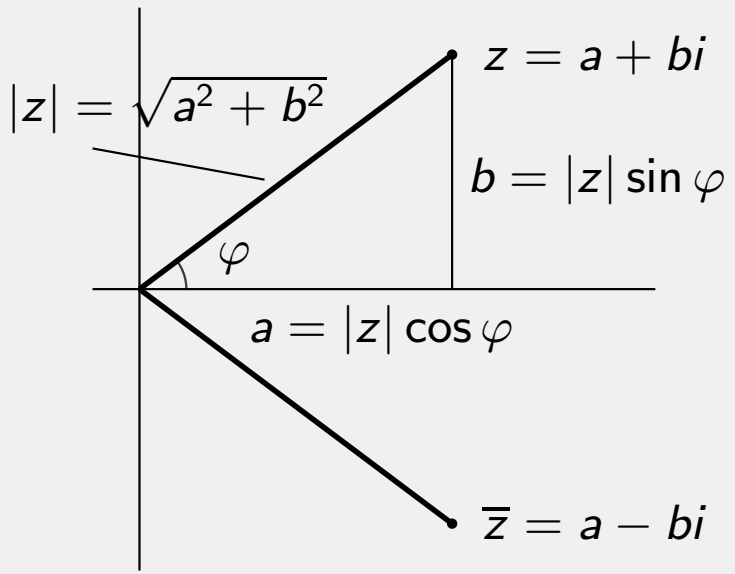
(e) In der Analysis wird gezeigt: $|z + w| \leq |z| + |w|$ (Dreiecksungleichung) und $|z \pm w| \geq \big||z| - |w|\big|$

Für die Multiplikation, Division, Potenzen und Wurzeln eignet sich eine alternative geometrische Beschreibung der komplexen Zahlen.

6.7 Polarkoordinaten in $\mathbb{C}$

Die komplexe Zahl $z = a + bi$ hat die **Polarkoordinaten**

- $r = |z| = \sqrt{a^2 + b^2}$ *Betrag*
  Das ist der Abstand zu 0
- φ *Argument*
  Das ist der Winkel zwischen der positiven reellen Achse und der Strecke von 0 zu z.
  Dabei ist $-\pi < \varphi <= \pi$



Die Darstellung von z in Polarkoordinaten lautet

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

Hierbei ist zu beachten:

- alle Winkel werden im **Bogenmaß** (Einheit rad) gemessen, wobei π rad dem Winkel 180^o entspricht. Umrechnung:
  α^o (α Grad) entspricht $\varphi = \dfrac{\alpha\pi}{180}$ rad
- Die Abbildung

$$\mathbb{C} \setminus \{0\} \to (0,\infty) \times (-\pi,\pi], \qquad a+bi \;\mapsto\; (r,\varphi)$$

  ist bijektiv. Die Umrechnungen lauten

$$\begin{aligned} a &= r\cos\varphi \\ b &= r\sin\varphi \end{aligned}$$

$$\begin{aligned} r &= \sqrt{a^2+b^2} \\ \varphi &= \begin{cases} \arccos(a/r), & \text{falls } b \geq 0, \\ -\arccos(a/r), & \text{falls } b < 0. \end{cases} \end{aligned}$$

  Hierbei wird der Hauptwert des Arcus-Cosinus mit Werten $0 \leq \arccos x \leq \pi$ verwendet.

6.8 Darstellung der Multiplikation, Division und Konjugation mit Polarkoordinaten

Für $z, w \in \mathbb{C} \setminus \{0\}$ mit $\varphi = arg(z)$, $\psi = arg(w)$, gilt:

- Multiplikation:

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

  (Multiplikation der Beträge und Addition der Argumente)

- Division für $w \neq 0$:

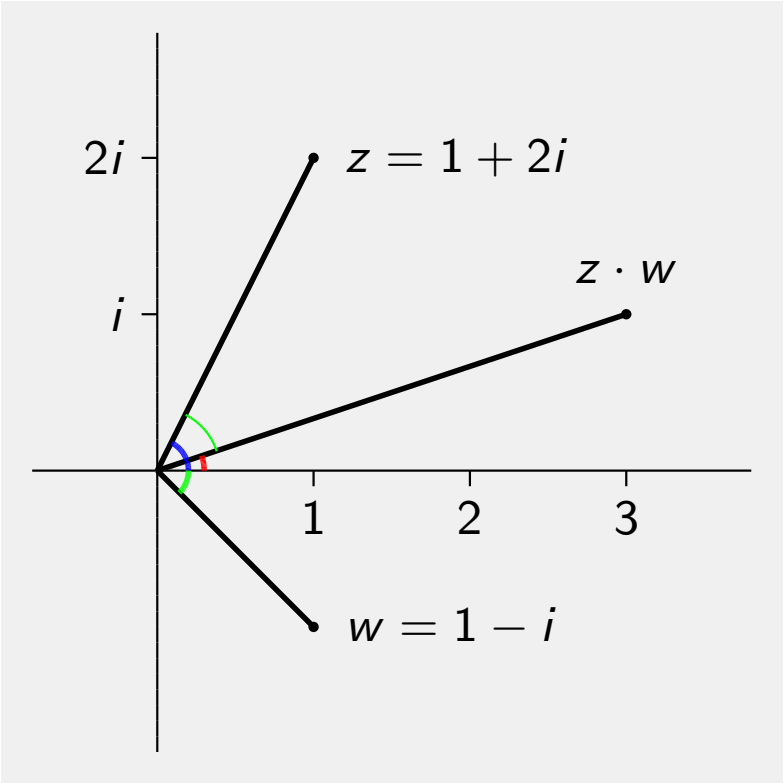
$$\frac{z}{w} = \frac{|z|}{|w|} \, (\cos(\varphi - \psi) + i \sin(\varphi - \psi)) \, .$$

  (Division der Beträge und Subtraktion der Argumente)

- Konjugation:

$$\overline{z} = |z| \, (\cos \varphi - i \sin \varphi) = |z| \, (\cos(-\varphi) + i \sin(-\varphi)) \, .$$

  (Spiegelung an der reellen Achse)



Mit $z \cdot w = (1+2i)(1-i) = 3+i$ ist

$$|z| = \sqrt{5},\ \varphi_z \approx 63°$$
$$|w| = \sqrt{2},\ \varphi_w = -45°$$
$$|zw| = \sqrt{10},\ \varphi_{zw} \approx 18°$$

6.9 Eulersche Formel

Wir setzen zunächst nur formal (als Kurzschreibweise)

$$e^{i\varphi} := \cos\varphi + i\sin\varphi,$$

wobei e die Eulersche Zahl ($\approx 2.7182...$) ist. Diese Formel lässt sich in der Analysis mit Hilfe der Taylorreihe der komplexen Exponentialfunktion beweisen.

Eine Anwendung der Additionstheoreme der sin- und cos-Funktionen ergibt dann

$$z = |z|e^{i\varphi}, \quad w = |w|e^{i\psi} \quad \Longrightarrow \quad z \cdot w = |z|\ |w|e^{i(\varphi+\psi)}.$$

Also erleichtert die Exponential-Schreibweise den Umgang mit den Polarkoordinaten (verwende die üblichen Potenzgesetze an Stelle der Additionstheoreme).

Als direkte Folgerung der Multiplikationsregel ergibt sich:

6.10 Moivresche Formel

Für $z = |z|(\cos\varphi + i\sin\varphi) = |z|e^{i\varphi}$ und $n \in \mathbb{N}$ gilt

$$z^n = |z|^n\big(\cos(n\varphi) + i\sin(n\varphi)\big) = |z|^n\ e^{in\varphi}.$$

Die komplexen Zahlen vom Betrag 1 haben die Form $e^{i\varphi} = \cos\varphi + i\sin\varphi$. Für spezielle Winkel ergeben sich die sogenannten Einheitswurzeln.

6.11 Die n-ten Einheitswurzeln

Sei n eine natürliche Zahl. Die komplexen Zahlen

$$\omega_{n,k} = e^{i2\pi k/n} = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}, \quad k = 0, 1, \ldots, n-1,$$

heißen die n-**ten Einheitswurzeln**; durch sie sind sämtliche komplexe Lösungen der Gleichung

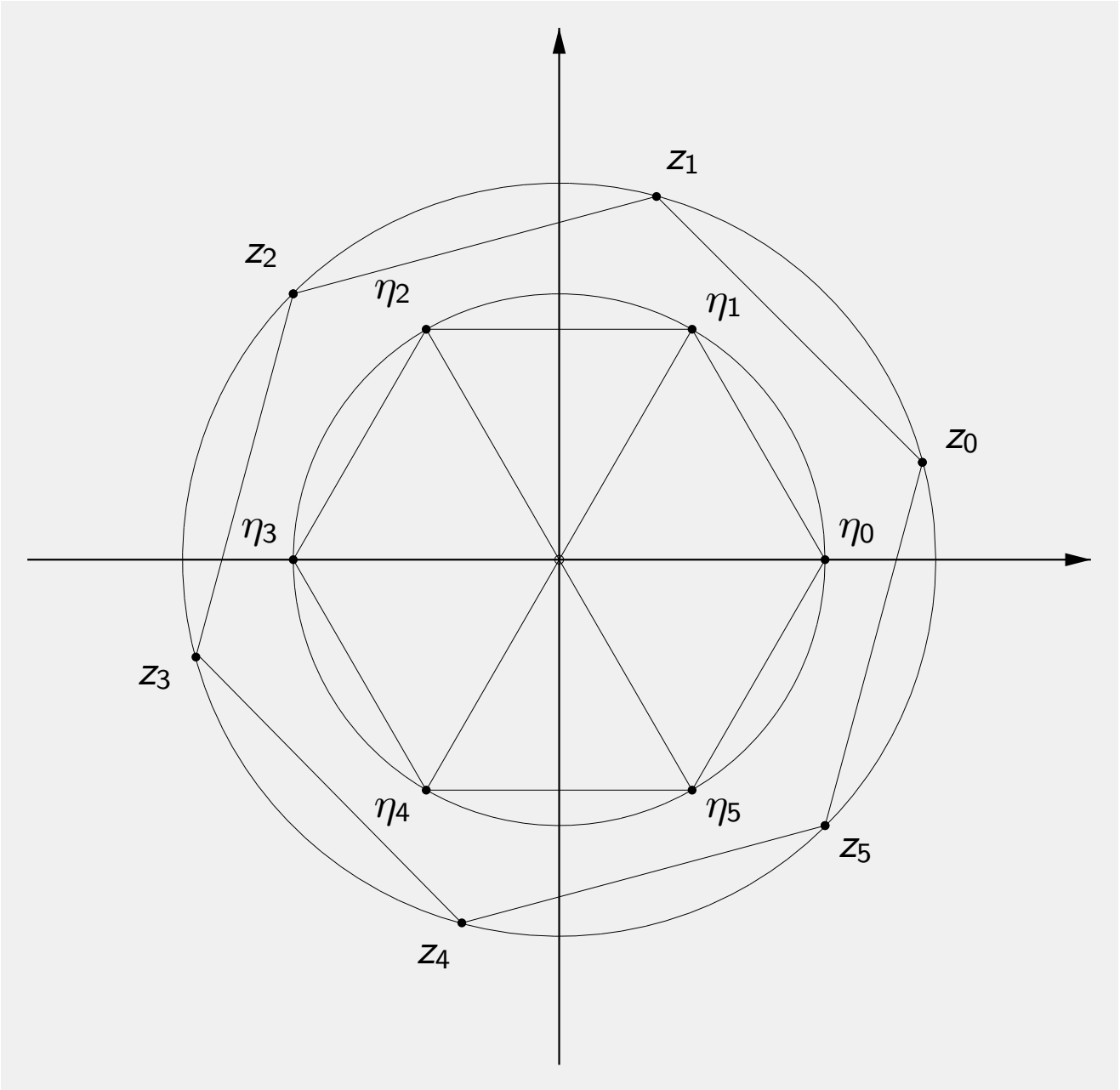
$$z^n = 1$$

gegeben.

6.12 Satz

Es sei $n \in \mathbb{N}$. Die Menge $\Omega_n := \{\omega_{n,k} \mid 0 \leq k \leq n-1\}$ der n-ten Einheitswurzeln bildet eine *Gruppe* bzgl. der Multiplikation komplexer Zahlen. Ihr neutrales Element ist $\omega_{n,0} = 1$.

Diese Gruppe ist isomorph zur abelschen Gruppe $(\mathbb{Z}/n\mathbb{Z}, \oplus)$ der Restklassen modulo n; ein Isomorphismus lautet $\phi : \mathbb{Z}/n\mathbb{Z} \to \Omega_n$, $[k]_n \mapsto \omega_{n,k}$ für $0 \leq k \leq n-1$.



Die sechsten Einheitswurzeln η_0 bis η_5 und die Lösungen von $z^6 = 8i$.

6.13 Satz: Die n-ten Wurzeln in $\mathbb{C}$

Es sei $w = |w|(\cos\varphi + i\sin\varphi) \neq 0$ und $n \in \mathbb{N}$.
Dann sind sämtliche Lösungen der Gleichung $\boxed{z^n = w}$ gegeben durch die n komplexen Zahlen

$$z_k = |w|^{1/n}\left(\cos\left(\frac{\varphi}{n} + \frac{2\pi k}{n}\right) + i\sin\left(\frac{\varphi}{n} + \frac{2\pi k}{n}\right)\right) \text{ mit } k = 0, 1, \ldots, n-1.$$

Ist z^* eine Lösung von $z^n = w$, so sind alle Lösungen durch $z_k = z^* \cdot \omega_{n,k}$ gegeben.

Schreibweise: Die *komplexe* Wurzel $\sqrt[n]{w}$ oder $w^{1/n}$ bezeichnet die Gesamtheit aller n verschiedenen n-ten Wurzeln von w.
(Im Gegensatz zum Reellen: $\sqrt{9} = 3$, und nicht -3.)

6.14 Beispiel:

Die 3-ten Wurzeln von $w = i = e^{i\pi/2}$ sind

$$z_0 = e^{i\pi/6} = \frac{\sqrt{3}}{2} + \frac{1}{2}i, \qquad z_1 = e^{i5\pi/6} = -\frac{\sqrt{3}}{2} + \frac{1}{2}i,$$

$$z_2 = e^{i3\pi/2} = e^{-i\pi/2} = -i.$$

Zum Abschluss dieses Abschnitts geben wir ein Resultat an, das die Einführung und die Verwendung der komplexen Zahlen begründet. Wie in 4.24 sei t eine Variable. Dann definiert

$$\mathbb{C}[t] := \left\{ \sum_{j=0}^{n} a_j t^j \mid n \in \mathbb{N}_0,\ a_j \in \mathbb{C} \text{ für } 0 \leq j \leq n \right\}$$

den Ring der *komplexen Polynome*. Die Begriffe des "Grades", der "Nullstelle" eines Polynoms und deren "Vielfachheit" übertragen wir wörtlich aus Abschnitt 4.D.

6.15 Fundamentalsatz der Algebra

Jedes komplexe Polynom $f \in \mathbb{C}[t]$, das nicht das Nullpolynom ist, hat **genau** $n = \deg(f)$ Nullstellen in $\mathbb{C}$ unter Berücksichtigung der Vielfachheit.

Beweisidee: Es genügt zu zeigen, dass jedes komplexe Polynom $f \in \mathbb{C}[t]$ vom Grad $\deg(f) \geq 1$ mindestens eine Nullstelle $a \in \mathbb{C}$ besitzt. Denn dann folgt mit der Polynomdivision $f = (z - a)g$ und $\deg(g) = \deg(f) - 1$. Der Rest folgt dann per Induktion.
Für die Existenz mindestens einer Nullstelle gibt es zahlreiche Beweise, derjenige von Gauß basiert auf Erkenntnissen über komplex-differenzierbare Funktionen (sog. holomorphe Funktionen), die in der Vorlesung Funktionentheorie behandelt werden.