Einschub: Ringe

R.1. Halbgruppe, Gruppe, Ring, Körper.

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

R1.1. Verknüpfung. Sei S eine Menge. Eine *Verknüpfung* auf S ist eine Abbildung $\mu\colon S \times S \to S$, statt $\mu(s_1, s_2)$ schreibt man manchmal $s_1 + s_2$ oder $s_1 s_2$ oder $s_1 * s_2$ oder $s_1 \circ s_2$ oder $\ldots$.

Halbgruppe. Eine *Halbgruppe* $H = (H, *)$ ist eine Menge H mit einer Verknüpfung (die $(h_1, h_2) \mapsto h_1 * h_2$ geschrieben wird), mit folgenden Eigenschaften:
(H1) Für alle $h_1, h_2, h_3 \in H$ gilt $(h_1 * h_2) * h_3 = h_1 * (h_2 * h_3)$ (Assoziativität).
(H2) Es gibt ein Element $e \in H$ mit $e * h = h = h * e$ für alle $h \in H$. (Einselement).

R1.2. Lemma. *Eine Halbgruppe H hat nur ein Einselement.* (Beweis: Sind Elemente $e, e' \in H$ gegeben mit $e * h = h = h * e$ und $e' * h = h = h * e'$ für alle $h \in H$, so ist $e = e * e' = e'$.) Dieser Beweis zeigt sogar: Das Einselement einer Halbgruppe ist die einzige "Rechts-Eins" und die einzige "Links-Eins"; dabei ist eine "Rechts-Eins" ein Element r mit $h * r = h$ für alle $h \in H$, eine "Links-Eins" $\ldots$. Man schreibt manchmal 1_H für das Einselement der Halbgruppe H. Ist H eine Halbgruppe, so heißt $h \in H$ *idempotent*, falls $h * h = h$ gilt. Das Einselement einer Halbgruppe ist idempotent, im allgemeinen wird es aber in einer Halbgruppe weitere idempotente Elemente geben.

Eine Halbgruppe H heißt *kommutativ* oder auch *abelsch* falls gilt: $h_1 * h_2 = h_2 * h_1$ für alle $h_1, h_2 \in H$. In abelschen Halbgruppen bezeichnet man oft die Verknüpfung mit dem Symbol $+$ und man spricht dann statt vom Einselement der Halbgruppe von der Null der Halbgruppe (Rechenregel: $0 + h = h = h + 0$, für alle $h \in H$).

R1.3. Zahlbereiche, die Halbgruppen sind:

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

R1.4. Ein Element h einer Halbgruppe $(H, \cdot)$ heißt *invertierbar*, wenn es ein $h' \in H$ mit $hh' = h'h = 1_H$ gibt. Existiert ein derartiges Element h', so ist es eindeutig bestimmt und wird das *zu h inverse* Element genannt, und man schreibt h^{-1} statt h' (die Eindeutigkeit sieht man so: ist auch $hh'' = h''h = 1_H$, so ist $h' = h' \cdot 1_H = h'(hh'') =$

$(h'h)h'' = 1_H \cdot h'' = h'')$. Sind die Elemente $h_1, h_2 \in H$ invertierbar, so ist auch h_1h_2 invertierbar und es gilt $(h_1h_2)^{-1} = h_2^{-1}h_1^{-1}$ (beachte die Reihenfolge).

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

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

In einer Gruppe G ist das Einselement e das einzige idempotente Element. (In einer Halbgruppe kann es viele idempotente Elemente geben.)

Sind $G = (G, *)$ und $H = (H, *)$ Gruppen, so ist ein *Gruppen-Homomorphismus* $f\colon G \to H$ eine Abbildung mit folgender Eigenschaften:
(1) $f(g_1 * g_2) = f(g_1) * f(g_2)$ für alle $g_1, g_2 \in G$.

Daraus folgt:
(2) $f(1_G) = 1_H$.
(3) $f(g^{-1}) = (f(g))^{-1}$ für alle $g \in G$.

R1.5. Beispiele von Gruppen:

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

Die Gruppen $(\mathbb{Z}/n\mathbb{Z}, +)$**.** Sei $n \geq 1$. Sei $n\mathbb{Z}$ die Menge der Vielfachen von n, also die Menge der ganzen Zahlen, die durch n ohne Rest teilbar sind. Für jede ganze Zahl a setze $\overline{a} = a + n\mathbb{Z}$. Beachte: *Es gilt $\overline{a_1} = \overline{a_2}$ genau dann, wenn $a_1 - a_2$ durch n teilbar ist.* Ist $0 \leq a < n$, so ist $\overline{a}$ die Menge der ganzen Zahlen, die bei Division durch n den Rest a liefern (man nennt dies eine Restklasse modulo n). Man schreibt $\mathbb{Z}/n\mathbb{Z}$ für die Menge der Restklassen modulo n, und man definiert auf dieser Menge eine Addition vermöge $\overline{a_1} + \overline{a_2} = \overline{a_1 + a_2}$. (Zu zeigen: dies ist wohl-definiert). *Mit dieser Addition ist $\mathbb{Z}/n\mathbb{Z}$ eine Gruppe.*

R1.6. Ringe. Definition: Ein *Ring* $R = (R, +, \cdot)$ ist eine Menge R mit zwei Verknüpfungen $+$ und $\cdot$, so dass die folgenden Eigenschaften erfüllt sind:
(R1) $(R, +)$ ist eine abelsche Gruppe.
(R2) $(R, \cdot)$ ist eine Halbgruppe, das
(R3) Sind r, r_1, r_2 Elemente von R, so gilt $r(r_1+r_2) = rr_1+rr_2$ und $(r_1+r_2)r = r_1r+r_2r$.

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

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

R1.7. Man nennt einen Ring R *nullteilerfrei,* wenn für je zwei Elemente $r, r' \in R$ mit $r \neq 0, r' \neq 0$ gilt: $rr' \neq 0$. Der Ring $\mathbb{Z}$ ist nullteilerfrei, jeder Körper ist nullteilerfrei.

Sind $R = (R, +, \cdot)$ und $S = (S, +, \cdot)$ Ringe, so ist ein *Ring-Homomorphismus* $f\colon R \to S$ eine Abbildung mit folgenden Eigenschaften:
(1) $f\colon (R, +) \to (S, +)$ ist ein Gruppen-Homomorphismus.
(2) $f(r_1 \cdot r_2) = f(r_1) \cdot f(r_2)$ für alle $r_1, r_2 \in R$.
(3) $f(1_R) = 1_S$.

R1.8. Beispiele von Ringen.

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

Die **Ringe** $\mathbb{Z}/n\mathbb{Z}$. Sei $n \geq 1$. Auf der abelschen Gruppe $\mathbb{Z}/n\mathbb{Z}$ definiert man eine Multiplikation durch $\overline{a_1} \cdot \overline{a_2} = \overline{a_1 a_2}$ (wieder ist zu zeigen, dass dies wohl-definiert ist). Auf diese Weise wird $\mathbb{Z}/n\mathbb{Z}$ zu einem kommutativen Ring. Ist n keine Primzahl, so ist $\mathbb{Z}/n\mathbb{Z}$ nicht nullteilerfrei.

Ein extremer Spezialfall: der **Nullring** $(R = \{0\}, +, \cdot)$. Die Grundmenge besteht aus einem einzigen Element (das dann sowohl Nullelement, als auch Einselement ist), Addition und Multiplikation sind natürlich eindeutig bestimmt $(0 + 0 = 0,\ 0 \cdot 0 = 0)$. Beachte: Für $n = 1$ ist $\mathbb{Z}/n\mathbb{Z}$ dieser Nullring. Und: Das Axiomensystem für Körper impliziert, dass ein Körper mindestens zwei Elemente besitzen muss, da $K \setminus \{0\}$ eine Gruppe ist, also nicht leer sein darf. Das übliche Axiomensystem für Ringe schließt nicht aus, dass ein Ring nur aus einem einzigen Element besteht.

Im Rahmen der Linearen Algebra sind inbesondere folgende Ringe von Interesse:

Der Endomorphismenring eines Vektorraums. Sei K ein Körper und V ein Vektorraum. Die Menge $\mathrm{End}(V)$ mit punktweiser Addition und der Hintereinanderschaltung als Multiplikation ist ein Ring.

Der Matrizenring $M(n \times n, K)$ aller $n \times n$-Matrizen mit Koeffizienten in einem Körper (bezüglich der Addition und Multiplipation von Matrizen). Es gilt: Ist V ein n-dimensionaler Vektorraum mit Basis $v_1, \ldots, v_n$, so ist die Zuordnung

$$M^{v_1,\ldots,v_n}_{v_1,\ldots,v_n}\colon \mathrm{End}(V) \to M(n \times n, K)$$

ein Isomorphismus von Ringen.

Allgemeiner: Für jeden Ring R und jede natürliche Zahl n kann man den Ring $M(n \times n, R)$ der $(n \times n)$-Matrizen mit Koeffizienten in R definieren: Man definiert die Addition und die Multiplikation von derartigen Matrizen genau wie im Fall, dass R ein Körper ist.

R1.9. Körper. Ein *Körper* $K = (K, +, \cdot)$ ist ein Ring, in dem die Menge $K^* = K \setminus \{0\}$ unter der Multiplikation abgeschlossen ist und $(K^*, \cdot)$ eine abelsche Gruppe bildet.

R1.10. Beispiele.

Die Zahlbereiche $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sind Körper.

Der Ring $\mathbb{Z}/n\mathbb{Z}$ ist genau dann ein Körper, wenn n eine Primzahl ist. Ist p eine Primzahl, so setzt man $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

R2. Der Polynomring $R[T]$.

R2.1. Definition. Sei R ein Ring. Sei $R[T]$ die Menge der Folgen $(a_0, a_1, \dots)$ von Elementen $a_i \in R$ für die $a_i = 0$ für $i \gg 0$ gilt (es gibt also ein $n \in \mathbb{N}_0$ mit $a_i = 0$ falls $i > n$). Wir betrachten auf $R[T]$ die komponentenweise Addition (also $(a_0, a_1, \dots) + (b_0, b_1, \dots) = (a_0 + b_0, a_1 + b_1, \dots)$. Die Multiplikation ist folgendermaßen definiert:

$$(a_0, a_1, \dots) \cdot (b_0, b_1, \dots) = (c_0, c_1, \dots)$$
$$\text{mit} \quad c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0 = \sum_{i+j=k} a_i b_j.$$

Es gilt: $(R[T], +, \cdot)$ *ist wieder ein Ring; ist R kommutativ, so ist auch $R[T]$ kommutativ.* Die Elemente von $R[T]$ nennt man Polynome mit Koeffizienten in R. Das Nullelement in $R[T]$ ist die Folge $0 = (0, 0, \dots)$, man nennt es auch das *Nullpolynom*. Ist $a \in R[T]$ and gilt $a_n \neq 0$, aber $a_m = 0$ für alle $m > n$, so nennt man n den *Grad* von a und schreibt $\deg a = n$; den Koeffizienten a_n nennt man den *höchsten Koeffizienten*. Ist a ein Polynom vom Grad 0 oder aber das Null-Polynom, so nennt man a ein *konstantes* Polynom. Beachte: $\deg a$ ist nur für $a \neq 0$ definiert (manchmal schreibt man auch $\deg 0 = -\infty$).

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

Ist R der Nullring, so ist auch $R[T]$ der Nullring. Ansonsten aber besteht $R[T]$ immer aus unendlich vielen Elementen, auch wenn R selbst endlich ist. Und: $R[T]$ ist nie ein Körper: der Nullring ist kein Körper, und ist R nicht der Nullring, so ist das Polynom T von Null verschieden, aber sicher nicht invertierbar (invertierbar in $R[T]$ sind nur konstante Polynome).

R2.2. Lemma. *Ist R nullteilerfrei, so gilt für von Null verschiedene Polynome $a, b \in R[T]$*

$$\deg(ab) = \deg a + \deg b$$

(offensichtlich erhält man den höchstens Koeffizienten von ab als Produkt der höchstens Koeffizienten von a und von b). Insbesondere gilt: *Ist R nullteilerfrei, so ist auch $R[T]$ nullteilerfrei.*

R2.3. Das Auswerten von Polynomen. Sei $a = \sum_i a_i T^i$ ein Polynom mit Koeffizienten in einem kommutativen Ring R. Ist $r \in R$, so setzt man $a(r) = \sum_i a_i r^i$.

Lemma. *Sei R ein kommutativer Ring. Sei $r \in R$. Die Auswertungsabbildung*

$$R[T] \to R, \quad \textit{definiert durch} \quad a \mapsto a(r)$$

für $a \in R[T]$ ist ein Ring-Homorphismus (dies folgt aus der Definition von Addition Multiplikation von Polynomen).

Alle Auswertungsabbildungen zusammen liefern eine Abbildung

$$e\colon R[T] \to \mathrm{Abb}(R, R) \quad \text{mit} \quad e(a)(r) = a(r)$$

für $a = a(T) \in R[T]$ und $r \in R$; man nennt die Abbildungen der Form $e(a)$ mit $a \in R[T]$ *polynomiale Abbildungen.*

Warnung. Die Abbildung e ist zwar für $R = \mathbb{R}$ injektiv, im allgemeinen aber nicht: Ist nämlich R ein endlicher Ring, so ist $\mathrm{Abb}(R, R)$ eine endliche Menge - dagegen besitzt der Polynomring $R[T]$ für $R \neq 0$ immer unendlich viele Elemente! Dies ist wichtig, wenn man zum Beispiel mit Polynomen mit Koeffizienten in einem endlichen Körper wie etwa $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (p Primzahl) arbeitet: so sind für $p = 2$ die Polynome $T, T^2, \ldots$ paarweise verschieden; dagegen sind die Abbildungen $e(T), e(T^2), \ldots$ alle gleich (es ist jeweils $0 \mapsto 0$ und $1 \mapsto 1$). Während man in der Analysis üblicherweise Polynome (mit reellen Koeffizienten) einfach als plynomiale Abbildungen einführt, kann man dies für Polynome mit Koeffizienten in einem beliebigen Körper nicht machen: Da gelten soll, dass zwei Polynome nur dann "gleich" sind, wenn ihre Koeffizienten übereinstimmen, wählt man den etwas ungewöhnliche Einstieg: Polynome sind nichts anderes als die Folge ihrer Koeffizienten ... .

R2.4. Nullstellen. Ist R kommutativer Ring, $a \in R[T]$ und $r \in R$, so nennt man r eine *Nullstelle* von a, falls $a(r) = 0$ gilt.

R2.5. Normierte Polynome. Sei R ein Ring und $f \in R[T]$ von Null verschieden. Ist der höchste Koeffizient von f gleich 1, so nennt man f *normiert.*

Ist K ein Körper und $f \in K[T]$ ein von Null verschiedenes Polynom, so lässt sich f eindeutig in der Form $f = c \cdot g$ mit einem normierten Polynom g und $c \in K \setminus \{0\}$ schreiben (dabei ist c gerade der höchste Koeffizient von f).

R3. Die euklid'schen Ringen $\mathbb{Z}$ und $K[T]$.

Vorbemerkung. Wir diskutieren in diesem Abschnitt gemeinsame Eigenschaften des Rings $\mathbb{Z}$ der ganzen Zahlen und der Polynomringe $K[T]$, wobei K ein Körper ist. In diesen Ringen ist das "Teilen mit Rest" möglich (man nennt derartige Ringe "euklid'sche Ringe"). Wir werden sehen, dass es in derartigen Ringen eine "eindeutige Primfaktorzerlegung" gibt. Ganz wichtig ist die "Bézout'sche Gleichung".

R3.1. Teilbarkeit. Sei $(H,\cdot)$ eine kommutative Halbgruppe. Seien $a,b\in H$. Wir schreiben $b|a$ (und sagen b *teilt* a oder auch: b ist ein *Teiler* von a), falls es ein $b'\in H$ gibt mit $bb'=a$. Man nennt ein Element $x\in H$ *irreduzibel*, wenn x nicht invertierbar ist, und wenn aus $x=ab$ folgt, dass a oder b invertierbar ist. Man nennt ein Element $x\in H$ *prim*, wenn x nicht invertierbar ist, und wenn aus $x|ab$ folgt, dass $x|a$ oder $x|b$ gilt.

Die Halbgruppen, an denen wir interessiert sind, sind von der Form $(R\setminus\{0\},\cdot)$, wobei R ein kommutativer nullteilerfreier Ring ist (nur dann ist $R\setminus\{0\}$ unter der Multiplikation abgeschlossen), und zwar für $R=\mathbb{Z}$ und $R=K[T]$.

R3.2. Lemma. *Sei R kommutativer nullteilerfreier Ring und $H=(R\setminus\{0\},\cdot)$. Dann gilt: Prime Elemente aus H sind irreduzibel.*

Beweis: Sei x prim in H, sei $x=ab$. Zu zeigen ist, dass a oder b invertierbar ist. Wegen der Primheit von x gilt $x|a$ oder $x|b$. Sei etwa $x|a$, also $xc=a$ für ein $a\in H$. Dann ist $x=ab=xcb$, also $x(1-cb)=0$. Wegen der Nullteilerfreiheit ist $1-cb=0$, also $cb=1$ und demnach ist b invertierbar.

Die übliche Definition einer Primzahl besagt gerade, dass dies ein irreduzibles Element in $(\mathbb{N}_1,\cdot)$ ist. Primzahlen sind sogar "prim", das soll nun bewiesen werden, aber das ist gar nicht offensichtlich. Zum Beispiel ist 13 Primzahl und kein Teiler von 19. Wieso gilt

$$13\mid 5681=19\cdot 299 \implies 13\mid 299\ ?$$

Warnung: Die Eindeutigkeit der Primfaktorzerlegung ist nichts Selbstverständliches! Hier ein Beispiel einer Halbgruppe H ohne eindeutige Primfaktorzerlegung: die der "Viererzahlen" $H=(\{1,4,8,12,16,\dots\},\cdot)=(\{1\}\cup 4\mathbb{N}_1,\cdot)$. Wir schreiben $b|_H a$, falls es $b'\in H$ gibt mit $bb'=a$. Die kleinsten Zahlen in H, die nicht irreduzible Elemente sind, sind $1,\ 16=4\cdot 4,\ 32=4\cdot 8$, also sind die Elemente

$$4,8,12,20,24,28$$

irreduzibel. Wir sehen: 4 ist irreduzibel in H, aber nicht prim, denn es gilt $4|_H 8\cdot 8=64$, aber 4 teilt in H nicht 8.

Auch gibt es Elemente, die ganz verschiedene Faktorisierungen mit Faktoren, die irreduzibel sind, haben:

$$64=8^2=4^3,\qquad 96=8\cdot 12=4\cdot 24.$$

Eines der Ziele dieses Abschnitts ist zu zeigen, dass

$$H=(\mathbb{Z}\setminus\{0\},\cdot)\quad\text{und}\quad H=(K[T]\setminus\{0\},\cdot)\ \text{(dabei sei } K \text{ ein Körper)}$$

Halbgruppen mit "eindeutiger Primfaktorzerlegung" sind

R3.3. Eindeutige Primfaktorzerlegung im Ring $\mathbb{Z}$. *Jede positive ganze Zahl a lässt sich eindeutig als Produkt*

$$a=p_1\dots p_n$$

schreiben mit Primzahlen $p_1 \le p_2 \le \cdots \le p_n$ *und* $n \ge 0$.

R3.4. Eindeutige Primfaktorzerlegung in Polynomringen. *Sei* K *ein Körper. Jedes normierte Polynom* $f \in K[T]$ *lässt sich in der Form*

$$f = p_1 \dots p_n$$

schreiben mit normierten irreduziblen Polynomen $p_1, p_2, \dots, p_n$ *und* $n \ge 0$. *Ist* $p_1 \dots p_n = q_1 \dots q_m$ *mit normierten irreduziblen Polynomen* p_i, q_j, *so ist* $n = m$, *und es gibt eine Permutation* σ *von* $\{1, 2, \dots, n\}$ *mit* $p_{\sigma(i)} = q_i$ *für alle* i.

Ist $f = p_1 \cdots p_n$ mit normierten irreduziblen Polynomen p_i, so nennt man die Anzahl der Indizes i mit $p = p_i$ die *Vielfachheit von* p *in* f. Ist $p = T - \delta$ mit $\delta \in K$, so nennt man die Vielfachheit von $T - \delta$ in f die *Vielfachheit der Nullstelle* δ.

R3.5. Beginn des Beweises: Existenz einer Faktorisierung. Es ist offensichtlich, dass sich jede positive ganze Zahl a in der Form

$$a = p_1 \dots p_n$$

mit irreduziblen positiven ganzen Zahlen $p_1 \le p_2 \le \cdots \le p_n$ schreiben lässt: Für $a = 1$ nimmt man $n = 0$. Ist $a > 1$, so verwendet man Induktion: Entweder ist a irreduzibel, dann nimmt man $n = 1$ und $p_1 = a$. Andernfalls ist $a = a'a''$ mit positiven ganzen Zahlen $a' < a$ und $a'' < a$. Nach Induktion schreibt man a' und a'' als Produkte ireduzibler positiver Zahlen und muss nur noch die Faktoren in die richtige Reihenfolge bringen.

Entsprechend zeigt man die Existenz einer Produktdarstellung

$$f = p_1 \dots p_n$$

für ein normiertes Polynom $f \in K[T]$ mit irreduziblen Faktoren p_i mit Induktion nach dem Grad von f.

Zu zeigen bleibt die **Eindeutigkeit** einer derartigen Faktorisierung. Dazu verwendet man das Teilen mit Rest.

R3.6. Teilen mit Rest.

Für $\mathbb{Z}$ besagt dies: **Satz.** *Sind* $a, b \in \mathbb{Z}$ *und ist* $b \ne 0$, *so gibt es* $q, r \in \mathbb{Z}$ *mit* $a = qb + r$ *und* $r = 0$ *oder* $|r| < |b|$.

Nun der Fall eines Polynomrings: **Satz.** *Sei* K *Körper. Sind* $a, b \in K[T]$ *und ist* $b \ne 0$, *so gibt es* $q, r \in K[T]$ *mit* $a = qb + r$ *und* $r = 0$ *oder* $\deg(r) < \deg(b)$.

(Teilen mit Rest: r ist der Rest, wenn wir versuchen, a durch b zu teilen. Dabei soll eben entweder $r = 0$ gelten (dann ist b Teiler von a) oder r soll zumindest "klein" sein, und zwar "kleiner" als b, dies wird durch $|r| < |b|$ bzw. $\deg(r) < \deg(b)$ formuliert.)

Ist $R = \mathbb{Z}$, so genügt es, den Fall $b > 0$ zu betrachten, ist $R = K[T]$, so genügt es, den Fall eines normierten Polynomes b zu betrachten: der allgemeine Fall folgt daraus recht mühelos, aber Beweis und Rechnungen werden einfacher (und üblicherweise wird man mit positiven ganzen Zahlen b, beziehungsweise normierten Polynomen b arbeiten).

Beweis im Fall $R = K[T]$. Für $a = 0$ ist nichts zu zeigen (nimm $q = 0,\ r = 0$). Also können wir $a \neq 0$ voraussetzen. Sei $a = \sum_{i=0}^{m} a_i T^i$ und $b = \sum_{j=1}^{n} b_i T^i$ mit $a_m \neq 0$ und $b_n \neq 0$. Ist $m < n$, so ist nichts zu zeigen: Nimm $q = 0$ und $r = a$, es ist $a = 0 \cdot b + r$ und $\deg r = \deg a < \deg b$. Sei nun $m \geq n$. Wir setzen voraus, dass b normiert ist also, ist $b_n = 1$. Bilde nun $a_m T^{m-n}$ und bilde die Differenz $c = a - a_m T^{m-n} b$. Wir bilden also die Differenz zweier Polynome vom Grad m, diese Differenz hat demnach Grad höchstens m. Der höchste Koeffizient ist $a_m - a_m = 0$, also ist $\deg c < m$. Nach Induktion über den Grad können wir voraussetzen, dass sich c durch b mit Rest teilen lässt, etwa $c = q'b + r'$, mit $\deg r' < \deg b$. Demnach ist

$$a = c + a_m T^{m-n} b = q'b + r' + a_m T^{m-n} b = \big(q' + a_m T^{m-n}\big) b + r'.$$

Wir setzen also $q = q' + a_m T^{m-n}$ und $r' = r$.

Hier ein Beispiel für das Teilen mit Rest: Sei $a = T^4 - T^3 + T - 1$, $b = T^3 - 1$. Dann ist

$$T^4 - T^3 + T - 1 = (T - 1)(T^3 - 1) + (2T - 2)$$

(hier ist also $q = T - 1$ und $r = 2T - 2$). Beim Rechnen geht man wie bei der schriftlichen Division vor:

$$\begin{array}{rrrrl} (T^4 & -T^3 & +T & -1\ ) : (T^3 - 1) & = \underbrace{T - 1}_{q} \\ \underline{T^4} & & \underline{-T} & & \\ & -T^3 & +2\,T & & \\ & \underline{-T^3} & & +1 & \\ & & \underbrace{2\,T} & \underbrace{-\,2} & \\ & & r & & \end{array}$$

R3.7. Folgerung (Abspalten einer Nullstelle) *Sei K ein Körper und $f \in K[T]$ und $\gamma \in K$. Genau dann gilt $f(\gamma) = 0$, wenn $T - \gamma$ ein Teiler von f ist.*

Beweis. Ist $T - \gamma$ ein Teiler von f, so ist offensichtlich $f(\gamma) = 0$. Denn aus $f = (T - \gamma)g$ mit $g \in K[T]$ folgt durch Einsetzen von γ, dass gilt

$$f(\gamma) = (\gamma - \gamma) g(\gamma) = 0$$

(hier verwenden wir, dass die Auswertungsabbildung $K[T] \to K$, die jedem Polynom seine Auswertung an der Stelle γ zuordnet, ein Ring-Homomorphismus ist, siehe R2.3), das Teilen mit Rest wird für diese Richtung nicht gebraucht.

Umgekehrt sei nun $f(\gamma) = 0$. Teile f durch $T - \gamma$ mit Rest, also $f = q \cdot (T - \gamma) + r$ mit Polynomen q, r, wobei entweder $r = 0$ gilt oder aber $r \neq 0$ und $\deg r < \deg(T - \gamma) = 1$. In jedem Fall ist r ein konstantes Polynom. Ersetze in $f = q \cdot (T - \gamma) + r$ die Variable T durch γ. Wir erhalten $r(\gamma) = 0$, d.h. das Einsetzen von γ in das konstante Polynom r liefert 0, das heißt aber: $r = 0$. (Auch hier haben wir R2.3 verwendet: die Auswertungsabbildung $K[T] \to K$ ist ein Ring-Homomorphismus).

Insbesondere gilt: *Sei K ein Körper und $f \in K[T]$. Besitzt f keine Nullstelle in K, so ist entweder f ein (von Null verschiedenes) konstantes Polynom, oder* $\deg f \geq 2$.

R3.8. Der größte gemeinsame Teiler. Fall $R = \mathbb{Z}$. Seien $a_1, \ldots, a_n \in \mathbb{Z}$ von Null verschiedene Elemente. Wir sagen, dass d der *größte gemeinsame Teiler* der Zahlen a_i ist und schreiben $d = \mathrm{ggT}(a_1, \ldots, a_n)$, falls gilt:
(1) $d > 0$.
(2) $d|a_i$ für $1 \leq i \leq n$.
(3) Ist $e \in \mathbb{Z}$ und gilt $e|a_i$ für alle i, so gilt auch $e|d$.

Fall $R = K[T]$, mit K ein Körper. Seien $a_1, \ldots, a_n \in K[T]$ von Null verschiedene Elemente. Wir sagen, dass d der *größte gemeinsame Teiler* der Polynome a_i ist und schreiben $d = \mathrm{ggT}(a_1, \ldots, a_n)$, falls gilt:
(1) d ist normiert.
(2) $d|a_i$ für $1 \leq i \leq n$.
(3) Ist $e \in \mathbb{Z}$ und gilt $e|a_i$ für alle i, so gilt auch $e|d$.

In beiden Fällen sieht man unmittelbar, dass ein derartiges Element d eindeutig bestimmt ist. Wir zeigen nun, dass es ein solches Element d auch immer gibt! Dazu brauchen wir das folgende Lemma:

Lemma. *Gilt $f = qg + r$, und ist $d = \mathrm{ggT}(g, r)$, so gilt auch $d = \mathrm{ggT}(f, g)$.*

Beweis: Nach Voraussetzung ist d Teiler von g und r, etwa $dd' = g$ und $dd'' = r$, also ist $d(qd' + d'') = dqd'' + dd'' = qd + r = f$, demnach ist T ein Teiler von f und g. Ist e ein beliebiger Teiler von f und g, etwa $ee' = f$ und $ee'' = g$, so ist $e(e' - qe'') = ee' - eqe'' = f - qg = r$, also ist e ein gemeinsamer Teiler von g und r. Aus $d = \mathrm{ggT}(g, r)$ folgt $e|d$.

R3.9. Satz (Bézout). *Sei $R = \mathbb{Z}$ oder $R = K[T]$ mit K Körper. Seien $a_1, \ldots, a_n \in R$. Dann gibt es $b = \mathrm{ggT}(a_1, \ldots, a_n)$ und es gibt $c_i \in R$ mit $b = \sum c_i a_i$.* (Der Satz besagt also: je n Elemente haben einen größten gemeinsamen Teiler und **dieser lässt sich als Linearkombination mit Koeffizienten in R darstellen.**)

Beweis: Es genügt, den Fall $n = 2$ zu beweisen, der allgemeine Fall folgt dann mit Induktion. Um nicht immer die Fälle $R = \mathbb{Z}$ und $R = K[T]$ unterschieden zu müssen, schreiben wir $\rho(z) = |z|$ für $z \in \mathbb{Z}$ und $\rho(f) = \deg(f)$ für $f \in K[T]$; es ist also $\rho\colon R\backslash\{0\} \to \mathbb{N}_0$ diejenige Abbildung, die beim Teilen mit Rest heranzuziehen ist (um zu formulieren, dass der jeweilige Rest "klein" ist).

Seien $f, g \in R$, beide von Null verschieden. Wir können annehmen, dass $\rho(f) \geq \rho(g)$ gilt (ansonsten vertausche f und g). Sei $f_0 = f, f_1 = g$. Teile f_0 durch f_1 mit Rest, also etwa $f_0 = q_1 f_1 + f_2$. Es ist entweder $f_2 = 0$ oder $\rho(f_1) > \rho(f_2)$. Ist $f_2 \neq 0$, so teilen wir f_1 durch f_2 mit Rest, usw. Allgemein erhalten wir eine Folge von Gleichungen

$$\begin{aligned} f_0 &= q_1 f_1 + f_2 \\ f_1 &= q_2 f_2 + f_3 \\ &\cdots \\ f_{i-1} &= q_i f_i + f_{i+1} \end{aligned}$$

mit $\rho(f_1) > \rho(f_2) > \cdots > \rho(f_i) > \rho(f_{i+1})$. Da jede absteigende Folge natürlicher Zahlen abbricht, muss dieses Verfahren abbrechen, etwa nach n Schritten:

$$(*) \qquad \begin{aligned} f_{n-2} &= q_{n-1} f_{n-1} + f_n \\ f_{n-1} &= q_n f_n \end{aligned}$$

Wir verwenden R3.8 mehrfach und sehen:

$$f_n = \mathrm{ggT}(f_{n-1}, f_n) = \cdots = \mathrm{ggT}(f_1, f_2) = \mathrm{ggT}(f_0, f_1) = \mathrm{ggT}(f, g)$$

das Element f_n ist also größter gemeinsamer Teiler von f und g. Damit ist die **Existenz** von $\mathrm{ggT}(f, g)$ gezeigt.

Die Rechnung liefert aber mehr: Die i-te Gleichung zeigt jeweils, dass sich f_{i+1} als Linearkombination von f_{i-1} und f_i ausdrücken lässt:

$$f_{i+1} = f_{i-1} - q_i f_i.$$

Wir verwenden nun zuerst die Gleichung $(*)$, um f_n als Linearkombination von f_{n-2} und f_{n-1} auszudrücken

$$f_n = f_{n-2} - q_{n-1} f_{n-1}$$

und ersetzen jeweils f_{i+1} durch $f_{i-1} - q_i f_i$, für $i = n-1, n-2, \ldots, 3, 2$. Dies zeigt: f_n lässt sich in der Form $af_0 + bf_1 = af + bg$ mit $a, b \in R$ schreiben. Damit ist der Satz bewiesen.

Man nennt dieses Verfahren den **Euklid'schen Algorithmus zur Bestimmung des ggT.**

Beispiel 1. Betrachte die Zahlen 255 und 221. Es ist

$$(1) \qquad 255 = 1 \cdot 221 + 34$$
$$(2) \qquad 221 = 6 \cdot 34 \ + 17$$
$$(3) \qquad 34 = 2 \cdot 17 \ + 0$$

demnach ist 17 der ggT von 255 und 221. Zurückrechnen liefert

$$\begin{aligned} 17 &\overset{(2)}{=} 221 - 6 \cdot 34 \\ &\overset{(1)}{=} 221 - 6 \cdot (255 - 221) \\ &= 7 \cdot 221 - 6 \cdot 255 \end{aligned}$$

Beispiel 2. Betrachte die beiden Polynome $f = T^3 + 2$ und $g = T^3 + T^2 + 1$. Wir teilen mit Rest:

$$\begin{aligned}
(1) \qquad T^3 + 2 &= 1 \cdot (T^3 + T^2 + 1) + (-T^2 + 1) \\
(2) \qquad (T^3 + T^2 + 1) &= (-T - 1) \cdot (-T^2 + 1) + (T + 2) \\
(3) \qquad (-T^2 + 1) &= (-T + 2) \cdot (T + 2) + (-3) \\
(4) \qquad (T + 2) &= (-\tfrac{1}{3}T - \tfrac{2}{3}) \cdot (-3)
\end{aligned}$$

Wir sehen also: die Polynome f und g sind teilerfremd. Rechnen wir rückwärts, so erhalten wir:

$$\begin{aligned}
-3 &\overset{(3)}{=} (-T^2+1)-(-T+2)(T+2)\\
&\overset{(2)}{=} (-T^2+1)-(-T+2)\big((T^3+T^2+1)-(-T-1)(-T^2+1)\big)\\
&= \big(1-(-T+2)(T+1)\big)(-T^2+1)-(-T+2)(T^3+T^2+1)\\
&= (T^2-T-1)(-T^2+1)-(-T+2)(T^3+T^2+1)\\
&\overset{(1)}{=} (T^2-T-1)\big((T^3+2)-(T^3+T^2+1)\big)-(-T+2)(T^3+T^2+1)\\
&= (T^2-T-1)(T^3+2)+\big(-(T^2-T-1)-(-T+2)\big)(T^3+T^2+1)\\
&= (T^2-T-1)f+(-T^2+2T-1)g,
\end{aligned}$$

also auch

$$1=\frac{1}{3}(-T^2+T+1)\cdot f+\frac{1}{3}(T^2-2T+1)\cdot g.$$

R3.10. Folgerung. *Sei $R=\mathbb{Z}$ oder $R=K[T]$ mit K Körper. Ist $p\in R$ irreduzibel und ist p ein Teiler von uv (dabei seien $u,v\in R$), so ist p ein Teiler von u oder von v.*

Beweis: Sei etwa $pc=uv$. Wir nehmen an, dass p kein Teiler von u ist. Dann sind p,u teilerfremd, also gibt es $a,b\in R$ mit $1=ap+bu$. Also ist $v=(ap+bu)v=apv+buv=apv+bpc=p(av+bc)$.

Beispiel: Wir haben oben gefragt, wieso aus $13\mid 19\cdot 299$ folgt, dass $13\mid 299$ gilt. Wie man sieht, muss man Bézout verwenden: Da 13 und 19 teilerfremd sind, gibt es ganze Zahlen a und b mit $1=13a+19b$ (nämlich $a=3$, $b=-2$), aus $13c=19\cdot 299$ folgt

$$\begin{aligned}
299\cdot 1 &= 299(13a+19b)\\
&= 299\cdot 13\cdot a+299\cdot 19\cdot b\\
&= 299\cdot 13\cdot a+13\cdot c\cdot b\\
&= 13(299a+cb).
\end{aligned}$$

Oft argumentiert man hier mit der Eindeutigkeit der Primfaktorzerlegun $5681=13\cdot 19\cdot 23$, aber die ist bisher noch gar nicht bewiesen! Hier der Beweis:

R3.11. Beweis der Eindeutigkeit der Primfaktorzerlegung für $R=\mathbb{Z}$ oder $R=K[T]$ mit K Körper.

Wir verwenden Induktion nach n. Sei $a=p_1p_2\cdots p_n=q_1q_2\cdots q_m$ mit irreduziblen Elementen p_i,q_i. Wir sehen, dass p_1 ein Teiler von $q_1\cdots q_m$ ist, also ist p_1 ein Teiler von q_j für ein j; nach Umnumerieren der q_i können wir voraussetzen $j=1$, also ist p_1 ein Teiler von q_1, etwa $p_1p_1'=q_1$. Da q_1 irreduzibel ist, muss p_1' invertierbar sein, also ist $p_1=q_1$. Für $n=1$ folgt aus $p_1=p_1(q_2\cdots q_m)$, dass $q_2\cdots q_m=1$ gilt, denn R ist nullteilerfrei und $p_1\neq 0$. Daraus folgt aber $m=1$.

Sei nun $n > 1$. Wieder verwenden wir die Nullteilerfreiheit. Aus $p_1 p_2 \cdots p_n = p_1 q_2 \cdots q_m$ schließen wir, dass gilt $p_2 \cdots p_n = q_2 \cdots q_m$. Nach Induktion sehen wir: es ist $n-1 = m-1$, und es gibt eine Permutation σ der Indizes $2, \ldots, n$, so dass $p_{\sigma(i)} = q_i$ alle für $i \geq 2$ gilt. Dies liefert die Behauptung.

R3.12. Satz. *Sei K ein Körper. Sei $f \in K[T]$ ein normiertes Polynom vom Grad n. Dann besitzt f höchstens n Nullstellen, dies seien die Elemente $\gamma_1, \ldots, \gamma_t$ (paarweise verschiedenen). Ist n_i die Vielfachheit von λ_i als Nullstelle von f, so gilt $\sum_{i=1}^{t} n_i \leq n$ und es gibt ein normiertes Polynom $g \in K[T]$ vom Grad $n - \sum n_i$ mit*

$$f = g \prod_{i=1}^{t} (T - \lambda_i)^{n_i}$$

Dies folgt unmittelbar aus der Eindeutigkeit der Primfaktorzerlegung für $R = K[T]$: ist $f = p_1 \cdots p_n$ mit normierten irreduziblen Polynomen, so unterscheiden wir, welche dieser Polynome p_i den Grad 1 haben: sie sind von der Form $T - \lambda$, dabei ist λ_i eine Nullstelle von f. Auch umgekehrt gilt wegen R3.7: Ist λ eine Nullstelle von f, so ist $T - \lambda$ ein Teiler von f, also, wegen der Eindeutigkeit der Primfaktorzerlegung von f ist $\lambda = \lambda_i$ für ein i. Das Polynom g ist Produkt der Polynome p_i mit $\deg p_i \geq 2$.

R3.13. Irreduzible Polynome. Für jeden Körper K sind die Polynome der Form $T - a$ mit $a \in K$ irreduzibel. Ob dies die einzigen normierten irreduziblen Polynome sind, hängt vom Körper K ab. Hier einige Spezialfälle:

$\mathbb{C}$. Der "Fundamentalsatz der Algebra" besagt gerade, dass jedes irreduzible Polynom über $\mathbb{C}$ linear ist; die einzigen normierten irreduziblen Polynome in $\mathbb{C}[T]$ sind also die Polynome der Form $T - a$ mit $a \in \mathbb{C}$, siehe R4.

$\mathbb{R}$. Der "Fundamentalsatz der Algebra" lässt sich auch so formulieren: jedes irreduzible Polynom über $\mathbb{R}$ hat Grad 1 oder 2. Die normierten irreduziblen Polynome in $\mathbb{R}[T]$ vom Grad 2 sind gerade die Polynome der Form $T^2 + a_1 T + a_0$ mit $a_1^2 < 4a_0$ (und dies sind gerade die Polynome der Form $(T - a)^2 + c$ mit $a, c \in \mathbb{R}$ und $c > 0$).

$\mathbb{Q}$. Zu jeder natürlichen Zahl $n \geq 1$ gibt es irreduzible Polynome in $\mathbb{Q}[T]$ vom Grad n, zum Beispiel $T^n - 2$. Das Studium der irreduziblen Polynome in $\mathbb{Q}[T]$ ist eine wichtige Aufgabe von Algebra und Zahlentheorie.

$\mathbb{F}_p$, mit p Primzahl. Auch hier gibt es zu jeder natürlichen Zahl $n \geq 1$ irreduzible Polynome in $\mathbb{F}_p[T]$ vom Grad n.

Bemerkung. Wir haben gesehen: In Ringen wie $\mathbb{Z}$ oder $K[T]$ kann jedes von Null verschiedene Element als Produkt von irreduziblen Elementen geschrieben werden. Eine derartige Faktorisierung zu finden kann aber mit viel Aufwand verbunden sein! Man verwendet dies heute zum Verschlüsseln von Nachrichten. Leicht dagegen ist die Bestimmung größter gemeinsamer Teiler, denn hier gibt es ein effektives Verfahren, den euklid'schen Algorithmus.

R4. Der Fundamentalsatz der Algebra.

R4.1. Der Körper der komplexen Zahlen $\mathbb{C}$. In der Analysis wurde der Körper $\mathbb{R}$ der reellen Zahlen eingeführt (siehe Röckner, §3) und auch mit dem Körper $\mathbb{C}$ der komplexen Zahlen (§13) gearbeitet.

Nach Definition gilt: $\mathbb{C} = (\mathbb{R}^2, +, \cdot)$, die Grundmenge ist also die Ebene $\mathbb{R}^2$, als Addition nimmt man die komponentenweise Addition, die Multiplikation wird folgendermaßen eingeführt:

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + y_1x_2),$$

Man rechnet leicht nach, dass man auf diese Weise einen Körper erhält, den *Körper $\mathbb{C}$ der komplexen Zahlen* (nicht ganz offensichtlich ist, dass es zu jeder komplexen Zahl $z \neq 0$ eine komplexe Zahl z' mit $zz' = 1$ gibt: Ist $z = (x, y)$, so nimm

$$z' = \big(\frac{x}{x^2 + y^2}, -\frac{y}{x^2 + y^2}\big).$$

Betrachtet man $\mathbb{R}^2$ als zweidimensionalen $\mathbb{R}$-Vektorraum, so kann man jedes Paar (x, y) mit $x, y \in \mathbb{R}$ in der Form $(x, y) = x(1, 0) + y(0, 1)$ schreiben, statt $(1, 0)$ schreibt man einfach 1, denn dies ist gerade das Einselement der Multiplikation von $\mathbb{C}$, statt $(0, 1)$ schreibt man i, also schreibt man statt (x, y) einfach $x + yi$. Nach Konstruktion ist $\mathbb{R}$ eine Teilmenge von $\mathbb{C}$, nämlich die x-Achse; die Punkte auf der y-Achse nennt man *reinimaginär*. Ist $z = x + yi$ mit $x, y \in \mathbb{R}$, so nennt man x den *Realteil* von z und y (oder auch yi) den *Imaginärteil* von z.

Konjugation. Man nennt $x - yi$ die zu $z = x + yi$ *konjugierte* komplexe Zahl und schreibt $\overline{z} = x - yi$. Geometrisch gesehen handelt es sich beim Konjugieren um das Spiegeln an der x-Achse. Dieses Konjugieren hat die folgenden Eigenschaften

$$\begin{aligned} \overline{\overline{z}} &= z \\ \overline{z_1 + z_2} &= \overline{z_1} + \overline{z_1}, \\ \overline{z_1 z_2} &= \overline{z_1} \cdot \overline{z_1}, \end{aligned}$$

die letzten beiden Gleichungen besagen gerade, dass das Konjugieren mit Addition und mit Multiplikation vertauscht, also ein Körper-Isomorphismus $\mathbb{C} \to \mathbb{C}$ ist.

Ist $z = x + yi \in \mathbb{C}$, so ist

$$z \cdot \overline{z} = (x + yi) \cdot (x - yi) = x^2 + y^2$$

immer reell. Beachte, dass auch $z + \overline{z} = 2x$ immer reell ist. Wegen

$$(T - z)(T - \overline{z}) = T^2 - (z + \overline{z})T + z\overline{z}$$

sieht man, dass z und $\overline{z}$ Nullstellen eines quadratischen Polynoms mit reellen Koeffizienten sind.

Betrag. Ist $z = x + iy \in \mathbb{C}$, so setzt man $|z| = \sqrt{x^2 + y^2}$, dies ist gerade die Länge des Vektors (x, y), also der Abstand vom Ursprung. Man nennt $|z|$ den Betrag von z. Wegen $z\overline{z} = x^2 + y^2$ ist also

$$|z| = \sqrt{x^2 + y^2} = \sqrt{z\overline{z}}.$$

Wie wir schon gesehen haben, verwendet man die Gleichung $z\overline{z} = |z|^2$, um für $z \neq 0$ die inverse komplexe Zahl z^{-1} zu finden:

$$z^{-1} = \frac{1}{|z|^2}\overline{z}.$$

Für den Betrag gelten folgende Rechenregeln:

- Es ist $|z|$ eine reelle Zahl mit $|z| \geq 0$.
- Genau dann ist $|z| = 0$, wenn $z = 0$ gilt.
- (Dreiecksungleichung): Sind $z_1, z_2 \in \mathbb{C}$, so ist

$$|z_1 + z_2| \leq |z_1| + |z_2|$$

- (Verträglichkeit mit der Multiplikation) Sind $z_1, z_2 \in \mathbb{C}$, so ist

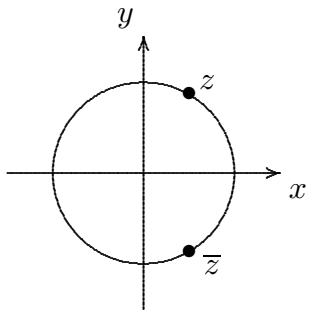
$$|z_1 z_2| = |z_1| \cdot |z_2|.$$

Ist $|z| = 1$, so liegt z auf dem Einheitskreis, hat also die Form

$$z = (\cos\phi, \sin\phi) = \cos\phi + i\sin\phi.$$

Ist $|z| = 1$, so ist $z^{-1} = \overline{z}$, und dies ist ebenfalls ein Punkt auf dem Einheitskreis.

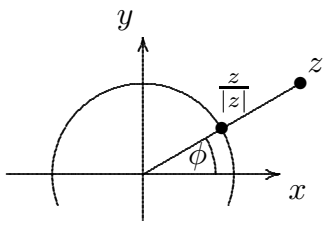
Beweis: Sei $z = x + yi$, also $\overline{z} = x - yi$. Wegen $1 = |z| = x^2 + y^2$ ist $z\overline{z} = x^2 + y^2 = 1$, also ist $\overline{z} = z^{-1}$. Und natürlich liegt mit (x, y) auch $(x, -y)$ auf dem Einheitskreis.



Ganz allgemein ist

$$z = |z|(\cos\phi + i\sin\phi)$$

mit $0 \leq \phi < 2\pi$, man nennt dies die *trigonometrische Darstellung* von z. Ist $z \neq 0$, so ist ϕ (und natürlich auch $|z|$) eindeutig bestimmt.



Seien nun zwei komplexe Zahlen

$$z_1 = |z_1|(\cos\phi_1 + i\sin\phi_1) \quad \text{und} \quad z_2 = |z_2|(\cos\phi_2 + i\sin\phi_2)$$

gegeben. Das Produkt ist

$$\begin{aligned} z_1 \cdot z_2 &= |z_1|(\cos\phi_1 + i\sin\phi_1)|z_2|(\cos\phi_2 + i\sin\phi_2) \\ &= |z_1||z_2|(\cos\phi_1 + i\sin\phi_1)|z_2|(\cos\phi_2 + i\sin\phi_2) \\ &= |z_1||z_2|\left(\cos\phi_1\cos\phi_2 - \sin\phi_1\sin\phi_2 + (\cos\phi_1\sin\phi_2 + \sin\phi_1\cos\phi_2)i\right) \\ &= |z_1||z_2|\left(\cos(\phi_1+\phi_2) + i\sin(\phi_1+\phi_2)\right), \end{aligned}$$

Hier haben wir die Additions-Theoreme für cos und sin verwendet. Man sieht: *Beim Multiplizieren werden die Beträge multipliziert, die Winkel addiert.*

R4.2. Lemma. *Sei z komplexe Zahl, n eine natürliche Zahl. Dann gibt es $z' \in \mathbb{C}$ mit $(z')^n = z$*, also eine n-te Wurzel.

Beweis: Aus der reellen Zahl $|z| \geq 0$ können wir die n-te Wurzel ziehen. Und natürlich können wir den Winkel ϕ durch n teilen. Man nimmt also

$$z' = \sqrt[n]{|z|}\left(\cos(\tfrac{\phi}{n}) + i\sin(\tfrac{\phi}{n})\right).$$

R4.3. Fundamentalsatz der Algebra (GAUSS, 1799). *Jedes nicht-konstante Polynom mit komplexen Koeffizienten hat eine komplexe Nullstelle.*

Beweis. Sei f nicht-konstantes Polynom mit komplexen Koeffizienten. Wegen des Minimumsatzes R4.5 gibt es $c \in \mathbb{C}$ mit $|f(z)| \geq |f(c)|$ für alle $z \in \mathbb{C}$. Nach dem Argand-Lemma R4.4 muss $f(c) = 0$ gelten.

R4.4. Lemma (ARGAND, 1814). *Sei f ein nicht-konstantes Polynom und $b \in \mathbb{C}$. Ist $f(b) \neq 0$, so gibt es $b' \in \mathbb{C}$ mit $|f(b')| < |f(b)|$.*

Beweis: Wir betrachten zuerst den Spezialfall $b = 0$. Das heißt, wir zeigen: *Sei f ein nicht-konstantes Polynom mit komplexen Koeffizienten. Ist $f(0) \neq 0$, so gibt es $c \in \mathbb{C}$ mit $|f(c)| < |f(0)|$.*

Beweis des Spezialfalls: Sei $f = \sum_{t=0}^{n} a_t T^t$, mit $a_n \neq 0$. Es ist $a_0 = f(0) \neq 0$. Wir können annehmen, dass $a_0 = 1$ ist (wir betrachten statt $f(z)$ das Polynom $\frac{1}{a_0}f(z)$). Wir suchen also ein c mit $|f(c)| < 1$.

Sei $1 \leq k < n$ minimal mit $a_k \neq 0$. Es ist also

$$\begin{aligned} f(T) &= 1 + a_k T^k + \cdots + a_n T^n \\ &= 1 + T^k(a_k + a_{k+1}T + \cdots a_n T^{n-k}) \\ &= 1 + T^k g(T), \end{aligned}$$

dabei ist also $g(T)$ das Polynom $g(T) = a_k + a_{k+1}T + \cdots a_nT^{n-k}$ und wie wir wissen ist $a_k \neq 0$. Wir setzen $a = a_k$. Es ist also $g(0) = a \neq 0$.

Wegen $g(0) = a$ und $\frac{1}{2}|a| > 0$ gibt es ein $\delta > 0$ mit

$$(*) \qquad |g(z) - a| \leq \tfrac{1}{2}|a| \quad \text{falls} \quad |z| < \delta.$$

(Hier verwenden wir, dass die Funktion $g(z)$ im Punkt $z = 0$ stetig ist.)

Sei

$$t = \min\{1, \tfrac{1}{2}|a|\delta^k\},$$

es ist also t eine reelle Zahl mit

$$0 < t \leq 1 \quad \text{und} \quad 0 < t \leq \tfrac{1}{2}|a|\delta^k.$$

Die letzte Ungleichung schreiben wir um:

$$\tfrac{t}{|a|} \leq \tfrac{1}{2}\delta^k < \delta^k.$$

Wie wir wissen, kann man aus jeder komplexen Zahl eine k-te Wurzel ziehen. Sei also c eine k-te Wurzel von $-\frac{t}{a}$, also

$$c^k = -\tfrac{t}{a}.$$

Es folgt

$$|c|^k = |\tfrac{t}{a}| < \delta^k, \quad \text{und daher} \quad |c| < \delta.$$

(Wurzelziehen aus positiven reellen Zahlen ist streng monoton.) Wegen $|c| < \delta$ liefert $(*)$ die Abschätzung

$$(**) \qquad |g(c) - a| \leq \tfrac{1}{2}|a|.$$

Also sehen wir

$$\begin{aligned} |f(c)| &= |1 + c^k g(c)| \\ &= |1 + c^k a + c^k g(c) - c^k a| \\ &\leq |1 + c^k a| + |c|^k |g(c) - a| \\ &\leq |1 - t| + |\tfrac{t}{a}| \cdot \tfrac{1}{2}|a| \\ &= 1 - t + \tfrac{1}{2}t = 1 - \tfrac{1}{2}t < 1. \end{aligned}$$

Das erste Ungleichungszeichen ist die Dreiecksungleichung und die Verträglichkeit der Betragsbildung mit der Multiplikation. Beim zweiten Ungleichungszeichen haben wir neben den Gleichungen $c^k a = -t$ und $|c|^k = |\frac{t}{a}|$ die Abschätzung $(**)$ verwendet. Schließlich verwenden wir: wegen $0 < t \leq 1$ gilt $|1 - t| = 1 - t$ und $|t| = t$.

Aus dem Spezialfall $b = 0$ folgt der allgemeine Fall unmittelbar: Ist nämlich f ein nicht-konstantes Polynom und $b \in \mathbb{C}$ mit $f(b) \neq 0$, so setzen wir $h(T) = f(T + b)$. Es ist

$h(0) = f(b) \neq 0$, also gibt es nach dem bewiesenen Spezialfall $c \in \mathbb{C}$ mit $|h(c)| < |h(0)|$. Für $b' = c + b$ ist also

$$f(b') = f(c + b) = h(c)$$

und demnach

$$|f(b')| = |h(c)| < |h(0)| = |f(b)|.$$

Damit ist das Argand-Lemma bewiesen.

R4.5. Minimumsatz von CAUCHY. *Sei $f(T)$ ein Polynom mit komplexen Koeffizienten. Es gibt $c \in \mathbb{C}$ mit $|f(z)| \geq |f(c)|$ für alle $z \in \mathbb{C}$.*

Beweis: Die polynomiale Abbildung $z \mapsto f(z)$ ist stetig, die Betragsabbildung $z \mapsto |z|$ ist stetig, also ist auch die Abbildung $z \mapsto |f(z)|$ stetig.

Man zeigt nun zuerst, dass es eine reelle Zahl r gibt mit $|f(z)| \geq |f(0)|$ für alle z mit $|z| \geq r$. Der Beweis ist der gleiche wie bei reellen Polynomen: man verwendet nur Betragsabschätzungen, die die Koeffizienten von $f(z)$ betreffen.

Zweitens: Wir betrachten die Abbildung $z \mapsto |f(z)|$ auf der Kreisscheibe

$$S = \{z \in \mathbb{C} \mid |z| \leq r\}.$$

Da S kompakt ist, nimmt f auf S sein Minimum an, es gibt also $c \in S$ mit $|f(c)| \leq |f(z)|$ für alle $z \in S$. Insbesondere ist auch $|f(c)| \leq |f(0)|$ und daher $|f(c)| \leq |f(0)| \leq |f(z)|$ für alle $z \in \mathbb{C} \setminus S$, also $|f(c)| \leq |f(z)|$ für alle $z \in \mathbb{C}$.

Aus dem Fundamentalsatz der Algebra folgt:

R4.6. Satz. *Jedes normierte reelle Polynom lässt sich als Produkt von normierten reellen Polynomen vom Grad 1 und 2 schreiben.*

Beweis: Sei $f(T) = \sum_{t=0}^{n} c_t T^t$ ein normiertes reelles Polynom (also mit reellen Koeffizienten c_t) mit Grad n. Wir fassen es auf als Polynom mit komplexen Koeffizienten. Nach dem Fundamentalsatz der Algebra gilt

$$f(T) = \prod_{i=1}^{t} (T - \alpha_i)^{n_i}$$

mit paarweise verschiedenen komplexen Zahlen α_i und $\sum n_i = n$. Unter der Konjugation ändern sich die Koeffizienten von $f(T)$ nicht (da alle c_t reelle Zahlen sind). Rechts dagegen erhalten wir die Faktoren $(T - \overline{\alpha}_i)$. Da das Konjugieren ein Ring-Homomrphismus $\mathbb{C}[T] \to \mathbb{C}[T]$ ist, gilt also

$$f(T) = \prod_{i=1}^{t} (T - \overline{\alpha}_i)^{n_i}.$$

Die Eindeutigkeit der Primfaktorzerlegung in $\mathbb{C}[T]$ zeigt: Ist $\alpha_i \notin \mathbb{R}$, so gibt es j mit $\alpha_j = \overline{\alpha}_i$ und $n_j = n_i$. Also ist $f(T)$ Produkt von Faktoren der Form $T - \alpha$ mit $\alpha \in \mathbb{R}$ und Faktoren der Form $(T - \alpha)(T - \overline{\alpha})$ mit $\alpha \in \mathbb{C} \setminus \mathbb{R}$. Beachte: Die Faktoren der Form $(T - \alpha)(T - \overline{\alpha})$ haben reelle Koeffizienten. Damit ist die Behauptung bewiesen.

Beachte: Diese Folgerung ist eine Aussage über **reelle Polynome,** ohne irgend einen Verweis auf die komplexen Zahlen. Unser Beweis (und jeder andere bisher bekannte Beweis) verwendet die komplexen Zahlen.

Zur Geschichte. Betrachtet man reelle Polynome vom Grad 2, so stellt man sofort fest, dass viele keine reelle Nullstelle haben. Als allgemeine Formel für die Nullstellen von $T^2 + pT + q$ möchte man schreiben:

$$\alpha = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q},$$

die rechte Seite ist aber nur definiert, falls

$$d = \frac{p^2}{4} - q \geq 0$$

gilt. Ist dagegen $d = \frac{p^2}{4} - q < 0$ so stellt sich das Problem, was man unter einer Wurzel einer negativen Zahl verstehen sollte. Es zeigt sich, dass es genügt, ein neues Symbol für eine Wurzel aus -1 einzuführen, wir haben es i genannt. Dann kann man die beiden Wurzeln aus d mit $\pm i\sqrt{-d}$ bezeichnen.

> **Warnung.** Grundsätzlich sollte man für negative Zahlen d nie $\sqrt{d}$ schreiben, da die Verwendung des Wurzelzeichens für negative Zahlen nicht eindeutig definiert werden kann und daher zu Rechenfehlern führen kann (und führen muss). Schreibt man stattdessen $i\sqrt{-d}$ so bezieht man sich auf das einmal gewählte Symbol i, damit ist **eine** Wurzel von -1 fest gewählt.

Ist man nur an reellen Zahlen interessiert, so sind komplexen Zahlen für das Arbeiten mit quadratischen Polynomen gar nicht hilfreich. Das ist aber anders, wenn man kubische Polynome betrachtet. Es gibt eine Nullstellenformel für kubische Polynome (von NICCOLO TARTALIA (1499-1557) und GIROLAMO CARDANO (1501-1576)), die reelle Nullstellen mit Hilfe komplexer Zahlen berechnet.

Die Rechenregeln für das Arbeiten mit "komplexen Zahlen" wurden von RAFAEL BOMBELLI (1526-1572) formuliert, und zwar in seinem Buch **L'Algebra** (1572).

CARL FRIEDRICH GAUSS (1777-1855) hat als erster den Fundamentalsatz der Algebra bewiesen: *Jedes nicht-konstante Polynom mit komplexen Koeffizienten besitzt eine Nullstelle.*