8. Polynome

Polynome über Körpern

Definition (Polynome)

Sei K ein Körper und X ein Unbekannte/Variable. Ein Ausdruck der Form

$$a_0X^0 + a_1X^1 + a_2X^2 + \cdots + a_nX^n = \sum_{i=0}^{n} a_iX^i$$

mit $n \in \mathbb{N}_0$ und Koeffizienten $a_0, \ldots, a_n \in K$, heißt Polynom (über K).

- Die Menge aller Polynome über K bezeichnen wir mit $K[X]$.
- Polynome der Form a_0X^0 heißen konstant.
- Der Körper K läßt sich in $K[X]$ durch $a \mapsto aX^0$ mit den konstanten Polynomen identifizieren und als Teilmenge von $K[X]$ auffassen.
- **Bem.:** Im Allgemeinen werden Polynome oft auch über kommutative Ringe mit 1 (z. B. über $\mathbb{Z}$) betrachtet.

Beispiel

$$1X^0 + \tfrac{7}{3}X^1 + (-0.01)X^2 + 0X^3 + 1X^4 + 0X^5 + \sqrt{2}X^6 \in \mathbb{R}[X]$$

Konventionen

- die Reihenfolge der Terme eines Polynoms ist unerheblich, aber zur besseren Übersicht gibt man die Terme meistens monoton aufsteigend oder absteigend in den Potenzen an
- X^0 ist für alle möglichen Werte 1 und wird oft weggelassen und nur der Koeffizient a_0 geschrieben
- für X^1 schreibt man einfach X
- Terme mit Koeffizient $0 \in K$ läßt man meistens weg
- Koeffizienten $a_i = 1$ läßt man auch meistens weg, außer für $i = 0$
- für Terme der Form $(-a)X^i$ „zieht" man das Minus in die Summe der Terme

Angewandt auf das Beispiel

$$1X^0 + \tfrac{7}{3}X^1 + (-0.01)X^2 + 0X^3 + 1X^4 + 0X^5 + \sqrt{2}X^6$$

ergibt sich die vereinfachte Darstellung

$$\sqrt{2}X^6 + X^4 - 0.01X^2 + \tfrac{7}{3}X + 1\,.$$

Polynome über $\mathbb{Z}/p\mathbb{Z}$

- neben den bekannten Polynomen über $\mathbb{R}$ und $\mathbb{Q}$, können wir nun auch Polynome über $\mathbb{Z}/p\mathbb{Z}$ für Primzahlen p betrachten:

$$[4]_5 X^3 + [-2]_5 X^2 + [1]_5 \in (\mathbb{Z}/5\mathbb{Z})[X]$$

- Zur Vereinfachung der Notation schreiben wir für die Koeffizienten anstelle der Restklassen einfach den Standardrepräsentanten:

$$[4]_5 X^3 + [-2]_5 X^2 + [1]_5 = 4X^3 + 3X^2 + 1 \in (\mathbb{Z}/5\mathbb{Z})[X]\,,$$

wobei

$$[4]_5 X^3 + [-2]_5 X^2 + [1]_5 = 4X^3 - 2X^2 + 1 \in (\mathbb{Z}/5\mathbb{Z})[X]$$

auch üblich ist.

Grad eines Polynoms

Definition (Grad)

Sei $p = \sum_{i=0}^{n} a_i X^i \in K[X]$ ein Polynom über einem Körper K. Der Grad von p ist das größte $i \in \{0, \dots, n\}$ mit $a_i \neq 0$ und wird mit $\operatorname{grad}(p)$ bezeichnet. Gilt $a_i = 0$ für alle $i \in \{0, \dots, n\}$, so nennt man p das Nullpolynom und setzt $\operatorname{grad}(p) = -\infty$.

Konstante Polynome sind dann entweder das Nullpolynom oder Polynome mit Grad 0.

Wenn p nicht das Nullpolynom ist, bezeichnet $a_{\operatorname{grad}(p)}$ den Leitkoeffizienten und p heißt normiert, falls der Leitkoffizient 1 ist.

- zwei Polynome $p = \sum_{i=0}^{n} a_i X^i$ und $q = \sum_{i=0}^{m} b_i X^i$ über dem gleichen Körper K sind gleich, wenn:
  - $\operatorname{grad}(p) = \operatorname{grad}(q)$
  - und $a_i = b_i$ für alle $i = 0, \dots, \operatorname{grad}(p)$.

$$0X^3 - X^2 + 0X + 3 = -X^2 + 0X + 3 = -X^2 + 3$$

Addition von Polynomen

Definition

Seien $p = \sum_{i=0}^{n} a_i X^i$ und $q = \sum_{i=0}^{m} b_i X^i$ Polynome über dem gleichen Körper K. Wir definieren die Summe $p+q$ koeffizientenweise

$$p+q := \sum_{i=0}^{\max\{m,n\}} (a_i + b_i) X^i \,,$$

wobei $b_{m+1} = \ldots = b_n = 0$ (falls $n > m$) b. z. w. $a_{n+1} = \ldots = a_m = 0$ (falls $m > n$).
Somit gilt $\mathrm{grad}(p+q) \leqslant \max\{\mathrm{grad}(p), \mathrm{grad}(q)\}$.

Beispiel: Für $p = X^4 + 3X^2 + 2$ und $q = 4X^4 + X^3 + 2X^2 - 1 \in (\mathbb{Z}/5\mathbb{Z})[X]$ erhalten wir

$$p+q = 5X^4 + X^3 + 5X^2 + 1 = X^3 + 1 \in (\mathbb{Z}/5\mathbb{Z})[X]$$

$\Longrightarrow \mathrm{grad}(p+q) = 3 < 4 = \max\{\mathrm{grad}(p), \mathrm{grad}(q)\}$ hier

Im Allgmeinen gilt: $\mathrm{grad}(p+q) < \max\{\mathrm{grad}(p), \mathrm{grad}(q)\}$
$\quad\Longleftrightarrow \mathrm{grad}(p) = \mathrm{grad}(q)$ und die Leitkoeffizienten sind additive Inverse in K.

Multiplikation von Polynomen

Definition

Seien $p = \sum_{i=0}^{n} a_i X^i$ und $q = \sum_{i=0}^{m} b_i X^i$ Polynome über dem gleichen Körper K. Wir definieren das Produkt $p \cdot q$ „durch ausmultiplizieren“

$$p \cdot q := \sum_{i=0}^{m+n} c_i X^i \quad \text{mit} \quad c_i := \sum_{j=0}^{i} a_j b_{i-j} = a_0 b_i + a_1 b_{i-1} + \cdots + a_i b_0$$

wobei (ähnlich wie bei der Addition) dafür $b_{m+1} = \ldots = b_{m+n} = 0$ und $a_{n+1} = \ldots = a_{m+n} = 0$ gesetzt wird.

Aus der Definition folgt direkt:

$$\operatorname{grad}(p \cdot q) \leqslant \operatorname{grad}(p) + \operatorname{grad}(q) \quad \text{mit} \quad c_{\operatorname{grad}(p)+\operatorname{grad}(q)} = a_{\operatorname{grad}(p)} \cdot b_{\operatorname{grad}(q)}$$

Da in Körpern das Produkt $a_{\operatorname{grad}(p)} \cdot b_{\operatorname{grad}(q)}$ zweier von Null verschiedener Elemente niemals Null ist, folgt somit auch

$$\operatorname{grad}(p \cdot q) = \operatorname{grad}(p) + \operatorname{grad}(q)$$

für Polynome über einem Körper K.

Beispiel

Für $p = X^3 + 3X^2 + 2$ und $q = 2X^2 - X + 4 \in (\mathbb{Z}/5\mathbb{Z})[X]$ erhalten wir

$$p \cdot q = (X^3 + 3X^2 + 2) \cdot (2X^2 - X + 4)$$

ausmultiplizieren ergibt

$$= 2X^5 + (-1 + 3 \cdot 2)X^4 + (4 - 3)X^3 + (3 \cdot 4 + 2 \cdot 2)X^2 - 2X + 8$$

und zusammenfassen und umrechnen in Standardrepräsentanten führt zu

$$= 2X^5 + 5X^4 + X^3 + 16X^2 - 2X + 8 = 2X^5 + X^3 + X^2 + 3X + 3\,.$$

Es gilt in $(\mathbb{Z}/5\mathbb{Z})[X]$ also

$$(X^3 + 3X^2 + 2) \cdot (2X^2 - X + 4) = 2X^5 + X^3 + X^2 + 3X + 3.$$

Verwirrender Abstecher

Betrachtet man Polynome über kommutative Ringe (mit 1), dann gilt die Gradformel für das Produkt im Allgemeinen nicht.

Beispiel: Für $p = 2X^3$ und $q = 3X^2 + 1$ in $(\mathbb{Z}/6\mathbb{Z})[X]$ gilt

$$p \cdot q = 6X^5 + 2X^3 = 2X^3 \in (\mathbb{Z}/6\mathbb{Z})[X]$$

$\Longrightarrow \mathrm{grad}(p \cdot q) = 3 < 5 = \mathrm{grad}(p) + \mathrm{grad}(q)$

Polynomringe

Satz

Für jeden Körper K ist die Menge der Polynome $K[X]$ zusammen mit der definierten Addition und Multiplikation für Polynome ein kommutativer Ring mit 1, wobei das Nullpolynom das neutrale Element der Addition und das konstante Polynom $1 = 1X^0$ das neutrale Element der Multiplikation ist.

Wir nennen $K[X]$ deswegen Polynomring (über K).

Beweis:

- Assoziativität und Kommutativität von $+$ vererbt sich von K
- Nullpolynom ist offensichtlich neutral bezüglich der Addition
- $p = \sum_{i=0}^{n} a_i X^i \in K[X] \implies -p := \sum_{i=0}^{n} (-a_i) X^i \in K[X]$

$\Rightarrow$ $(K[X], +)$ ist eine abelsche Gruppe

- Assoziativität und Kommutativität von $\cdot$ vererbt sich von K
- konstantes Einspolynom $1 = 1X^0$ ist neutral bezüglich der Multiplikation

$\Rightarrow$ $(K[X], \cdot)$ ist ein kommutatives Monoid

- Distributivgesetzte kann man nachrechnen $\square$

Auch Polynome $R[X]$ über kommutative Ringe R mit 1 bilden einen solchen.

Eigenschaften von Polynomringen

- $K[X]$ ist ein Ring
- $K[X]$ enthält eine Kopie von K
- $K[X]$ hat ein Element X
- $K[X]$ wird von K und X erzeugt: jedes Element kann in der Form $\sum_{i=0}^{n} a_i X^i$ dargestellt werden, mit allen a_i in K.
- Keine unerwartete Gleichungen: $\sum_{i=0}^{n} a_i X^i = \sum_{i=0}^{n} b_i X^i$ gilt nur dann, wenn $a_i = b_i$ für alle $i \leqslant n$.

Teilbarkeit für Polynome

Definition

Sei K ein Körper und $p, q \in K[X]$ Polynome. Das Polynom p ist ein Vielfaches von q, falls es ein Polynom $m \in K[X]$ gibt, sodass

$$p = q \cdot m\,.$$

Wir schreiben dafür $q \mid p$ und sagen q teilt p, oder q ist ein Teiler von p.

Teilt ein Polynom $r \in K[X]$ sowohl p als auch q, dann ist r ein gemeinsamer Teiler von p und q.

Das Polynom r ist ein größter gemeinsamer Teiler von p und q ($\neq$ Nullpolynom), wenn es ein gemeinsamer Teiler mit maximalem Grad ist.

Der größte gemeinsame Teiler von einem Polynom p und dem Nullpolynom ist p, insbesondere auch, falls p selbst das Nullpolynom ist.

Beispiel: In $\mathbb{Z}/5\mathbb{Z}$ gilt

$$(X^3 + 3X^2 + 2) \cdot (2X^2 - X + 4) = 2X^5 + X^3 + X^2 + 3X + 3\,.$$

$\Rightarrow X^3 + 3X^2 + 2$ und $2X^2 - X + 4$ sind Teiler von $2X^5 + X^3 + X^2 + 3X + 3$.

Einheiten in $K[X]$

- $p \in (K[X])^\times$, falls es ein $q \in K[X]$ mit $p \cdot q = 1 = 1X^0$ gibt
- $\operatorname{grad}(1) = 0$ und da K ein Körper ist, gilt

$$\operatorname{grad}(p \cdot q) = \operatorname{grad} p + \operatorname{grad} q$$

$\Rightarrow$ nur die konstanten Polynome mit Grad 0 können Einheiten sein

- tatsächlich gibt es für jedes $a \in K \setminus \{0\}$ ein multiplikativ Inverses $a^{-1} \in K \setminus \{0\}$ und für die konstanten Polynome $p = aX^0$ und $q = a^{-1}X^0$ gilt

$$p \cdot q = (a \cdot a^{-1})X^0 = 1X^0$$

Satz

Für jeden Körper K sind die Einheiten des Polynomrings $K[X]$ genau die konstanten Polynome vom Grad 0, d. h.

$$(K[X])^\times = \left\{aX^0 \colon a \in K \setminus \{0\}\right\}.$$

Größte gemeinsame Teiler

- wie man an den konstanten Polynomen leicht sieht, sind größte gemeinsame Teiler nicht eindeutig bestimmt
- z. B. für $p_1 = aX^0$, $p_2 = bX^0 \in K[X]$ mit $a, b \neq 0$ teilt jedes Polynom $m = cX^0$ mit $c \neq 0$ sowohl p_1 als auch p_2 und da jeder Teiler von p_1 und p_2 Grad 0 haben muss, ist ein jedes solches m ein größter gemeinsamer Teiler
- auch für Polynome mit höheren Grad tritt diese Phänomen auf, da

$$m \mid p_1 \quad \text{und} \quad m \mid p_2 \qquad \Longrightarrow \qquad a \cdot m \mid p_1 \quad \text{und} \quad a \cdot m \mid p_2$$

  für alle $m, p_1, p_2 \in K[X]$ und $a \in K \setminus \{0\}$
- ein größter gemeinsamer Teiler zweier Polynome läßt sich wie der ggT zweier ganzer Zahlen mit dem EUKLIDischen Algorithmus bestimmen
- EUKLIDischer Algorithmus in $\mathbb{Z}$ beruht auf der Division mit Rest
- analog führen wir die Division mit Rest in $K[X]$ ein

$\longrightarrow$ Polynomdivision

Polynomdivision

Satz

Sei K ein Körper und seien $p, m \in K[X]$ Polynome mit $m \neq 0$, dann gibt es Polynome $q, r \in K[X]$ mit $p = q \cdot m + r$ und $\text{grad}(r) < \text{grad}(m)$.

Beweis: Sei $p = \sum_{i=0}^{n} a_i X^i$ und $m = \sum_{i=0}^{k} b_i X^i$ mit $\text{grad}(p) = n$ und $\text{grad}(m) = k$. Der folgende Algorithmus der Polynomdivision ermittelt Polynome q und r mit den gewünschten Eigenschaften.

1. Falls $n < k$, dann geben wir $q = 0$ und $r = p$ aus.
2. Initialisiere $s = p$
3. Solange $\ell := \text{grad}(s) \geqslant k$ und $s = \sum_{i=0}^{\ell} d_i X^i$:
   - Setze $c_{\ell-k} = \frac{d_\ell}{b_k}$.
   - Setze $s := s - c_{\ell-k} X^{\ell-k} \cdot m$.
4. Gib $r = s$ und $q = \sum_{i=0}^{n-k} c_i X^i$ aus.

Algorithmus terminiert, da sich in jedem Durchlauf von 3 der Grad von s um mindestens 1 verringert und $k \geqslant 0$ gilt. Tatsächlich hat $c_{\ell-k} X^{\ell-k} \cdot m$ Leitkoeffizienten $c_{\ell-k} \cdot b_k = d_\ell$ und Grad ℓ genau wie s. Somit hat das Polynom $s - c_{\ell-k} X^{\ell-k} \cdot m$ einen geringeren Grad.

Korrektheit der Polynomdivision

Die Korrektheit beweisen wir mit Induktion nach n und betrachten dafür die rekursive Version des Algorithmus:

1. Falls $n < k$, dann gib $q = 0$ und $r = p$ zurück.
2. Finde rekursiv q' und r für die Division von $p' = p - \frac{a_n}{b_k}X^{n-k} \cdot m$ durch m, sodass
$$p' = q' \cdot m + r \qquad \text{und} \qquad \operatorname{grad}(r) < k = \operatorname{grad}(m)\,. \tag{$*$}$$
3. Gib $q = q' + \frac{a_n}{b_k}X^{n-k}$ und r zurück.

Induktionsanfang für $n < k$: In diesem Fall liefert 1 eine Lösung, da dann $\operatorname{grad}(p) = n < k = \operatorname{grad}(r)$ und offensichtlich $p = 0 \cdot m + p$.

Induktionsschritt (mit allen Vorgängern) auf n: Da $\operatorname{grad}(p') < \operatorname{grad}(p) = n$, folgt mit der Induktionsvoraussetzung, dass in Schritt 2 q' und $r \in K[X]$ gefunden werden, die $(*)$ erfüllen. Einsetzen ergibt dann

$$p = p' + \frac{a_n}{b_k}X^{n-k} \cdot m \overset{(*)}{=} q' \cdot m + r + \frac{a_n}{b_k}X^{n-k} \cdot m = \left(q - \frac{a_n}{b_k}X^{n-k}\right) \cdot m + r + \frac{a_n}{b_k}X^{n-k} \cdot m\,.$$

$$\Longrightarrow p = q \cdot m - \frac{a_n}{b_k}X^{n-k} \cdot m + r + \frac{a_n}{b_k}X^{n-k} \cdot m = q \cdot m + r \qquad \square$$

Bemerkungen zur Polynomdivision

- die im Beweis angegebenen Algorithmen der Polynomdivison lassen sich effizient implementieren, wenn die Division im entsprechenden Körper K effizient realisierbar ist
- bei der Berechnung der Koeffizienten von q wird durch den Leitkoeffizienten von m geteilt, was in Polynomringen über Körpern immer möglich ist
- in Polynomringen $R[X]$ über kommutativen Ringen R mit 1 müßte man zusätzlich fordern, dass der Leitkoeffizient b_k von m eine Einheit ist, d. h. $b_k \in R^\times$
- mithilfe der Polynomdivision lässt sich der EUKLIDische Algorithmus von $\mathbb{Z}$ direkt auf Polynomringe $K[X]$ übertragen, um einen größten gemeinsamen Teiler von zwei gegebenen Polynomen $p_1, p_2 \in K[X]$ zu berechnen

Beispiel Polynomdivision

Gegeben seien Polynome $p = X^4 - 3X^2 + 5X - 3$ und $m = X - 1$ aus $\mathbb{R}[X]$ und gesucht sind q und r mit $p = q \cdot m + r$ und $\mathrm{grad}(r) < \mathrm{grad}(m) = 1$.

$$\begin{array}{rrrrl}
X^4 & & -\,3X^2 & +\,5X & -\,3 = (X-1)(X^3+X^2-2X+3) \\
-\,X^4 & +\,X^3 & & & \\
\hline
& X^3 & -\,3X^2 & & \\
& -\,X^3 & +\,X^2 & & \\
\hline
& & -\,2X^2 & +\,5X & \\
& & 2X^2 & -\,2X & \\
\hline
& & & 3X & -\,3 \\
& & & -\,3X & +\,3 \\
\hline
& & & & 0
\end{array}$$

$\Longrightarrow q = X^3 + X^2 - 2X + 3$ und $r = 0$

- über den Strichen auf der linken Seite steht der aktuelle Term $-c_{\ell-k}X^{\ell-k} \cdot m$
- unter den Strichen steht der aktuell relevante Teil von s
- unter dem letzten Strich (wenn $\mathrm{grad}(s) < \mathrm{grad}(m)$) steht das Restpolynom r
- auf der rechten Seite steht $m \cdot (c_{n-k}X^{n-k} + \cdots + c_{\ell-k}X^{\ell-k} \dots)$ und am Ende der Rechnung $m \cdot q$
- wegen dem „=“ muß am Ende der Rechnung auf der rechten Seite noch $+r$ ergänzt werden (entfällt oben, da hier $r = 0$)

Weiteres Beispiel Polynomdivision

Für $p = X^4 - X^2 + 3X + 2$ und $m = X^2 - 2X + 1$ aus $\mathbb{R}[X]$ ergibt die Polynomdivision:

$$
\begin{array}{rrrrrl}
X^4 & & -X^2 & +3X & +2 & = \left(X^2 - 2X + 1\right)\left(X^2 + 2X + 2\right) + 5X \\
\underline{-X^4} & \underline{+2X^3} & \underline{-X^2} & & & \\
 & 2X^3 & -2X^2 & +3X & & \\
 & \underline{-2X^3} & \underline{+4X^2} & \underline{-2X} & & \\
 & & 2X^2 & +X & +2 & \\
 & & \underline{-2X^2} & \underline{+4X} & \underline{-2} & \\
 & & & 5X & &
\end{array}
$$

Hier ist der Quotient $q = X^2 + 2X + 2$ und der Rest $r = 5X$.

EUKLIDischer Algorithmus in Polynomringen

- wie in $\mathbb{Z}$ kann man größte gemeinsame Teiler von Polynomen mit Hilfe des EUKLIDischen Algorithmus berechnen
- der Grad übernimmt die Rolle des Betrages bei den ganzen Zahlen und die Polynomdivision die Rolle der ganzzahligen Division in $\mathbb{Z}$
- dabei teilt man ausgehend von p_1 und p_2, also in jedem Schritt mit der Polynomdivision das Polynom p_1 mit dem größeren Grad durch das Polynom mit dem kleineren Grad p_2 und ersetzt dann p_1 durch p_2 und p_2 durch r
- sobald p_2 das Nullpolynom ist, ist p_1 ein größter gemeinsamer Teiler gefunden
- im Unterschied zur Situation bei ganzen Zahlen, kann es bei Polynomen passieren, dass die beiden gegebenen Polynome p_1 und p_2 denselben Grad haben, ohne dass die beiden Polynome einander teilen
- in diesem Falle ist es egal, ob man zunächst das eine Polynom durch das andere teilt oder umgekehrt
- die Korrektheit diese Verfahrens beweist man ebenso wie die Korrektheit des EUKLIDischen Algorithmus in $\mathbb{Z}$, mit Induktion nach $\mathrm{grad}(p_1) + \mathrm{grad}(p_2)$, kombiniert mit der Proposition, dass für $p_1 = q \cdot p_2 + r$ mit $\mathrm{grad}(r) < \mathrm{grad}(p_2)$ jeder größte gemeinsame Teiler von p_2 und r auch ein größter gemeinsamer Teiler von p_1 und p_2 ist

Beispiel größter gemeinsamer Teiler in Polynomringen

Für $p_1 = X^3 - 3X^2 + 5X - 3$ und $p_2 = X^3 - 1$ aus $\mathbb{R}[X]$ suchen wir einen größten gemeinsamen Teiler.
Beide Grade sind gleich und es ist egal, wie wir beginnen. Wir teilen p_1 durch p_2:

$$\begin{array}{rl} X^3 - 3X^2 + 5X - 3 & = \big(X^3 - 1\big)1 - 3X^2 + 5X - 2 \\ -\,X^3 \qquad\qquad\qquad + 1 & \\ \hline -\,3X^2 + 5X - 2 & \end{array}$$

Der Rest ist $r_1 = -3X^2 + 5X - 2$ und im nächsten Schritt teilen wir p_2 durch r_1.

Beispiel größter gemeinsamer Teiler in Polynomringen

Polynomdivision $p_2 = X^3 - 1$ durch $r_1 = -3X^2 + 5X - 2$ ergibt:

$$
\begin{array}{rrrrl}
X^3 & & & -1 & = \big(-3X^2+5X-2\big)\big(-\tfrac{1}{3}X-\tfrac{5}{9}\big)+\tfrac{19}{9}X-\tfrac{19}{9} \\
-X^3 & +\tfrac{5}{3}X^2 & -\tfrac{2}{3}X & & \\
\hline
 & \tfrac{5}{3}X^2 & -\tfrac{2}{3}X & -1 & \\
 & -\tfrac{5}{3}X^2 & +\tfrac{25}{9}X & -\tfrac{10}{9} & \\
\hline
 & & \tfrac{19}{9}X & -\tfrac{19}{9} &
\end{array}
$$

Der Rest ist $r_2 = \frac{19}{9}(X-1)$ und im nächsten Schritt teilen wir $r_1 = -3X^2 + 5X - 2$ durch r_2. Da das Polynom $\frac{19}{9}(X-1)$ genau dieselben Teiler wie $X - 1$ hat und auch genau dieselben Polynome teilt, können wir aber einfach auf $r_2' = X - 1$ übergehen.

Beispiel größter gemeinsamer Teiler in Polynomringen

Polynomdivision $r_1 = -3X^2 + 5X - 2$ durch $r_2' = X - 1$ ergibt:

$$\begin{array}{r}
-3X^2 + 5X - 2 = (X-1)(-3X+2) \\
\underline{3X^2 - 3X \phantom{{}-2}} \\
2X - 2 \\
\underline{-2X + 2} \\
0
\end{array}$$

Der Rest ist 0, also ist $X - 1$ ein größter gemeinsamer Teiler von den Ausgangspolynomen $p_1 = X^3 - 3X^2 + 5X - 3$ und $p_2 = X^3 - 1$.
Tatsächlich ist $X - 1$ ein gemeinsamer Teiler:

$$p_1 = X^3 - 3X^2 + 5X - 3 = (X - 1) \cdot (X^2 - 2X + 3)$$

und

$$p_2 = X^3 - 1 = (X - 1) \cdot (X^2 + X + 1)\,.$$

Das Lemma von Bézout für Polynome

Lemma (Bézout)

Für alle Polynome p, $q \in K[X]$ gibt es Polynome s, $t \in K[X]$, sodass

$$\mathrm{ggT}(x, y) = sp + tq\,.$$

- Der $\mathrm{ggT}(p, q)$ kann als Linearkombination von p und q dargestellt werden.
- Für teilerfremde p, $q \in \mathbb{Z}$ gibt es somit s, $t \in \mathbb{Z}$ mit $sp + tq = 1$.

- Wie bei den ganzen Zahlen kann man s und t mit dem erweiterten euclidischen Algorithmus finden.
- Wir nennen ein Polynom p *irreduzibel* wenn es nicht möglich ist, p als Produkt von Polynomen von echt kleinerem Grad darzustellen.
- Mit diesem Lemma kann man beweisen, dass jedes Polynom eindeutig als Produkt von irreduzibeln Polynomen darstellbar ist.
- Allerdings ist die Eindeutigkeit hier nur bis auf Multiplikation mit Konstanten.

Polynomfunktionen

- Polynome wurden bis jetzt als algebraische Objekte des Rings $K[X]$ betrachtet
- im Folgenden betrachten wir Polynome (wie aus der Schule bekannt) als Funktionen von K nach K

Definition (Polynomfunktion)

Sei K ein Körper und $p = \sum_{i=0}^{n} a_i X^i$ ein Polynom in $K[X]$. Die Polynomfunktion $f_p\colon K \to K$ ist gegeben durch

$$x \mapsto \sum_{i=0}^{n} a_i x^i \in K \quad \text{für alle } x \in K\,.$$

- Üblicherweise wird das Polynom p und die Polynomfunktion f_p gleichgesetzt und wir schreiben einfach $p(x)$ für $f_p(x)$.
- In diesem Fall ist aber x ein Element aus dem Körper K, welches **NICHT** mit der Unbekannten X des Polynomrings zu verwechseln ist.

Polynomfunktion vs. Polynom

- für jeden Körper K gibt es unendlich viele verschiedene Polynome in $K[X]$, z. B. die Polynome X^n für $n \in \mathbb{N}$
- für endliche Körper K gibt es aber nur endlich viele verschiedene Polynomfunktionen, da es höchstens $|K|^{|K|}$ verschiedene Funktionen $g\colon K \to K$ gibt

  Bemerkung: tatsächlich hat für eine gegebene Funktion $g\colon K \to K$ das Polynom

$$p = \sum_{a \in K} g(a) \prod_{b \in K \setminus \{a\}} \frac{X - b}{a - b}$$

  eine Polynomfunktion, die jedem $a \in K$ den Wert $g(a)$ zuordnet

$\Rightarrow$ für endliche Körper K gibt es verschiedene Polynome p und $q \in K[X]$, die die gleiche Polynomfunktion haben $\longrightarrow$ Schubfachprinzip

Beispiel: $p = X$ und $q = X^3$ in $(\mathbb{Z}/3\mathbb{Z})[X]$

$$p(0) = 0\,, \qquad p(1) = 1\,, \qquad p(2) = 2$$

und

$$q(0) = 0\,, \qquad q(1) = 1\,, \qquad q(2) = 2$$

Nullstellen

Definition (Nullstelle)

Sei K ein Körper und $p \in K[X]$. Ein Element $a \in K$ heißt Nullstelle von (der Polynomfunktion) p, falls $p(a) = 0$.

Satz

Ein Element $a \in K$ ist genau dann eine Nullstelle von p, wenn das Polynom $X - a$ ein Teiler von p im Polynomring $K[X]$ ist.

Beweis: („$\Longrightarrow$“) Sei $p(a) = 0$ und betrachte $q, r \in K[X]$ gegeben durch die Polynomdivision von p geteilt durch $m = X - a$, d. h. $p = q \cdot (X - a) + r$ und wegen $\mathrm{grad}(r) < \mathrm{grad}(X - a) = 1$, ist $r = r' \cdot X^0$ konstant für ein $r' \in K$. Somit gilt für die Polynomfunktion

$$0 = p(a) = q(a) \cdot (a - a) + r(a) = q(a) \cdot 0 + r' = r' .$$

$\Rightarrow r = 0 \cdot X^0$ ist das Nullpolynom und $p = q \cdot (X - a)$, d. h. $(X - a) \mid p$ in $K[X]$ ✓

(„$\Longleftarrow$“) Falls p ein Vielfaches von $(X - a)$ ist, dann existiert $q \in K[X]$ mit $p = q \cdot (X - a)$. Für die Polynomfunktion ergibt sich also

$$p(a) = q(a) \cdot (a - a) = q(a) \cdot 0 = 0$$

und somit ist a eine Nullstelle. □

Nullstellen und Grad

Korollar

Ein Polynom $p \in K[X]$ vom Grad $n \geqslant 0$ hat höchstens n Nullstellen.

Beweis: (Induktion nach n)

Induktionsanfang für $n = 0$: klar, da konstante Polynome vom Grad 0 die Form $p = a_0 X^0$ mit $a_0 \in K \setminus \{0\}$ haben (Nullpolynom hat Grad $-\infty$)
$\Rightarrow p(a) = a_0 \neq 0$ für alle $a \in K \Rightarrow$ keine Nullstelle ✓

Induktionsschritt $n \to n+1$: Sei $p \in K[X]$ mit Grad $n+1$ und a eine beliebige Nullstelle. Nach dem Satz gibt es $q \in K[X]$, sodass

$$p = q \cdot (X - a)\,.$$

Wegen der Gradformel für Produkte von Polynomen über Körpern ist $\mathrm{grad}(q) = n$. Nach Induktionsvoraussetzung hat q höchstens n Nullstellen. Für jede Nullstelle $b \in K \setminus \{a\}$ von p gilt wegen $0 = p(b) = q(b) \cdot (b - a)$ auch $q(b) = 0$, d. h. b ist auch eine Nullstelle von q.
$\Rightarrow p$ hat neben a höchstens n weitere Nullstellen (die von q) □

Nullstellen bestimmen

- für Polynome $p = a_1 X + a_0 \in K[X]$ vom Grad 1 können wir einfach auflösen und dann ist
$$a = -a_0 a_1^{-1}$$
die Nullstelle der Polynomfunktion p
- für (normierte) Polynome vom Grad 2 in $\mathbb{R}[X]$ gibt es die p-q-Formel
- für Polynome vom Grad 3 und 4 in $\mathbb{R}[X]$ gibt es ebenfalls geschlossene Formeln (Cardano-Formeln), die allerdings recht kompliziert sind
- mithilfe tieferer Methoden der Algebra kann man zeigen, dass es für Polynome vom Grad mindestens 5 in $\mathbb{R}[X]$ keine geschlossene Formel gibt
- es gibt aber numerische Verfahren zur Approximation von Nullstellen für beliebige Polynome aus $\mathbb{R}[X]$
- für Polynome $p \in K[X]$ von beliebigen Grade kann man mithilfe des Satzes, nachdem eine Nullstelle $a \in K$ gefunden wurde, mithilfe der Polynomdivision das Polynom q mit
$$p = q \cdot (X - a)$$
bestimmt werden und dann können die Nullstellen für q gesucht werden

$\longrightarrow$ hilfreich da $\mathrm{grad}(q) < \mathrm{grad}(p)$

p-q-Formel

Satz

Sei $X^2 + pX + q$ ein normiertes (d. h. Leitkoeffizient ist 1) Polynom vom Grad 2 in $\mathbb{R}[X]$ mit Nullstelle $a \in \mathbb{R}$. Dann gilt $q \leqslant p^2/4$ und

$$a = -\frac{p}{2} - \sqrt{\frac{p^2}{4} - q} \qquad \text{oder} \qquad a = -\frac{p}{2} + \sqrt{\frac{p^2}{4} - q}\,.$$

Bemerkung: Wir können $X^2 + pX + q$ faktorisieren als $(X - a)(X - b)$ für ein $b \in \mathbb{R}$. Also gelten $a + b = -p$ und $ab = q$. Der Mittelwert von $aundb$ ist also $-\frac{p}{2}$. a und b sind gleich weit von diesem Mittelwert weg; angenommen $a = -\frac{p}{2} + c$ und $b = -\frac{p}{2} - c$. Dann

$$q = ab = \left(-\frac{p}{2} + c\right)\left(-\frac{p}{2} - c\right) = \left(-\frac{p}{2}\right)^2 - c^2 = \frac{p^2}{4} - c^2$$

und deshalb $c^2 = \frac{p^2}{4} - q$. Also gelten $q \leqslant \frac{p^2}{4}$ und $c = \pm\sqrt{\frac{p^2}{4} - q}$, woraus folgt

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

. $\square$

Ganzzahlige Nullstellen

Satz (Lemma von Gauss)

Sei $p = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{R}[X]$ ein normiertes (d. h. Leitkoeffizient ist 1) Polynom vom Grad $n > 0$ mit ganzzahligen Koeffizienten. Dann ist jede Nullstelle $b \in \mathbb{Q}$ von p ein ganzzahliger (es gilt also sogar $b \in \mathbb{Z}$) Teiler von a_0.

Beweis von $b \in \mathbb{Z}$: Sei $b \in \mathbb{Q} \setminus \{0\}$ eine Nullstelle von p und $b = \frac{y}{z}$ für teilerfremde ganze Zahlen y und z mit $y \neq 0$ and $z \geqslant 1$. Wir zeigen $z = 1$.

Da $b = y/z$ eine Nullstelle von p ist, gilt

$$0 = p(b) = \left(\frac{y}{z}\right)^n + a_{n-1} \cdot \left(\frac{y}{z}\right)^{n-1} + \cdots + a_1 \cdot \left(\frac{y}{z}\right) + a_0 \,. \qquad (*)$$

Wir multiplizieren die Gleichung mit z^n, stellen nach y^n um und erhalten

$$y^n = z \cdot \left(- a_{n-1}y^{n-1} - \cdots - a_1 y z^{n-2} - a_0 z^{n-1}\right).$$

Da alle Koeffizienten $a_{n-1}, \ldots, a_0$ sowie y und z ganzzahlig sind, ist die rechte Seite ein ganzzahliges Vielfaches von z. Somit muss y^n ein ganzzahliges Vielfaches von z sein. Da $y \neq 0$ und $z \geqslant 1$ teilerfremd sind, kann z nur 1 sein. Insbesondere ist $b = y$ also ganzzahlig.

Lemma von Gauss – Beweis von $b \mid a_0$

Satz (Lemma von Gauss)

Sei $p = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{R}[X]$ ein normiertes (d. h. Leitkoeffizient ist 1) Polynom vom Grad $n > 0$ mit ganzzahligen Koeffizienten. Dann ist jede Nullstelle $b \in \mathbb{Q}$ von p ein ganzzahliger (es gilt also sogar $b \in \mathbb{Z}$) Teiler von a_0.

Beweis von $b \mid a_0$: Es ist zu zeigen, dass $b = y$ ein ganzzahliger Teiler von a_0 ist.

Ausgangspunkt ist wieder $(*)$. Da wir aber bereits wissen, dass $z = 1$ ist und somit $b = y \neq 0$ ist, erhalten wir nun

$$0 = b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 \,.$$

Diesmal stellen wir nach a_0 um und Klammern b aus. Somit gilt

$$a_0 = b\big(-b^{n-1} - a_{n-1}b^{n-2} - \cdots - a_2 b - a_1\big)\,.$$

Nun folgt aus der Ganzzahligkeit von $b = y$ und $a_{n-1}, \ldots, a_1$, dass die rechte Seite ein ganzahliges Vielfaches von b ist.

Da $a_0 \in \mathbb{Z}$ folgt somit auch, dass a_0 ein ganzzahliges Vielfaches von b ist. $\square$

Ein letztes Beispiel

Gesucht sind die Nullstellen von $p = X^3 - 6X^2 + 11X - 6 \in \mathbb{R}[X]$. Falls es ganzzahlige Nullstellen b gibt, so sind dies nach dem Lemma von Gauss ganzzahlige Teiler des konstanten Terms -6, d. h.

$$b \in \{-6, -3, -2, -1, 1, 2, 3, 6\}\,.$$

Wir probieren die 1 und erhalten $p(1) = 1 - 6 + 11 - 6 = 0$.
Polynomdivision p durch $X - 1$ liefert

$$\begin{array}{rrrrl}
X^3 & -\,6X^2 & +\,11X & -\,6 & = \big(X-1\big)\big(X^2 - 5X + 6\big) \\
-\,X^3 & +\,X^2 & & & \\ \hline
 & -\,5X^2 & +\,11X & & \\
 & 5X^2 & -\,5X & & \\ \hline
 & & 6X & -\,6 & \\
 & & -\,6X & +\,6 & \\ \hline
 & & & 0 &
\end{array}$$

Die Nullstellen von $X^2 - 5X + 6$ bestimmen wir mit der p-q-Formel und erhalten

$$\frac{5}{2} \pm \sqrt{\frac{25}{4} - 6} = \frac{5}{2} \pm \sqrt{\frac{1}{4}} = \frac{5}{2} \pm \frac{1}{2} \quad \Longrightarrow \quad \text{Nullstellen } 2 \text{ und } 3\,.$$

Das Polynom p vom Grad 3 hat also genau die drei Nullstellen 1, 2 und 3.

Kongruenzen in Polynomringe

Genau so, wie wir Restklassenringe als quotienten von $\mathbb{Z}$ definiert haben, können wir auch Restklassenringe von Polynomringe $K[X]$ definieren. Zuerst müssen wir Kongruenz modulo ein Polynom m definieren.

Definition

Polynome p, $q \in K[X]$ sind kongruent modulo m für ein Polynom $m \in K[X]$, falls p und q denselben Rest haben bei Division durch m. In diesem Fall sagen wir auch, p ist kongruent zu q modulo m und schreiben

$$p \equiv q \pmod{m} .$$

Bemerkungen

- $p \equiv q \pmod{m} \iff m \mid p - q$
- Kongruenz modulo m definiert Äquivalenzrelation auf $K[X]$.

Restklassen

Definition (Restklassen)

Für jede Polynome $m \in K[X]$ und $p \in K[X]$ heißt die Äquivalenzklasse

$$[p]_m := \{q \in \mathbb{Z} \colon p \equiv q \pmod{m}\}$$

die Restklasse von p modulo m.

- Wir nennen die Menge der Restklassen $K[X]/mK[X]$.
- Wir können Addition und Multiplikation darauf definieren durch:
  - $[p]_m + [q]_m := [p+q]_m$
  - $[p]_m \cdot [q]_m := [p \cdot q]_m$
- Die Menge der Restklassen mit diesen Operationen bildet einen Ring $(K[X]/mK[X], +, \cdot)$.
- $[X]_m$ ist eine Nullstelle von m in diesem Ring: $m([X]_m) = [m]_m = [0]_m$.

Eigenschaften von Polynomrestklassenringen

- $K[X]/mK[X]$ ist ein Ring
- $K[X]/mK[X]$ enthält eine Kopie von K (wir identifizieren $a \in K$ mit $[aX^0]_m$)
- m hat eine Nullstelle $[X]_m$ in $K[X]/mK[X]$
- $K[X]/mK[X]_m$ wird von K und $[X]_m$ erzeugt: jedes Element kann in der Form $\sum_{i=0}^n a_i[X]_m^i$ dargestellt werden, mit allen a_i in K.
- Keine unerwartete Gleichungen: $\sum_{i=0}^n a_i[X]_m^i = \sum_{i=0}^n b_i[X]_m^i$ gilt nur dann, wenn $\sum_{i=0}^n (a_i - b_i)X^i$ durch m teilbar ist

Polynomrestklassenkörper

Satz

Sei m ein Polynom in $K[X]$. Der Ring $K[X]/mK[X]$ ist genau dann ein Körper, wenn m irreduzibel ist.

Beweis: („$\Longrightarrow$“) Sei $m = p \cdot q$. Dann gilt in dem Körper $K[X]/mK[X]$ die Gleichung $[p]_m \cdot [q]_m = [m]_m = [0]_m$ und deshalb o.B.d.A. $[p]_m = [0]_m$, d.H., $m|p$ und deshalb $\text{Grad}(p) \geqslant \text{Grad}(m)$. ✓

(„$\Longleftarrow$“) Sei $[p]_m \in (K[X]/mK[X])^\times$. Dann $m \not| p$. Da m irreduzibel ist, gilt $\text{ggT}(p, m) = 1$. Nach dem Lemma von Bézout für Polynome gibt es Polynome s und t mit

$$1 = sp + tm \equiv sp \pmod{m}$$

und deshalb

$$[1]_m = [s]_m [p]_m \,.$$

Deshalb ist $[s]_m$ ein multiplikativ Inverses zu $[p]_m$ in $K[X]/mK[X]$. □

Implementation der komplexen Zahlen

Was wollen wir von den komplexen Zahlen?

- $\mathbb{C}$ sollte ein Körper sein
- $\mathbb{C}$ sollte eine Kopie von $\mathbb{R}$ enthalten
- -1 sollte in $\mathbb{C}$ eine Quadratwurzel haben
- sonst sollte es keine unnötige Elemente oder unerwartete Gleichungen geben

Also setzen wir $\mathbb{C} := \mathbb{R}[X]/(X^2+1)\mathbb{R}[X]$. Damit $\mathbb{C}$ ein Körper ist, brauchen wir

Satz

X^2+1 ist irreduzibel in $\mathbb{R}[X]$.

Beweis: Angenommen nicht. Dann gibt es Polynome p und q von Grad $\leqslant 1$ mit $X^2+1 = pq$. Dann gilt $\mathrm{Grad}(p) = \mathrm{Grad}(q) = 1$ und deshalb o.B.d.A $p = X - a$ und $q = X - b$ für reele Zahlen a und b. Es gilt

$$X^2+1 = (X-a)(X-b) = X^2-(a+b)X+ab\,,$$

woraus folgen $a+b=0$ und $ab=1$. Dann $b=-a$ und deshalb $-a^2=1$, was keine Lösung in $\mathbb{R}$ hat. $\square$

Erinnerung: Eigenschaften von Polynomrestklassenringen

- $K[X]/mK[X]$ ist ein Ring
- $K[X]/mK[X]$ enthält eine Kopie von K (wir identifizieren $a \in K$ mit $[aX^0]_m$)
- m hat eine Nullstelle $[X]_m$ in $K[X]/mK[X]$
- $K[X]/mK[X]_m$ wird von K und $[X]_m$ erzeugt: jedes Element kann in der Form $\sum_{i=0}^n a_i[X]_m^i$ dargestellt werden, mit allen a_i in K.
- Keine unerwartete Gleichungen: $\sum_{i=0}^n a_i[X]_m^i = \sum_{i=0}^n b_i[X]_m^i$ gilt nur dann, wenn $\sum_{i=0}^n (a_i - b_i)X^i$ durch m teilbar ist

Arithmetik von komplexen Zahlen

Wir setzen $i := [X]_{X^2+1}$. Also gilt $i^2 = -1$ in $\mathbb{C}$. Jede komplexe Zahl ist darstellbar in der Form

$$a_0 + a_1 i + a_2 i^2 + a_3 i^3 + \cdots + a_n i^n = (a_0 - a_2 + a_3 - \ldots) + (a_1 - a_3 + a_5 - \ldots)i$$

Also hat jede komplexe Zahl die Form $a + bi$, für reele Zahlen a und b. Weiterhin gilt $a + ib = c + id$ nur dann, wenn $X^2 + 1 | (a - c) + (b - d)X$, also wenn $a = c$ und $b = d$.

Addition: $a + bi + c + di = (a + c) + (b + d)i$

Multiplikation: $(a + bi)(c + di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i$

Multiplikative Inversen in $\mathbb{C}$

Wir wollen ein multiplikativ Inverses zu $a + bi$ in $\mathbb{C}$ berechnen. Das heißt, wir wollen ein multiplikativ Inverses zu $[a + bX]_{X^2+1}$ in $\mathbb{R}[X]/(X^2 + 1)\mathbb{R}[X]$ berechnen. Wir müssen Polynome s und t finden wie in dem Lemma von Bézout, sodass $s(a + bX) + t(X^2 + 1) = 1$. Wir wenden also das EUKLIDsche Algorithmus an. Polynomdivision ergibt

$$X^2 + 1 = (bX + a)\left(\frac{1}{b}X - \frac{a}{b^2}\right) + 1 + \frac{a^2}{b^2}$$

Diese Gleichung können wir weiter umformen:

$$b^2(X^2 + 1) = (bX + a)(bX - a) + b^2 + a^2$$

$$1 = \frac{a - bX}{a^2 + b^2}(a + bX) + \frac{b^2}{a^2 + b^2}(X^2 + 1)$$

Das multiplikativ inverses zu $a + bi$ ist also $\frac{a-bi}{a^2+b^2}$. Wir überprüfen:

$$\frac{a - bi}{a^2 + b^2}(a + bi) = \frac{a^2 - (bi)^2}{a^2 + b^2} = \frac{a^2 + b^2}{a^2 + b^2} = 1$$

Eigenschaften von $\mathbb{C}$

- $\mathbb{C}$ ist ein Körper
- $\mathbb{C}$ erweitert den Körper $\mathbb{R}$
- Es gibt eine Quadratwurzel i von -1 in $\mathbb{C}$
- Die Funktion $\mathbb{R}^2 \to \mathbb{C}; (a, b) \mapsto a + bi$ ist eine Bijektion
- Operationen:
  - $(a + bi) + (c + di) = (a + c) + (b + d)i$
  - $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$
  - $(a + bi)^{-1} = \frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2} i$

Komplexe Konjugation

Definition

Für eine komplexe Zahl $z = a + bi$ mit $a, b \in \mathbb{R}$ heißt $\overline{z} = a - bi$ die zu z **konjugierte** komplexe Zahl.

Satz

Für alle $z, z' \in \mathbb{C}$ gilt $\overline{z + z'} = \overline{z} + \overline{z'}$ und $\overline{zz'} = \overline{z} \cdot \overline{z'}$.

Beweis: Sei $z = a + bi$ und $z' = a' + b'i$. Dann

$$\begin{aligned} \overline{z + z'} &= \overline{(a + a') + (b + b')i} = (a + a') - (b + b')i \\ &= (a - bi) + (a' - b'i) = \overline{z} + \overline{z'} \end{aligned}$$

und

$$\begin{aligned} \overline{zz'} &= \overline{(aa' - bb') + (ab' + a'b)i} = (aa' - bb') - (ab' + a'b)i \\ &= (a - bi)(a' - b'i) = \overline{z} \cdot \overline{z'} \end{aligned}$$

Dies zeigt die Behauptung. $\square$

Real- und Imaginärteil

Definition

Für eine komplexe Zahl $z = a + bi$ mit $a, b \in \mathbb{R}$ heißt $a = \Re(z)$ der **Realteil** von z und $b = \Im(z)$ der **Imaginärteil** von z.

- Für jedes $z \in \mathbb{C}$ gilt also $z = \Re(z) + \Im(z)i$.
- Die konjugiert komplexe Zahl kann man in der Form $\overline{z} = \Re(z) - \Im(z)i$ schreiben.
- Es gelten die Formeln

$$\Re(z) = \frac{z + \overline{z}}{2} \quad \text{und} \quad \Im(z) = \frac{z - \overline{z}}{2i},$$

  denn für $z = a + bi$ ist $z + \overline{z} = (a + bi) + (a - bi) = 2a$ und $z - \overline{z} = (a + bi) - (a - bi) = 2bi$.
- Beispiele: $\overline{i} = -i$, $\Re(i) = 0$ und $\Im(i) = 1$.

Betrag (1)

Für jede komplexe Zahl $z = a + bi$ gilt

$$z\overline{z} = (a + bi)(a - bi) = a^2 - (bi)^2 = a^2 + b^2 \geqslant 0\,.$$

Definition

Für eine komplexe Zahl $z = a + bi$ heißt $\sqrt{z\overline{z}} = \sqrt{a^2 + b^2}$ der **Betrag** von z und man schreibt $|z| = \sqrt{a^2 + b^2}$.

Bemerkung: Für $z \in \mathbb{R}$ stimmt dies mit der üblichen Definition von $|z|$ überein.

Satz

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

(a) $\max(|\Re(z)|, |\Im(z)|) \leqslant |z| \leqslant |\Re(z)| + |\Im(z)|$.

(b) $|z + z'| \leqslant |z| + |z'|$ (Dreiecksungleichung)

(c) $|zz'| = |z||z'|$

Betrag (2)

Beweis:

(a) Schreibe $z = a + bi$. Dann ist $a^2 + b^2 \geqslant a^2$, also $|z|^2 \geqslant |\Re(z)|^2$. Wegen $|z| \geqslant 0$ folge $|z| \geqslant |\Re(z)|$. Ebenso sieht man $|z| \geqslant |\Im(z)|$ und damit ingesamt $|z| \geqslant \max(|\Re(z)|, |\Im(z)|)$. Außerdem

$$\big(|\Re(z)| + |\Im(z)|\big)^2 = \big(|a| + |b|\big)^2 = |a|^2 + 2|a||b| + |b|^2 \geqslant a^2 + b^2 = |z|^2\,,$$

also $|\Re(z)| + |\Im(z)| \geqslant |z|$.

(c) Es gilt

$$|zz'|^2 = zz' \cdot \overline{zz'} = zz' \cdot \overline{z}\,\overline{z'} = z\overline{z} \cdot z'\overline{z'} = |z|^2|z'|^2 = (|z||z'|)^2$$

und daher in der Tat $|zz'| = |z||z'|$.

Betrag (3)

(b) Die Behauptung ist äquivalent zu $|z+z'|^2 \leqslant (|z|+|z'|)^2$. Da

$$\begin{aligned}
|z+z'|^2 &= (z+z')(\overline{z}+\overline{z'}) \\
&= z\overline{z} + z\overline{z'} + z'\overline{z} + z'\overline{z'} \\
&= |z|^2 + z\overline{z'} + \overline{z\overline{z'}} + |z'|^2 \\
&= |z|^2 + 2\Re z\overline{z'} + |z'|^2 \\
&\leqslant |z|^2 + 2|z\overline{z'}| + |z'|^2 \\
&= |z|^2 + 2|z||\overline{z'}| + |z'|^2 \\
&= |z|^2 + 2|z||z'| + |z'|^2 \\
&= (|z|+|z'|)^2
\end{aligned}$$

ist dies in der Tat der Fall. $\square$

Quadratwurzeln in $\mathbb{C}$ (1)

Satz

Für jede komplexe Zahl $z \neq 0$ gibt es genau zwei komplexe Zahlen w mit $w^2 = z$.

Beweis:

Da $\mathbb{C}$ ein Körper ist, kann das Polynom $X^2 - z \in \mathbb{C}[X]$ höchstens zwei komplexe Nullstellen haben, d.h. es kann höchstens zwei solche Zahlen w geben. Wenn es eine solche Zahl w gibt, dann ist $(-w)^2 = z$, d.h. $-w$ ist auch so eine Zahl. Wegen $z \neq 0$ ist dabei $w \neq 0$, d.h. $w \neq -w$. Damit bleibt zu zeigen, dass es mindestens eine solche Zahl w gibt.
Schreibe $z = a + bi$. Wenn $b = 0$ ist $z \in \mathbb{R}$. D.h. falls $a \geqslant 0$ tut's $w = \sqrt{a}$. Ist hingegen $a < 0$, so tut's $w = \sqrt{-a} \cdot i$.
Sei nun $b > 0$. Wir suchen $x, y \in \mathbb{R}$ mit $(x + yi)^2 = (a + bi)$, d.h.

$$x^2 - y^2 = a \quad \text{und} \quad 2xy = b\,.$$

Quadratwurzeln in $\mathbb{C}$ (2)

Es muss auch $x^2 + y^2 = |w|^2 = |w^2| = |z| = \sqrt{a^2 + b^2}$ sein, also

$$x^2 = \frac{(x^2 + y^2) + (x^2 - y^2)}{2} = \frac{\sqrt{a^2 + b^2} + a}{2}$$

und

$$y^2 = \frac{(x^2 + y^2) - (x^2 - y^2)}{2} = \frac{\sqrt{a^2 + b^2} - a}{2}.$$

Setzt man

$$x = \sqrt{\frac{\sqrt{a^2 + b^2} + a}{2}} \quad \text{und} \quad y = \sqrt{\frac{\sqrt{a^2 + b^2} - a}{2}}$$

so ist in der Tat $x^2 - y^2 = a$ und

$$\begin{aligned}(2xy)^2 = 4x^2y^2 &= \left(\sqrt{a^2 + b^2} + a\right)\left(\sqrt{a^2 + b^2} - a\right) \\ &= \left(\sqrt{a^2 + b^2}\right)^2 - a^2 = (a^2 + b^2) - a^2 = b^2,\end{aligned}$$

d.h. $2xy = b$.

Falls $b < 0$ gibt's w mit $w^2 = \overline{z}$, also $\overline{w}^2 = z$. Damit ist alles gezeigt. $\square$

Quadratische Polynome über $\mathbb{C}$

Satz

Es sei $P(X) \in \mathbb{C}[X]$ ein normiertes Polynom vom Grad 2. Dann gibt es zwei komplexe Zahlen α_1 und α_2 mit $P(X) = (X - \alpha_1)(X - \alpha_2)$.

Beweis:

Schreibe $P(X) = X^2 + pX + q$ mit $p, q \in \mathbb{C}$. Nach dem vorigem Satz gibt es eine komplexe Zahl w mit $w^2 = p^2/4 - q$. Setze $\alpha_1 = -\frac{p}{2} + w$ und $\alpha_2 = -\frac{p}{2} - w$. Dann ist in der Tat

$$\begin{aligned}(X - \alpha_1)(X - \alpha_2) &= \left(X + \tfrac{p}{2} - w\right)\left(X + \tfrac{p}{2} + w\right) = \left(X + \tfrac{p}{2}\right)^2 - w^2 \\ &= \left(X^2 + pX + \tfrac{p^2}{4}\right) - \left(\tfrac{p^2}{4} - q\right) = X^2 + pX + q = P(X).\end{aligned}$$

Also sind α_1 und α_2 wie gewünscht. $\square$

Bemerkungen

- Wenn wir in $\mathbb{C}$ arbeiten, benutzen wir das Symbol $\sqrt{}$ nicht (mehr).
- Wenn $\alpha_1 \neq \alpha_2$, so sind α_1 und α_2 die beiden Nullstellen von $P(X)$.
- Wenn $\alpha_1 = \alpha_2$, so nennt man α_1 eine **doppelte Nullstelle** von $P(X)$.

Die komplexe Zahlenebene

- Erinnerung: Die reellen Zahlen werden oft mit einer Zahlengeraden dargestellt.
- In Analogie hierzu schlug Gauß (1831) vor, die komplexen Zahlen in einer Ebene darzustellen. Dabei entspricht der Punkt mit Koordinaten (a, b) der komplexen Zahl $a + bi$.
- Die Addition komplexer Zahlen entspricht dabei der Addition von **Vektoren** (vgl. Kräfteparallelogramm in der Physik).
- Frage: Wie kann man die Multiplikation veranschaulichen?

Beispiele

- Mal 2: Zentrische Streckung am Ursprung mit Faktor 2.
- Mal -1: Spiegelung am Ursprung (=Drehung um 180°).
- Mal i: Wegen $(a + bi)i = -b + ai$ wird hier der Punkt (a, b) auf $(-b, a)$ abgebildet. Drehung um 90° gegen den Uhrzeigersinn.
- Mal $-i$: Drehung um 270° gegen den Uhrzeigersinn.

Exkurs: Sinus und Kosinus (1)

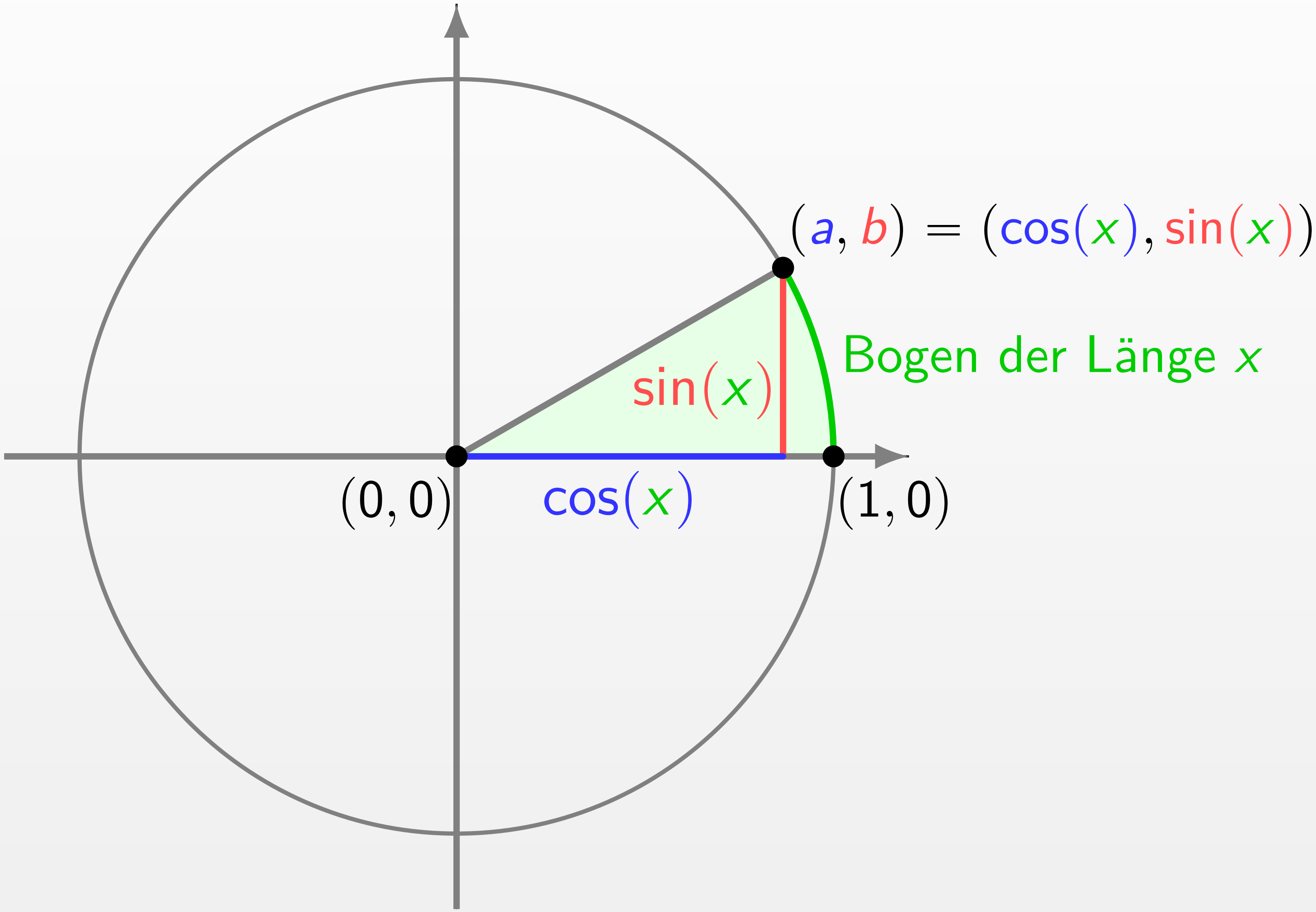


Abbildung : Sinus und Kosinus am Einheitskreis

Exkurs: Sinus und Kosinus (2)

Insbesondere gilt $\sin(0) = 0$ und $\cos(0) = 1$.
Den halben Umfang des Einheitskreises bezeichnen wir mir π. Man kann zeigen, dass π irrational ist und dass $\pi \approx 3.1415926535$. Im Bild erkennt man

$$\sin(\pi/2) = 1, \quad \cos(\pi/2) = 1$$

sowie

$$\sin(\pi) = 0, \quad \cos(\pi) = -1\,.$$

Satz (Additionstheoreme)

Für alle $\alpha, \beta \in \mathbb{R}$ gelten die Formeln

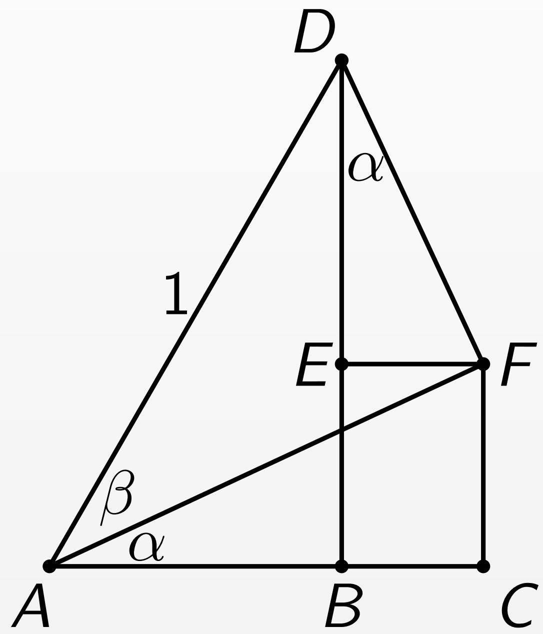
$$\sin(\alpha + \beta) = \sin(\alpha)\cos(\beta) + \cos(\alpha)\sin(\beta)$$

und

$$\cos(\alpha + \beta) = \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta)\,.$$

Beweis der Additionstheoreme – Sinus

Die Formel für $\sin(\alpha + \beta)$ überlegen wir uns so:

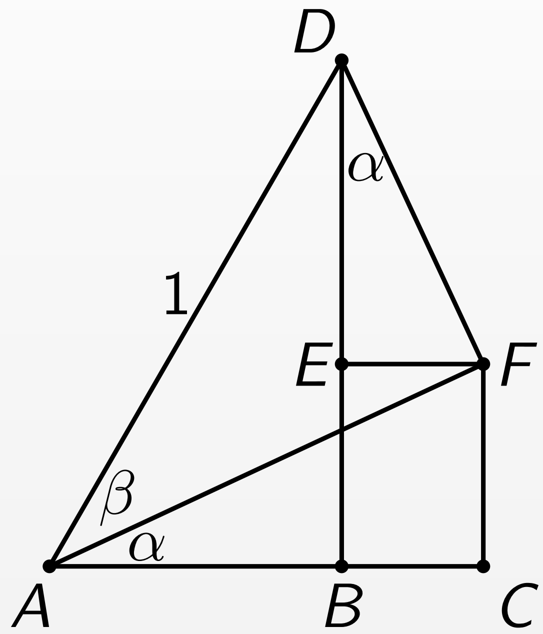


Im Bild gilt

$$\begin{aligned}\sin(\alpha + \beta) = |BD| = |BE| + |ED| &= |FC| + |ED| \\ &= \sin(\alpha)|AF| + \cos(\alpha)|DF| \\ &= \sin(\alpha)\cos(\beta) + \cos(\alpha)\sin(\beta)\,.\end{aligned}$$

Beweis der Additionstheoreme – Cosinus

Die Formel für $\cos(\alpha+\beta)$ erhalten wir analog:



$$
\begin{aligned}
\cos(\alpha+\beta) &= |AB| = |AC| - |BC| = |AC| - |EF| \\
&= \cos(\alpha)|AF| - \sin(\alpha)|DF| \\
&= \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta)\,.
\end{aligned}
$$

Weitere Eigenschaften von Sinus und Cosinus

- Für alle $x \in \mathbb{R}$ gelten die Gleichungen

$$\begin{aligned} \sin(x+\pi/2) &= \cos(x), \quad & \cos(x+\pi/2) &= -\sin(x)\,, \\ \sin(x+\pi) &= -\sin(x), \quad & \cos(x+\pi) &= -\cos(x)\,, \\ \sin(x+2\pi) &= \sin(x), \quad & \cos(x+2\pi) &= \cos(x)\,. \end{aligned}$$

- Für alle $x \in \mathbb{R}$ ist

$$\sin(-x) = -\sin(x) \qquad \text{und} \qquad \cos(-x) = \cos(x)\,.$$

- Für alle $x \in \mathbb{R}$ gilt $\sin(x)^2 + \cos(x)^2 = 1$. (Trigonometrische Pythagoras)
- Umgekehrt gibt es zu gegebenem Paar $(a, b) \in \mathbb{R}$ genau ein $x \in [0, 2\pi)$ mit $a = \cos(x)$ und $b = \sin(x)$.

Der Einheitskreis

Den Einheitskreis $S^1 \subseteq \mathbb{R}^2$ können wir als

$$S^1 = \{(a,b) \in \mathbb{R}^2 \colon a^2 + b^2\}$$

schreiben (Pythagoras). Es gilt auch

$$S^1 = \{(\cos(\varphi), \sin(\varphi)) \in \mathbb{R}^2 \colon \varphi \in \mathbb{R}\}$$

Wenn dabei φ von 0 bis 2π wächst, wird S^1 einmal in $(1,0)$ beginnend gegen den Uhrzeigersinn durchlaufen. Zu jedem Punkt $(a,b) \in S^1$ gibt es eine eindeutig bestimmte Zahl $\varphi \in [0, 2\pi)$ mit $a = \cos(\varphi)$ und $b = \sin(\varphi)$. Mit der Identifikation $\mathbb{C} = \mathbb{R}^2$ erhalten wir

$$S^1 = \{z \in \mathbb{C} \colon |z| = 1\}\,,$$

denn für $z = a + bi$ ist

$$|z| = 1 \iff |z|^2 = 1 \iff a^2 + b^2 = 1\,.$$

Alternativ ist

$$S^1 = \{\cos(\varphi) + i\sin(\varphi) \colon \varphi \in \mathbb{R}\}\,.$$

Multiplikation auf dem Einheitskreis

Für die Multiplikation zweier Zahlen auf dem Einheitskreis erhalten wir die Formel

$$\begin{aligned}&\big(\cos(\varphi)+i\sin(\varphi)\big)\big(\cos(\psi)+i\sin(\psi)\big)\\&=\big(\cos(\varphi)\cos(\psi)-\sin(\varphi)\sin(\psi)\big)+i\big(\sin(\varphi)\cos(\psi)+\cos(\varphi)\sin(\psi)\big)\\&=\cos(\varphi+\psi)+i\sin(\varphi+\psi)\,,\end{aligned}$$

wobei im letzen Schritt die Additionstheoreme benutzt wurden.
Wenn man also zwei Zahlen aus S^1 **multipliziert**, erhält man wieder eine aus S^1 und die zugehörigen "Winkel" werden **addiert**.

Satz

$(S^1,\cdot)$ ist eine Untergruppe von $(\mathbb{C}\setminus\{0\},\cdot)$

Beweis:
Das neutrale Element ist $1=\cos(0)+i\sin(0)$, wobei 0 neutral in $(\mathbb{R},+)$ ist.
Das Inverse von $z=\cos(\varphi)+i\sin(\varphi)$ ist $z^{-1}=\cos(-\varphi)+i\sin(-\varphi)$ $\square$

Polardarstellung komplexer Zahlen (1)

Bemerkung: Man kann weiter rechnen und erhält für $z \in S^1$ die praktische Formel $z^{-1} = \overline{z}$. Denn für $z = \cos(\varphi) + i\sin(\varphi)$ gilt

$$z^{-1} = \cos(\varphi) - i\sin(\varphi) = \overline{z}\,.$$

Satz

Jede komplexe Zahl z kann man in der Form $z = r\big(\cos(\varphi) + i\sin(\varphi)\big)$ mit $r \geqslant 0$ und $0 \leqslant \varphi < 2\pi$ schreiben. Dabei ist r eindeutig durch z bestimmt und falls $z \neq 0$ ist auch φ eindeutig bestimmt.

Beweis:

Existenz: Für $z = 0$ tun's $r = \varphi = 0$. Sei nun $z \neq 0$. Setze $r = |z|$ und beachte $r > 0$. Die komplexe Zahl $w = \frac{z}{r}$ erfüllt $z = rw$, also $|z| = |r||w|$, d.h. $r = r|w|$. Wegen $r \neq 0$ folgt $|w| = 1$. Also gibt's φ mit $0 \leqslant \varphi < 2\pi$ und $w = \cos(\varphi) + i\sin(\varphi)$. Insgesamt haben wir

$$z = rw = r\big(\cos(\varphi) + i\sin(\varphi)\big)\,,$$

wie gewünscht.

Polardarstellung komplexer Zahlen (2)

Eindeutigkeit:
Wenn $z = r\big(\cos(\varphi) + i\sin(\varphi)\big)$ mit $r \geqslant 0$ und $0 \leqslant \varphi < 2\pi$, dann

$$|z| = |r|\big|\cos(\varphi) + i\sin(\varphi)\big| = r \cdot 1 = r\,,$$

was die Eindeutigkeit von r zeigt. Falls $z = 0$ sind wir fertig. Sei also ab jetzt $z \neq 0$ und damit $r \neq 0$. Dann ist $z/r = \cos(\varphi) + i\sin(\varphi)$, was nur eine Lösung für φ mit $0 \leqslant \varphi < 2\pi$ hat. $\square$

Das Produkt zweier komplexer Zahlen $z_1 = r_1\big(\cos(\varphi_1) + i\sin(\varphi_1)\big)$ und $z_2 = r_1\big(\cos(\varphi_2) + i\sin(\varphi_2)\big)$ ist

$$z_1 z_2 = r_1 r_2\big(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)\big)\,.$$

Merke: Wenn man zwei komplexe Zahlen in der Zahlenebene multipliziert, werden die **Beträge multipliziert** und die **Winkel addiert**.

Berechnung von Potenzen in $\mathbb{C}$

Satz (de Moivre)

Es seien $z = r\big(\cos(\varphi) + i\sin(\varphi)\big)$ eine komplexe Zahl und $n \in \mathbb{N}_0$. Dann gilt $z^n = r^n\big(\cos(n\varphi) + i\sin(n\varphi)\big)$.

Beweis:

Vollständige Induktion nach n. Der Induktionsanfang $(n = 0)$ ist klar. Im Induktionsschritt von n auf $n+1$ argumentieren wir

$$\begin{aligned} z^{n+1} = z^n \cdot z &= r^n\big(\cos(n\varphi) + i\sin(n\varphi)\big) \cdot r\big(\cos(\varphi) + i\sin(\varphi)\big) \\ &= r^{n+1}\big(\cos(n\varphi + \varphi) + i\sin(n\varphi + \varphi)\big) \\ &= r^{n+1}\big(\cos((n+1)\varphi) + i\sin((n+1)\varphi)\big)\,. \end{aligned}$$

Damit sind wir fertig. $\square$

Beispiel

Aufgabe: Man berechne $(1+i)^{2020}$.

Lösung: Zuerst wollen wir $z = 1 + i$ in der Form $r\big(\cos(\varphi) + i\sin(\varphi)\big)$ schreiben. Wegen $|1+i| = \sqrt{1^2+1^2} = \sqrt{2}$ ist dabei $r = \sqrt{2}$. Nun brauchen wir einen Winkel φ mit $\cos(\varphi) = \sin(\varphi) = \sqrt{1/2}$. Wir setzen also $\varphi = \pi/4$. Nun finden wir mit der Formel von de Moivre

$$(1+i)^{2020} = \sqrt{2}^{2020}\left(\cos\frac{2020\pi}{4} + i\sin\frac{2020\pi}{4}\right).$$

Es gilt nun $\sqrt{2}^{2020} = 2^{\frac{2020}{2}} = 2^{1010}$. Es gilt auch

$$\cos\frac{2020\pi}{4} = \cos\big(505\pi\big) = \cos(\pi) = -1$$

und analog

$$\sin\frac{2020\pi}{4} = \sin\big(505\pi\big) = \sin(\pi) = 0\,.$$

Insgesamt ist daher $(1+i)^{2020} = -2^{1010}$.