Tutorium:
Diskrete Mathematik

Vorbereitung der Klausur am 09.02.2023
(Teil 2)

2. Februar 2023

Steven Köhler

mathe@stevenkoehler.de

mathe.stevenkoehler.de

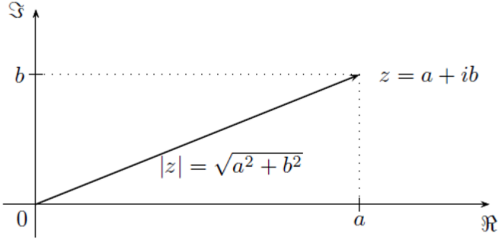
Komplexe Zahlen

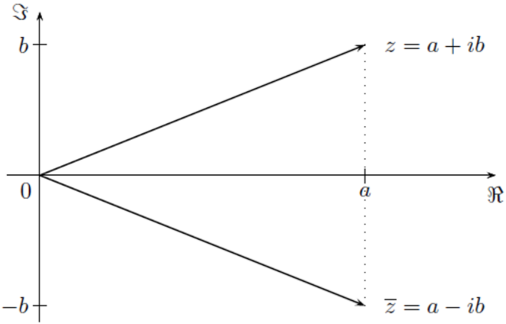
Komplexe Zahlen I

Es sei $z = a + ib \in \mathbb{C}$. Dann heißt

- a *Realteil* von z (Bezeichnung: $a = \operatorname{Re} z$ oder $a = \Re z$);
- b *Imaginärteil* von z (Bezeichnung: $b = \operatorname{Im} z$ oder $b = \Im z$);
- $|z| = \sqrt{a^2 + b^2}$ *absoluter Betrag* von z;
- $\overline{z} = a - ib$ *konjugiert komplexe Zahl* zu z.

Komplexe Zahlen II



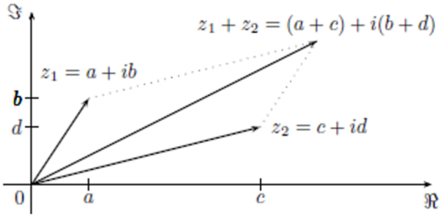


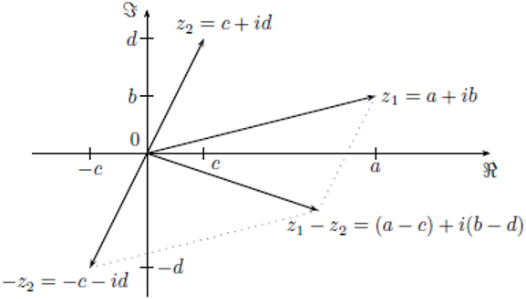
Rechnen mit komplexen Zahlen I

Addition & Subtraktion

Es seien $z_1 = a_1 + ib_1$ und $z_2 = a_2 + ib_2$. Dann ist

$$z_1 \pm z_2 = \left(a_1 \pm a_2\right) + i\left(b_1 \pm b_2\right)$$





Rechnen mit komplexen Zahlen II

Multiplikation, Division & Potenzieren

Es seien $z = a + ib$, $z_1 = a_1 + ib_1$ und $z_2 = a_2 + ib_2$. Dann ist

$$z_1 \cdot z_2 = \Big(a_1 a_2 - b_1 b_2\Big) + i\Big(a_1 b_2 + a_2 b_1\Big)$$

$$\frac{z_1}{z_2} = \left(\frac{a_1 a_2 + b_1 b_2}{a_2^2 + b_2^2}\right) + i \left(\frac{a_2 b_1 - a_1 b_2}{a_2^2 + b_2^2}\right)$$

$$z^n = (a + ib)^n = \sum_{k=0}^{n} \binom{n}{k} a^k (ib)^{n-k}$$

Rechnen mit komplexen Zahlen III

Aufgabe 1

Es seien $z_1 = 6 + i$ und $z_2 = 2 - 3i$ zwei komplexe Zahlen. Berechne $z_1 + z_2$, $z_1 - z_2$, $z_1 \cdot z_2$ sowie $\frac{z_1}{z_2}$. Gib die Ergebnisse jeweils in der Form $z = a + ib$ an.

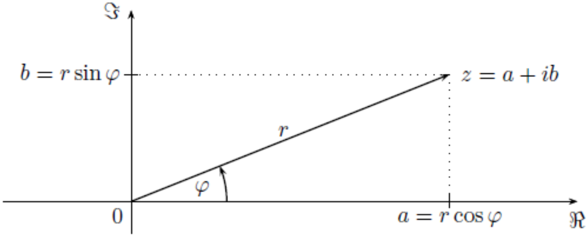
Polarkoordinatendarstellung I

Komplexe Zahlen können alternativ auch mit Hilfe der folgenden *Polarkoordinatendarstellung* angegeben werden:

$$z = r \cdot \Big(\cos(\varphi) + i \sin(\varphi)\Big).$$

Die Bezeichnungen sind bei dieser Darstellung wie folgt:

- r: *Betrag* von z;
- φ: *Argument* von z.



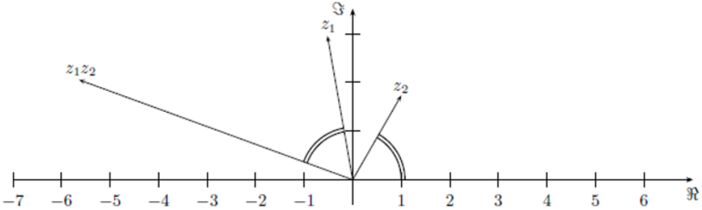
Polarkoordinatendarstellung II

Es seien $z = r(\cos\varphi + i\sin\varphi)$, $z_1 = r_1(\cos\varphi_1 + i\sin\varphi_1)$ und $z_2 = r_2(\cos\varphi_2 + i\sin\varphi_2)$. Dann gilt:

$$z_1 z_2 = r_1 r_2 \Big(\cos\left(\varphi_1 + \varphi_2\right) + i\sin\left(\varphi_1 + \varphi_2\right)\Big);$$

$$\frac{z_1}{z_2} = \frac{r_1}{r_2}\Big(\cos\left(\varphi_1 - \varphi_2\right) + i\sin\left(\varphi_1 - \varphi_2\right)\Big)$$

$$z^n = r^n\Big(\cos\left(n\cdot\varphi\right) + i\sin\left(n\cdot\varphi\right)\Big).$$



Polarkoordinatendarstellung III

Aufgabe 2

Gegeben seien zwei komplexe Zahlen z_1 und z_2 in Polarkoordinatendarstellung:

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

Zeige, dass für das Produkt der beiden Zahlen z_1 und z_2 die folgende Aussage gilt:

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

Umrechnung der Darstellungsformen I

Zu einer gegebenen komplexen Zahl $z \in \mathbb{C}$ mit $z = a + ib$ ist die Polarkoordinatendarstellung

$$z = r \cdot \Big(\cos(\varphi) + i \sin(\varphi)\Big),$$

wobei sich r und φ wie folgt berechnen lassen:

$$r = \sqrt{a^2 + b^2}$$

$$\varphi = \begin{cases} \arccos\left(\frac{a}{r}\right) & , \text{ für } b \geq 0 \\ 2\pi - \arccos\left(\frac{a}{r}\right) & , \text{ für } b < 0 \end{cases}$$

Umrechnung der Darstellungsformen II

Aufgabe 3

Gegeben seien die beiden komplexen Zahlen $z_1 = 3 - 3i$ und $z_2 = 5\left(\cos\left(\frac{\pi}{8}\right) + i\sin\left(\frac{\pi}{8}\right)\right)$.

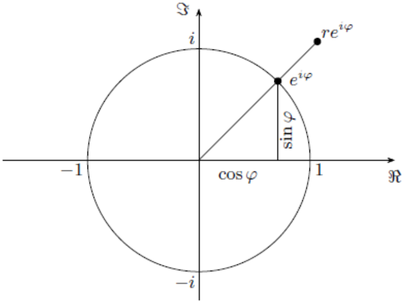
a) Bestimme Betrag und Argument von $z = z_1^3 \cdot z_2$.

b) Es sei $z = z_1 - z_2$. Gib $\overline{z}$ in der Form $a + ib$ an.

Die komplexe Exponentialfunktion

Eine weitere Möglichkeit zur Darstellung komplexer Zahlen ergibt sich durch die Verwendung der komplexen Exponentialfunktion:

$$r \cdot e^{i\varphi} \;=\; r \cdot \Big(\cos(\varphi) + i\sin(\varphi)\Big)$$



Polarkoordinatendarstellung III

Aufgabe 4

Beweise den Satz von de Moivre für alle $n \in \mathbb{Z}$ mit $n \geq 0$. Dieser besagt, dass für alle $z \in \mathbb{C}$ mit $r, \varphi \in \mathbb{R}$ und $n \in \mathbb{Z}$ stets

$$z^n = r^n \cdot \left(\cos(n\varphi) + i \sin(n\varphi)\right)$$

gilt.

Aufgaben zur Wiederholung

Vollständige Induktion I

Aufgabe 5

Zeige mithilfe einer vollständigen Induktion, dass die folgende Aussage für alle $n \geq 4$ gilt:

$$n! > 2^n.$$

Vollständige Induktion II

Aufgabe 6

Zeige mithilfe einer vollständigen Induktion, dass die folgende Aussage für alle $n \in \mathbb{N}$ mit $n \geq 3$ gilt:

$$n \cdot \sqrt{n} > n + \sqrt{n}.$$

Vollständige Induktion III

Aufgabe 7

Zeige mithilfe einer vollständigen Induktion, dass die folgende Aussage für alle $n \in \mathbb{N}$ gilt:

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

Abbildungen I

Aufgabe 8

Entscheide, ob die folgende Abbildung injektiv ist. Begründe deine Aussage!

$$\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$$
$$f(n, m) = (n + 2m, 2n - m)$$

Abbildungen II

Aufgabe 9

Entscheide, ob die folgende Abbildung surjektiv ist. Begründe deine Aussage!

$$\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$$
$$f(n, m) = (n + 2m, m + 7)$$

Abbildungen III

Aufgabe 10

Entscheide, ob die folgende Abbildung surjektiv ist. Begründe deine Aussage!

$$\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$$
$$f(n, m) = (2n + m, m + 7)$$

Abbildungen IV

Aufgabe 11

Es seien A und B (endliche) Mengen und $g : A \to B$ eine Abbildung. Zeige, dass g genau dann surjektiv ist, wenn für alle $C \subseteq B$ die Gleichung $g(g^{-1}(C)) = C$ gilt.

Abbildungen V

Aufgabe 12

Es seien A und B (endliche) Mengen und $f : A \to B$ eine Abbildung. Zeige, dass f genau dann injektiv ist, wenn für alle $C \subseteq A$ die Gleichung $|C| = |f(C)|$ gilt.

RSA I

Zum Erzeugen des öffentlichen und des privaten Schlüssels werden die folgenden Schritte ausgeführt:

1. Auswahl von zwei verschiedenen Primzahlen p und q.
2. Bestimmen des RSA-Moduls $N = p \cdot q$.
3. Berechnen des Werts $\varphi(N) = (p-1) \cdot (q-1)$.
4. Auswahl einer zu $\varphi(N)$ teilerfremden Zahl e mit $1 < e < \varphi(N)$.
5. Berechnen des Werts d mit $1 < d < \varphi(N)$, so dass gilt:

$$e \cdot d \equiv 1 \pmod{\varphi(N)}.$$

Man erhält den *öffentlichen Schlüssel* (e, N) sowie den *privaten Schlüssel* (d, N).

RSA II

Beim *Verschlüsseln* einer Nachricht m (mit $1 \leq m < N$) kann die verschlüsselte Nachricht c (mit $1 \leq c < N$) wie folgt berechnet werden:

$$m^e \equiv c \pmod{N}.$$

Beim *Entschlüsseln* einer verschlüsselten Nachricht c kann die ursprüngliche Nachricht m wie folgt berechnet werden:

$$c^d \equiv m \pmod{N}.$$

RSA III

Aufgabe 13

Gegeben sei die folgende verschlüsselte Nachricht $c = 12$ und der zugehörige öffentliche RSA-Schlüssel $(37, 143)$. Berechne die unverschlüsselte Nachricht m.

RSA IV

Aufgabe 14

Seien (e, N) und (d, N) ein öffentlicher und der dazugehörige private RSA-Schlüssel. Zeige, dass es sich bei $m' \equiv c^d \pmod{N}$ tatsächlich um die unverschlüsselte Nachricht m handelt, wenn für die verschlüsselte Nachricht $c \equiv m^e \pmod{N}$ gilt.

Kombinatorik I

Für das Ziehen von k Elementen aus einer n-elementigen Menge gelten die folgenden Formeln:

	mit Reihenfolge	ohne Reihenfolge
mit Zurücklegen	n^k	$\binom{k+n-1}{k}$
ohne Zurücklegen	$n^{\underline{k}}$	$\binom{n}{k}$

Kombinatorik II

Aufgabe 15

a) Bestimme die Anzahl der Permutationen $\pi \in S_5$, für die $\pi(2) < \pi(3)$ gilt.

b) Bestimme die Anzahl der surjektiven Abbildungen $A \to B$ mit $|A| = |B| = 42$.

c) Bestimme den Koeffizienten von x^2y^3 in $(x + y)^5$.

d) Bestimme den Koeffizienten von $x^2y^3z^5$ in $(x + y + z)^{10}$.

e) Bestimme die Anzahl der Möglichkeiten, 12 (nicht unterscheidbare) Bonbons derart auf 7 Kinder zu verteilen, sodass jedes Kind mindestens ein Bonbon bekommt.