

Mathematik I

Vorlesung 7 - Komplexe Zahlen und endliche Körper

Prof. Dr. Sandra Eisenreich

13. November 2023

Hochschule Landshut

7.1 Komplexe Zahlen

Motivation komplexe Zahlen

Die reellen Zahlen sind der größte Zahlenraum, in dem wir uns bisher bewegt haben. Aber leider reicht dieser noch nicht.

Führen wir uns vor Augen, wie sich unser Zahlenraum immer mehr erweitert hat:

- \mathbb{N} : 4 Äpfel, drei Brötchen...
- \mathbb{Z} : Erweiterung von \mathbb{N} durch negative Zahlen.
- \mathbb{Q} : So kommt man zu den Brüchen.
- \mathbb{R} : Erweiterung von \mathbb{Q} durch irrationale Zahlen reellen Zahlen. Problem: die Gleichung $x^2 = -1$ hat eine theoretische Lösung, wir nennen sie i , die aber nicht in den reellen Zahlen liegt. Es muss also nochmal eine größere Menge geben.
- \mathbb{C} : Erweiterung von \mathbb{R} um i . Das sind die **komplexen Zahlen**.

Anwendungen in der Informatik: z.B. 3D-Game-Engines.

Ziel: Konstruiere eine Menge \mathbb{C} , die \mathbb{R} enthält und eine Lösung i der Gleichung $x^2 = -1$.

Definition

Wir definieren die Menge

$$\mathbb{C} := \{(x, y) \in \mathbb{R}^2 \mid x, y \in \mathbb{R}\} = \mathbb{R}^2$$

und fassen die reellen Zahlen \mathbb{R} als die Teilmenge $\mathbb{R} = \{(x, 0) \in \mathbb{R}^2 \mid x \in \mathbb{R}\}$ auf.

Wir führen nun eine Addition und eine Multiplikation auf \mathbb{C} ein:

- Addition: $(x, y) + (x', y') := (x + x', y + y')$
(z.B. $(1, 2) + (-1, 3) = (0, 5)$)
- Multiplikation: $(x, y) \cdot (x', y') := (x \cdot x' - y \cdot y', x \cdot y' + y \cdot x')$
(z.B. $(1, 2) \cdot (-1, 3) = (1 \cdot (-1) - 2 \cdot 3, 1 \cdot 3 + 2 \cdot (-1)) = (-7, 1)$)

Satz

$(\mathbb{C}, +, \cdot)$ ist ein Körper, der sogenannte Körper der **komplexen Zahlen**.

Beweis. → Mitschrift

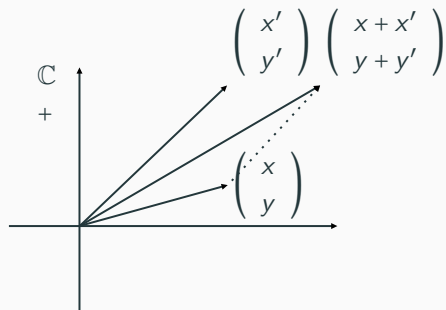
Satz

Fasst man \mathbb{R} als die Teilmenge $\{(x, 0) | x \in \mathbb{R}\}$ von \mathbb{C} auf, so ist \mathbb{R} auf natürliche Weise eine Teilmenge von \mathbb{C} . Schreibt man $i = (0, 1)$, so gilt: $(x, y) = x + i \cdot y$ und $i^2 = -1$.

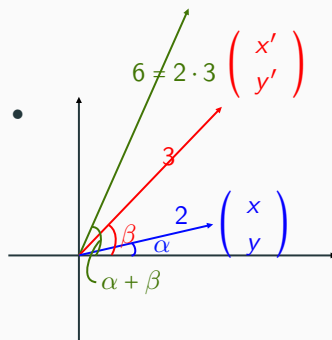
Beweis. → Mitschrift.

Geometrie der Addition und Multiplikation

Addition von komplexen Zahlen:



Multiplikation von kompl. Zahlen:



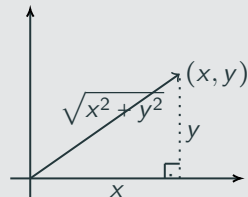
Merke: Beim Multiplizieren werden Längen multipliziert und Winkel zur x-Achse addiert.

Rechnen mit komplexen Zahlen

Definition

Sei $z = x + iy \in \mathbb{C}$ eine komplexe Zahl. Dann definieren wir

$\operatorname{Re}(z) := x$	(Realteil von z)
$\operatorname{Im}(z) := y$	(Imaginärteil von z)
$\bar{z} := x - iy$	(konjugiert Komplexe zu z)
$ z := \sqrt{x^2 + y^2}$	(Betrag von z)



Satz

Für $z = x + iy$ gilt:

$$z \cdot \bar{z} = |z|^2$$

$$z + \bar{z} = 2 \cdot \operatorname{Re}(z)$$

$$z - \bar{z} = 2i \cdot \operatorname{Im}(z)$$

Beweis. → Mitschrift

Brüche von komplexen Zahlen

Die Gleichung $z \cdot \bar{z} = |z|^2$ kann man dazu verwenden, um einen Bruch $\frac{z}{z'} = \frac{x+iy}{x'+iy'}$ wieder in eine komplexe Zahl der Form $a + bi$ umzuformen:

Rechenregel

Um $\frac{z}{z'}$ in die Form $a + bi$ zu bringen, gehe wie folgt vor:

- erweitere den Bruch mit z' :

$$\frac{z}{z'} = \frac{z \cdot \overline{z'}}{z' \cdot \overline{z'}} = \frac{z \cdot \overline{z'}}{|z'|^2}$$

Dadurch wird der Nenner eine reelle Zahl.

- multipliziere den Zähler aus:

$$\frac{z \cdot \overline{z'}}{|z'|^2} = \frac{(x + iy)(x' - iy')}{x'^2 + y'^2} = \frac{xx' + yy'}{x'^2 + y'^2} + i \cdot \frac{x'y - xy'}{x'^2 + y'^2}$$

Geometrie der komplexen Zahlen

Sei $z = x + iy$ eine komplexe Zahl. Man kann sie auf zwei Arten beschreiben:

- über die Koordinaten x und y , also $x + iy$.
- über den Winkel α , den der Vektor mit der x -Achse einschließt, zusammen mit der Länge $|z|$ des Vektors.

Wie kommt man von einer Beschreibung zur anderen? Mit Schulgeometrie.

Satz

Sei $z = x + iy$ eine komplexe Zahl.

- *Der Winkel α ist $\alpha = \arctan\left(\frac{y}{x}\right)$*
- *Die Länge von z ist $|z|$.*

Umgekehrt: Hat man den Winkel α und die Länge $|z|$ einer komplexen Zahl gegeben, so erhält man die Koordinaten als

$$x = |z| \cdot \cos(\alpha), \quad y = |z| \cdot \sin(\alpha), \quad \text{also}$$

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

Satz (Fundamentalsatz der Algebra)

Jedes Polynom $p \in \mathbb{C}[x]$ von Grad n besitzt genaue n komplexe Nullstellen z_1, \dots, z_n (mehrfache Nullstellen treten entsprechend der Multiplizität häufig auf), und es gilt

$$p(x) = a_0 + a_1x + \dots + a_nx^n = a_n(x - z_1) \dots (x - z_n)$$

(d.h. p zerfällt in Linearfaktoren). Wir sagen auch, dass \mathbb{C} **algebraisch abgeschlossen** ist, da jede Polynomgleichung in \mathbb{C} lösbar ist.

Beispiel für Linearfaktorzerlegung:

$$2 \cdot x^4 - 8x^3 + 14x^2 - 24x + 24 = 2 \cdot (x - 2)(x - 2)(x - i\sqrt{3})(x + i\sqrt{3})$$

Satz

Hat $p \in \mathbb{C}[x]$ nur reelle Koeffizienten, dann ist für jede Nullstelle $z \in \mathbb{C} \setminus \mathbb{R}$ auch \bar{z} eine Nullstelle, d.h. nicht-reelle Nullstellen treten immer als Paar auf.

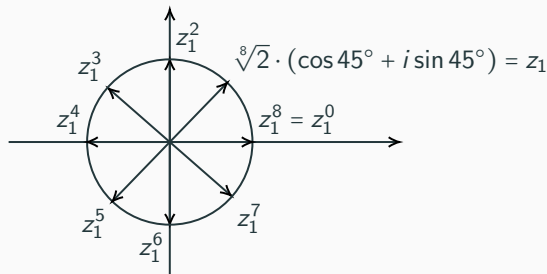
Beweis. → Mitschrift

Beispiel

Alle 8 Lösungen der Gleichung $z^8 = 2$:

$$z = \sqrt[8]{2} \cdot (\cos k \cdot 45^\circ + i \cdot \sin 45^\circ) \text{ bzw. } z = \left[\sqrt[8]{2} \cdot (\cos 45^\circ + i \cdot \sin 45^\circ) \right]^k \text{ für } k = 0, 1, \dots, 7.$$

Die 8 Lösungen liegen also äquidistant verteilt auf dem Kreis mit Radius $\sqrt[8]{2}$



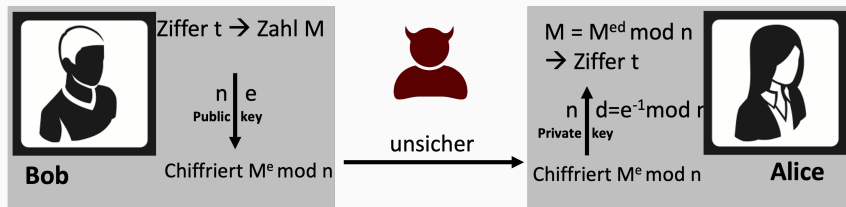
7.2 Endliche Körper

Motivation

Erinnerung: Restklassen und Modulo-Rechnen braucht man für Verschlüsselungsverfahren und viele andere Dinge.

Meist sind dabei auch Primzahlen involviert. Warum? Weil $\mathbb{Z}/p\mathbb{Z}$ für eine Primzahl p nicht nur ein Ring, sondern ein Körper mit endlich vielen Elementen ist, und deswegen viele nützliche Eigenschaften hat!

Diese Tatsache ist der Knackpunkt des RSA-Verschlüsselungsverfahrens, das wir in diesem Kapitel endlich lernen.



Sei $m \in \mathbb{N}$ und $R = \mathbb{Z}/m\mathbb{Z}$ der zugehörige Restklassenring.

Frage: für welche m ist R ein Körper?

- $\mathbb{Z}/2\mathbb{Z}$ ist ein Körper.
- $\mathbb{Z}/m\mathbb{Z}$ ist ein Ring für alle m .
- $\mathbb{Z}/12\mathbb{Z}$ ist kein Körper, da es z.B. für $\bar{9} \in \mathbb{Z}/12\mathbb{Z}$ kein Inverses bzgl. der Multiplikation gibt.
Wir beweisen dies mit Widerspruch \rightarrow Mitschrift.

Satz

Sei $m \in \mathbb{N}$ und $\mathbb{Z}/m\mathbb{Z}$ der zugehörige Restklassenring. Dann ist $x \in \mathbb{Z}/m\mathbb{Z}$ genau dann invertierbar bzgl. der modularen Multiplikation, falls $\text{ggT}(x, m) = 1$.

$(\mathbb{Z}/m\mathbb{Z})^\times := \{x \in \mathbb{Z}/m\mathbb{Z} \mid \text{ggT}(m, x) = 1\}$ ist eine multiplikative Gruppe.

Folgerung

$(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ ist genau dann ein Körper, wenn m eine Primzahl ist.

Beweis. → Mitschrift.

Definition

Man nennt $\mathbb{Z}/p\mathbb{Z}$ für p prim auch “**Galois-Körper**” oder “**Galois-Field**”, Bezeichnung ist $GF(p)$.

Satz (Kleiner Fermat)

Ist p eine Primzahl, so gilt für alle $\bar{a} \in \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$:

$$\bar{a}^{p-1} = \bar{1}.$$

Beispiele: → Mitschrift

Beweis: → Mitschrift

RSA-Algorithmus (Publik Key Verschlüsselung)

Aufgabe: Person A möchte Nachrichten erhalten (von Person B). Die übertragende Nachricht soll verschlüsselt sein und nur von A entschlüsselt werden können.

1. Schritt (Erzeugung eines Schlüssels durch Person A)

- Wahl von zwei großen Primzahlen p, q ($p, q \approx 2^{1024}$)
- Berechnung von $n = p \cdot q$ und $m = (p - 1)(q - 1)$
- e = Encryption key, zufällig gewählt in $(\mathbb{Z}/m)^{\times} = \{x \in \mathbb{Z}/m \mid \text{ggT}(x, m) = 1\}$
- Berechnung von $d = e^{-1}$ in $(\mathbb{Z}/m)^{\times}$, d.h. $e \cdot d \equiv 1 \pmod{m}$ mit dem Euklidischen Algorithmus

Public Key: e, n (kann jeder abfragen)

Private Key: d (kennt nur A)

Wir “glauben” (schlaue Mathematiker glauben):

- d kann man nicht berechnen in vernünftiger Zeit, wenn man m nicht kennt.
- p, q können nicht in vernünftiger Zeit berechnet werden.

2. Schritt Verschlüsseln/Entschlüsseln

Person B möchte Nachricht $M \in \{1, \dots, n-1\}$ an Person A schicken.

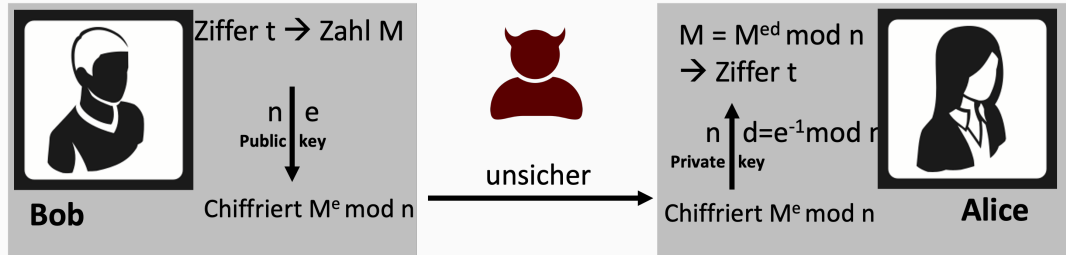
Verschlüsseln: Berechne $S = M^e \bmod n$ (das macht Person B)

Entschlüsseln: Person A berechnet $M' = S^d \bmod n$

(Jemand, der d nicht kennt, kann diesen Schritt nicht ausführen!)

Behauptung: $M = M'$

(also $M = M^{ed} \bmod p \cdot q$ für $d = e^{-1} \bmod (p-1) \cdot (q-1)$.)



Beweis. \rightarrow Mitschrift.