Grundwissen Lineare Algebra
Zusammenfassung der 4.Vorlesungswoche

Dozent: Dr. Jan-David Hardtke

Universität Leipzig, Institut für Mathematik

3. bis 7. Mai 2021

Zusammenfassung der 4.Vorlesungswoche

Auf den folgenden Seiten werden die wesentlichen Inhalte der 4.Vorlesungswoche zusammengefasst.
Dies kann und soll **kein Ersatz für die Lektüre des Skriptes** sein. Insbesondere wird für die Beweise hier meist nur auf das Skript verwiesen.

In dieser Woche geht es um den allgemeinen Begriff eines (algebraischen) Körpers und insbesondere um den Körper der komplexen Zahlen und die Restklassenkörper. Das sind die **Abschnitte III.2 bis III.4 im Skript**.

Körper

Definition

Sei K eine nicht leere Menge versehen mit zwei Verknüpfungen $+ : K \times K \to K$ und $\cdot : K \times K \to K$. Dann heißt $(K, +, \cdot)$ ein **Körper**, falls folgendes gilt:

1) $(K, +)$ ist eine kommutative Gruppe.
2) $(K \setminus \{0\}, \cdot)$ ist eine kommutative Gruppe.
3) Es gilt das Distributivgesetz

$$a(b + c) = ab + ac \quad \forall a, b, c \in K.$$

Beispiele: $\mathbb{R}$ und $\mathbb{Q}$ bilden mit der üblichen Addition und Multiplikation einen Körper, $\mathbb{Z}$ dagegen nicht.

Der Körper der komplexen Zahlen

Definition

Für alle $(a_1, b_1), (a_2, b_2) \in \mathbb{R}^2$ setzen wir

$$(a_1, b_1) + (a_2, b_2) := (a_1 + a_2, b_1 + b_2)$$

und

$$(a_1, b_1) \cdot (a_2, b_2) := (a_1 a_2 - b_1 b_2, a_1 b_2 + a_2 b_1).$$

Satz: $(\mathbb{R}^2, +, \cdot)$ ist ein Körper.

Diesen nennen wir den Körper der **komplexen Zahlen** und bezeichnen ihn mit $\mathbb{C}$.

Der Körper der komplexen Zahlen

Definition

Die komplexe Zahl $i := (0, 1)$ wird **imaginäre Einheit** genannt.

Wichtige Bemerkung: Es gilt $i^2 = -1$ und $(a, b) = a + ib$ für alle $a, b \in \mathbb{R}$.
Damit ist die Multiplikation komplexer Zahlen einfacher:

$$(a + ib)(c + id) = ac + iad + ibc + i^2 bd = ac - bd + i(ad + bc).$$

Beispiel: $(1 + i)(2 + i) = 2 + 2i + i + i^2 = 1 + 3i$

Der Körper der komplexen Zahlen

Definition

Sei $z = a + ib$ eine komplexe Zahl. Dann heißt $\mathrm{Re}(z) := a$ der **Realteil** und $\mathrm{Im}(z) := b$ der **Imaginärteil** von z. Ferner heißt $\overline{z} := a - ib$ die **komplex konjugierte Zahl** von z.

Berechnung von Brüchen in $\mathbb{C}$ durch Erweitern mit dem Konjugierten des Nenners:

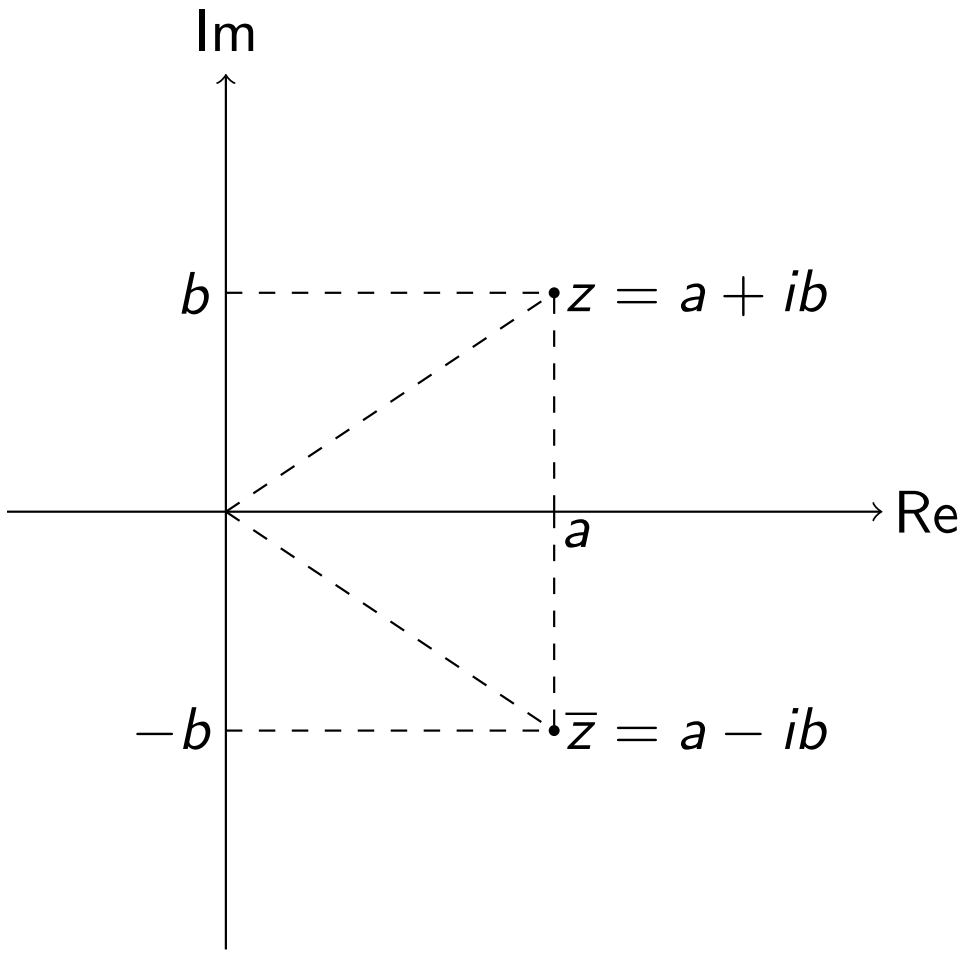
$$\frac{a+ib}{c+id} = \frac{(a+ib)(c-id)}{(c+id)(c-id)} = \frac{(a+ib)(c-id)}{c^2+d^2}$$

Beispiel:

$$\frac{1+i}{3+2i} = \frac{(1+i)(3-2i)}{(3+2i)(3-2i)} = \frac{3-2i+3i-2i^2}{9+4} = \frac{5}{13} + \frac{1}{13}i.$$

Der Körper der komplexen Zahlen

Geometrisch ist die komplexe Konjugation eine Spiegelung an der reellen Achse:

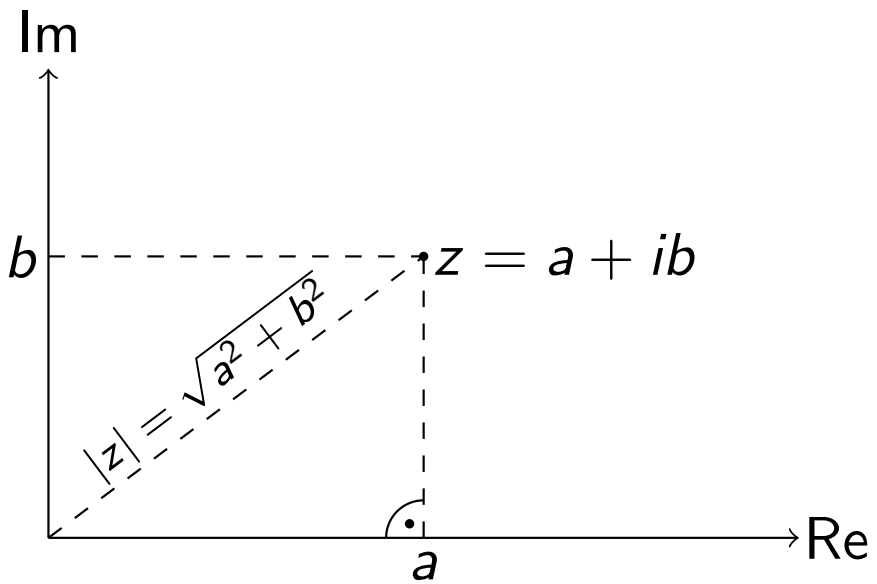


Der Körper der komplexen Zahlen

Definition

Für $z = a + ib$ heißt $|z| := \sqrt{a^2 + b^2}$ der **Betrag** von z.

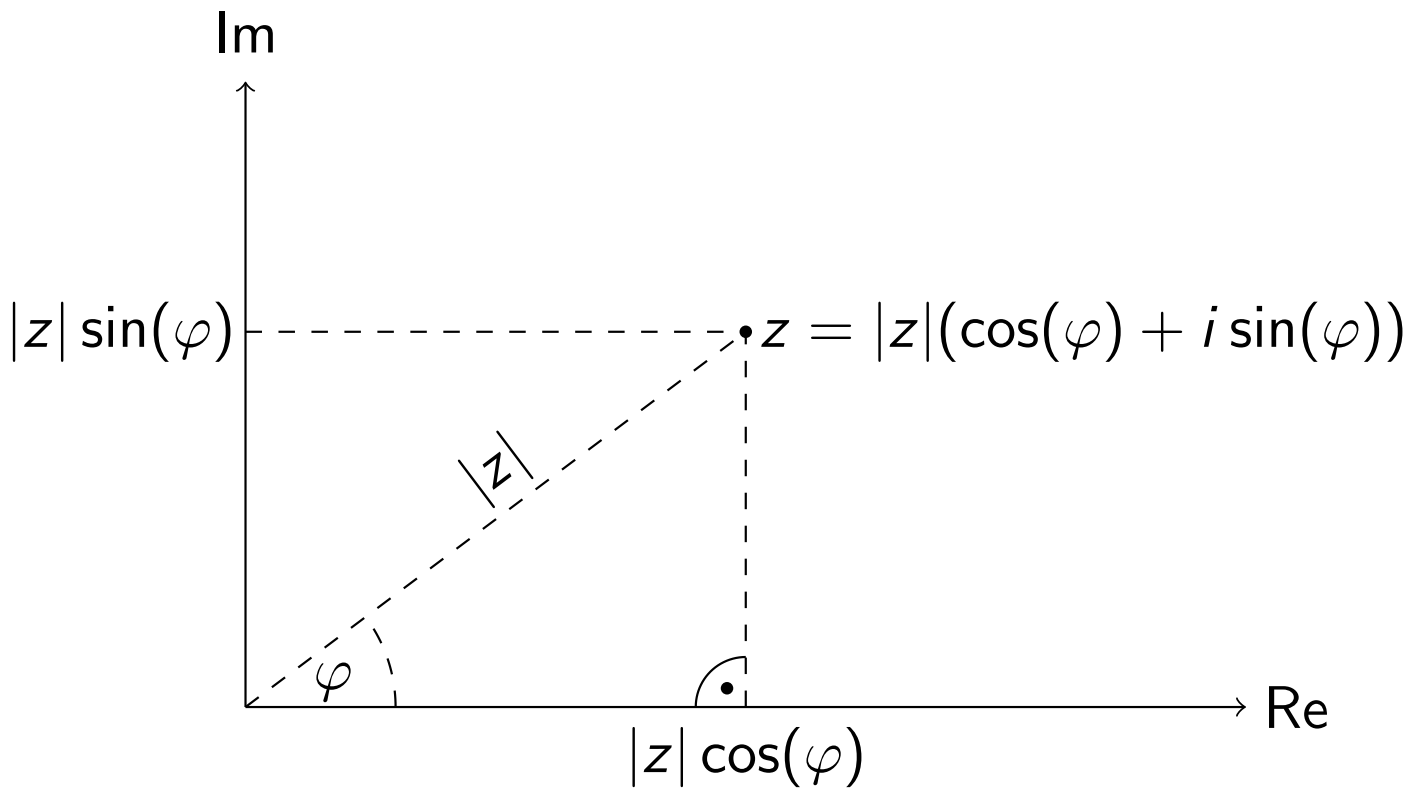
Nach dem Satz des Pythagoras ist $|z|$ der Abstand von z zum Koordinatenursprung.



Der Körper der komplexen Zahlen

Polarkoordinatendarstellung komplexer Zahlen mittels Betrag $|z|$ und Winkel φ:

$$\mathrm{Re}(z) = |z|\cos(\varphi), \quad \mathrm{Im}(z) = |z|\sin(\varphi)$$



Der Körper der komplexen Zahlen

Multiplikation in Polarkoordinatendarstellung:

$$z = |z|(\cos(\varphi) + i\sin(\varphi)) \qquad w = |w|(\cos(\psi) + i\sin(\psi))$$

Additionstheoreme für Sinus und Kosinus:

$$\sin(\varphi + \psi) = \sin(\varphi)\cos(\psi) + \cos(\varphi)\sin(\psi)$$
$$\cos(\varphi + \psi) = \cos(\varphi)\cos(\psi) - \sin(\varphi)\sin(\psi)$$

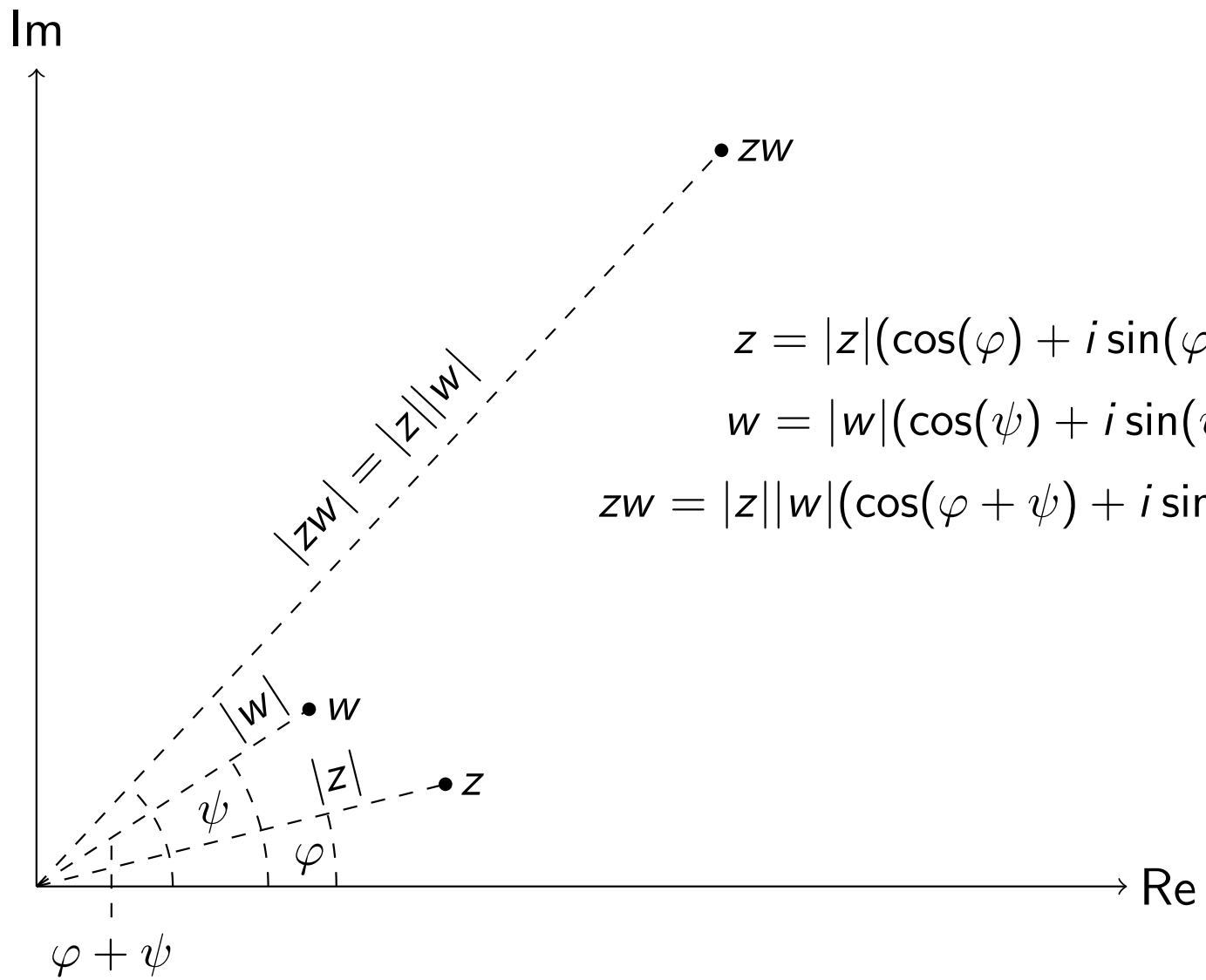
Daraus folgt:

$$zw = |z||w|(\cos(\varphi + \psi) + i\sin(\varphi + \psi))$$

Bei der Multiplikation in $\mathbb{C}$ werden also die Beträge wie gewohnt multipliziert und die Winkel werden addiert.

Der Körper der komplexen Zahlen

Multiplikation in Polarkoordinatendarstellung:



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

$$w = |w|(\cos(\psi) + i\sin(\psi))$$

$$zw = |z||w|(\cos(\varphi + \psi) + i\sin(\varphi + \psi))$$

Restklassenkörper

Definition

Sei M eine nicht leere Menge. Eine **Äquivalenzrelation** auf M ist eine Teilmenge $R \subseteq M \times M$, die die folgenden Bedingungen erfüllt:

(i) $(a, a) \in R$ für alle $a \in M$ (Reflexivität).

(ii) Für alle $a, b \in M$ gilt: $(a, b) \in R \Rightarrow (b, a) \in R$ (Symmetrie).

(iii) Für alle $a, b, c \in M$ gilt: $(a, b) \in R$ und $(b, c) \in R \Rightarrow (a, c) \in R$ (Transitivität).

Anstelle von $(a, b) \in R$ schreibt man auch aRb.

Für $a \in M$ heißt

$$[a]_R := \{b \in M : (a, b) \in R\}$$

die von a erzeugte **Äquivalenzklasse** (bzgl. R).

Restklassenkörper

Beispiele:
1) Sei M irgendeine nicht leere Menge und $R := \{(a, a) : a \in M\}$.
Dann ist R eine Äquivalenzrelation auf M und $[a]_R = \{a\}$ für alle $a \in M$.

2) Sei $R := \left\{(a, b) \in \mathbb{R}^2 : |a| = |b|\right\}$.
Dann ist R eine Äquivalenzrelation auf $\mathbb{R}$ und $[a]_R = \{-a, a\}$ für alle $a \in \mathbb{R}$.

3) Sei $R := \left\{(a, b) \in \mathbb{R}^2 : a - b \in \mathbb{Q}\right\}$.
Dann ist R eine Äquivalenzrelation und $[a]_R = \{a + q : q \in \mathbb{Q}\}$ für alle $a \in \mathbb{R}$.

Restklassenkörper

Lemma

Sei M eine nicht leere Menge und R eine Äquivalenzrelation auf M. Weiter seien $a, b \in M$. Dann sind folgende Aussagen äquivalent:

(i) $(a, b) \in R$

(ii) $[a]_R = [b]_R$

(iii) $[a]_R \cap [b]_R \neq \emptyset$

Beweis: Siehe Lemma III.4.3. im Skript.

Restklassenkörper

Definition

Sei $m \in \mathbb{N}$ mit $m \geq 2$ und seien $a, b \in \mathbb{Z}$. Dann heißt a **kongruent** zu b **modulo** m (in Zeichen: $a \equiv b \mod m$), falls $a - b$ teilbar durch m ist.
Wir setzen $R_m := \{(a, b) \in \mathbb{Z}^2 : a \equiv b \mod m\}$.

Beispiele: $6 \equiv 2 \mod 2$, $15 \equiv 3 \mod 4$, $-2 \equiv 8 \mod 5$

Lemma

R_m ist eine Äquivalenzrelation auf $\mathbb{Z}$.

Beweis: Siehe Lemma III.4.5. im Skript.

Restklassenkörper

Lemma

Sei $m \in \mathbb{N}$ mit $m \geq 2$ und seien $a, b \in \mathbb{Z}$. Seien $q_1, q_2 \in \mathbb{Z}$ und $r_1, r_2 \in \mathbb{N}_0$ mit $a = q_1 m + r_1$, $b = q_2 m + r_2$ und $r_1, r_2 < m$.
Dann gilt: $a \equiv b \mod m \Leftrightarrow r_1 = r_2$

Zwei Zahlen a und b sind also genau dann kongruent modulo m, wenn sie bei Division durch m denselben Rest lassen.

Beweis: Siehe Lemma III.4.6. im Skript.

Restklassenkörper

Für die Äquivalenzklassen (Restklassen) schreiben wir kurz $[a]_m$ anstelle von $[a]_{R_m}$ und setzen

$$\mathbb{Z}_m := \{[a]_m : a \in \mathbb{Z}\}.$$

Lemma

Die Menge $\mathbb{Z}_m$ ist endlich mit m Elementen. Genauer gilt

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

wobei die Klassen $[0]_m, [1]_m, \ldots, [m-1]_m$ paarweise verschieden sind.

Beweis: Siehe Lemma III.4.7. im Skript.

Restklassenkörper

Addition und Multiplikation in $\mathbb{Z}_m$:

$$[a]_m + [b]_m := [a+b]_m \qquad [a]_m \cdot [b]_m := [ab]_m \quad \forall a, b \in \mathbb{Z}.$$

Wichtige Bemerkung: Diese Operationen sind wohldefiniert, d. h. aus $[a]_m = [c]_m$ und $[b]_m = [d]_m$ folgt $[a+b]_m = [c+d]_m$ und $[ab]_m = [cd]_m$ (Beweis im Skript).

Lemma

$(\mathbb{Z}_m, +)$ ist eine kommutative Gruppe und $(\mathbb{Z}_m, \cdot)$ ist ein kommutatives Monoid. Ferner gilt das Distributivgesetz in $(\mathbb{Z}_m, +, \cdot)$.

Restklassenkörper

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

Beweis: Siehe Satz III.4.9. im Skript.

Für $p \in \mathbb{P}$ heißt $\mathbb{Z}_p$ der zugehörige **Restklassenkörper**.

Kleiner Satz von Fermat: Sei p eine Primzahl und $a \in \mathbb{N}$ sei nicht durch p teilbar. Dann gilt $a^{p-1} \equiv 1 \mod p$.

Korollar: Für alle Primzahlen p und alle $a \in \mathbb{N}$ gilt $a^p \equiv a \mod p$.

Beweise: Siehe Satz III.4.10 und Korollar III.4.11. im Skript.

Restklassenkörper

Definition

Für $n \in \mathbb{N}$ bezeichne $\varphi(n)$ die Anzahl aller $a \in \{1, \ldots, n\}$ mit $\mathrm{ggT}(a, n) = 1$ (**Eulersche φ-Funktion**).

Beispiel: Für eine Primzahl p ist $\varphi(p) = p - 1$.

Satz von Euler: Für alle natürlichen Zahlen $n \geq 2$ und alle $a \in \mathbb{N}$ mit $\mathrm{ggT}(a, n) = 1$ gilt $a^{\varphi(n)} \equiv 1 \mod n$.

Restklassenkörper

Definition

Für $n \in \mathbb{N}$ sei

$$n! := \prod_{i=1}^{n} i = 1 \cdot 2 \ldots n.$$

$n!$ wird gelesen als n-**Fakultät**.
Zusätzlich definiert man noch $0! := 1$.

Beispiele: $1! = 1 \quad 2! = 2 \quad 3! = 6 \quad 4! = 24 \quad 5! = 120$

Satz von Wilson: Sei $n \in \mathbb{N}$ mit $n \geq 2$. Dann gilt: n ist eine Primzahl genau dann, wenn $(n-1)! + 1$ durch n teilbar ist.

Beweis: Siehe Satz III.4.14. im Skript.