

Satz 2.53.

$$\forall n, m \in \mathbb{N} : n \leq m \text{ oder } n - m \in \mathbb{N}. \quad (: P_n(m))$$

Beweis-Idee: für fixes n Induktion in m , hierbei Lemma 2.52 für $m = 1$ und $k = n - m$ nutzen.

Wir haben also gezeigt: $m < n$ in $\mathbb{N} \Rightarrow m \leq n - 1$, denn $n - m \in \mathbb{N}$ also $n - m \geq 1$.

Definition 2.54. $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup (-\mathbb{N})$ sind die ganzen Zahlen.

Proposition 2.55. a) $\mathbb{Z} = \mathbb{N} - \mathbb{N} = \{n - m : n, m \in \mathbb{N}\}$.

b) (Deshalb) $\forall x, y \in \mathbb{Z} : x + y, x - y, x \cdot y \in \mathbb{Z}$.

Beweis: Idee - In a) nur $\mathbb{Z} \supset \mathbb{N} - \mathbb{N}$ nichttrivial, nutzen Lemma 2.53. Für b): nutze a) und Lemma 2.51 (mit oder ohne FU).

Definition 2.56. $\mathbb{Q} = \{\frac{p}{q} : p \in \mathbb{Z} \text{ \& } q \in \mathbb{N}\}$ sind die rationalen Zahlen. Also $q \neq 0!$

Klarerweise $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

Bemerkung 2.57. $(\mathbb{Q}, +_{\mathbb{R}}, \cdot_{\mathbb{R}})$ mit $\mathbb{P}_{\mathbb{Q}} = \mathbb{P} \cap \mathbb{Q}$ erfüllt die 9 Körperaxiome und die 3 Anordnungsaxiome, dies lässt sich einfach überprüfen — da $\frac{p}{q} \frac{m}{n} = \frac{pm}{qn}$ und $\frac{p}{q} + \frac{m}{n} = \frac{pn+qm}{qn}$, führen die Operation $+, \cdot$ von $\mathbb{Q} \times \mathbb{Q}$ nach \mathbb{Q} zurück, $-\frac{p}{q} = \frac{-p}{q}$ und $(\frac{p}{q})^{-1} = \frac{q}{p}$ für $p > 0$, $(\frac{p}{q})^{-1} = \frac{-q}{-p}$ für $p < 0$ zeigt die Existenz der Inversen in \mathbb{Q} .

Starke Induktion

mal etwas Neues

Satz 2.58. WOHLORDNUNG DER NATÜRLICHEN ZAHLEN Sei $M \subset \mathbb{N}$ nichtleer, dann existiert $\min M$.

Beweis– Idee: – Für beliebiges aber fixes solches M mit Induktion (Korollar 2.44) in n zeigen:

$$\forall n \in \mathbb{N} : \exists m \in M : m \leq n \Rightarrow \exists \min M.$$

Korollar 2.59. STARKES INDUKTIONSPRINZIP Sei P eine mathematische Aussage, so dass $P(1)$ und $\forall n \in \mathbb{N} : (\forall k \in \mathbb{N} : k \leq n \Rightarrow P(k)) \Rightarrow P(n+1)$. Dann gilt $P(n)$ für jedes $n \in \mathbb{N}$.

Beweis– Idee: Betrachte $M = \{n \in \mathbb{N} : P(n) \text{ falsch} \}$. Falls $M \neq \emptyset$ gibt es einen Widerspruch für $n = \min M - 1 \in \mathbb{N}$ da wegen $P(1)$ sicher $\min M \neq 1$.

Bemerkungen

- auch als Prinzip der "least criminals" bekannt, eine gute Übersetzung wäre: die kleinsten/ersten "Bösewichte" im Sinne von minimalen Gegenbeispielen. Es ist oftmals einfacher, die Existenz solcher als die Existenz allgemeiner Gegenbeispiele auszuschliessen.
- warum *starkes* Induktionsprinzip genannt: Um das entscheidende $P(n+1)$ zu beweisen, können wir nunmehr $P(1), P(2), \dots, P(n)$ voraussetzen. Bisher konnten wir nur $P(n)$ annehmen und also haben wir nun eine "stärkere" Beweismethode, die es erlaubt, mehr und "stärkere" Aussagen zu beweisen.
- eine einfacherere (meine Lieblings-)Formulierung, die allerdings von der bekannten Formulierung " $\Rightarrow P(n+1)$ " abweicht ist folgende.

Sei P eine mathematische Aussage, so dass für jedes $n \in \mathbb{N}$ $P(n)$ gilt, falls

$$\forall k \in \mathbb{N} : k < n \Rightarrow P(k). \text{ Dann gilt } P(n) \text{ für alle } n \in \mathbb{N}.$$

(DIY: zB $P(1)$ gilt dann)

Definition 2.60. Wir sagen p ist Primzahl, wenn $p \in \mathbb{N}$, $p > 1$ und
 $(p = n \cdot m, \text{ mit } n, m \in \mathbb{N}) \Rightarrow (n = 1 \text{ oder } m = 1)$.

Behauptung: Jedes $n \in \mathbb{N}$ mit $n > 1$ ist Produkt (eventuell einfaktorieles) endlich vieler Primzahlen. (Die Eindeutigkeit der Produktdarstellung ist viel tiefliegender!)

Beweis-Idee: Mit starker Induktion einfachst, mit Kor. 2.44 (schwache Induktion) unklar!

Lemma 2.61. $\forall n \in \mathbb{N} : (\exists k \in \mathbb{N} : n = 2k \text{ oder } \exists l \in \mathbb{N} : n = 2l - 1)$, und nur einer der Fälle tritt ein. (nennen n dann gerade bzw ungerade).

Beweis–Idee: Induktion, Widerspruch zu $1 = \min \mathbb{N}$ für Eindeutigkeit des Falles.

Satz 2.62. (Der Klassiker) $\sqrt{2} \notin \mathbb{Q}$, d.h. die Diagonale im Einheitsquadrat ist irrational.

Beweis– Idee: Mit ζ , betrachte eine Bruchdarstellung mit kleinstem Nenner. Zeige Zähler & Nenner gerade, wir können also kürzen! $M = \{q \in \mathbb{N} : \exists p \in \mathbb{N} : p^2/q^2 = 2\} \neq \emptyset$.

Rational versus Reell

Weil nicht alle reellen Zahlen rational sind, müssen wir das Verhältnis von \mathbb{Q} und \mathbb{R} studieren. Wir beginnen mit der folgenden Aussage, die auf Archimedes zurückgeführt wird, obwohl er Eudoxos von Knidos als Urheber erwähnt. Die Bezeichnung "Axiom" ist zwar in der Literatur aus historischen Gründen üblich, in der Theorie der reellen Zahlen jedoch unbegründet, da es sich hier um eine Konsequenz aus unseren 13 Axiomen handelt.

Satz 2.63. (Archimedisches "Axiom") *Die Menge \mathbb{N} der natürlichen Zahlen ist in \mathbb{R} nicht von oben beschränkt.*

Beweis-Idee: Mit ζ , betrachte dazu $\sup \mathbb{N}$ und Approximationsprinzip.

Korollar 2.64. (Eudoxos) $\forall x \in \mathbb{R} : x > 0 \Rightarrow \exists n \in \mathbb{N} : \frac{1}{n} < x$

Beweis-Idee: folgt direkt aus dem Archimedischen Axiom.

Nunmehr können wir zeigen, dass obwohl nicht alle Zahlen rational sind, die rationalen Zahlen zumindest alle Zahlen gut annähern können.

Satz 2.65. (Rationale Zahlen sind dicht) *Für alle $x < y$ reell existiert $z \in \mathbb{Q}$, die $x < z < y$ erfüllt.*

Beweis-Idee: Erst nach \mathbb{R}_+ verschieben (dh oBdA $2 < x$). Nun führen kleine $\frac{1}{n}$ -Schritte zum Ziel!

Die komplexen Zahlen

Als letzten Körper führen wir die komplexen Zahlen ein, in diesem Körper ist die in \mathbb{R} unlösbare Gleichung $x^2 + 1 = 0$ leicht lösbar.

Definition 2.66. Wir betrachten $\mathbb{C} = \mathbb{R} \times \mathbb{R} = \{(a, b) : a, b \in \mathbb{R}\}$ mit den Operationen

$$(a, b) + (c, d) = (a + c, b + d), (a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

Dann ist \mathbb{C} ein Körper mit Nullelement $(0, 0)$ (neutral für "+") und Einselement $(1, 0)$ (neutral für "·").

Bemerkung 2.67.

- nur die Axiome (MA), (MK) und (DG) erfordern etwas Arbeit
- für $(a, b) \neq (0, 0)$ ist $(a/(a^2 + b^2), -b/(a^2 + b^2))$ das multiplikative Inverse !!
- $\mathbb{R} \equiv \mathbb{R} \times \{0\} \subset \mathbb{C}$, d.h. $x \rightarrow (x, 0)$ gibt \mathbb{R} als Unterkörper von \mathbb{C} - wir haben $x + y \rightarrow (x, 0) + (y, 0)$ und $x \cdot y \rightarrow (x, 0) \cdot (y, 0)$
- $(0, 1)^2 = (-1, 0)$!! Wir schreiben i für $(0, 1)$ und $a + bi$ für (a, b) Somit $i^2 = -1$ und \mathbb{C} kann nicht angeordnet werden, d.h. es gibt kein $\mathbb{P} \subset \mathbb{C}$, das (O.1), (O.2) und (O.3) erfüllt.
- Definition von "·" lässt sich "motivieren" aus Körperaxiomen und $(0, 1)^2 = (-1, 0)$.

Definition 2.68. Für $z = a + bi = (a, b) \in \mathbb{C}$ definieren wir

$$\operatorname{Re}(z) = a, \operatorname{Im}(z) = b, |z| = \sqrt{a^2 + b^2} \text{ Realteil, Imaginärteil und Betrag von } z$$

sowie

$$\bar{z} = a - bi \text{ die zu } z \text{ komplex konjugierte Zahl.}$$

Wie in \mathbb{R} ist $|z|$ der Abstand von z zum Ursprung (\mathbb{C} wird mit der Euklidischen Ebene \mathbb{R}^2 identifiziert).

Lemma 2.69. $\forall z, w \in \mathbb{C}$

- a) $\overline{z + w} = \bar{z} + \bar{w}, \overline{z \cdot w} = \bar{z} \cdot \bar{w} !$
- b) $\bar{\bar{z}} = z, |z| = \sqrt{z \cdot \bar{z}} = |\bar{z}|, \operatorname{Re}(z) = (z + \bar{z})/2, \operatorname{Im}(z) = (z - \bar{z})/2i.$

Beweis: Zweite Teilbehauptung von a) die wichtigste, zB für Satz 2.70.c)&d).

Satz 2.70. Für alle $z, w \in \mathbb{C}$

- a) $|Re(z)| \leq |z|, |Im(z)| \leq |z|$ und $|Re(z)| = |z| \Leftrightarrow Im(z) = 0 \Leftrightarrow z \in \mathbb{R}$
- b) $|z| \geq 0, |z| = 0 \Leftrightarrow z = 0$ (wie in \mathbb{R})
- c) $|z \cdot w| = |z| \cdot |w|$ Multiplikativität (wie in \mathbb{R})
- d) $|z + w| \leq |z| + |w|$ Δ -Ungleichung (wie in \mathbb{R})

Beweis:

Proposition 2.71. Komplexe Quadratwurzeln Für gegebenes $c \in \mathbb{C}$ suchen wir alle (da kein "Positives" ausgezeichnet ist) $w \in \mathbb{C}$ mit $w^2 = c$.

Hierbei $w^2 = 0 \Leftrightarrow w = 0$, und wenn $c \neq 0$ dann ist

$$w_1 = \sqrt{\frac{|c| + \operatorname{Re}(c)}{2}} + \sigma \sqrt{\frac{|c| - \operatorname{Re}(c)}{2}} i \text{ wo } \sigma = \begin{cases} 1 & \text{für } \operatorname{Im}(c) \geq 0 \\ -1 & \text{für } \operatorname{Im}(c) < 0 \end{cases}$$

eine Lösung, die einzige andere Lösung ist $w_2 = -w_1$.

Jede quadratische Gleichung

$$0 = z^2 + az + b = (z + \frac{a}{2})^2 - (\frac{a^2}{4} - b) = (z + \frac{a}{2} + w)(z + \frac{a}{2} - w)$$

wobei $w^2 = \frac{a^2}{4} - b$ kann somit in \mathbb{C} gelöst werden.

Beweis-Idee: $|c| = |w|^2 = (\operatorname{Re}(w))^2 + (\operatorname{Im}(w))^2$ und $\operatorname{Re}(c) = (\operatorname{Re}(w))^2 - (\operatorname{Im}(w))^2$ nutzen um $(\operatorname{Re}(w))^2$ und $(\operatorname{Im}(w))^2$ einfachst zu bestimmen!

Im Zusammenhang mit der Exponentialfunktion und der Eulerschen Formel werden wir bald einen geometrischeren Zugang zu den komplexen Zahlen \mathbb{C} finden, der diese als Ebene und die Rechenoperationen als geometrische Verschiebungen und Drehstreckungen interpretiert.

Zum Beispiel, wenn $(0, z, w) \in \mathbb{C}$ ein Dreieck Δ in der komplexen Ebene darstellt und $u \in \mathbb{C}$, dann hat das Dreieck $(0+u = u, z+u, w+u)$ wieder Seiten der Länge $|z|, |w|, |z-w|$ (also kongruent und parallel zu Δ) und das Dreieck $(0 \cdot u = 0, z \cdot u, w \cdot u)$ Seiten der Länge $|z| \cdot |u|, |w| \cdot |u|, |z-w| \cdot |u|$, ist also ähnlich zu Δ und hat somit die gleichen Winkel!!