Wiederholung:

$\mathbb{Z}^\times := \mathbb{Z} \setminus \{\overline{(0,0)}\}$

Die Menge $\mathbb{Q}$ der rationalen Zahlen ist die Menge der Äquivalenzklassen in $\mathbb{Z} \times \mathbb{Z}^\times$ bezüglich der Relation

$$(p,q) \sim_{\mathbb{Q}} (r,s) \Leftrightarrow p \cdot s = r \cdot q$$

$\widehat{(p,q)}$ bezeichnet die Äquivalenzklasse

$$\{(r,s) \in \mathbb{Z} \times \mathbb{Z}^\times : (r,s) \sim_{\mathbb{Q}} (p,q)\}$$

Def: Wir definieren Addition und Multiplikation auf $\mathbb{Q}$ durch.

(i) $\widehat{(p,q)} + \widehat{(r,s)} := \widehat{((p \cdot s) + (r \cdot q) \;,\; r \cdot s)}$

(ii) $\widehat{(p,q)} \cdot \widehat{(r,s)} := \widehat{(p \cdot r \;,\; q \cdot s)}$

Aufgabe: Überzeugen Sie sich, dass $\sim_{\mathbb{Q}}$ tatsächlich eine Äquivalenzrelation ist, und dass „+" und „·" über $\mathbb{Q}$ wohldefiniert sind.
Welche Rechenregeln gelten auch für $\mathbb{Q}$?

In Zukunft verwenden wir die Standardnotation für Elemente aus $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ usw., und verwenden auch die üblichen Rechenregeln für $+, \cdot, \leq, -, \frac{m}{n}$ usw. ohne Beweis.

Das „absichtliche Vergessen" ist also jetzt zu Ende.

Kapitel 1: Teilbarkeit und der euklidische Algorithmus

Motivation: Wir wollen die diophantische Gleichung $aX+bY=c$ lösen ($a,b,c \in \mathbb{N}$ sind fix). „Diophantisch" heisst ganzzahlig.

Unter welchen Bedingungen existiert eine Lösung in $\mathbb{N}$?
Wenn es keine Lösung in $\mathbb{N}$ gibt, wie müssen wir $\mathbb{N}$ erweitern, sodass die Gleichung immer eine Lösung hat?

Gestalt der Gleichung	Lösungsbedingung in $\mathbb{N}$ (bzw. in $\mathbb{Z}$)	„Immer lösbar" führt zu
$a+X=b$	$\leq$	$\mathbb{Z}$
$aX=b$	Teilbarkeit	$\mathbb{Q}$ (oder auch nur $\mathbb{Q}^+$)
$aX+bY=c$	ggT	$\mathbb{Q}$

Def: Seien $m,n \in \mathbb{Z}$, $m \neq 0$. Wir sagen m <u>teilt</u> n (bezeichnet „$m|n$") $\Leftrightarrow \exists l \in \mathbb{Z}$ sodass $n = ml$
Dann sagen wir auch m ist <u>Teiler</u> von n.

Def: Der <u>Betrag</u> einer Zahl $n \in \mathbb{Z}$ ist

$$|n| := \begin{cases} n & \text{wenn } n \in \mathbb{N} \\ -n & \text{wenn } n \notin \mathbb{N} \end{cases}$$

Bemerkungen: (i) $m,n \in \mathbb{Z}^\times$ und $m|n \Rightarrow |m| \leq |n|$

(ii) $m \cdot n = 1 \Rightarrow m=n=1$ oder $m=n=-1$.

Lemma 1.1: $\forall i, j, k, \ell, m, n \in \mathbb{Z}$ gelten die üblichen Rechenregeln

(i) $n \mid n$ und $-n \mid n$ $(n \neq 0)$

(ii) $n \mid 0$ $(n \neq 0)$

(iii) $1 \mid n$ und $-1 \mid n$

(iv) $\ell \mid m$ und $m \mid n \Rightarrow \ell \mid n$

(v) $m \mid n \iff \ell m \mid \ell n$ $(\ell \neq 0)$

(vi) $k \mid m$ und $\ell \mid n \Rightarrow k\ell \mid mn$

(vii) $\ell \mid m$ und $\ell \mid n \Rightarrow \ell \mid im + jn$

(viii) $m \mid n \Rightarrow m \mid \ell n$

(ix) $m \mid n$ und $n \mid m \Rightarrow m = \pm n$

Bemerkung: Aus (i), (iv) und (ix) folgt, dass die Teilbarkeitsrelation eine partielle Ordnung von $\mathbb{N}^+$ ist.

Beweis: Alle Aussagen folgen (fast) direkt aus der Definition.

Def: Der <u>größte gemeinsame Teiler</u> von $m, n \in \mathbb{Z}^\times$ (bezeichnet „$ggT(m,n)$" oder einfach „(m,n)") ist die größte Zahl $\ell \in \mathbb{N}^+$ sodass $\ell \mid m$ <u>und</u> $\ell \mid n$.

Wir sagen m und n sind <u>teilerfremd</u> wenn $(m,n) = 1$.

Das <u>kleinste gemeinsame Vielfaches</u> von m und n (bezeichnet „$kgV(m,n)$" oder einfach $[m,n]$) ist die kleinste Zahl $k \in \mathbb{N}^+$ sodass $m \mid k$ <u>und</u> $n \mid k$.

Bemerkung: Da $1 \mid m$, $1 \mid n$ und m und n nur endlich viele Teiler haben, existiert (m,n).

Da $n \mid |mn|$ und $n \mid |mn|$ existiert $[m,n]$

Lemma 1.2: (Division mit Rest)

$\forall\, m, n \in \mathbb{Z},\ m \neq 0 \quad \exists\, q, r \in \mathbb{Z}$ sodass

$n = qm + r$ und $r \in \{0, 1, \ldots, |m|-1\}$

Beweis: Wir nehmen o.B.d.A. an, dass $m \in \mathbb{N}^+$ (ansonsten betrachte $-m$ und $-q$).

Betrachte $\{n - xm : x \in \mathbb{Z}\} \cap \mathbb{N}$

Der Schnitt ist nichtleer, also sei r sein kleinstes Element und $q \in \mathbb{Z}$ sodass $n - qm = r$.

Dann ist $n - (q+1)m = r - m < r$

Also nach Definition von r ist $r - m < 0$

$\Rightarrow r \leq m - 1 = |m| - 1.$

Also ist $r \in \{0, 1, \ldots, |m| - 1\}$ □

Satz 1.3: Seien $m, n \in \mathbb{Z}^\times$, $a := (m,n)$ und $b \in \mathbb{Z}$

Dann hat die Gleichung $mX + nY = b$ eine ganzzahlige Lösung $x, y \in \mathbb{Z} \Leftrightarrow a \mid b$.

Insbesondere existieren $x, y \in \mathbb{Z}$ sodass $mx + ny = (m,n)$

Beweis: $\Rightarrow$: Sei $x, y \in \mathbb{Z}$ eine ganzzahlige Lösung

$a \mid m$ und $a \mid n \Rightarrow a \mid mx + ny$

$\Rightarrow a \mid b$

$\Leftarrow$: Sei $M := \{mx+ny : x,y \in \mathbb{Z}\}$
und k die kleinste Zahl in $M \cap \mathbb{N}^+$

Angenommen $k \nmid m$. Dann $\exists q, r \in \mathbb{Z}$ sodass
$m = qk + r$ und $r \in \{0, \dots, k-1\}$
aber es gilt auch $r \neq 0$ (weil $k \nmid m$)
Also $0 < r < k$.
Dann ist $r = m - qk = m - q(mx+ny)$
$= (1-qx)m + (-qy)n \in M \cap \mathbb{N}^+$
$\lightning$ zur Definition von k.

Also gilt $k \mid m$
Ähnlich gilt $k \mid n$
Also ist $k \leq a$, aber wir haben schon bewiesen,
dass $a \mid k$ also ist $a \leq k$.
Daraus folgt $k = a$.

Es sei jetzt $b \in \mathbb{Z}$ mit $a \mid b$
Dann ist $b = ca$ für ein $c \in \mathbb{Z}$
und $a = mx+ny$ für ein Paar $x, y \in \mathbb{Z}$
also ist $b = c(mx+ny)$
$= (cx)m + (cy)n \in M$. □

Bemerkung: Das heisst $m\mathbb{Z} + n\mathbb{Z} = (m,n)\mathbb{Z}$

Notation: $aX = \{ax : x \in X\}$
$X + Y = \{x+y : x \in X, y \in Y\}$

Korollar 1.4: Seien $k, l, m, n \in \mathbb{Z}^\times$, l ein gemeinsamer Teiler von m und n. Dann gilt

(i) $l \mid (m,n)$

(ii) $(km, kn) = |k|(m,n)$

(iii) $\left(\frac{m}{l}, \frac{n}{l}\right) = \frac{(m,n)}{|l|}$

(iv) $[m,n] = \frac{|mn|}{(m,n)}$

Bemerkung: Wegen (i) hätten wir (m,n) auch anders definieren können, und zwar als die eindeutige Zahl $a \in \mathbb{N}^+$ sodass $b \mid a$ für alle gemeinsamen Teiler b von m und n.

Beweis: (i), (ii) und (iii): Aufgabe.

(iv): Sei $|m| = a(m,n)$

$|n| = b(m,n)$

Dann ist $\frac{|mn|}{(m,n)} = a|n| = b|m|$ ein gemeinsames Vielfaches von m und n,

also ist $[m,n] \leq \frac{|mn|}{(m,n)}$.

Andererseits sei $[m,n] = c|m| = d|n|$

Dann ist $\frac{|cd||mn|}{[m,n]} = |d||n| = |c||m|$ ein gemeinsamer Teiler von $|cd||m|$ und $|cd||n|$

Also gilt $(|cd||m|, |cd||n|) \geq \frac{|cd||mn|}{[m,n]}$

Aus (ii) folgt $|cd|(m,n) \geq \frac{|cd||mn|}{[m,n]}$

$\Rightarrow (m,n) \geq \frac{|mn|}{[m,n]}$

$\Rightarrow [m,n] \geq \frac{|mn|}{(m,n)} \Rightarrow [m,n] = \frac{|mn|}{(m,n)}$ □

Wie können wir die Darstellung $(m,n) = mx + ny$ finden?

Der euklidische Algorithmus

Seien $m, n \in \mathbb{Z}^\times$, $|m| < |n|$

Wir definieren $r_0 := |n|$

$r_1 := |m|$

und rekursiv $r_{k+1} := r_{k-1} - q_k r_k \in \{0, \dots, r_k - 1\}$

für ein $q_k \in \mathbb{Z}$

Satz 1.5: Die r_k bilden eine monoton fallende Folge in $\mathbb{N}$ und das letzte r_k ungleich 0 ist (m,n).

Beweis: nächstes Mal

Bemerkung: Mit dem euklidischen Algorithmus kann man jedes r_k, und insbesondere (m,n), als ganzzahlige Kombination von m und n ($\pm r_1$ und $\pm r_0$) darstellen

$$r_2 = r_0 - q_1 r_1$$

$$r_3 = r_1 - q_2 r_2 = r_1 - q_2 (r_0 - q_1 r_1)$$

$$= (1 + q_1 q_2) r_1 + (-q_2) r_0$$

$$\vdots$$