

SÄTZE:

Seien $a \neq 0, b \neq 0, a, b \in \mathbb{Z}$

dann ist $d = \text{ggT}(a, b) > 0$ genau dann, Wenn:

- (1) $\exists_{r, s \in \mathbb{Z}}$, so dass: $d = ra + sb$
- (2) Für jedes Paar $r, s \in \mathbb{Z}$ mit $ra + sb \neq 0$ gilt: $d \mid (ra + sb)$

(a) Wenn $a, b, c \in \mathbb{Z}$ mit $\text{ggT}(a, b) = 1$ und $a \mid b \cdot c$ dann ist $a \mid c$

(b) Eine Zahl $p \neq 0, p \neq \pm 1$ ist genau dann Primzahl, wenn: $p \mid a \cdot b \Leftrightarrow p \mid a \vee p \mid b$

Sei $n \neq 0 \in \mathbb{Z}$. Dann gibt es genau eine Darstellung der Form $n = u \cdot p_1 \cdot p_2 \cdot \dots \cdot p_k$, wobei $u = \pm 1$ und $0 \leq p_1 \leq p_2 \leq \dots \leq p_k$

Sei $M / \sim = \{[a] \mid a \in M\}$ wobei $a = \{x \in M \mid x \sim a\}$
Dann liegt jedes Element aus M in genau einer Äquivalenzklasse!

Rechenoperationen in $\mathbb{Z}/n\mathbb{Z}$:

$$[a] + [b] := [a + b]$$

$$[a] \cdot [b] := [a \cdot b]$$

ES GELTEN ALLE RECHENGESETZE DER \mathbb{Z}

Inverses Element einer Äquivalenzklasse:

Wenn $\text{ggT}(n, a) = 1$, dann hat dir Gleichung $[a] \cdot x = [1]$ genau eine Lösung in $\mathbb{Z}/n\mathbb{Z}$

Sei n Primzahl $\wedge n \nmid a \Rightarrow \exists_{a' \in \mathbb{Z}}$ mit $[a] \cdot [a'] = [1]$ in $\mathbb{Z}/n\mathbb{Z}$

Zu jeder Untergruppe $U \subset \mathbb{Z}$ existiert ein $n \in \mathbb{Z}$, so daß:

$$\forall_{u \in U, z \in \mathbb{Z}} u = n \cdot z \quad (\text{oder: } U = n \cdot \mathbb{Z})$$

$D_n :=$ Gruppe der Konruenztransformationen

$D_5 := \{1, t, t^2, t^3, t^4, s, st, st^2, st^3, st^4\}$ mult. Gruppe

Es gilt in D_5 : $tst = s, s^2 = 1, t^5 = 1$; Das liefert: $sts = t$

Allgemein: D_n hat $2n$ Elemente. $s^2 = 1, t^n = 1, tst = s$
 D_n nicht abelsch f. $n > 2$

$$\text{ord}(\langle g \rangle) = \min\{k \geq 1 \mid g^k = 1\}$$

Sei G endliche Gruppe. Dann gilt:

- (a) Wenn $U \in G$ Untergr., so ist $\text{ord}(U)$ Teiler v. $\text{ord}(G)$
- (b) Wenn $g \in G$, dann ist $\text{ord}(g)$ Teiler von $\text{ord}(G)$
- (c) Wenn $g \in G$ dann $g^{\text{ord}(G)} = 1$

(kleiner Fermatscher Satz)

- (a) Wenn p Primzahl und $p \nmid a$, so ist $a^{p-1} \equiv 1 \pmod{p}$
- (b) Wenn $\text{ggT}(a, n) = 1$, so ist $a^{\varphi(n)} \equiv 1 \pmod{p}$

Sei $f: G \rightarrow H$ Gruppenhom. Dann gilt

- (a) $\ker(f) \subset G$ Untergruppe
- (b) $\text{im}(f) \subset H$ Untergruppe
- (c) f injektiv $\Leftrightarrow \ker(f) = \{e_G\}$

DEFINITIONEN:

Für $n \in \mathbb{N} \setminus \{0\}$ $\varphi := \#\{k \mid 1 \leq k < n, \text{ggT}(k, n) = 1\}$

- (1) p Primzahl $\Rightarrow \varphi(p) = p - 1$
- (2) p Primzahl $\Rightarrow \varphi(p^n) = p^{n-1}(p - 1)$ für $n \geq 1$
- (3) $\text{ggT}(m, n) = 1 \Rightarrow \varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$

Für eine Abbildung $f: A \rightarrow B$ gilt

- injektiv $\Leftrightarrow a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$ für $a_1, a_2 \in A$
- surjektiv $\Leftrightarrow \forall_{b \in B} \exists_{a \in A}$, so das: $f(a) = b$
- bijektiv $\Leftrightarrow f$ injektiv and f surjektiv

Äquivalenzrelation in Menge M : Abb.R: $M \times M \rightarrow \{0, 1\}$

- (1) Reflexivität: $\forall_{a, b \in M} a \sim a$
- (2) Symmetrie: $\forall_{a, b \in M} (a \sim b \Rightarrow b \sim a)$
- (3) Transitivität: $\forall_{a, b, c \in M} (a \sim b \wedge b \sim c \Rightarrow a \sim c)$

Menge $G \neq \emptyset$, Abbildung $\varphi: G \times G \rightarrow G$; $\varphi(a, b) \Leftrightarrow a * b$

(1) (Assoziativität) $\forall_{a, b, c \in G} a * (b * c) = (a * b) * c$

(2) (neutrales Element) $\exists_{e \in G} \forall_{a \in G} e * a = a$

(3) (inverses Element) $\forall_{a \in G} \exists_{a' \in G} a' * a = e$

abelsch: (4) (kommutativ) $\forall_{a, b \in G} a * b = b * a$

(a) \exists genau EIN neutrales El. $e \in G$

(b) $\forall_{a \in G} a * e = a$

(c) $\forall_{a \in G} \exists$ genau EIN $a' \in G \mid a' * a = e$, auch: $a * a' = e$

(d) Wenn $a * b = c * b \Rightarrow a = c$

Sei $(G, *)$ Gruppe, $U \subset G$ Untergruppe, falls:

- (1) $U \neq \emptyset$
- (2) $\forall_{a, b \in U} a * b \in U$
- (3) $a' = a^{-1} \in U$

Seien $(G, *)$ und (H, \circ) Gruppen. Abbildung: $f: G \rightarrow H$

f Gruppenhomomorphismus $\Leftrightarrow \forall_{a, b \in G} f(a * b) = f(a) \circ f(b)$

f Isomorphismus $\Leftrightarrow f$ bijektiv $\wedge f$ Gruppenhom.

Sei $g \in (G, *)$ beliebig. Dann ist:

$\langle g \rangle := \{g^k \mid k \in \mathbb{Z}\} \subset G$ Untergruppe

Sie heißt von g erzeugte Untergruppe von G

(Im Falle $(G, +)$: $\langle g \rangle := \{g \cdot k \mid k \in \mathbb{Z}\}$)

Sei $U \subset G$ Untergruppe. U zyklisch $\Leftrightarrow \exists$ mit $\langle g \rangle = U$

Sei $(G, *)$ eine Gruppe

(a) $\text{ord}(G) := \#G$ Ordnung der Gruppe G

(b) Für $g \in G$ gilt $\text{ord}(g) = \text{ord}(\langle g \rangle)$

Sei $f: G \rightarrow H$ ein Gruppenhom.

(a) $\ker(f) := \{g \in G \mid f(g) = e_H\}$ heißt Kern von f

(b) $\text{im}(f) := \{f(g) \mid g \in G\} \subset H$ heißt Bild von f

SÄTZE

Wenn G abelsche Gruppe ist u. $U \subset G$ Untergruppe, dann ist durch $[a] * [b] := [a * b]$ eine abelsche Gruppenstruktur auf G/U definiert.
 G nicht abelsch: trotzdem wohldefiniert, wenn
 $\forall r \in U, r' \in U$ mit $r * b = b * r'$

(Homomorphiesatz)
 Sei $f: G \rightarrow H$ Gruppenhomomorphismus und $G/\ker(f)$ mit vererbter Gruppenstruktur.
 Dann ist $\bar{f}: G/\ker(f) \rightarrow \text{im}(f)$ mit $\bar{f}([a]) := f(a)$ ein Isomorphismus

Wenn $m, n \in \mathbb{Z}$ mit $\text{ggT}(m, n) = 1$ und $a \in \mathbb{Z}$ mit $[a]_n \in \mathbb{Z}/n\mathbb{Z}$ und $[a]_m \in \mathbb{Z}/m\mathbb{Z}$ die zugehörigen Restklassen bezeichne:
 $f: \mathbb{Z}/nm\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, gegeben durch $f([a]_{nm}) := ([a]_n, [a]_m)$ ist ein Isomorphismus

Sei K ein Körper und $f, g \in K[x]$ mit $\text{def}(f) \geq \text{deg}(g)$
 Dann gibt es $r, h \in K[x]$ mit $f - h \cdot g = r$; $\text{deg}(r) < \text{deg}(g)$

(1) Wenn $f, g \in K[x]$ dann ist $d = \text{ggT}(f, g)$, falls Leitkoeff. $d = 1$ ist; r, s in $K[x]$ existieren mit $d = r \cdot f + s \cdot g$ und für beliebige a, b in $K[x]$ ist $d | af + bg$
 (2) Wenn $f, g, h \in K[x]$ mit $\text{ggT}(f, g) = 1$ und $f | g \cdot h$, so $f | h$
 (3) Ein Polynom f in $K[x]$ ist irreduzibel genau dann wenn aus $f | hg \cdot h$ stets folgt: $f | g \vee f | h$
 Irreduzibel $\Leftrightarrow f = g \cdot h$ mit g Konstante $\vee h$ Konstante
 (4) Jedes $f \in K[x]$ mit $f \neq 0$ besitzt eine (bis auf Reihenfolge) eindeutige Zerlegung $f = u \cdot p_1 \cdot p_2 \cdot \dots \cdot p_n$, wobei $u \in K^\times$ und $p_i \in K[x]$ irreduzibel ist Leitkoeff. 1

Sei R Ring und $I \subset R$ ein Ideal, dann ist auf der additiven Gruppe R/I durch $[a] \cdot [b] := [a \cdot b]$ die Struktur eines Ringes definiert

Sei K ein Körper, $I \subset K[x]$ ein Ideal, dann $\exists \langle f \rangle = I$ (also ist I ein Hauptideal)

Sei R ein Ring
 (a) $a \in R$ Nullteiler $\Leftrightarrow \exists b \in R \setminus \{0\}$ $a \cdot b = 0$
 (b) $a \in R$ Einheit $\Leftrightarrow \exists b \in R$ $a \cdot b = 1$
 (c) Ring R Nullteilerfrei $\Leftrightarrow 0 \in R$ ist einziger Nullteiler

Homomorphiesatz für Ringe
 Sei $\varphi: R \rightarrow S$ ein Ringhomomorphismus. Dann ist $\ker(\varphi) \subset R$ ein Ideal, $\text{im}(\varphi) \subset S$ Unterring und $\bar{\varphi}: R/\ker(\varphi) \cong \text{im}(\varphi)$ ist ein Ringhomomorph. wobei $\bar{\varphi}([a]) := \varphi(a)$

Chinesischer Restsatz
 Seien $m, n \in \mathbb{Z}$ teilerfremd, d.h. $\text{ggT}(m, n) = 1$.
 Dann ist die Abbildung: $\mathbb{Z}/mn\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ die $[a]_{mn}$ auf $([a]_m, [a]_n)$ abbildet, ein Ringisomorphismus.

DEFINITIONEN

Eine Untergruppe $U \subset G$ heißt Normalteiler falls:
 $\forall g \in G, u \in U \exists u' \in U$ mit $u * g = g * u'$

Eine Menge K mit zwei (binären) Verknüpfungen $+$: $K \times K \rightarrow K, \cdot$: $K \times K \rightarrow K$ heißt Körper, wenn:
 (1) $(K, +)$ ist abelsche Gruppe (mit neutr. Element $0 \in K$)
 (2) (K^\times, \cdot) ist abelsche Gruppe, wobei $K^\times := K \setminus \{0\}$
 (3) Distributivges.: $\forall a, b, c \in K$ $(a + b) \cdot c = a \cdot c + b \cdot c$

Eine Menge R mit zwei (binären) Verknüpfungen $+$: $R \times R \rightarrow R, \cdot$: $R \times R \rightarrow R$ heißt Ring, wenn:
 (1) $(R, +)$ ist abelsche Gruppe (mit neutr. Element $0 \in R$)
 (2) (R, \cdot) ist assoziativ, kommutativ, und es gibt ein neutrales Element 1 in R
 (3) Distributivges.: $\forall a, b, c \in R$ $(a + b) \cdot c = a \cdot c + b \cdot c$

Sei R ein Ring, dann heißt eine Teilmenge $R' \subset R$ Unterring falls:
 (1) Bezüglich Addition ist $R' \subset R$ Untergruppe
 (2) $\forall a, b \in R'$ ist $a \cdot b \in R'$
 (3) $1 \in R'$

Seien R, R' Ringe und $\varphi: R \rightarrow R'$ eine Abbildung, dann heißt φ Ringhomomorphismus falls $\forall a, b \in R$ gilt:
 (1) $\varphi(a + b) = \varphi(a) + \varphi(b)$
 (2) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$
 (3) $\varphi(1) = 1$

Sei R ein Ring. Der Polynomring über R ist der Ring
 $R[x] := \left\{ \sum_{i=0}^n a_i x^i \mid n \in \mathbb{N}_0 \wedge a_i \in R \right\}$
 mit Addition: $\left(\sum_{i=0}^n a_i x^i \right) + \left(\sum_{j=0}^m b_j x^j \right) := \sum_{l=0}^{\max(n,m)} a_l x^l$
 und Mult.: $\left(\sum_{i=0}^n a_i x^i \right) \cdot \left(\sum_{j=0}^m b_j x^j \right) := \sum_{l=0}^{n+m} \left(\sum_{k=0}^l a_k b_{l-k} \right) \cdot x^l$

Sei R ein Ring, $a, b \in R$. Dann heißt a Teiler von b ($a | b$) genau dann wenn es ein $c \in R$ gibt mit $a \cdot c = b$

Sei K ein Körper und f, g in $K[x]$
 Dann heißt $d \in K[x]$ ggT von f und g ($d = \text{ggT}(f, g)$), wenn:
 Leitkoeff. von $d = 1$ ($d = \sum_{i=0}^n a_i x^i$ mit $a_n = 1$)
 und $d | f$ und $d | g$, und aus $d' | f, d' | g$ folgt immer $d' | d$

Sei R ein Ring, $I \subset R$ heißt Ideal, falls $I \subset R$ additive Untergruppe und für $r \in R, a \in I$ gilt stets $r \cdot a \in I$

Für beliebigen Ring R und f_1, \dots, f_k ist
 $\langle f_1, \dots, f_k \rangle := \left\{ \sum_{i=1}^k r_i f_i \mid r_i \in R \right\} \subset R$
 das von den f_i erzeugte Ideal
 Sei $f \in R$, dann ist $\langle f \rangle = \{ n \cdot f \mid n \in R \} = f \cdot R$ ein Hauptideal

