


1. Die ganzen Zahlen

1.1 Def $b \in \mathbb{Z}$ heißt Teiler von $a \in \mathbb{Z}$, falls $\exists c \in \mathbb{Z}$:
 $bc = a$. Wir schreiben $b \mid a$,
 b teilt a .

1.2 Satz (Division mit Rest)
Seien $a, b \in \mathbb{Z}$, $b \neq 0$, dann
 $\exists!$ $q, r \in \mathbb{Z}$ mit
 $a = qb + r$, $0 \leq r < b$.
 r nennen wir Rest.

Beweis: $\exists b > 0$. Die Menge
 $\{w \in \mathbb{Z} \mid a < bw\}$ hat ein
minimales Element $q+1$. Es
gilt $qb \leq a < (q+1)b$ und für
 $r = a - qb$ gilt
 $0 \leq a - qb < (q+1)b - qb = b$.

Eindeutigkeit:

$$\text{Sei } a = q_1 b + r_1 = q_2 b + r_2$$

$\in \mathbb{Z}$ $r_2 \geq r_1$. Dann ist

$$\begin{aligned} 0 \leq r_2 - r_1 &= a - q_2 b - (a - q_1 b) \\ &= (q_1 - q_2) b \Rightarrow b \mid r_2 - r_1 \end{aligned}$$

$$\text{Aber } 0 \leq r_2 - r_1 < b \Rightarrow$$

$$0 = r_2 - r_1 \Rightarrow r_2 = r_1 \Rightarrow q_2 = q_1$$

□

1.3 Def (Kongruenz)

$$a \equiv b \pmod{m}$$

a ist kongruent zu b modulo m

$$: \Leftrightarrow m \mid a - b$$

$(\Rightarrow)$ a und b haben bei Division durch m denselben Rest.

1.4 Def Seien $a, b \in \mathbb{Z} \setminus \{0\}$.

Wir nennen $d \in \mathbb{N} \setminus \{0\}$ den größten gemeinsamen Teiler von a und b , $\text{ggT}(a, b)$, wenn

1) $d \mid a, d \mid b$

2) $\forall c \in \mathbb{Z} : c \mid a \text{ und } c \mid b \Rightarrow c \mid d$.

1.5 Bemerkung: Es gibt höchstens einen $\text{ggT}(a, b)$: Angenommen, d, d' erfüllen beide 1), 2) aus 1.4.

Wende 2) auf d an, so folgt $d \mid d'$,

genauso $d' \mid d \Rightarrow \exists c : c \cdot d = d'$,

$$\exists c' : c' \cdot d' = d \Rightarrow c \cdot c' \cdot d' = d'$$

$$\Rightarrow c \cdot c' = 1. \text{ Da } c, c' \in \mathbb{Z} \Rightarrow$$

$$c, c' \in \{1, -1\}, \text{ da } d, d' > 0 \Rightarrow$$

$$c = c' = 1 \Rightarrow d = d'.$$

Gibt es einen ggT ? Ja, Beweis konstruktiv:

1.6 Euklidischer Algorithmus:

Da $\text{ggT}(a, b) = \text{ggT}(-a, b) = \text{ggT}(-a, -b)$
können wir $\mathbb{Z}$ ohne Einschränkung,
o. B. d. A. ohne Beschränkung der Allgemeinheit)
annehmen, daß $0 < b < a$.

1. Schritt: $a_1 := a, b_1 := b$

2. Schritt: Berechne eine Division mit

$$\text{Rest} \quad a_1 = q_1 b_1 + r_1$$

Wenn $r_1 = 0$ dann ist

$$\text{ggT}(a, b) = b_1, \text{ stop.}$$

Sonst setze $a_2 := b_1, b_2 := r_1$

und wiederhole Schritt 2 mit
diesen.

Beweis:

Terminierung: Der Algorithmus liefert bei jedem

Durchlauf von Schritt 2 eine Zahl r_i

mit $0 \leq r_i = b_{i+1} < b_i$. In jedem

Schritt wird b echt kleiner, das geht
nur endlich oft und endet nach
endlich vielen Schritten mit $r_n = 0$.

Korrektheit: Sei N die Anzahl der

Durchläufe von Schritt 2,

Induktion nach N .

| A: Falls $N=1$ gilt $a = a_1 = q_1 b_1 + r_1$
mit $r_1=0$, also $a = q_1 \cdot b$, also
 $b \mid a$. Damit $b \mid a$, $b \mid b$ und $\forall c$
mit $c \mid a$, $c \mid b$ gilt $c \mid b \Rightarrow$
 $b = \text{ggT}(a, b)$.

| V: Wenn der Algorithmus nach N Schritten
endet, liefert er den ggT der
Anfangszahlen.

| S: Wir zeigen: auch wenn er nach $N+1$
Schritten stoppt, liefert er den ggT der
Anfangszahlen.

Sei (a_1, b_1) ein Zahlenpaar, für das
er nach $N+1$ Schritten stoppt.

Dann stoppt er für (a_2, b_2) bereits
nach N Schritten, nach IV gilt also
 $b_{N+1} = \text{ggT}(a_2, b_2) =: d$.

Das erste Durchlaufen liefert

$$a_1 = q_1 b_1 + b_2 \quad \text{und} \quad a_2 = b_1.$$

$$\text{Da } d \mid a_2, d \mid b_2 \Rightarrow d \mid b_1 \text{ und}$$

$$d \mid q_1 b_1 + b_2, \text{ also } d \mid a_1.$$

$$\text{Sei } c \in \mathbb{Z} \text{ mit } c \mid a_1, c \mid b_1$$

$$\Rightarrow c \mid a_2 \text{ und } c \mid a_1 - q_1 b_1$$

$$\Rightarrow c \mid a_2 \text{ und } c \mid b_2 \Rightarrow c \mid d \quad \square$$

Bsp $a = 104, b = 47$

i	(a_i, b_i)	$a_i - q_i b_i = b_{i+1}$
1	$(104, 47)$	$104 - 2 \cdot 47 = 10$
2	$(47, 10)$	$47 - 4 \cdot 10 = 7$
3	$(10, 7)$	$10 - 1 \cdot 7 = 3$
4	$(7, 3)$	$7 - 2 \cdot 3 = 1$
5	$(3, 1)$	$3 - 3 \cdot 1 = 0$

$\Rightarrow \text{ggT}(104, 47) = 1.$

Rückwärtseinsetzen liefert noch mehr:

$$\begin{aligned}
 1 &= 7 - 2 \cdot 3 = 7 - 2 \cdot (10 - 1 \cdot 7) = \\
 &= 3 \cdot 7 - 2 \cdot 10 = 3 \cdot (47 - 4 \cdot 10) - 2 \cdot 10 = \\
 &= 3 \cdot 47 - 14 \cdot 10 = 3 \cdot 47 - 14 \cdot (104 - 2 \cdot 47) \\
 &= (-14) \cdot 104 + 31 \cdot 47.
 \end{aligned}$$

1.7 Satz Seien $a, b \in \mathbb{Z} \setminus \{0\}, d \in \mathbb{N}$

$d = \text{ggT}(a, b) \Leftrightarrow$

- 1) $\exists r, s \in \mathbb{Z}$ mit $d = ra + sb$
- 2) Jede ganze Zahl der Form $ra + sb$ ist durch d teilbar.

"Bézout-Gleichung"

Beweis:

- " $\Rightarrow$ " 1) euklidischer Algorithmus
mit Rückwärtseinsetzen
2) klar

" $\Leftarrow$ " Sei $d' = ra + sb$ eine Zahl, die
1) + 2) erfüllt, sei $d = \text{ggT}(a, b)$.

Wegen " $\Rightarrow$ " $\exists r', s' \in \mathbb{Z}$ mit
 $d = r'a + s'b$ und d erfüllt 2).

Da $d' = ra + sb$ folgt mit 2) für d :
 $d \mid d'$. Weil $d = r'a + s'b$ und d'

n.v. 2) erfüllt, folgt $d' \mid d$.

Damit gilt $d = d'$.

□

1.8 Satz (Chinesischer Restsatz)

Seien $n_1, \dots, n_r \in \mathbb{N}_{>0}$ paarweise
teilerfremd (i.e. $\text{ggT}(n_i, n_j) = 1$

$\forall i \neq j$), $a_1, \dots, a_r \in \mathbb{Z}$, dann
ist das Kongruenzgleichungssystem

$$x \equiv a_1 \pmod{n_1}$$

$$\vdots$$

$$x \equiv a_r \pmod{n_r}$$

lösbar. Die Lösung ist eindeutig
mod $n := n_1 \cdot \dots \cdot n_r$.

Beweis: Setze $\hat{n}_i = \frac{n}{n_i}$ und
schreibe mit dem euklidischen
Algorithmus und Rückwärtseinsetzen
 $1 = \text{ggT}(n_i, \hat{n}_i) = x_i n_i + y_i \hat{n}_i$.

Dann ist $y_i \hat{n}_i \equiv 0 \pmod{n_j} \quad \forall j \neq i$
 $y_i \hat{n}_i \equiv 1 \pmod{n_i}$

Setze $x = \sum_{i=1}^r a_i y_i \hat{n}_i$, dann gilt

$$x \equiv a_i \pmod{n_i} \quad \forall i.$$

Zahlen der Form $x + kn$ mit
 $k \in \mathbb{Z}$ lösen das Kongruenzgleichungss-
system ebenso.

Sind x, x' Lösungen, dann gilt

$$n_i \mid (x - x') \quad \forall i \quad \Rightarrow$$

$$n \mid (x - x') \quad \Rightarrow \text{die Lösung}$$

ist eindeutig mod n . $\square$

Bsp Löse $x \equiv 1 \pmod{5}$

$$x \equiv 3 \pmod{6}$$

$$x \equiv -2 \pmod{7}$$

$$n = 5 \cdot 6 \cdot 7 = 210$$

$$\hat{n}_1 = 6 \cdot 7 = 42$$

$$\hat{n}_2 = 5 \cdot 7 = 35$$

$$\hat{n}_3 = 5 \cdot 6 = 30$$

$$\text{ggT}(5, 42): \quad 42 = 8 \cdot 5 + 2$$

$$5 = 2 \cdot 2 + 1$$

$$\begin{aligned} \Rightarrow 1 &= 5 - 2 \cdot 2 = 5 - 2 \cdot (42 - 8 \cdot 5) \\ &= (-2) \cdot 42 + 17 \cdot 5 \end{aligned}$$

$$\text{ggT}(6, 35): \quad 35 = 5 \cdot 6 + 5$$

$$6 = 1 \cdot 5 + 1$$

$$\begin{aligned} \Rightarrow 1 &= 6 - 5 = 6 - (35 - 5 \cdot 6) \\ &= (-1) \cdot 35 + 6 \cdot 6 \end{aligned}$$

$$\text{ggT}(7, 30) : \quad 30 = 4 \cdot 7 + 2$$

$$7 = 3 \cdot 2 + 1$$

$$\Rightarrow 1 = 7 - 3 \cdot 2 = 7 - 3 \cdot (30 - 4 \cdot 7) \\ = (-3) \cdot 30 + 13 \cdot 7$$

Setze

$$x = 1 \cdot (-2) \cdot 42 + 3 \cdot (-1) \cdot 35 + (-2) \cdot (-3) \cdot 30 \\ = -9$$

$$-9 \equiv 1 \pmod{5}, \quad -9 \equiv 3 \pmod{6}, \quad -9 \equiv -2 \pmod{7}$$

Die kleinste positive Lösung ist

$$-9 + 210 = 201.$$

$$201 \equiv 1 \pmod{5},$$

$$201 \equiv 3 \pmod{6}, \quad \text{denn } 198 = 33 \cdot 6$$

$$201 \equiv -2 \pmod{7}, \quad \text{denn } 203 = 29 \cdot 7$$

Den chinesischen Restsatz werden wir noch verallgemeinern.

1.9 Def Seien $a, b \in \mathbb{Z}$.

$m \in \mathbb{Z}$ heißt kleinstes gemeinsames

Vielfaches von a, b , $m = \text{kgV}(a, b)$,

wenn

$$1) \quad a|m, \quad b|m$$

$$2) \quad \text{Für } m' \in \mathbb{Z} \text{ mit } a|m', \quad b|m' \\ \text{gilt } m|m'.$$

Das kgV ist bis auf Vorzeichen eindeutig (Übung).

1.10 Def $p \in \mathbb{N}$ heißt Primzahl,
falls $p > 1$ und p besitzt keine
weiteren positiven Teiler außer 1
und p .

Anders gesagt:

falls $p = ab$ mit $a, b \in \mathbb{N}_{>0}$,
so folgt $a = 1$ oder $b = 1$.

1.11 Def $a \in \mathbb{Z}$ heißt zerlegbar /
reduzibel, wenn $\exists \quad b \neq \pm 1, \quad c \neq \pm 1,$
 $b, c \in \mathbb{Z}$ mit $a = bc$.

Eine von ± 1 verschiedene Zahl, die
nicht zerlegbar ist, heißt Primzahl.

1.12 Satz Seien $a, b, c, d, e \in \mathbb{Z}$.

1) Sei $\text{ggT}(c, d) = 1$ und $c \mid de$
 $\Rightarrow c \mid e$.

2) $p \neq 0, 1, -1$ ist Primzahl $\Leftrightarrow$
 $\forall a, b \in \mathbb{Z} : p \mid ab$ gilt
 $p \mid a$ oder $p \mid b$.

Beweis:

1) $\exists r, s : 1 = rc + sd \Rightarrow$
 $e = erc + esd$. Da $c \mid de$
 $\Rightarrow c \mid esd$, da auch
 $c \mid erc$ folgt $c \mid e$.

2) " $\Leftarrow$ " Sei $p = ab \Rightarrow p \mid ab$
 $\Rightarrow \exists p \mid a$, also $a = rp$ für
ein $r \in \mathbb{Z} \Rightarrow p = b rp \Rightarrow$
 $br = 1$. Da $b, r \in \mathbb{Z}$ folgt
 $b = r = 1$ oder $b = r = -1$
 $\Rightarrow p$ ist nicht zerlegbar $\Rightarrow$

p ist Primzahl.

" $\Rightarrow$ " Sei p Primzahl und $p \nmid ab$.

Angenommen $p \nmid a$. Da p Primzahl ist, hat es nur die Teiler $\pm 1, \pm p$

$\Rightarrow \text{ggT}(p, a) = 1 \stackrel{1)}{\Rightarrow} p \nmid b. \quad \square$

1.13 Satz (Eindeutige Primfaktorzerlegung)

Jedes $0 \neq n \in \mathbb{Z}$ lässt sich in eindeutiger Weise als $n = u p_1 \cdots p_k$ schreiben, wobei $u = \pm 1$ das Vorzeichen ist und $1 < p_1 \leq \cdots \leq p_k$ Primzahlen.

Beweis: Falls $n < 0$ setze $u = -1$, sonst $u = 1$. Betrachte $n > 0$.

Existenz: Per Induktion nach n .

$n = 2$ ist Primzahl. Ist $n > 2$ Primzahl, so ist die gewünschte Darstellung $k = 1, p_1 = n$.

Ist $n > 2$ keine Primzahl, dann ist $n = ab$ mit $a, b > 1$.

Da $a, b < n$ gibt es die

gesuchte Darstellung für a, b nach Induktionsvoraussetzung. Nach Umsortieren gibt es damit auch die gesuchte Darstellung für n .

Eindeutigkeit: Induktion über k .

Sei $k=1$, $n = p_1$ Primzahl.

Falls $p_1 = p_1' \cdots p_\ell'$ so folgt $\ell=1$ und $p_1 = p_1'$ nach Def von Primzahl.

Sei $k > 1$, $n = p_1 \cdots p_k = p_1' \cdots p_\ell'$

$\Rightarrow p_k \mid p_1' \cdots p_\ell' \xrightarrow{1.12.2)} \exists i:$

$p_k \mid p_i'$. Da beide prim sind,

folgt $p_k = p_i' \Rightarrow p_1 \cdots p_{k-1} = p_1' \cdots p_{i-1}' p_{i+1}' \cdots p_\ell'$

Da nach Induktionsvoraussetzung für Produkt von $k-1$ Primzahlen die Eindeutigkeit gegeben ist, folgt, daß diese Faktoren gleich sind.

Damit sind auch die Faktoren
von $p_1 \dots p_{k-1} p_k = p_1' \dots p_i' \dots p_k'$
gleich. $\square$

1.14 Satz (Euklid)

Es gibt unendlich viele Primzahlen.

Beweis: Angenommen, es gäbe endlich
viele Primzahlen, $p_1, \dots, p_n > 0$.

$$\text{Setze } N = \prod_{i=1}^n p_i + 1.$$

Wegen des Satzes 1.13 über die
Primfaktorzerlegung $\exists$ Primzahl p ,
die N teilt $\Rightarrow \exists i = 1, \dots, n :$

$$p = p_i \Rightarrow p_i \mid N - \prod_{j=1}^n p_j = 1$$

$$\Rightarrow p_i \mid 1 \quad \text{↯} \quad \square$$

Notation: Für $x \in \mathbb{R}$ setze

$$\lfloor x \rfloor := \max \{ n \in \mathbb{Z} \mid n \leq x \}$$

$$\lceil x \rceil := \min \{ n \in \mathbb{Z} \mid n \geq x \}$$

die untere / obere Gaußklammer.

Bemerkung:

Sei $n \in \mathbb{N}$, $n > 1$, n keine Primzahl.
Ein Primteiler p von n erfüllt

$$p \leq \lfloor \sqrt{n} \rfloor.$$

Daraus ergibt sich ein Primzahltest:
 $n > 1$ ist Primzahl $\Leftrightarrow n$ ist durch
keine Primzahl $p \leq \lfloor \sqrt{n} \rfloor$ teilbar.

Sieb des Eratosthenes:

Um alle positiven Primzahlen $\leq N$
zu bestimmen, streiche aus der
Liste aller ganzen Zahlen $2, \dots, N$
alle Vielfachen von 2 außer 2,
alle Vielfachen von 3 außer 3, ...

Nach $\lfloor \sqrt{N} \rfloor$ kann man aufhören.

Es bleiben nur Primzahlen stehen.

2. Gruppen

2.1 Definition und erste Beispiele, Untergruppen, Gruppe homomorphismen

2.1.1 Def Eine Gruppe ist eine Menge G zusammen mit einer Verknüpfung (d.h. einer Abb)

$$*: G \times G \longrightarrow G : (x, y) \mapsto x * y,$$

so daß folgende Eigenschaften gelten:

1) (Assoziativität) $\forall x, y, z \in G:$

$$(x * y) * z = x * (y * z)$$

Wir schreiben dann $x * y * z$

2) (Existenz des Neutralen)

$$\exists e \in G : e * x = x \quad \forall x \in G$$

3) (Existenz von Inversen)

$$\forall x \in G \exists x' \in G : x' * x = e$$

Man nennt x' das Inverse von x und schreibt x^{-1} .

Wir bezeichnen die Gruppe mit

$(G, *)$ oder auch nur G , falls $*$ aus dem Kontext klar ist.

Gilt zusätzlich

4) (Kommutativität) $x * y = y * x$
 $\forall x, y \in G$

so heißt G abelsch oder kommutativ.

Bsp 1) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ sind
abelsche Gruppen. 0 ist neutrales, $-x$ das
inverse zu x .

2) $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$ sind
abelsche Gruppen. 1 ist neutrales, $\frac{1}{x}$
das inverse zu x .

3) Ist M eine Menge, so ist
 $\text{Sym}(M) := \{f: M \rightarrow M, f \text{ bijektiv}\}$
mit der Komposition von Abb
eine Gruppe. Es gilt Assoziativität
(Analysis), id_M ist Neutrales,
die Umkehrabb (Analysis) das inverse.
Enthält M mehr als 2 Elemente,
so ist $\text{Sym}(M)$ nicht abelsch:

Seien x_1, x_2, x_3 in M , definiere

$$f: M \rightarrow M: \begin{cases} x_1 \mapsto x_2 \\ x_2 \mapsto x_3 \\ x_3 \mapsto x_1 \\ x \mapsto x \quad \forall x \neq x_1, x_2, x_3 \end{cases}$$

$$g: M \rightarrow M: \begin{cases} x_1 \mapsto x_2 \\ x_2 \mapsto x_1 \\ x \mapsto x \quad \forall x \neq x_1, x_2 \end{cases}$$

Dann ist $f \circ g(x_1) = f(x_2) = x_3$
 $g \circ f(x_1) = g(x_2) = x_1$

also ist $f \circ g \neq g \circ f$.

Ist $M = \{1, \dots, n\}$, so schreiben wir
 $S_n := \text{Sym}(M)$ und bezeichnen
 sie als Permutationsgruppe oder
symmetrische Gruppe und ihre
 Elemente als Permutationen.

Mehr zur Permutationsgruppe S_n :

Wir beschreiben ein Element $\sigma \in S_n$

wie folgt:

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$$

2.1.2 Def:

Eine Permutation σ , für die es
 $\{a_1, \dots, a_k\} \cup \{b_1, \dots, b_{n-k}\} = \{1, \dots, n\}$

gibt mit

$$b = \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_{k-1} & a_k & b_1 & \dots & b_{n-k} \\ a_2 & a_3 & a_4 & \dots & a_k & a_1 & b_1 & \dots & b_{n-k} \end{pmatrix}$$

heißt k-Zykel.

Wir schreiben kurz $b = (a_1 a_2 \dots a_k)$.

$$((a_1 a_2 \dots a_k) = (a_2 a_3 \dots a_k a_1) \text{ etc})$$

Ein 2-Zykel heißt Transposition.

Eine Transposition (ij) vertauscht genau zwei Zahlen i und j und hält die anderen fest.

Eine Transposition $(i \ i+1)$ heißt

Nachbartransposition.

Bsp

$$\mathcal{S}_2 = \{ \text{id}, (12) \}$$

$$\mathcal{S}_3 = \{ \text{id}, (12), (13), (23), (123), (132) \}$$

2.1.3 Satz $|\mathcal{S}_n| = n! := n \cdot (n-1) \cdot \dots \cdot 1$

Beweis: Um eine Permutation σ festzulegen, müssen wir Bilder für alle Zahlen $1, \dots, n$ festlegen. Für 1 gibt es n Möglichkeiten, für 2 $n-1$ (denn $\sigma(1)$ geht nicht) usw. Also gibt es insgesamt $n!$ Möglichkeiten, die alle Elemente der S_n liefern. $\square$

2.1.4 Prop

Jede Permutation kann als Produkt von disjunkten Zykeln geschrieben werden.

Bsp $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 5 & 6 & 1 & 2 & 8 & 7 \end{pmatrix} \in S_8$

Verfolge die Zahlen:

$$1 \mapsto 3 \mapsto 5 \mapsto 1$$

$$2 \mapsto 4 \mapsto 6 \mapsto 2$$

$$7 \mapsto 8 \mapsto 7$$

$$\sigma = (135)(246)(78).$$

Beweis von 2.1.4 : Konstruktiv :

Für $i \in \{1, \dots, n\}$ ist i in einem Zykel, man kann ihn mit i beginnend aufschreiben: $(i \ b(i) \ b^2(i) \ \dots \ b^{k-1}(i))$ bis man k findet mit $b^k(i) = i$.

Es ist nicht möglich, daß $b^k(i) = b^j(i)$ für $0 < j < k$, denn da b bijektiv ist, folgt dann $b^{k-j+1}(i) = i$ und man hätte schon früher geendet.

Betrachte ein j , das nicht im ersten Zykel liegt und fahre fort. $\square$

Zykel der Länge 1 lassen wir weg:

$$(12)(36)(4)(5) = \begin{pmatrix} 1 & 2 & 3 & 6 & 4 & 5 \\ 2 & 1 & 6 & 3 & 4 & 5 \end{pmatrix} \\ = (12)(36)$$

2.1.5 Lemma Sei $(G, *)$ eine

Gruppe.

1. Das neutrale Element ist eindeutig bestimmt und hat die Eigenschaft

$$x * e = x \quad \forall x \in G.$$

2. Sei $x \in G$. Das Inverse x^{-1} ist eindeutig bestimmt und erfüllt

$$x * x^{-1} = e.$$

3. Für $x, y \in G$ gilt $(x^{-1})^{-1} = x$
und $(x * y)^{-1} = y^{-1} * x^{-1}.$

Übung.

Notation: Als Verknüpfungssymbol verwenden wir oft „ $\cdot$ “ und schreiben dann 1 für das Neutrale und x^{-1} oder $\frac{1}{x}$ für Inverse. Verwenden wir „ $+$ “, schreiben wir 0 bzw. $-x$. Dies ist nur eine Schreibweise, angelehnt an die üblichen Bsp.

Notation: Sei $(G, \cdot)$ eine Gruppe, $x \in G$. Wir setzen $x^0 := e$ und für $i \in \mathbb{N}$ rekursiv $x^i := x \cdot x^{i-1}$,
und $x^{-i} = (x^{-1})^i$.

Man sieht leicht, daß $x^i \cdot x^j = x^{i+j},$

$$(x^i)^j = x^{ij}.$$

2.1.6 Def Die Ordnung $|G|$ einer Gruppe ist die Anzahl ihrer Elemente, falls G endlich ist, und ∞ sonst.

2.1.7 Def Erfüllt G nur 2.1 (1), so heißt G Halbgruppe (Bsp: $(\mathbb{N}_{>0}, +)$), erfüllt G 2.1 (1) und (2), so heißt G Monoid (Bsp: $(\mathbb{N}, +)$).

2.1.8 Bsp (freie Gruppen)

Sei $A = \{a, b, c, \dots\}$ eine endliche Menge. Ein Wort über dem Alphabet A ist eine endliche Folge $w = a_1 \dots a_n$ mit $n \in \mathbb{N}_{>0}$, $a_i \in A$. Ist w^1 ein weiteres Wort, so definiert Hintereinanderschreiben eine assoziative Verknüpfung $\circ$ auf der Menge aller Wörter G . Wir erhalten eine Halbgruppe. Fügen wir das leere Wort

e hinzu, ist $(G, \circ)$ Monoid.

Fügen wir weitere Buchstaben $a^{-1}, b^{-1}, \dots$

mit der Regel $aa^{-1} = a^{-1}a = e$,

$bb^{-1} = b^{-1}b = e, \dots$ zu, so erhalten

wir die freie Gruppe erzeugt von A .

Zum Beispiel ist $(\mathbb{Z}, +)$ die freie Gruppe erzeugt von $\{1\}$.

2.1.9 Def Sei $(G, \cdot)$ eine Gruppe.

$U \subset G$ heißt Untergruppe, falls $(U, \cdot)$ (mit der Einschränkung $\cdot|_{U \times U}$) wieder eine Gruppe ist

2.1.10 Proposition: (Untergruppenkriterium)

Sei $(G, \cdot)$ Gruppe und $\emptyset \neq U \subset G$.

U ist Untergruppe $\Leftrightarrow$

$\forall x, y \in U: xy \in U$ und $x^{-1} \in U$.

Beweis:

" $\Rightarrow$ " Damit $(U, \cdot)$ Gruppe ist, muß
• $\cdot|_{U \times U} : U \times U \rightarrow U$ gelten, also $xy \in U$
für $x, y \in U$. N.V. existieren die
Inversen in U . Da die Inversen in
 G eindeutig sind, ist x^{-1} (das
Inverse in G) in U .

" $\Leftarrow$ " Da $xy \in U \quad \forall x, y \in U$ ist
• $\cdot|_{U \times U} : U \times U \rightarrow U$. Assoziativität gilt,
da sie in G gilt. Da $U \neq \emptyset$
 $\exists x \in U$, n. V. $\exists$ damit auch $x^{-1} \in U$,
und dann $x^{-1} \cdot x = e \in U$. Da e
Neutrales in G ist, ist es das auch
in U . Die Inversen existieren
n. V. in U . $\square$

Bsp 1) $(\{-1, 1\}, \cdot)$ ist Untergruppe
von $(\mathbb{Q} \setminus \{0\}, \cdot)$.

2) $\mathbb{Z} \subset \mathbb{Q}$, $\mathbb{Z} \subset \mathbb{R}$, $\mathbb{Q} \subset \mathbb{R}$
jeweils mit $+$ sind Untergruppen.

3) Sei $n \in \mathbb{Z}$, setze $n\mathbb{Z} := \{nz \mid z \in \mathbb{Z}\}$
 die Menge aller durch n teilbaren
 Zahlen. $(n\mathbb{Z}, +)$ ist Untergruppe
 von $(\mathbb{Z}, +)$ (Übung).

2.1.11 Def Seien $(G, \cdot)$, $(H, *)$
 Gruppen, $f: G \rightarrow H$ eine Abbildung.
 f heißt (Gruppen-) Homomorphismus
 (struktur erhaltende Abb), falls
 $\forall x, y \in G \quad f(x \cdot y) = f(x) * f(y)$.

Bsp 1) $a \in \mathbb{R}$, $f_a: (\mathbb{R}, +) \rightarrow (\mathbb{R}, +):$
 $x \mapsto ax$
 $f_a(x+y) = a(x+y) = ax + ay = f_a(x) + f_a(y)$
 $\Rightarrow f_a$ ist Morphismus.

2) Sei $(G, \cdot)$ eine Gruppe, $g \in G$.
 Die Rechtstranslation

$$R_g: G \rightarrow G: x \mapsto xg$$

und die Linkstranslation

$$L_g: G \rightarrow G: x \mapsto gx$$

sind keine Gruppenhomomorphismen
 für $g \neq e$, denn z.B.

$L_g(g \cdot g) = g^3$, $L_g(g) \cdot L_g(g) = g^4$,
 wäre $g^3 = g^4$, so würde durch Mult
 mit $(g^3)^{-1}$ folgen $e = g \nabla$.

3) Die Konjugation mit g

$$\hat{i}_g: G \rightarrow G: x \mapsto g^{-1} x g$$

ist ein bijektiver Morphismus:

$$\begin{aligned}
 \hat{i}_g(x \cdot y) &= g^{-1} x \cdot y \cdot g = g^{-1} x e y g \\
 &= g^{-1} x g g^{-1} y g = \hat{i}_g(x) \cdot \hat{i}_g(y)
 \end{aligned}$$

Surjektiv: $g x g^{-1}$ ist Urbild von x ,

$$\text{denn } \hat{i}_g(g x g^{-1}) = g^{-1} g x g^{-1} g = e x e = x$$

Injektiv: Sei $\bar{g}^{-1} x g = \bar{g}^{-1} y g$, dann

folgt nach Mult von links mit g
 und von rechts mit g^{-1} $x = y$.

2.1.12 Lemma

Seien $f_1: (G_1, \cdot) \rightarrow (G_2, *)$

$f_2: (G_2, *) \rightarrow (G_3, \times)$

Gruppenhomomorphismen, dann ist auch

$f_2 \circ f_1: (G_1, \cdot) \rightarrow (G_3, \times)$ ein

Gruppenhomomorphismus.

Beweis: $f_2 \circ f_1(g \cdot h) = f_2(f_1(g \cdot h)) =$

$$f_2(f_1(g) * f_2(h)) = f_2(f_1(g)) * f_2(f_1(h)).$$

□

2.1.13 Def Sei $f: (G, \cdot) \rightarrow (H, *)$
ein Morphismus.

- 1) f heißt Monomorphismus, falls f injektiv.
- 2) " Epimorphismus, falls f surjektiv.
- 3) " Isomorphismus, falls f bijektiv.
- 4) " Endomorphismus, falls $G = H$.
- 5) " Automorphismus, falls f
Endo- + Isomorphismus ist.

Existiert für Gruppen G, H ein Isomorphismus, so schreiben wir $G \cong H$, G ist isomorph zu H .
Isomorphie ist eine Äquivalenzrelation (siehe 2.1.12 + 2.1.14).

Bsp Die Konjugation id ist ein Automorphismus.

2.1.14 Proposition: Sei $f: (G, \cdot) \rightarrow (H, *)$
ein Morphismus.

- 1) $f(e_G) = e_H$
- 2) $f(x^{-1}) = f(x)^{-1} \quad \forall x \in G$

3) Ist f bijektiv, so ist $f^{-1}: H \rightarrow G$ ein Morphismus.

4) Ist $\emptyset \neq U \subset G$ Untergruppe, so ist auch $f(U) \subset H$ Untergruppe.

5) Ist $\emptyset \neq V \subset H$ Untergruppe, so ist auch $f^{-1}(V) \subset G$ Untergruppe.

6) Im f ist Untergruppe von H .

7) $\text{Ker } f := f^{-1}(e_H)$, der Kern von f , ist Untergruppe von G .

Beweis:

1) $f(e_G) = f(e_G \cdot e_G) = f(e_G) * f(e_G)$, durch Multiplikation mit $f(e_G)^{-1}$ erhält man $f(e_G) = e_H$.

2) $f(x^{-1} \cdot x) = f(e_G) = e_H = f(x^{-1}) \cdot f(x)$, aus der Eindeutigkeit der Inversen folgt $f(x)^{-1} = f(x^{-1})$.

3) Ist f bijektiv, so existiert die Umkehrabb $f^{-1}: H \rightarrow G$.

Seien $u, v \in H$, setze $x = f^{-1}(u)$, $y = f^{-1}(v)$, dann gilt

$$\begin{aligned} f^{-1}(u * v) &= f^{-1}(f(x) * f(y)) = \\ f^{-1}(f(x \cdot y)) &= \text{id}_G(x \cdot y) = \end{aligned}$$

$$x \cdot y = f^{-1}(u) \cdot f^{-1}(v).$$

4) Seien $u, v \in f(U) \Rightarrow$

$$\exists x, y \in U : f(x) = u, f(y) = v.$$

Da U Untergruppe ist, gilt

$$xy \in U \Rightarrow f(xy) = f(x) * f(y) = u * v \in f(U).$$

Auch $x^{-1} \in U$ und damit $f(x^{-1}) \stackrel{2)}{=} f(x)^{-1} = u^{-1} \in f(U).$

Da $U \neq \emptyset$ ist $f(U) \neq \emptyset$, damit ist das Untergruppukriterium 1.8.4 erfüllt und $f(U) \subset H$ ist Untergruppe

5) genauso

6) folgt aus 4), da G Untergruppe von G ist.

7) folgt aus 5), da $(\{e_H\}, *)$ Untergruppe von H ist. □

2.1.15 Lemma

Sei $f: (G, \cdot) \rightarrow (H, *)$ Morphismus,

f injektiv $\Leftrightarrow \text{Ker } f = \{e_G\}$

Beweis: " $\Rightarrow$ " Da $f(e_G) = e_H$, ist $e_G \in \text{Ker } f$. Für $x \in \text{Ker } f$ gilt $f(x) = e_H \Rightarrow f(x) = f(e_G) \Rightarrow x = e_G$, da f injektiv $\Rightarrow \text{Ker } f = \{e_G\}$.

" $\Leftarrow$ " Seien $x, y \in G$ mit $f(x) = f(y)$
 $\Rightarrow e_H = f(x) * f(y)^{-1} = f(x) * f(y^{-1}) = f(x \cdot y^{-1})$
 $\Rightarrow x \cdot y^{-1} \in \text{Ker } f = \{e_G\}$
 $\Rightarrow x y^{-1} = e_G \Rightarrow x = y$.

□

2.2 Faktorgruppen

2.2.1 Def Sei G eine Gruppe und $\sim$ eine Äquivalenzrelation auf G . $\sim$ heißt mit der Gruppenstruktur verträglich, falls $\forall x, y, z \in G$:
 $x \sim y \Rightarrow zx \sim zy$.

2.2.2 Def Sei $U \subset G$ eine Untergruppe.

Für U definieren wir eine Äquivalenzrelation auf G durch

$$x \sim y \quad :\Leftrightarrow \quad x^{-1}y \in U$$

für $x, y \in G$.

2.2.3 Lemma Die Relation $\sim$ ist eine mit der Gruppenstruktur verträgliche Äquivalenzrelation.

Eine Äquivalenzklasse ist

$$[x] = x \cdot U := \{x \cdot u \mid u \in U\}$$

Beweis:

Reflexivität: $x \sim x$, da $x^{-1}x = e \in U$

Symmetrie: $x \sim y \Rightarrow x^{-1}y \in U \Rightarrow$
 $(x^{-1}y)^{-1} = y^{-1}(x^{-1})^{-1} = y^{-1}x \in U$
 $\Rightarrow y \sim x$

Transitivität: $x \sim y, y \sim z \Rightarrow$
 $x^{-1}y, y^{-1}z \in U \Rightarrow (x^{-1}y) \cdot (y^{-1}z) =$
 $x^{-1}(yy^{-1})z = x^{-1}ez = x^{-1}z \in U$
 $\Rightarrow x \sim z$

Verträglich: $x \sim y \Rightarrow x^{-1}y \in U \Rightarrow$
 $x^{-1}z^{-1}zy = (zx)^{-1}zy \in U \Rightarrow$
 $zx \sim zy.$

Sei $[x]$ eine Äquivalenzklasse,
 $y \in [x] \Rightarrow x \sim y \Rightarrow x^{-1}y \in U,$
setze $u := x^{-1}y$, dann ist $y = xu$
 $\Rightarrow [x] \subset x \cdot U.$

Sei $y \in x \cdot U \Rightarrow y = x \cdot u$ für ein
 $u \in U \Rightarrow x^{-1}y = u \in U \Rightarrow$
 $y \in [x]$
 $\Rightarrow [x] = x \cdot U. \quad \square$

Die Menge aller Äquivalenzklassen
wird mit G/U bezeichnet,
 $x \cdot U$ heißt Restklasse von x
modulo U .

Bsp: $G = \mathbb{Z}$, $U = n\mathbb{Z}$, $G/U = \mathbb{Z}/n\mathbb{Z}$
Eine Äquivalenzklasse $[x]$ ist
die Restklasse $\{y \mid y \equiv x \pmod{n}\}.$

$\mathbb{Z}/n\mathbb{Z}$ erbt die Gruppenstruktur von $\mathbb{Z}$, i.e. die Verknüpfung $[a] + [b] = [a+b]$ ist wohldefiniert.

Das funktioniert nicht für beliebige U , sondern nur für Normalteiler:

2.2.4 Def Eine Untergruppe $U \subset G$ heißt normal oder Normalteiler falls

$\forall x \in G, u \in U$ gilt

$$xu \in U \quad U \cdot x := \{u' \cdot x \mid u' \in U\}.$$

Dies ist äquivalent zu:

$\forall x \in G, u \in U$ gilt

$$xux^{-1} \in U.$$

Ist G abelsch, so ist jede Untergruppe Normalteiler.

Bsp 1) $n\mathbb{Z}$ ist Normalteiler.

2) $U = \{id, (12)\} \subset S_3$ ist kein Normalteiler, denn für $b = (23) \in S_3$ gilt $b \circ (12) \circ b^{-1} = (23)(12)(23) = (13) \notin U$

2.2.5 Satz Sei $(G, \cdot)$ eine Gruppe.

1) Eine Untergruppe $U \subset G$ ist
Normalteiler $\Leftrightarrow$ auf G/U
ist die Operation

$$[x] \cdot [y] = [xy] \in G/U$$

wohldefiniert.

2) Ist $U \subset G$ Normalteiler, dann ist
 $(G/U, \cdot)$ mit der in 1) definierten
Verknüpfung eine Gruppe mit
Neutralem $[e] = U$, für
inverse gilt $[x]^{-1} = [x^{-1}]$.

Man nennt G/U die Faktorgruppe
von G nach U .

Die Restklassenabbildung

$$\pi: G \longrightarrow G/U: x \longmapsto [x]$$

ist ein Gruppenhomomorphismus
mit $\text{Ker}(\pi) = U$.

Beweis:

1) " $\Rightarrow$ " Sei U ein Normalteiler,
 $[x], [y] \in G/U$. Sei $x' \in [x]$,
 $y' \in [y] \Rightarrow x' = xu, y' = yv$
für $u, v \in U$.

$$\Rightarrow x'y' = xuyv.$$

Wir wollen zeigen, $x'y' \in [x \cdot y] = xyU$,
also $xuyv \in xyU$. Da $v \in U$
ist dies äquivalent zu

$$xuy \in xyU \Leftrightarrow uy \in yU$$

Das gilt, da U Normalteiler ist.

" $\Leftarrow$ " Sei $x \in G, u \in U$.

$$U = e \cdot U = [e] = [x \cdot x^{-1}]$$

$$\begin{aligned} \text{n.v.} \quad [x] \cdot [x^{-1}] &= [x \cdot u] \cdot [x^{-1}] \\ &= [x \cdot u \cdot x^{-1}] \end{aligned}$$

also ist $xux^{-1} \in U$ und

U ist Normalteiler.

2) Wegen 1) ist die Operation wohldefiniert.

$$[e] \cdot [x] = [e \cdot x] = [x], \text{ also}$$

ist $[e] = U$ Neutrales.

$$[x^{-1}] \cdot [x] = [x^{-1}x] = [e],$$

also ist $[x^{-1}]$ Inverses zu x .

$$\pi(x \cdot y) = [x \cdot y] = [x] \cdot [y]$$

$$= \pi(x) \cdot \pi(y)$$

$$\text{Kern}(\pi) = \{x \in G \mid [x] = [e] = U\}$$

$$= U.$$

□

Bsp $n\mathbb{Z} \subset \mathbb{Z}$ ist Normalteiler

Die Addition in $\mathbb{Z}/n\mathbb{Z}$ ist wohldefiniert.

Wir schreiben $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$.

2.2.6 Satz (Homomorphiesatz)

Ist $f: G \rightarrow H$ ein Morphismus,
dann gilt:

1) $\text{Ker}(f)$ ist Normalteiler von G

2) Die durch f induzierte Abb.

$$\tilde{f}: G/\text{Ker}f \longrightarrow \text{Im } f:$$
$$[x] \longmapsto f(x)$$

ist wohldefiniert und ein Isomorphismus.

Beweis:

1) Sei $u \in \text{Ker}(f)$, $x \in G \Rightarrow$

$$f(x u x^{-1}) = f(x) f(u) f(x)^{-1}$$
$$= f(x) e_H f(x)^{-1} = f(x) f(x)^{-1} = e_H$$
$$\Rightarrow x u x^{-1} \in \text{Ker}(f)$$

Damit ist $\text{Ker}(f)$ Normalteiler.

2) Sei $[x] = [x'] \in G/\text{Ker}f$

$$\Rightarrow x \sim x' \Rightarrow x^{-1} x' \in \text{Ker}f$$

$$\Rightarrow e_H = f(x^{-1} x') = f(x)^{-1} f(x')$$

$$\Rightarrow f(x) = f(x')$$

Also ist $\tilde{f}$ wohldefiniert.

$$\tilde{f}([x] \cdot [y]) = \tilde{f}([xy]) = f(xy) = f(x) f(y) = \tilde{f}([x]) \tilde{f}([y])$$

also ist $\tilde{f}$ Morphismus.

$\tilde{f}$ ist offensichtlich surjektiv.

Seien $[x], [y] \in G/\ker f$ mit

$$f(x) = \tilde{f}([x]) = \tilde{f}([y]) = f(y)$$

$$\Rightarrow e_{\#} = f(x)^{-1} f(y) = f(x^{-1}y)$$

$$= f(x^{-1}y) \Rightarrow x^{-1}y \in \ker f$$

$$\Rightarrow x \sim y \Rightarrow [x] = [y], \text{ also}$$

ist $\tilde{f}$ injektiv. $\square$

2.3 Erzeugnisse und zyklische Gruppen

2.3.1 Def Sei G eine Gruppe,

$S \subset G$ eine Teilmenge.

Dann ist

$$\langle S \rangle := \bigcap_{\substack{S \subset U \subset G \\ U \text{ Untergruppe}}} U$$

die von S erzeugte Untergruppe.

2.3.2 Lemma:

$$\langle S \rangle = \{ \text{Wörter in } S \text{ bzw. den Inversen der Elemente von } S \}$$

Beweis:

" $\subset$ ", da die rechte Seite Untergruppe U mit $S \subset U$ ist

" $\supset$ ", die rechte Seite ist in jeder Untergruppe, die S enthält, und daher auch im Schnitt. $\square$

Bsp

1) $GL_n(K)$ (die Gruppe der invertierbaren $n \times n$ -Matrizen über einem Körper K) wird erzeugt von Elementarmatrizen, da man jede Matrix vollen Rangs mit Elementarmatrizen (elementaren Zeilenumformungen) auf die reduzierte Zeilenstufenform, also die

Einheitsmatrix $\mathbb{1}_n$, bringen kann.

2) $\mathbb{Z}$ wird von 1 erzeugt.

3) S_n wird von Nachbartranspositionen erzeugt (siehe ggf. Lineare Algebra 1).

4) $\mathbb{Z}/n\mathbb{Z}$ wird von $[1]$ erzeugt.

2.3.3 Def Sei G eine Gruppe,

$$K = \left\{ \underbrace{(ab)(ba)^{-1}}_{= aba^{-1}b^{-1}} \mid a, b \in G \right\} \quad \text{ist}$$

die Menge der Kommutatoren in G ,

$$[G, G] := \langle K \rangle \quad \text{die von } K$$

erzeugte Kommutatorgruppe.

Bemerkung: $[G, G] = \{e\} \Leftrightarrow G$ abelsch

2.3.4 Lemma $[G, G]$ ist ein

Normalteiler.

Beweis: Sei $g \in G$, $u = aba^{-1}b^{-1} \in [G, G]$.

Dann gilt

$$gu g^{-1} = gaba^{-1}b^{-1}g^{-1} =$$

$$ga(g^{-1}g)b(g^{-1}g)a^{-1}(g^{-1}g)b^{-1}g^{-1} =$$

$$gag^{-1}gbg^{-1}ga^{-1}g^{-1}gb^{-1}g^{-1} =$$

$$gag^{-1}gbg^{-1}(gag^{-1})^{-1}(gbg^{-1})^{-1} \in [G, G].$$

Mit Produkten von Kommutatoren verfährt
man analog. $\square$

2.3.5 Korollar Sei G eine Gruppe,

U ein Normalteiler.

G/U ist abelsch $\Leftrightarrow U \supset [G, G]$

Insbesondere ist $G/[G, G]$ abelsch.

Beweis: $[a][b] = [b][a] \quad \forall a, b \Leftrightarrow$

$$[a][b][a]^{-1}[b]^{-1} = [e] \quad \forall a, b \Leftrightarrow$$

$$[aba^{-1}b^{-1}] = [e] \quad \forall a, b \Leftrightarrow$$

$$U = e \cdot U = [e] \supset \langle U \rangle = [G, G] \quad \square$$

2.3.6 Def

Eine Gruppe G heißt zyklisch,
falls $\exists g \in G : G = \langle g \rangle$

Bsp: $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ sind zyklisch.

2.3.7 Def

Sei $g \in G$, $\text{ord}(g) := |\langle g \rangle|$
heißt die Ordnung von g .

Bsp:

1) Für $[2] \in \mathbb{Z}/6\mathbb{Z}$ ist $\text{ord}([2]) = 3$,
denn $\langle [2] \rangle = \{ [0], [2], [4] \}$

2) Die Ordnung eines k -Zykels
in S_n ist k .

2.3.8 Satz (Lagrange)

Sei G eine endliche Gruppe, U eine Untergruppe. Dann gilt

$$|G| = |U| \cdot |G/U|$$

Insbesondere ist die Ordnung einer Untergruppe ein Teiler der Gruppenordnung.

Beweis: Die Äquivalenzrelation für U (siehe Def. 2.2.2) zerlegt G disjunkt in $|G/U|$ Äquivalenzklassen. Wegen 2.2.3 hat jede Klasse die Form $x \cdot U$, also $|x \cdot U| = |U|$ Elementen. $\square$

2.3.9 Korollar

Sei G endlich, $g \in G$. Dann gilt $\text{ord}(g) \mid |G|$.

2.3.10 Korollar

Sei G eine Gruppe von Primzahlordnung. Dann ist G zyklisch.

Beweis: Sei $g \in G \setminus \{e\}$. Da $\langle g \rangle \subset G$ Untergruppe ist, folgt
 $\text{ord}(g) = |\langle g \rangle| \mid |G| \stackrel{\text{Primzahl}}{\Rightarrow} |\langle g \rangle| = |G| \Rightarrow \langle g \rangle = G. \quad \square$

2.3.11 Satz Sei G zyklisch.
 Falls G unendliche Ordnung hat, so ist $G \cong \mathbb{Z}$.

Falls $|G| = m$, so ist $G \cong \mathbb{Z}_m$.

Beweis:

Sei $G = \langle g \rangle$.

Setze $f(n) := g^n$, dann ist

$f: \mathbb{Z} \rightarrow G$ ein Gruppenhomomorphismus (denn $f(n+m) = g^{n+m} = g^n \cdot g^m = f(n) \cdot f(m)$).

f ist surjektiv.

Damit ist $\text{Ker}(f) \subset \mathbb{Z}$ eine Untergruppe, also $\text{Ker}(f) = m\mathbb{Z}$ für ein m .

Falls $m=0$ ist $G \cong \mathbb{Z}$, falls

$m \neq 0$ ist $G \cong \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$.

Der erste Fall tritt ein genau dann,
wenn $|G| = \infty$, der zweite genau dann,
wenn G endlich. $\square$

2.3.12 Satz Sei G zyklisch.

Jede Untergruppe von G ist zyklisch.

Beweis: Sei $G = \langle g \rangle$ und $U = \{e\}$. Sei
 $a := \min \{ j \in \mathbb{N} \setminus \{0\} \mid g^j \in U \}$.

Beh: $U = \langle g^a \rangle$

" $\supset$ " klar.

" $\subset$ " Sei $u \in U$. Da $u \in G$

$\exists b \in \mathbb{Z}: u = g^b$.

Schreibe b nach Division mit
Rest als $b = q \cdot a + r$ mit $0 \leq r < a$.

Dann gilt $u = g^b = g^{q \cdot a + r} =$

$g^{qa} \cdot g^r = (g^a)^q \cdot g^r \Rightarrow$

$g^r = u \cdot (g^a)^{-q} \in U$

$$\Rightarrow r = 0 \Rightarrow u = (g^a)^q \in \langle g^a \rangle.$$

□

2.3.13 Satz (Untergruppen zyklischer Gruppen)

Sei G eine Gruppe, $g \in G$.

$$1) \text{ ord}(g) = \min \{n \in \mathbb{N}_{>0} \mid g^n = e\}$$

$$\text{Insbesondere } g^{\text{ord}(g)} = e, \\ \langle g \rangle = \{e, g, g^2, \dots, g^{\text{ord}(g)-1}\}$$

$$2) g^n = e \Leftrightarrow \text{ord}(g) \mid n$$

3) Hat g endliche Ordnung und
ist $f \in \mathbb{N}$, so gilt

$$\text{ord}(g^f) = \frac{\text{ord}(g)}{\text{ggT}(\text{ord}(g), f)}$$

4) Hat g endliche Ordnung n und
ist $d \in \mathbb{N}$, $d \mid n$, so sind die

Elemente von Ordnung d mit

$d \mid d$ in der von g erzeugten
zyklischen Untergruppe genau
die $g^{k \cdot \frac{n}{d}}$ mit $k \in \mathbb{N}$.

Dabei hat $g^{k \cdot \frac{n}{d}}$ Ordnung d

$$\Leftrightarrow \text{gg}^T(k, d) = 1.$$

5) Ist G zyklisch der Ordnung n ,
so gibt es zu jedem Teiler $d|n$
genau eine Untergruppe U_d der
Ordnung d .

Beweis:

1) $\langle g \rangle$ ist zyklisch, mit 2.3.7
ergibt sich $\langle g \rangle \cong \begin{cases} \mathbb{Z} \\ \mathbb{Z}_m \end{cases}$

Falls $\langle g \rangle \cong \mathbb{Z}$, so ist $\text{ord}(g) = \infty$
und $\{n \in \mathbb{N}_{>0} \mid g^n = e\}$ ist
unbeschränkt, da $f: \mathbb{Z} \rightarrow G: 1 \mapsto g$
Isomorphismus ist und $g^n = f(n) \neq e$
für $n \neq 0$.

Falls $\langle g \rangle \cong \mathbb{Z}_m$, so ist $\text{ord}(g) = m$
und $\mathbb{Z}_m \rightarrow G: [1] \mapsto g$ ist
Isomorphismus.

Da $m = \min \{n \mid \overbrace{[1] + \dots + [1]}^{n \text{ Summanden}} = 0\}$
ist auch $m = \min \{n \mid g^n = e\}$.

2) " $\Rightarrow$ " $g^n = e \Rightarrow \min \{j \mid g^j = e\} \leq n$
 $\Rightarrow \text{ord}(g) \leq n$. Sei $\text{ord}(g) = m$, schreibe
 $n = q \cdot m + r$, $0 \leq r < m$ (Division mit Rest).
 Dann ist $e = g^n = g^{q \cdot m + r} = (g^m)^q \cdot g^r$
 $= e \cdot g^r$, da $r < m$ und $g^r = e$ folgt
 $r = 0 \Rightarrow n = q \cdot m \Rightarrow m \mid n \Rightarrow$
 $\text{ord}(g) \mid n$.

" $\Leftarrow$ " $\text{ord}(g) \mid n \Rightarrow \exists q: n = q \cdot \text{ord}(g)$
 $\Rightarrow g^n = g^{q \cdot \text{ord}(g)} = (g^{\text{ord}(g)})^q = e$

3) Sei $m = \text{ord}(g)$. Sei $j \in \mathbb{N}$
 und $d = \text{ggT}(m, j)$

Beh: $\frac{m}{d} = \min \{k \in \mathbb{N}_{>0} \mid (g^j)^k = e\}$
 $= \text{ord}(g^j)$

Da $(g^j)^{\frac{m}{d}} = (g^m)^{\frac{j}{d}} = e$ ist

$\frac{m}{d} \in \{k \mid (g^j)^k = e\}$

$\Rightarrow \text{ord}(g^j) \leq \frac{m}{d}$.

Sei $r \in \{k \mid (g^j)^k = e\} \Rightarrow$

$$(g^j)^r = e \Rightarrow g^{jr} = e$$

$\Rightarrow m \mid jr \Rightarrow jr$ ist ein

gemeinsames Vielfaches von m

und j . Damit folgt

$$\frac{mr}{d} = \text{kgV}(m, j) \mid jr.$$

Insbesondere $\frac{m}{d} \mid r$.

$$\Rightarrow \frac{m}{d} \mid \min \{k \mid (g^j)^k = e\}$$

$$\Rightarrow \frac{m}{d} \mid \text{ord}(g^j)$$

Da auch $\text{ord}(g^j) \leq \frac{m}{d} \Rightarrow$

$$\frac{m}{d} = \text{ord}(g^j).$$

4) Sei d ein Teiler von n ,
 d' ein Teiler von d und

$g^j \in \langle g \rangle$ ein Element der Ordnung

$$d' = \frac{n}{\text{ggT}(n, j)}.$$

$$\Rightarrow \frac{n}{\text{ggT}(n, j)} \mid d \Rightarrow \frac{n}{d} \mid \text{ggT}(n, j)$$

Da $\text{ggT}(n, j) \mid j$ folgt $\frac{n}{d} \mid j$

$$\Rightarrow \exists k: j = k \cdot \frac{n}{d}.$$

Damit ist $g^j = g^{k \frac{n}{d}}$ in der gewünschten Form dargestellt.

Sei umgekehrt ein Element der Form $g^{k \cdot \frac{n}{d}}$ gegeben, wir wollen zeigen, daß $\text{ord}(g^{k \frac{n}{d}}) \mid d$.

$$\text{Es gilt } \text{ord}(g^{k \frac{n}{d}}) = \frac{n}{\text{ggT}(n, k \frac{n}{d})},$$

$$\text{und } \frac{n}{d} \mid \text{ggT}(n, k \frac{n}{d})$$

$$\Rightarrow \frac{n}{\text{ggT}(n, k \frac{n}{d})} \mid d$$

$$\Rightarrow \text{ord}(g^{k \frac{n}{d}}) \mid d.$$

$$\text{Es gilt } \text{ord}(g^{k \frac{n}{d}}) = d \Leftrightarrow$$

$$\begin{aligned} \frac{n}{\text{ggT}(n, k \frac{n}{d})} &= d \Leftrightarrow \frac{n}{d} = \text{ggT}(n, k \frac{n}{d}) \\ &= \text{ggT}(d \cdot \frac{n}{d}, k \cdot \frac{n}{d}) \Leftrightarrow \end{aligned}$$

$$\text{gg}^T(k, d) = 1.$$

5) Zu jedem Teiler $d|n$
 betrachte $U_d := \langle g^{\frac{n}{d}} \rangle$. Diese
 Untergruppe hat Ordnung d , da

$$\text{ord}(g^{\frac{n}{d}}) = \frac{n}{\text{gg}^T(n, \frac{n}{d})} = d.$$

Wegen 4) sind alle Elemente der
 Ordnung d (da $d|d$) von
 der Form $g^{k \frac{n}{d}}$ und damit in
 U_d enthalten.

Sei U' eine Untergruppe der
 Ordnung d . Wegen 2.3.8 ist

U' zyklisch $\Rightarrow \exists h \in G$,
 $\text{ord}(h) = d$, $U' = \langle h \rangle$.

Dann ist aber $h \in U_d \Rightarrow$

$U' \subset U_d \Rightarrow U' = U_d.$

□

2.3.14 Def Sei G eine Gruppe.

Wir definieren auf $\{U \mid U \text{ ist Untergruppe von } G\}$ eine Teilordnung durch $U \leq U' \iff U \subset U'$

Wir stellen diese Relation als Diagramm (Verband) dar.

Für $n \in \mathbb{N}_{>0}$ definieren wir auf $\{d \mid d \mid n\}$ eine Teilordnung durch $d \leq d' \iff d \mid d'$.

2.3.15 Korollar

Der Untergruppenverband einer zyklischen Gruppe der Ordnung n ist gleich dem der Teiler von n .

Beweis:

Sei $G = \langle g \rangle$. Jede Untergruppe ist von der Form $U_d = \langle g^{\frac{n}{d}} \rangle$
 $= \{ g^{k \cdot \frac{n}{d}} \mid k \in \mathbb{N} \}.$

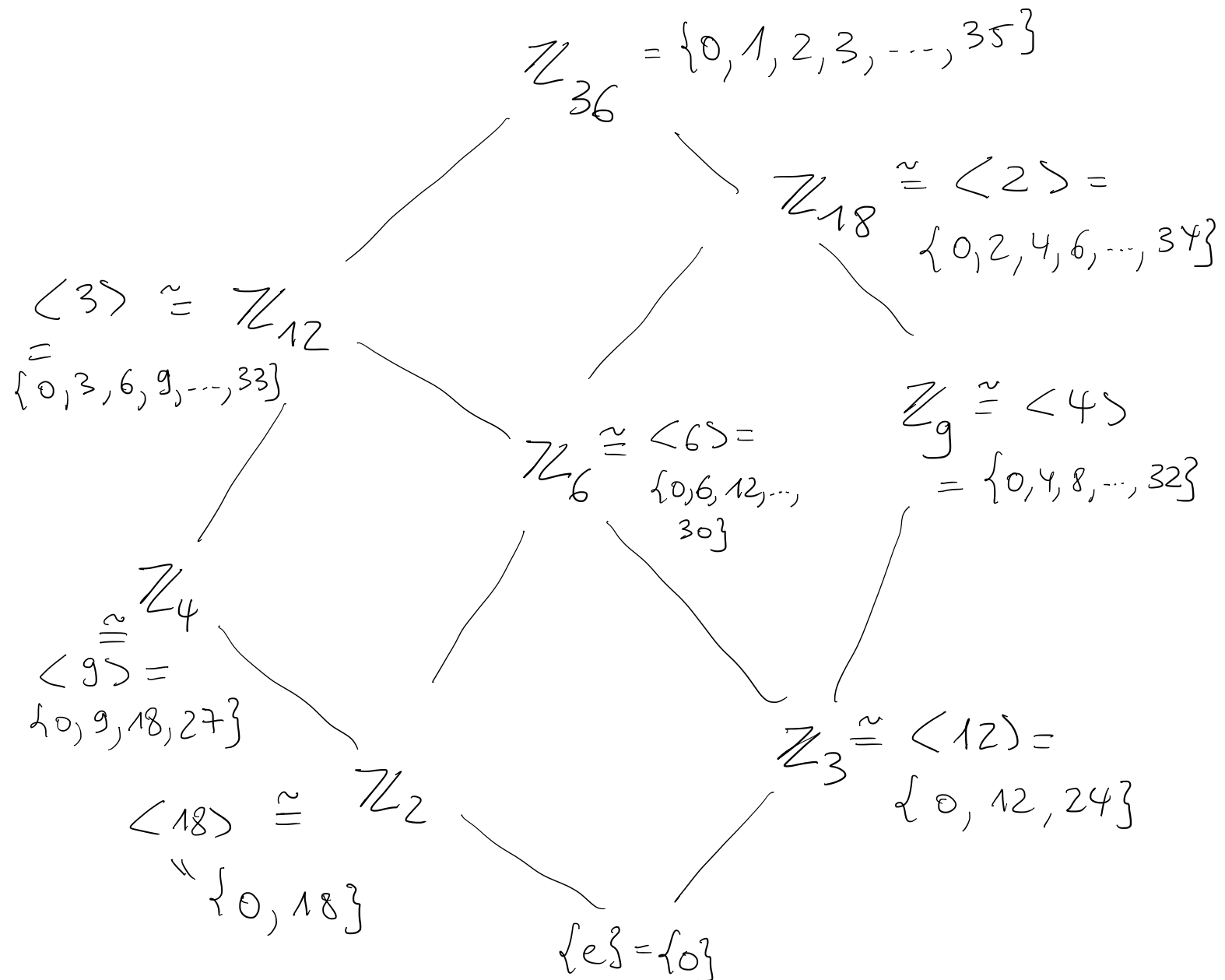
Daher gilt $U_d \subset U_{d'} \Leftrightarrow$

$\frac{n}{d}$ ist ein Vielfaches von $\frac{n}{d'}$

$$\Leftrightarrow d \mid d' \Leftrightarrow d \leq d' \quad \square$$

Bsp Der Untergruppenverband von

$\mathbb{Z}_{36}$ ist



2.4 Freie Gruppen und Relationen

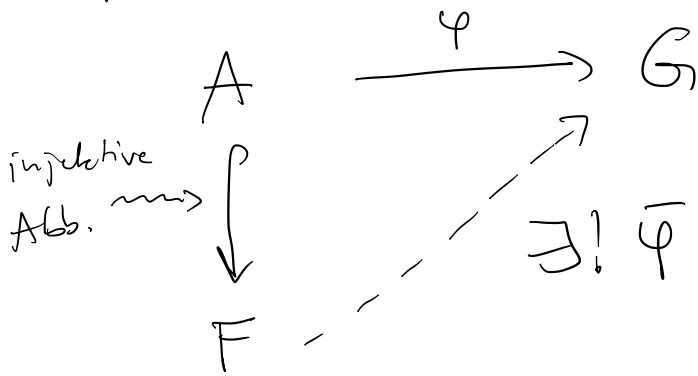
Wir verallgemeinern / abstrahieren Bsp. 2.1.8:

2.4.1 Def Sei A eine endliche Menge.

Eine Gruppe F heißt frei erzeugt von A , falls F folgende universelle Eigenschaft erfüllt:

$\forall$ Gruppe G und Abb $\varphi: A \rightarrow G$

$\exists!$ Morphismus $\bar{\varphi}: F \rightarrow G$, der φ erweitert:



Eine Gruppe heißt frei, wenn eine Menge $A \subset F$ existiert, die F frei erzeugt.

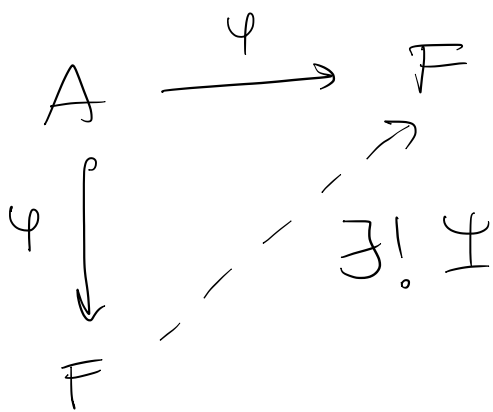
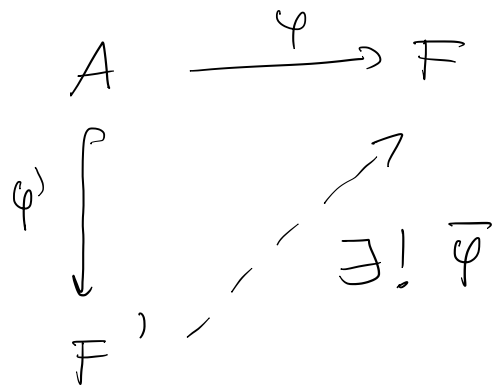
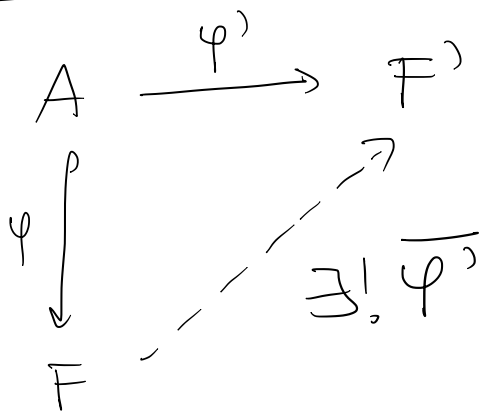
Bsp $\mathbb{Z}$ ist frei, $\mathbb{Z}$ wird frei erzeugt von 1. $\mathbb{Z}$ wird nicht von $\{2,3\}$ frei erzeugt, aber $\mathbb{Z} = \langle 2,3 \rangle$.

Insbesondere enthält nicht jede erzeugende Teilmenge eine frei erzeugende Teilmenge.

2.4.2 Prop (freie Gruppe, Eindeutigkeit)

Sei A eine endliche Menge. Dann existiert höchstens eine frei von A erzeugte Gruppe F (bis auf kanonische Isomorphie).

Beweis: Seien F, F' frei erzeugt von A .



$$\Psi = \text{id}_F$$

läßt das Diagramm kommutieren,

$$\Psi = \bar{\varphi}' \circ \bar{\varphi} \quad \text{auch,}$$

aus der Eindeutigkeit von Ψ folgt

$$\text{id}_F = \bar{\varphi}' \circ \bar{\varphi}. \quad \text{Genauso} \quad \text{id}_{F'} = \bar{\varphi} \circ \bar{\varphi}'.$$

$$\Rightarrow F \cong F'.$$

□

Kanonisch: die Isomorphismen $F \rightarrow F'$,
 $F' \rightarrow F$ sind id auf S und
sind die einzigen Isomorphismen, die
 $\text{id}|_S$ erweitern, wegen der Eindeutigkeit
in der universellen Eigenschaft.

2.4.3 Satz (freie Gruppe, Existenz)

Sei A eine endliche Menge. Dann existiert
eine von A frei erzeugte Gruppe.

Beweis: Wir zeigen, daß die Gruppe
aus Bsp. 2.18 die universelle Eigenschaft
erfüllt:

$$F = \text{Menge der Wörter in } A \text{ und } A^{-1} / \sim$$

$$= \{a_1 \dots a_n \mid n \in \mathbb{N}, a_i \in A \cup A^{-1}\} / \sim$$

wobei $\forall$ Wörter x, y , $a \in A$:

$$x a a^{-1} y \sim xy, \quad x a^{-1} a y \sim xy$$

Hinterinanderschreiben ist assoziativ,
das leere Wort ε ist neutrales, in umgekehrter
Reihenfolge schreiben und invertieren liefert
Inverse. $A \subset F$.

Sei G eine weitere Gruppe,

$\varphi: A \rightarrow G$ eine Abb.

Wir konstruieren rekursiv eine Abb φ^* von der Menge der Wörter durch:

$$\varepsilon \mapsto e$$

$$a \cdot x \mapsto \varphi(a) \cdot \varphi^*(x)$$

$$a^{-1} \cdot x \mapsto \varphi(a)^{-1} \cdot \varphi^*(x)$$

$\forall a \in A$, Wort x .

Nach Def ist φ^* kompatibel mit der Äquivalenzrelation $\sim$ auf der Menge der Wörter, und liefert damit

$\bar{\varphi}: F \rightarrow G$, ein Morphismus ist. $\square$

2.4.4 Korollar Sei F frei erzeugt von A , dann ist $\langle A \rangle = F$.

Beweis: Die freie Gruppe aus Bsp. 2.18 bzw. Satz 2.4.3 ist von A erzeugt, und sie ist eidentg. $\square$

2.4.5 Prop Sei F eine freie Gruppe. Alle freien Erzeugendensysteme haben die gleiche Anzahl, den Rang von F .

Beweis: F sei frei erzeugt von A , $|A|=n$. Die Menge der Homomorphismen $F \rightarrow \mathbb{Z}_2$, $\text{Hom}(F, \mathbb{Z}_2)$, erfüllt $|\text{Hom}(F, \mathbb{Z}_2)| = 2^n$, also hängt n nur von F ab und nicht von A . $\square$

Wir schreiben F_n für die von n Elementen frei erzeugte Gruppe.

Bsp $F_1 \cong \mathbb{Z}$

Bem 1) $\mathbb{Z} \times \mathbb{Z} = \mathbb{Z}^2$ ist nicht frei erzeugt von $\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, denn

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{ist eine Relation,}$$

die zusätzlich zu den Inversen

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} -1 \\ 0 \end{pmatrix} = e \quad \dots \quad \text{erfüllt ist.}$$

Man kann z.B. nicht $\begin{pmatrix} 1 \\ 0 \end{pmatrix} \mapsto (12)$,

$\begin{pmatrix} 0 \\ 1 \end{pmatrix} \mapsto (13) \in S_3$ abbilden, denn

somit

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \mapsto (12) \circ (13) \neq$$

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \end{pmatrix} \mapsto (13) \circ (12)$$

nicht wohl-definiert.

In der Tat ist $\mathbb{Z}^2$ nicht frei.

2) Endliche Gruppen sind nicht frei, da ein Element g endliche Ordnung hat, also $\exists r: g^r = e$ und somit gibt es eine zusätzliche Relation. Man kann nicht

$g \mapsto 1 \in \mathbb{Z}$ abbilden, da

$g^r = e \mapsto 0 \neq r = 1 + \dots + 1$ nicht wohl-definiert.

$$g^r = g \circ \dots \circ g$$



2.4.6 Korollar Eine Gruppe G ist

endlich erzeugt $(\Leftrightarrow)$

$G \cong F_n / N$ für eine freie Gruppe F_n und einen Normalteiler N .

Beweis: " $\Leftarrow$ " klar

" $\Rightarrow$ " Sei $G = \langle A \rangle$, $|A| = n < \infty$.

Mit der universellen Eigenschaft

finden wir $\pi: F_n \rightarrow G$,

der surjektiv ist, da $G = \langle A \rangle$.

Setze $N = \text{Ker}(\pi)$, dann folgt aus

dem Homomorphiesatz $G \cong F_n / N$. $\square$

2.4.7 Def

Sei G eine Gruppe, $A \subset G$.

$\langle A \rangle^\Delta$ ist der kleinste Normalteiler von G , der A enthält:

$$\langle A \rangle^\Delta = \bigcap_{\substack{A \subset N \subset G \\ N \text{ Normalteiler}}} N.$$

2.4.8 Lemma

$$\langle A \rangle^\Delta = \left\{ g_1 \alpha_1^{\varepsilon_1} g_1^{-1} \cdots g_m \alpha_m^{\varepsilon_m} g_m^{-1} \mid \right. \\ \left. m \in \mathbb{N}, \varepsilon_i \in \{\pm 1\}, g_i \in G, \alpha_i \in A \right\}$$

Siehe Lemma 2.3.2.

2.4.9 Def (Erzeuger und Relationen)

$$\langle A \mid R \rangle := F / \langle R \rangle^\Delta,$$

wobei F die frei von A erzeugte Gruppe ist, $\langle R \rangle^\Delta$ ist die Gruppe erzeugt von A mit Relationen R .

$\langle A \mid R \rangle$ heißt Präsentation der Gruppe.

Bsp

$$1) \langle x \mid x^n \rangle \cong \mathbb{Z}_n$$

$$2) \langle x, y \mid xyx^{-1}y^{-1} \rangle \cong \mathbb{Z}^2$$

$\tilde{\mathbb{Z}}$ man schreibt manchmal
auch $xyx^{-1}y^{-1} = e$
oder $xy = yx$

$$\begin{aligned} x &\longmapsto \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ y &\longmapsto \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{aligned}$$

$$3) \langle x, y \mid xyx^{-1} = y^2, yxy^{-1} = x^2 \rangle \\ = \{e\} :$$

$$\begin{aligned} x &= x(yx^{-1}x)y^{-1} = (xyx^{-1})xy^{-1} \\ &= y^2xy^{-1} = y(yxy^{-1}) = \\ &= yx^2 \quad \Rightarrow \quad e = yx \quad \Rightarrow \end{aligned}$$

$$y = x^{-1}$$

$$y^{-2} = x^2 = yxy^{-1} = yy^{-1}y^{-1} = y^{-1}$$

$$\Rightarrow y = e \quad \Rightarrow x = e.$$

$$4) \quad \langle a, b \mid a^2 = b^2 = (ab)^3 = e \rangle \stackrel{\sim}{=} S_3:$$

$$a \mapsto (12), \quad b \mapsto (13)$$

$$ab \mapsto (12)(13) = (132), \quad \text{es gilt} \\ (132)^3 = e, \quad \text{dies ist verträglich} \\ \text{mit der Relation } (ab)^3 = e.$$

Die Gruppe $G = \langle a, b \mid a^2 = b^2 = (ab)^3 = e \rangle$ besteht aus Wörtern in a, b , wobei a und b abwechselnd hintereinander kommen.

$$\text{Es gilt } (bab)^2 = babbab = e \\ \text{und } (aba)(bab) = (ab)^3 = e$$

$$\Rightarrow aba = (bab)^{-1} = bab.$$

Möglichkeiten für Wörter außer a, b, e :

$$\text{I. } abab \dots ab \quad \text{II. } abab \dots aba$$

$$\text{III. } babab \dots ba \quad \text{IV. } babab \dots bab$$

I Höchstens 2 Wiederholungen, da $(ab)^3 = e$.

$$\text{Aber } abab = babb = ba.$$

Also nur ab .

$$\text{II } ababa = aabaa = b$$

Also nur aba .

III Nur ba , IV $bab = aba$

$$\Rightarrow G = \{e, a, b, ab, ba, aba\}$$

Die Zuordnung $a \mapsto (12)$,

$b \mapsto (13)$ heißt einen

Isomorphismus $G \rightarrow S_3$

$$\begin{array}{ccccccccc} G = \{ e & , & a & , & b & , & ab & , & ba & , & aba \} \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ S_3 = \{ id & , & (12) & , & (13) & , & (132) & , & (123) & , & (23) \} \end{array}$$

Bem: Folgende universelle Eigenschaft
gilt für Gruppen, die durch
Erzeuger und Relationen gegeben sind:

$\forall$ Gruppen G , Abb $\varphi: A \rightarrow G$

mit $\varphi^*(r) = e$ in $G \quad \forall r \in R$

(wobei φ^* den auf den Wörtern
konstruierten Morphismus aus Satz
2.4.3 (Existenz freie Gruppe) bezeichnet)

$\exists!$ Gruppenhomomorphismus

$\bar{\varphi}: \langle A \mid R \rangle \rightarrow G$ mit

$$\bar{\varphi} \circ \pi = \varphi :$$

$$\begin{array}{ccc}
 A & \xrightarrow{\varphi} & G \\
 \downarrow \pi & \nearrow \exists! \bar{\varphi} & \\
 F_{|A|} & & \\
 \downarrow & & \\
 F_{|A|} / \langle R \rangle = \langle A | R \rangle & &
 \end{array}$$

Dies folgt aus der universellen Eigenschaft für freie Gruppen, und für Faktorgruppen:

G/N , $\pi: G \rightarrow G/N$ erfüllen folgende universelle Eigenschaft: $\forall$ Gruppen H , Morphismen $\varphi: G \rightarrow H$ mit

$N \subset \text{Ker}(\varphi) \quad \exists! \bar{\varphi}: G/N \rightarrow H$
mit $\bar{\varphi} \circ \pi = \varphi :$

$$\begin{array}{ccc}
 G & \xrightarrow{\varphi} & H \\
 \downarrow \pi & \nearrow \exists! \bar{\varphi} & \\
 G/N & &
 \end{array}$$

Die universelle Eigenschaft für Faktorgruppen zeigt man wie beim Homomorphiesatz, indem wir $\bar{\varphi}([g]) = \bar{\varphi}(g \cdot N) = \varphi(g)$ setzen.

3. Ringe

3.1 Ringe und Ideale

3.1.1 Def Eine Menge R mit einer Verknüpfung $+$ $= R \times R \rightarrow R$ und $\cdot : R \times R \rightarrow R$, $(R, +, \cdot)$, heißt (kommutativer) Ring (mit 1), falls

- 1) $(R, +)$ eine abelsche Gruppe ist (mit Neutralem 0)
- 2) $(R, \cdot)$ ein kommutatives Monoid ist (mit Neutralem 1)
- 3) (Distributivität) $\forall a, b, c \in R$:
$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

Bsp

1) $\mathbb{Z}$

2) $\mathbb{Z}_n$. Wir haben bisher die abelsche Gruppe $(\mathbb{Z}_n, +)$ betrachtet.

Wir definieren zusätzlich

$$\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n : [a] \cdot [b] = [a \cdot b].$$

Dies ist wohldefiniert:

$$\text{Sei } [a'] = [a], [b'] = [b] \Rightarrow$$

$$a - a' = k \cdot n, \quad b - b' = l \cdot n \quad \text{für } k, l \in \mathbb{Z}$$

$\Rightarrow$

$$[a' \cdot b'] = [(a - kn)(b - ln)] =$$

$$[ab + n(-kb - al + kln)] = [ab].$$

Wegen der Eigenschaften der Multiplikation auf $\mathbb{Z}$ ist die Operation assoziativ und kommutativ, und $[1]$ ist Neutrales.

Die Distributivität wird auch von $\mathbb{Z}$ vererbt.

3) Jeder Körper ist ein Ring.

4) Sei K ein Körper, der Polynomring $K[x]$ ist ein Ring.

3.1.2 Lemma (Einfache Rechenregeln)

Sei R ein Ring, $x, y, z \in R$. Dann gilt:

$$1) \quad -(-x) = x$$

$$2) \quad -(x+y) = -x + (-y) = -x - y$$

$$3) \quad x + y = z \Leftrightarrow x = z - y$$

$$4) \quad x \cdot 0 = 0 \cdot x = 0$$

$$5) \quad (-x) \cdot y = x \cdot (-y) = -xy$$

$$6) \quad (-x) \cdot (-y) = xy$$

$$7) \quad x(y - z) = xy - xz$$

$$8) \quad (-1) \cdot x = -x.$$

Beweis:

1), 2) haben wir in 2.1.5 3) für beliebige Gruppen gezeigt (hier nur in der Schreibweise +).

3) " $\Rightarrow$ " Addiere $-y$ auf beiden Seiten

" $\Leftarrow$ " Addiere y "

"Kürzungsregel"

$$4) \quad 0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x \Rightarrow \\ 0 \cdot x = 0 \quad \text{wegen der Kürzungsregel.}$$

$$5) \quad xy + (-x) \cdot y = (x - x) \cdot y = 0 \cdot y = 0$$

$$\Rightarrow -xy = (-x) \cdot y$$

genauso für $x \cdot (-y)$.

$$6) \quad (-x) \cdot (-y) \stackrel{5)}{=} - (x \cdot (-y)) \stackrel{5)}{=} -(-xy) \\ \stackrel{1)}{=} xy$$

$$7) \quad x(y-z) = x(y+(-z)) = xy + x(-z) \\ = xy + (-xz) = xy - xz$$

$$8) \quad 0 = 0 \cdot x = (-1+1) \cdot x = (-1) \cdot x + x \\ \Rightarrow (-1) \cdot x = -x. \quad \square$$

3.1.3 Def Sei R ein Ring.
 $a \in R$ heißt Einheit, falls $\exists b \in R$:
 $ab = 1$.

$(R^*, \cdot)$ ist die Einheitsgruppe.

a heißt Nullteiler, falls $\exists b \neq 0$,
 $b \in R$: $ab = 0$.

Bsp

- 1) Sei K ein Körper. $K^* = K \setminus \{0\}$.
 K hat keine Nullteiler außer 0.
- 2) $\mathbb{Z}^* = \{\pm 1\}$. $\mathbb{Z}$ hat keine Nullteiler außer 0.
- 3) $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$
2 und 3 sind Nullteiler, da $2 \cdot 3 = 6 = 0$
4 ist Nullteiler, da $3 \cdot 4 = 12 = 0$
 $\mathbb{Z}_6^* = \{1, 5\}$, denn $1 \cdot 1 = 1$ und $5 \cdot 5 = 25 = 1$.
 $\Rightarrow \mathbb{Z}_6 = \{\text{Nullteiler}\} \cup \{\text{Einheiten}\}$
- 4) In $K[x]$ gibt es keine Nullteiler außer 0.
 $(K[x])^* = K^*$

3.1.4 Def Sei $\emptyset \neq U \subset R$, so daß U mit der Einschränkung von $+$ und $\cdot$ wieder ein Ring ist (nicht notwendig mit 1), dann ist U ein Unterring.

Bsp $2\mathbb{Z} \subset \mathbb{Z}$ ist ein Unterring (ohne 1).

3.1.5 Def Seien R, S Ringe.

$\varphi: R \rightarrow S$ heißt Ringhomomorphismus

$$\Leftrightarrow \varphi(a+b) = \varphi(a) + \varphi(b)$$

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) \quad \forall a, b \in R.$$

Sind R und S Ringe mit 1 , so verlangen wir außerdem $\varphi(1_R) = 1_S$.

Bem Bild und Kern von Ringhomomorphismen sind Untertringe (siehe Z.1.14 für Gruppen).

3.1.6 Def Sei R ein kommutativer

Ring mit 1 . Ein Ideal $I \subset R$

ist eine nicht-leere Teilmenge mit

$$a+b \in I, \quad r \cdot a \in I$$

$$\forall a, b \in I, \quad r \in R.$$

3.1.7 Lemma Ein Ideal ist eine

Untergruppe bez $+$.

Beweis:

$$\text{Da } r \cdot a \in I \quad \forall r \in R, a \in I$$

$$\text{folgt } (-1) \cdot a = -a \in I \quad \forall a \in I.$$

Damit erfüllt I das Untergruppenkriterium bez. $+$. $\square$

Bemerkung: Wegen Lemma 3.1.6, und da die Addition in R abelsch ist, ist $(R/I, +)$ abelsche Gruppe mit $[0] = 0 + I$ als Neutralem. Die Def eines Ideals ist so gewählt, daß auch die Mult nach R/I vererbt wird:

3.1.8 Satz (Quotientenring / Faktorring)

Sei R ein Ring, I ein Ideal.

Dann ist R/I mit den repräsentantenweise definierten Operationen ein Ring mit $[1] = 1 + I$ als Neutralem bez. $\cdot$, der Quotientenring / Faktorring.

Beweis:

Betrachte $[r_1] = [r_1']$, $[r_2] = [r_2']$

in R/I , dann ist $r_1' = r_1 + a$,
 $r_2' = r_2 + b$ mit $a, b \in I \Rightarrow$

$$[r_1' \cdot r_2'] = [(r_1 + a)(r_2 + b)] =$$

$$\left[r_1 r_2 + \underbrace{r_1 b}_{\in I} + \underbrace{r_2 a}_{\in I} + \underbrace{ab}_{\in I} \right]$$

$$= [r_1 r_2].$$

Damit ist die Multiplikation wohldefiniert. Die weiteren Eigenschaften werden vererbt. $\square$

3.1.9 Lemma: Seien R, S Ringe,

$\varphi: R \rightarrow S$ ein Ringhomomorphismus.

Dann ist $\text{Ker}(\varphi)$ ein Ideal.

Beweis: Seien $a, b \in \text{Ker}(\varphi) \Rightarrow$

$$\varphi(a+b) = \varphi(a) + \varphi(b) = 0 + 0 = 0 \Rightarrow$$

$a+b \in \text{Ker}(\varphi)$. Sei $r \in R \Rightarrow$

$$\varphi(r \cdot a) = \varphi(r) \cdot \varphi(a) = \varphi(r) \cdot 0 = 0$$

$$\Rightarrow r \cdot a \in \text{Ker}(\varphi). \quad \square$$

3.1.10 Satz (Homomorphiesatz)

Seien R, S Ringe, $\varphi: R \rightarrow S$ ein Ringhomomorphismus.

Dann ist $R / \text{Ker} \varphi \cong \text{Im } \varphi$.

Beweis: Aus dem Homomorphiesatz für Gruppen 2.2.6 folgt, daß

es einen Isomorphismus $\tilde{\varphi}: R/\ker(\varphi) \rightarrow \text{Im } \varphi$ der additiven Gruppen gibt.

Dieser ist Ringhomomorphismus, denn

$$\begin{aligned}\tilde{\varphi}([r_1] \cdot [r_2]) &= \varphi(r_1 \cdot r_2) = \\ \varphi(r_1) \cdot \varphi(r_2) &= \tilde{\varphi}([r_1]) \cdot \tilde{\varphi}([r_2]).\end{aligned}$$

□

3.1.11 Def Sei R ein Ring,
 $A \subset R$.

$$\langle A \rangle := \bigcap_{\substack{A \subset I \subset R \\ I \text{ Ideal}}} I$$

heißt das von A erzeugte Ideal.

3.1.12 Lemma

$$\langle a_1, \dots, a_n \rangle = \left\{ \sum_{i=1}^n r_i a_i \mid r_i \in R \right\}$$

Beweis Übung.

Bemerkung: Lemma 3.1.12 gilt analog für $\langle A \rangle$, $|A| = \infty$, dann läßt man rechts nur endliche Summen zu.

Bsp $\langle 1 \rangle = R$.

3.2 Der Polynomring

3.2.1 Def Sei R ein Ring.

Der Polynomring $R[x]$ ist definiert als

$$R[x] = \{ a_0 + a_1 x + \dots + a_n x^n, a_i \in R, n \in \mathbb{N} \}$$

Wir definieren für

$$f = \sum_{k=0}^n a_k x^k \quad \text{und} \quad g = \sum_{k=0}^m b_k x^k \in R[x]$$

die Summe

$$f + g = \sum_{k=0}^{m+n} (a_k + b_k) x^k,$$

wobei wir die Konvention verwenden,
daß $a_k = 0$ für $k > n$ und
 $b_k = 0$ für $k > m$,

und das Produkt

$$f \cdot g = \sum_{k=0}^{m+n} \left(\sum_{i=0}^k a_i b_{k-i} \right) x^k$$

(das ist $(a_n x^n + \dots + a_0) \cdot (b_m x^m + \dots + b_0)$
ausmultipliziert).

Insbesondere ist für

$$f = x^i = 1 \cdot x^i + 0 \cdot x^{i-1} + \dots + 0$$

$$g = x^j = 1 \cdot x^j + 0 \cdot x^{j-1} + \dots + 0$$

$$f \cdot g = x^i \cdot x^j = \sum_{k=0}^{i+j} \underbrace{\left(\sum_{l=0}^k a_l b_{k-l} \right)}_{\substack{\text{falls } k < i+j, \text{ ist} \\ \text{immer einer der beiden} \\ \text{Koeffizienten} = 0.}} x^k = x^{i+j}$$

Wie man leicht nachrechnet, ist $R[x]$ ein kommutativer Ring mit 1.

$$\text{Ist } f = \sum_{k=0}^n a_k x^k \text{ und } a_n \neq 0,$$

so heißt $n =: \deg(f)$ der

Grad von f . Wir setzen $\deg(0) = -\infty$.

Der Leitkoeffizient von $f \neq 0$, $LC(f)$,
ist a_n , wobei $n = \deg(f)$.

Es gilt

$$\deg(f+g) \leq \max\{\deg f, \deg g\} \text{ und}$$

$$\deg(f+g) = \max\{\deg f, \deg g\} \Leftrightarrow$$

$$\deg f \neq \deg g \text{ oder } \deg f = \deg g \text{ und } LC(f) \neq -LC(g)$$

$$\deg(f \cdot g) \leq \deg f + \deg g \quad \text{und} \\ \deg(f \cdot g) = \deg f + \deg(g) \Leftrightarrow$$

$$LC(f) \cdot LC(g) \neq 0$$

Bsp: In $\mathbb{Z}_6[x]$ ist

$$(2x + 1) \cdot (3x^2 + 2x + 1) =$$

$$6x^3 + (2 \cdot 2 + 3 \cdot 1)x^2 + (2 \cdot 1 + 1 \cdot 2)x$$

$$+ 1 \cdot 1 = 0x^3 + 1 \cdot x^2 + 4 \cdot x + 1$$

$$= x^2 + 4x + 1.$$

Bem Wir erhalten Polynomringe
in mehreren Veränderlichen
rekursiv durch

$$R[x_1, \dots, x_n] := R[x_1, \dots, x_{n-1}][x_n]$$

3.2.2 Def (K -Algebra)

Ein K -Vektorraum, auf dem zusätzlich eine Multiplikation $\circ: A \times A \rightarrow A$ definiert ist, so daß $(A, +, \circ)$ ein Ring mit 1 ist, heißt K -Algebra, falls die Skalarmultiplikation mit der Ringmultiplikation $\circ$ verträglich ist:

$$\forall \lambda \in K, x, y \in A:$$

$$\lambda \circ (x \circ y) = (\lambda \circ x) \circ y = x \circ (\lambda \circ y)$$

Ist $K = \mathbb{R}$ ein Ring und A ein $\mathbb{R}$ -Modul mit verträglicher zusätzlicher Multiplikation, so nennen wir A $\mathbb{R}$ -Algebra.

Bsp

- 1) Sei K ein Körper. $\text{Mat}(n \times n, K)$ ist K -Algebra.
- 2) Sei K ein Körper, V ein K -Vektorraum. $\text{End}_K(V)$ ist K -Algebra.
- 3) Sei R ein Ring, $\emptyset \neq X$ eine Menge.
 $\text{Abb}(X, R) = \{ f: X \rightarrow R \}$

ist mit der punktweisen Addition
 $f+g(x) = f(x) + g(x)$ und Mult
 $f \cdot g(x) = f(x) \cdot g(x) \quad \forall x \in X$

ein Ring.

Wir definieren zusätzlich die Skalar-
multiplikation

$$(\lambda \cdot f)(x) = \lambda \cdot f(x) \quad \forall x \in X, \lambda \in \mathbb{R}$$

und erhalten so eine $\mathbb{R}$ -Algebra.

Bemerkung: Wir können eine $\mathbb{R}$ -Algebra
auch auffassen als einen (kommutativen) Ring
 $(A, +, \cdot)$ und einen
Ringhomomorphismus $\varphi: \mathbb{R} \rightarrow A$,
der die Skalarmultiplikation darstellt
($\lambda \mapsto \lambda \cdot 1_A$).

3.2.3 Bsp Sei R ein Ring mit 1 ,
dann ist die charakteristische Abb.

$$\chi: \mathbb{Z} \rightarrow R: n \mapsto n \cdot 1_R = \underbrace{1_R + \dots + 1_R}_{n\text{-Mal}}$$

ein Ringhomomorphismus.

Durch χ wird R zu einer $\mathbb{Z}$ -Algebra.

$$\forall n \in \mathbb{Z}, r \in R: X(n) \cdot r = (1_R + \dots + 1_R) \cdot r \\ = r + \dots + r = r \cdot (1_R + \dots + 1_R) = r \cdot X(n).$$

3.2.4 Def Seien A_1, A_2 R -Algebren,
mit $i_1: R \rightarrow A_1, i_2: R \rightarrow A_2$.

Ein Ringhomomorphismus $\varphi: A_1 \rightarrow A_2$
heißt R -Algebren-Homomorphismus,
falls $\varphi \circ i_1 = i_2$:

$$\begin{array}{ccc} A_1 & \xrightarrow{\varphi} & A_2 \\ i_1 \uparrow & \nearrow i_2 & \\ R & & \end{array}$$

Anders gesagt:

φ ist mit allen

3 Operationen verträglich:

$$\varphi(a+b) = \varphi(a) + \varphi(b)$$

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

$$\varphi(\lambda \cdot a) = \varphi(i_1(\lambda) \cdot a) =$$

$$\varphi(i_1(\lambda)) \cdot \varphi(a) = i_2(\lambda) \cdot \varphi(a)$$

$$= \lambda \cdot \varphi(a)$$

$$\forall a, b \in A_1 \\ \lambda \in R.$$

3.2.5 Satz (Universelle Eigenschaft des Polynomrings)

Sei R ein kommutativer Ring mit 1,
 A eine R -Algebra, $a \in A$.

Dann $\exists!$ R -Algebrenhomomorphismus

$$\varphi: R[x] \rightarrow A \quad \text{mit} \quad x \mapsto a,$$

den Einsetzungshomomorphismus.

Das Bild von φ heißt die von a
erzeugte Unter algebra $\langle a \rangle \subset A$.

Analog bei mehreren Veränderlichen.

Beweis: Durch $\varphi(a_0 + a_1 x + \dots + a_n x^n) =$
 $a_0 + a_1 a + \dots + a_n a^n$ ist der
eindeutige Homomorphismus gegeben. $\square$

Bsp

1) Sei V ein K -Vektorraum.
 $\text{End}_K(V)$ ist K -Algebra, und
wir kennen den Homomorphismus

$$\varphi_f: K[x] \rightarrow \text{End}_K(V) : x \mapsto f$$

bzw.

$$\varphi_A: K[x] \rightarrow \text{Mat}(n, K) : x \mapsto A$$

Das charakteristische Polynom und das Minimalpolynom eines Endomorphismus / einer Matrix sind im Kern.

2) Sei $d \in \mathbb{Z}$, $\sqrt{d} \in \mathbb{C}$,
betrachte $\varphi: \mathbb{Z}[x] \longrightarrow \mathbb{C}$
 $x \longmapsto \sqrt{d}$

Dann ist

$$\text{Im}(\varphi) = \mathbb{Z}[\sqrt{d}]$$

$$= \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}, \text{ denn } d^2 \in \mathbb{Z}.$$

Der Begriff des Ideals ist auch durch Nullstellenmengen von Polynomen motiviert:

3.2.6 Def Seien $f_1, \dots, f_r \in K[x_1, \dots, x_n]$

Setze $V(f_1, \dots, f_r) = \{p \in K^n \mid f_i(p) = 0 \forall i\}$

die affine Varietät der f_i (die

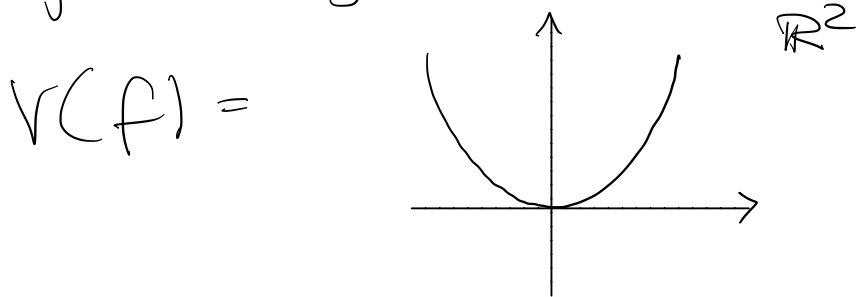
gemeinsame Nullstellenmenge).

Bsp

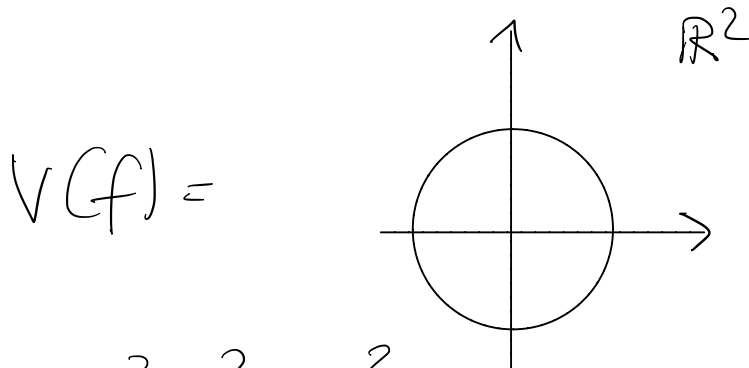
1) $V(1) = \emptyset, \quad V(0) = K^n$

2) Seien $f_i = \sum a_{ij} x_j - b_i$
lineare Polynome, $A = (a_{ij})$, $b = (b_i)$,
dann ist $V(f_1, \dots, f_r) = \text{Lös}(A, b)$
ein affiner Unterraum des K^n .

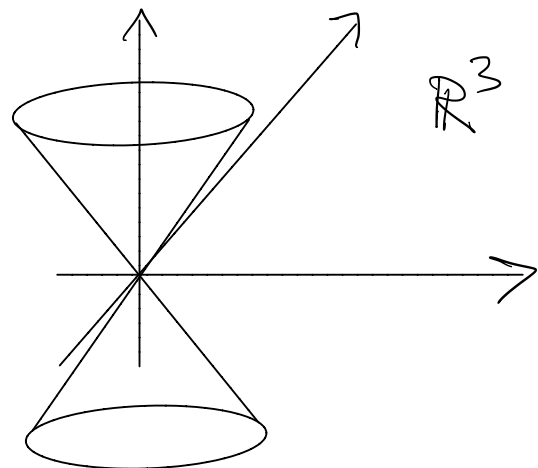
3) $f = x^2 - y \in \mathbb{R}[x, y]$



4) $f = x^2 + y^2 - 1$

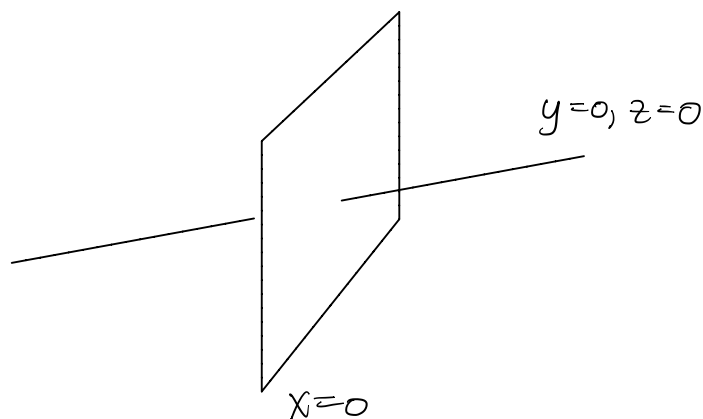


5) $f = x^2 + y^2 - z^2$



$$6) \quad f_1 = xy, \quad f_2 = xz,$$

$$V(f_1, f_2) =$$



Bemerkung:

$V(f_1, \dots, f_r)$ hängt nur von dem von den f_i erzeugten Ideal $I = \langle f_1, \dots, f_r \rangle$ ab, denn wenn $f_1(p) = \dots = f_r(p) = 0$, dann auch $\sum r_i f_i(p) = 0$ für $r_i \in K[x_1, \dots, x_n]$.

3.2.7 Def Sei $I \subset K[x_1, \dots, x_n]$ ein Ideal, dann ist

$$V(I) = \{p \in K^n \mid f(p) = 0 \quad \forall f \in I\}$$

die Nullstellenmenge von I .

Wir werden sehen (Noethersche Ringe), daß $V(I)$ eine affine Varietät ist, da jedes $I \subset K[x_1, \dots, x_n]$ endlich erzeugt ist.

Ist $V \subset K^n$, so ist

$I(V) := \{ f \in K[x_1, \dots, x_n] \mid f(p) = 0 \ \forall p \in V \}$
das Verschwundungsideal von V

3.2.8 Lemma $I(V)$ ist ein Ideal.

Beweis: Seien $f, g \in I(V) \Rightarrow$
 $f(p) = 0 = g(p) \ \forall p \in V \Rightarrow f+g(p) = 0$
 $\forall p \in V \Rightarrow f+g \in I(V)$. Sei
 $r \in K[x] \Rightarrow (r \cdot f)(p) = 0 \ \forall p \in V$
 $\Rightarrow r \cdot f \in I(V)$. $\square$

Ideale kommen bei der Betrachtung
geometrischer Objekte, die durch
polynomiale Gleichungen gegeben sind,
in natürlicher Weise vor.

3.3 Noethersche Ringe

3.3.1 Satz Sei R ein

kommutativer Ring mit 1.

Dann sind äquivalent:

- 1) Jedes Ideal $I \subset R$ ist endlich erzeugt.

2) Jede aufsteigende Kette

$I_1 \subset I_2 \subset I_3 \subset \dots$ von Idealen
wird stationär, i.e. $\exists m$ mit
 $I_m = I_{m+1} = I_{m+2} = \dots$

3) Jede nicht-leere Menge von
Idealen besitzt bezüglich der
Inklusion ein maximales Element.

Erfüllt R diese Eigenschaften, so
heißt R noethersch.

Beweis:

"1) $\Rightarrow$ 2)" : Sei $I_1 \subset I_2 \subset \dots$ eine
Kette von Idealen. Dann ist

$I = \bigcup_{i=1}^{\infty} I_i$ ein Ideal:

Sei $a, b \in I$

$\Rightarrow \exists j_1, j_2 \in \mathbb{N} : a \in I_{j_1}, b \in I_{j_2},$

$\exists j_1 < j_2$, dann ist $a \in I_{j_1} \subset I_{j_2},$

also $a, b \in I_{j_2} \Rightarrow a+b \in I_{j_2}$

$\Rightarrow a+b \in I$

Sei $a \in I, r \in R$

$\Rightarrow \exists j : a \in I_j \Rightarrow r-a \in I_j$

$$\Rightarrow r a \in I$$

¹⁾
 $\Rightarrow I = \langle a_1, \dots, a_r \rangle$ ist endlich erzeugt.

Für jedes $a_i \exists j_i$ mit $a_i \in I_{j_i}$.

Sei $k = \max \{j_i \mid i = 1, \dots, r\}$, dann

ist $a_1, \dots, a_r \in I_k \Rightarrow$

$\langle a_1, \dots, a_r \rangle \subset I_k \Rightarrow I \subset I_k$

$\Rightarrow$ ab k ist die Kette stationär. $\square$

"2) $\Rightarrow$ 3)": Angenommen, (3) gilt nicht.

Dann gibt es eine Menge M von Idealen, so daß $\forall I \in M \exists$

$I' \in M : I \subsetneq I'$

Rekursiv können wir eine Kette erzeugen, die nicht stationär wird.

"3) $\Rightarrow$ 1)": Sei I ein Ideal. Betrachte

$M = \{ J \subset I \mid J \text{ ist endlich erzeugtes Ideal} \}$

$M \neq \emptyset$, denn $\langle 0 \rangle \in M$.

Sei J ein maximales Element von

M. $\exists a_1, \dots, a_r : J = \langle a_1, \dots, a_r \rangle$.

Angenommen, $J \subsetneq I$, dann

$\exists a \in I \setminus J$, $J \subsetneq \langle a_1, \dots, a_r, a \rangle \subset I$

$\Rightarrow \langle a_1, \dots, a_r, a \rangle \in M \quad \nleftrightarrow$ zur

Maximalität von $J \Rightarrow J = I$

ist endlich erzeugt. $\square$

Bsp: $\mathbb{Z}$ ist noethersch. Jede
Untergruppe bez. + ist von der
Form $n\mathbb{Z} = \langle n \rangle$, also von
einem Element erzeugt.

3.3.2 Lemma

R hat nur zwei Ideale $\Leftrightarrow$

R ist Körper

Beweis:

" $\Rightarrow$ " $\{0\}, R$ sind Ideale. Sie sind
die einzigen. Für $a \neq 0, a \in R$

folgt damit $\langle a \rangle = R \Rightarrow$

$\exists r \in R : r \cdot a = 1 \Rightarrow a$ ist

invertierbar und R ist ein Körper.

" $\Leftarrow$ " $\{0\}, R$ sind Ideale. Sei
 $I \subset R$ ein Ideal mit $0 \neq a \in I$
 $\Rightarrow a^{-1} \cdot a = 1 \in I \Rightarrow r \cdot 1 = r \in I$
 $\forall r \in R \Rightarrow I = R \Rightarrow$ es gibt
keine weiteren Ideale.

3.3.3 Korollar Ein Körper K ist
noethersch.

Beweis: K hat nur zwei Ideale,
 $K = \langle 1 \rangle, \{0\} = \langle 0 \rangle$, beide sind
endlich erzeugt. $\square$

3.3.4 Satz (Hilberts Basissatz)

R noethersch $\Rightarrow R[x]$ noethersch

3.3.5 Korollar

R noethersch $\Rightarrow R[x_1, \dots, x_n]$ noethersch.

Beweis: Hilberts Basissatz 3.3.4 und
Induktion. $\square$

3.3.6 Korollar

Sei K ein Körper,
 $K[x_1, \dots, x_n]$ ist noethersch.

Beweis: Hilberts Basissatz 3.3.4 und Induktion mit Induktionsanfang 3.3.3. $\square$

3.3.7 Korollar

Die Verschwindungsmenge $V(I)$ eines Ideals $I \subset K[x_1, \dots, x_n]$ (Def. 3.2.7) ist eine affine Varietät (Def. 3.2.6).

Beweis: Da $I = \langle f_1, \dots, f_r \rangle$ endlich erzeugt, ist $V(I) = V(f_1, \dots, f_r)$. $\square$

3.3.8 Def.

Sei $f = a_k x^k + \dots + a_0 \in R[x]$ ein Polynom. $a_i x^i$ heißt Term von f , x^i Monom, a_i Koeffizient, $a_k x^k$ der Leitterm $LT(f)$, x^k Leitmonom ($LM(f)$). Falls $LC(f) = 1$, heißt f normiert.

Beweis von Hilberts Basissatz 3.3.4:

Angenommen, $R[x]$ wäre nicht noethersch $\Rightarrow \exists I$ nicht endlich erzeugt. Sei $0 \neq f_1 \in I$ mit

$\deg(f_1)$ minimal, $0 \neq f_2 \in I \setminus \langle f_1 \rangle$ mit
 $\deg(f_2)$ minimal, usw.

$$\Rightarrow \deg(f_1) \leq \deg(f_2) \leq \dots$$

Wir erhalten eine aufsteigende
Kette von Idealen in R :

$$\langle LC(f_1) \rangle \subset \langle LC(f_1), LC(f_2) \rangle \subset \dots$$

Da R noethersch ist, wird sie
stationär, i.e. $\exists k$:

$$\langle LC(f_1), \dots, LC(f_k) \rangle = \langle LC(f_1), \dots, LC(f_k), LC(f_{k+1}) \rangle$$

$$\Rightarrow \exists b_j \in R:$$

$$LC(f_{k+1}) = \sum_{j=1}^k b_j LC(f_j)$$

$$\text{Setze } g := \sum_{j=1}^k b_j \cdot x^{\deg(f_{k+1}) - \deg(f_j)} \cdot f_j.$$

Dann ist $g \in I$ und

$$LC(g) = \sum_{j=1}^k b_j LC(f_j) = LC(f_{k+1})$$

$$\Rightarrow \deg(g - f_{k+1}) < \deg(f_{k+1}).$$

Aber $g - f_{k+1} \in I \setminus \langle f_1, \dots, f_k \rangle$, denn
 $g - f_{k+1} \in I$ und wäre $g - f_{k+1} \in$
 $\langle f_1, \dots, f_k \rangle$, dann wäre, da $g \in$
 $\langle f_1, \dots, f_k \rangle$ auch $f_{k+1} \in \langle f_1, \dots, f_k \rangle \swarrow$.
 Also ist $R[x]$ noethersch. $\square$

3.4 Nullteilerfreie Ringe

3.4.1 Def Ein kommutativer Ring
 mit 1 ohne nicht-triviale Nullteiler (3.1.3)
 heißt nullteilerfrei oder Integritätsbereich
 oder Integritätsring.

Bsp: $\mathbb{Z}$, $K[x]$, K sind nullteilerfrei.

3.4.2 Def Sei R nullteilerfrei.

Wir definieren auf $R \times R \setminus \{0\}$ eine
 Äquivalenzrelation $(a, b) \sim (c, d) : (\Leftrightarrow)$
 $a d = c b$. Wir schreiben $\frac{a}{b}$ für
 die Äquivalenzklasse $[(a, b)]$.

Auf der Menge der Äquivalenzklassen

definieren wir durch $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$

und $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ eine Addition

und Multiplikation. Damit erhalten

wir den Quotientenkörper $\text{Quot}(R)$.

Er ist der kleinste Körper, in dem R eingebettet werden kann:

$$R \rightarrow \text{Quot}(R): a \mapsto \frac{a}{1}.$$

Bsp: $\mathbb{Z} \subset \mathbb{Q}$.

3.4.3 Def Sei K ein Körper,

$\chi: \mathbb{Z} \rightarrow K: n \mapsto n \cdot 1_K$ die charakteristische Abb. aus Def. 3.2.3.

Dann ist $\ker(\chi) \subset \mathbb{Z}$ ein Ideal, also $\ker(\chi) = p\mathbb{Z}$ für ein $p \in \mathbb{N}$.

1. Fall: $p=0 \Leftrightarrow \chi$ injektiv

Dann läßt sich χ zu einem Monomorphismus $\chi: \mathbb{Q} \hookrightarrow K$ fortsetzen.

2. Fall: $p > 0$. Dann ist

$\mathbb{Z}_p \hookrightarrow K$ wegen des Homomorphie-
satzes 3.1.10 ein Unterring von K .
Da K nullteilerfrei ist, muß auch
 $\mathbb{Z}_p$ nullteilerfrei sein.

Wäre $p = a \cdot b$ zerlegbar, so wären
 $0 \neq a, b \in \mathbb{Z}_p$ Nullteiler, denn
 $ab = p = 0 \not\equiv$. Damit ist p prim.

In beiden Fällen nennen wir
 $p = \text{char}(K)$ die Charakteristika
des Körpers K .

Bsp: $\text{char}(\mathbb{Q}) = 0$, $\text{char}(\mathbb{Z}_p) = p$.
($\mathbb{Z}_p$ ist ein Körper, siehe Übung).

3.4.4 Def Sei R ein kommutativer
Ring mit 1. Ein Ideal $P \subsetneq R$
heißt Primideal, wenn $\forall a, b \in R$
gilt: $a \cdot b \in P \Rightarrow a \in P$ oder
 $b \in P$

Ein Ideal $m \subsetneq R$ heißt maximales
Ideal, wenn für Ideale I mit

$m \subsetneq I \subset \mathbb{R}$ gilt $I = \mathbb{R}$.

3.4.5 Lemma Sei $p \in \mathbb{Z}$, $p > 0$.
 $p\mathbb{Z}$ ist Primideal $\Leftrightarrow p$ prim.

Beweis:
" $\Leftarrow$ " Sei $ab \in p\mathbb{Z} \Rightarrow p \mid ab \xrightarrow{1.12} p \mid a$ oder $p \mid b \Rightarrow a \in p\mathbb{Z}$ oder $b \in p\mathbb{Z} \Rightarrow p\mathbb{Z}$ ist Primideal
" $\Rightarrow$ " Sei $p = ab \Rightarrow ab \in p\mathbb{Z} \Rightarrow \exists a \in p\mathbb{Z} \Rightarrow p \mid a \Rightarrow \exists k: p \cdot k = a \Rightarrow p = p \cdot k \cdot b \Rightarrow k \cdot b = 1 \Rightarrow b = \pm 1 \Rightarrow p$ ist nicht zerlegbar $\Rightarrow p$ ist prim. $\square$

3.4.6 Lemma $p\mathbb{Z} \subset \mathbb{Z}$ ist maximal für p prim.

Beweis: Sei $\langle p \rangle \subsetneq I \Rightarrow \exists q \in I$, $q \notin \langle p \rangle \Rightarrow p \nmid q \Rightarrow \text{ggT}(p, q) = 1 \Rightarrow \exists k, l: kp + lq = 1 \in I \Rightarrow I = \mathbb{Z} \Rightarrow \langle p \rangle$ ist maximal. $\square$

Bsp $\langle 0 \rangle \subset \mathbb{Z}$ ist Primideal, aber nicht maximal.

$6\mathbb{Z} \subset \mathbb{Z}$ ist kein Primideal, denn $2 \cdot 3 = 6 \in 6\mathbb{Z}$ aber $2 \notin 6\mathbb{Z}$, $3 \notin 6\mathbb{Z}$.
 $6\mathbb{Z} \subset \mathbb{Z}$ ist auch nicht maximal, denn $6\mathbb{Z} \subsetneq 3\mathbb{Z} \subsetneq \mathbb{Z}$.

3.4.7 Satz Sei $I \subsetneq R$ ein Ideal.

- 1) I Primideal $\Leftrightarrow R/I$ nullteilerfrei
- 2) I maximal $\Leftrightarrow R/I$ Körper

Beweis:

1) " $\Rightarrow$ " Seien $[a], [b] \in R/I$ mit $[a] \cdot [b] = [0] \Rightarrow ab \in I \Rightarrow a \in I$ oder $b \in I \Rightarrow [a] = [0]$ oder $[b] = [0] \Rightarrow$ es gibt keine Nullteiler.

" $\Leftarrow$ " Sei $ab \in I$ aber $a \notin I$, $b \notin I$, dann ist $[a] \neq [0]$, $[b] \neq [0]$ und $[a][b] = [ab] = [0] \Rightarrow [a], [b]$ sind Nullteiler.

2) " $\Rightarrow$ " Sei m maximal, $[a] \neq [0]$
in $R/m \Rightarrow a \notin m \Rightarrow$
 $m \subsetneq \langle m, a \rangle = R \Rightarrow \exists m \in m,$
 $r \in R : m + ra = 1 \Rightarrow$
 $[ra] = [1] \in R/m \Rightarrow$
 $[a]$ ist invertierbar mit $[a]^{-1} = [r]$.

" $\Leftarrow$ " Sei R/m Körper und
 $m \subsetneq I$ ein Ideal. Sei
 $a \in I \setminus m$. Dann ist $[a] \neq [0]$
in $R/m \Rightarrow \exists b \in R :$
 $[a][b] = [1] \Rightarrow 1 - ab \in m$
 $\Rightarrow \underbrace{1 - ab}_{\in m \subset I} + \underbrace{ab}_{\in I} = 1 \in I$
 $\Rightarrow I = R$.
 $\Rightarrow m$ ist maximal. $\square$

3.4.8 Korollar I maximal $\Rightarrow I$ prim

Beweis: I maximal $\Rightarrow R/I$ Körper $\Rightarrow$
 R/I nullteilerfrei $\Rightarrow I$ prim. $\square$

3.4.9 Korollar

$\langle 0 \rangle \subset R$ ist Primideal $(\Leftrightarrow)$

R nullteilerfrei.

3.5 Faktorielle Ringe

3.5.1 Def Sei R ein kommutativer Ring,
 $a, b \in R$, a teilt b , $a \mid b$,
falls $\exists c \in R : ca = b$.

3.5.2 Lemma (Regeln für Teilbarkeit)
Sei R nullteilerfrei, seien $a, b, c, d \in R$.

- 1) (Kürzungsregel) $c \neq 0, ac = bc \Rightarrow a = b$
- 2) $a \mid 0, a \mid a, 1 \mid a$
- 3) $a \mid b, u \in R^* \Rightarrow au \mid b, a \mid ub$
- 4) $R^* = \{a \mid a \mid 1\}$
- 5) $a \mid u$ mit $u \in R^* \Rightarrow a \in R^*$
- 6) $c \neq 0, ca \mid cb \Leftrightarrow a \mid b$
- 7) $c \mid a, c \mid b \Rightarrow c \mid xa + yb \quad \forall x, y \in R$
- 8) $a \mid b, c \mid d \Rightarrow ac \mid bd$

Beweis:

- 1) $ac = bc \Rightarrow ac - bc = 0 \Rightarrow (a - b)c = 0$
Da R nullteilerfrei ist und $c \neq 0$
folgt $a - b = 0 \Rightarrow a = b$.
- 2) Da $0 \cdot a = 0, 1 \cdot a = a, a \cdot 1 = a$

$$3) \quad a|b \Rightarrow \exists c: ac=b \Rightarrow a \cdot u \cdot (u^{-1}c) = b \Rightarrow au|b, \quad a(cu)=ub \Rightarrow a|ub$$

$$4) \quad R^* = \{a \mid \exists b: ab=1\} = \{a \mid a|1\}$$

$$5) \quad a|u \Rightarrow \exists c: ac=u \Rightarrow a(cu^{-1}) = uu^{-1}=1 \Rightarrow a \in R^*$$

$$6) \quad \Rightarrow "ca|cb \Rightarrow \exists d: cad=cb$$

$$\xRightarrow{c \neq 0, 1)} ad=b \Rightarrow a|b.$$

" $\Leftarrow$ " klar

$$7) \quad c|a, c|b \Rightarrow \exists d, e: cd=a, ce=b$$

$$\Rightarrow c \cdot (dx+ey) = cd x + ce y = ax + by$$

$$\Rightarrow c|ax+by$$

$$8) \quad a|b, c|d \Rightarrow \exists e, f: ae=b, cf=d$$

$$\Rightarrow ac(ef) = bd \Rightarrow ac|bd \quad \square$$

3.5.3 Def

Sei R nullteufrei, $a, b \in R$.

a, b heißen assoziert : $\Leftrightarrow \exists u \in R^* : au=b$.

3.5.4 Lemma Sei R nullteufrei.

a, b assoziiert $\Leftrightarrow a|b, b|a \Leftrightarrow \langle a \rangle = \langle b \rangle$

Beweis: a, b assoziiert $\Rightarrow \exists u \in R^*$;
 $au = b \Rightarrow a|b$, außerdem gilt
 $bu^{-1} = a \Rightarrow b|a$.

Es gelte $b|a, a|b \Rightarrow \exists c, d$;
 $ac = b, bd = a \Rightarrow a \in \langle b \rangle$,
 $b \in \langle a \rangle \Rightarrow \langle a \rangle \subset \langle b \rangle, \langle b \rangle \subset \langle a \rangle$
 $\Rightarrow \langle a \rangle = \langle b \rangle$.

Es gelte $\langle a \rangle = \langle b \rangle \Rightarrow b \in \langle a \rangle$

und $a \in \langle b \rangle \Rightarrow \exists c, d$:

$$a \cdot c = b, b \cdot d = a$$

1. Fall: Sei $a = 0 \Rightarrow b = c \cdot a = c \cdot 0 = 0$

$\Rightarrow a$ und b sind assoziiert

2. Fall: $a \neq 0$. Aus $a \cdot c \cdot d = a$

folgt dann mit der Kürzungsregel

$$cd = 1 \Rightarrow c, d \in R^* \Rightarrow$$

a und b sind assoziiert. $\square$

Bsp

1) $a, b \in \mathbb{Z}$ sind assoziiert $\Leftrightarrow |a| = |b|$

2) Sei K ein Körper. Dann sind
 $a, b \neq 0$ assoziiert.

3) Seien $f, g \in R[x]$. f, g sind
assoziiert $\Leftrightarrow \exists u \in R^* : f = ug$.

3.5.5 Def Sei R nullteilerfrei.

Sei $0 \neq a \in R \setminus R^*$

1) a heißt irreduzibel (unzerlegbar) $:\Leftrightarrow$

falls $a = bc$ mit $b, c \in R$ folgt
 $b \in R^*$ oder $c \in R^*$

2) a heißt prim $:\Leftrightarrow$

falls $a \mid bc$ für $b, c \in R$ folgt
 $a \mid b$ oder $a \mid c$

Bemerkung: In $\mathbb{Z}$ ist prim und
irreduzibel äquivalent (Satz 1.12)

3.5.6 Lemma Sei R nullteilerfrei.

$a \in R$ sei prim $\Rightarrow a$ ist irreduzibel.

Beweis: Sei a prim, sei $a = bc$

$\Rightarrow a \mid bc \Rightarrow \exists d : a \mid b \Rightarrow \exists d :$

$ad = b \Rightarrow a = acd \xrightarrow{\text{kürzen}} 1 = cd$

$\Rightarrow c \in R^* \Rightarrow a$ ist irreduzibel.

□

Bemerkung Im Allgemeinen folgt aus
irreduzibel nicht prim, ein Bsp
davon gibt es in den Übungen:
 $2 \in \mathbb{Z}[\sqrt{-5}]$ ist irreduzibel, aber
nicht prim.

3.5.7 Lemma Sei R nullteilerfrei,
 $0 \neq a \in R \setminus R^*$

$\langle a \rangle$ ist Primideal $\Leftrightarrow a$ prim

Beweis: " $\Rightarrow$ " Sei $\langle a \rangle$ Primideal,

$a \mid bc \Rightarrow bc \in \langle a \rangle \Rightarrow \exists b \in \langle a \rangle$
 $\Rightarrow a \mid b \Rightarrow a$ prim.

" $\Leftarrow$ " Sei a prim, $bc \in \langle a \rangle \Rightarrow$
 $a \mid bc \Rightarrow \exists a \mid b \Rightarrow b \in \langle a \rangle$
 $\Rightarrow \langle a \rangle$ Primideal. $\square$

3.5.8 Lemma Sei R nullteilerfrei,
 $0 \neq a \in R \setminus R^*$

$\langle a \rangle$ maximal $\Rightarrow a$ irreduzibel

Beweis: Sei $a = bc \Rightarrow a \in \langle b \rangle$
 $\Rightarrow \langle a \rangle \subset \langle b \rangle$

Falls $\langle a \rangle = \langle b \rangle \Rightarrow b \in \langle a \rangle \Rightarrow$
 $\exists d: ad = b \Rightarrow a = adc \stackrel{\text{Kürzen}}{\Rightarrow}$
 $dc = 1 \Rightarrow c \text{ Einheit.}$

Falls $\langle a \rangle \subsetneq \langle b \rangle \Rightarrow \langle b \rangle = R$
 $\Rightarrow 1 \in \langle b \rangle \Rightarrow \exists d: bd = 1$
 $\Rightarrow b \text{ Einheit}$

$\Rightarrow a$ ist irreduzibel. $\square$

Bsp Es gibt irreduzible Elemente,
 die kein maximales Ideal erzeugen.

$$f = xy - 1 \in \mathbb{C}[x, y]$$

f ist irreduzibel, wäre es zerlegbar,
 so müßte es in zwei Polynome
 vom Grad 1 zerfallen $ax + by + c, dx + ey + f$
 man rechnet nach, daß es das
 nicht tut.

$xy - 1 \in \langle x - 1, y - 1 \rangle$, denn

$$xy - 1 = y(x - 1) + y - 1$$

$$x - 1 \notin \langle xy - 1 \rangle$$

$$\Rightarrow \langle xy - 1 \rangle \subsetneq \langle x - 1, y - 1 \rangle \subsetneq \mathbb{C}[x, y]$$

3.5.9 Satz

Sei R noethersch, $0 \neq a \in R \setminus R^*$.

Dann ist $a = g_1 \cdots g_r$ ein Produkt von irreduziblen Elementen.

Beweis Ist a irreduzibel, ist nichts zu zeigen. Ist a zerlegbar $\Rightarrow \exists a_1, b_1 \in$

$R \setminus R^*$, $a = a_1 b_1$. Sind a_1, b_1 irreduzibel, fertig. Sonst $\exists a_1$ zerlegbar

$\Rightarrow \exists a_2, b_2 : a_1 = a_2 b_2$ usw.

So produzieren wir eine Kette

$$\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \dots$$

die wegen noethersch stationär wird

$$\Rightarrow \exists k : \langle a_k \rangle = \langle a_{k+1} \rangle$$

$$\Rightarrow \exists c : a_{k+1} = a_k \cdot c$$

$$\Rightarrow a_k = a_{k+1} b_{k+1} = a_k c b_{k+1}$$

$$\Rightarrow c b_{k+1} = 1 \Rightarrow b_{k+1} \in R^*$$

$$\Rightarrow a_k \text{ ist irreduzibel}$$

und $a = a_1 \cdots a_k$ ist ein Produkt von irreduziblen Elementen.

□

3.5.10 Def Ein nullteilerfreier Ring, in dem jedes $0 \neq a \in R \setminus R^*$ eine bis auf Vertauschung und Einheiten eindeutige Darstellung $a = p_1 \cdots p_r$ mit p_i prim besitzt, heißt faktoriell (ZPE „Zerlegung in Primfaktoren ist eindeutig“, UFD „unique factorization domain“)

Bsp $\mathbb{Z}$ ist faktoriell.

3.5.11 Prop Sei R faktoriell.
 a irreduzibel $\Rightarrow a$ prim.

Insbesondere sind wegen Lemma 3.5.6 die beiden Begriffe in faktoriellen Ringen äquivalent.

Beweis: Sei a irreduzibel, schreibe $a = p_1 \cdots p_r$ als Produkt von Primfaktoren, dann muß $r=1$ und $a = p_1$ gelten. $\square$

3.5.12 Satz Sei R nullteilerfrei.

R faktoriell $\Leftrightarrow$ jedes $0 \neq a \in R \setminus R^*$ besitzt eine bis auf Vertauschung und Einheiten eindeutige Darstellung als Produkt von irreduziblen Elementen.

Beweis:

" $\Rightarrow$ " Existenz: a besitzt eine Darstellung als Produkt von Primfaktoren, jedes Primelement ist irreduzibel.

Eindeutigkeit: Jede Zerlegung in irreduzible Faktoren ist auch eine Zerlegung in Primfaktoren und letztere ist n. V. eindeutig.

" $\Leftarrow$ " Beh: jedes irreduzible Element ist prim.

Dann folgen Existenz und Eindeutigkeit der Zerlegung in Primfaktoren aus der Existenz und Eindeutigkeit der Zerlegung in irreduzible Faktoren.

Sei p irreduzibel und $p \mid ab$

Ist $a \in R^* \Rightarrow p \mid b$.

Ist $a = 0 \Rightarrow p \mid a$

Also können wir annehmen,
 $a, b \in R \setminus (R^* \cup \{0\})$.

$\exists c: pc = ab$. Beide Seiten
haben eindeutige Zerlegungen in irreduzible
Elemente, p ist n. V. irreduzibel,
damit ist p einer der Faktoren von
 a oder b (bis auf Einheit) $\Rightarrow$
 $p|a$ oder $p|b$.
 $\Rightarrow p$ ist prim. $\square$

Bsp

1) $R = \mathbb{C}[x, y, z, w] / (xy - zw)$ ist null-
teilerfrei, da $xy - zw \in \mathbb{C}[x, y, z, w]$ prim.

R ist nicht faktoriell:

x, y, z, w sind irreduzibel, aber

$xy = zw$ ist nicht eindeutig als
Produkt von irreduziblen Elementen.

Wegen Satz 3.5.12 kann R daher
nicht faktoriell sein.

2) $R = \mathbb{Z}[\sqrt{-3}] =$

$$\{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

Beh: R ist nicht faktoriell.

Wir bestimmen die Einheiten von R :

$$(a + b\sqrt{-3})(c + d\sqrt{-3}) = 1 \Rightarrow$$

$$|a + b\sqrt{-3}| |c + d\sqrt{-3}| = 1 \Rightarrow b, d = 0,$$

$$a, c \in \{\pm 1\} \Rightarrow R^* = \{\pm 1\}.$$

Beh.: 2 ist irreduzibel.

$$\text{Angenommen, } 2 = (a + b\sqrt{-3})(c + d\sqrt{-3})$$

$$\Rightarrow 4 = (a^2 + 3b^2)(c^2 + 3d^2)$$

Einer dieser Faktoren muß 1 sein,

$$\text{also } \exists a \in \{\pm 1\}, b = 0 \Rightarrow a + b\sqrt{-3}$$

ist Einheit

Analog sieht man $1 \pm \sqrt{-3}$ ist irreduzibel.

Damit sind

$$2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$$

verschiedene Zerlegungen in irreduzible Elemente.

Wegen Satz 3.5.12 kann R daher nicht faktoriell sein.

3.5.13 Satz

Ein noetherscher nullteilerfreier Ring
ist faktoriell $\Leftrightarrow$ jedes irreduzible
Element ist prim.

Beweis:

" $\Rightarrow$ " 3.5.11.

" $\Leftarrow$ " Wegen Satz 3.5.9 besitzt

$a \in R \setminus (R^* \cup \{0\})$ eine Darstellung
als Produkt von irreduziblen
Elementen, damit besitzt es auch
eine als Produkt von Primfaktoren.

Eindeutigkeit: wie im Satz 1.12
über die Eindeutigkeit der Primfaktor-
zerlegung in $\mathbb{Z}$:

Induktion über $k = \text{Anzahl Faktoren}$.

Sei $k=1$, $a = p_1$ prim.

Falls $p_1 = p_1' \cdots p_l'$ so folgt

$l=1$ und $p_1 = p_1'$, da p_1 irreduzibel.

Sei $k > 1$, $a = p_1 \cdots p_k = p_1' \cdots p_l'$

$\Rightarrow p_k \mid p_1' \cdots p_l' \xrightarrow{p_k \text{ prim}} \exists i:$

$p_k \mid p_i'$. Da beide prim sind,

folgt p_k ist assoziiert zu p_i' .

$\Rightarrow \exists u \in R^*: u p_1 \cdots p_{k-1} =$

$p_1' \cdots p_{i-1}' p_{i+1}' \cdots p_l'$

Da nach Induktionsvoraussetzung
für Produkt von $k-1$ Primalelementen
die Eindeutigkeit gegeben ist, folgt,
daß diese Faktoren gleich sind
(bis auf Einheiten). $\square$

3.5.14 Def Sei R nullteilerfrei,

$a, b \in R$.

d ist ein größter gemeinsamer Teiler
von a, b , $\text{ggT}(a, b)$, wenn

1) $d|a, d|b$

2) $\forall d' : d'|a, d'|b \Rightarrow d'|d$

m ist ein kleinstes gemeinsames Vielfaches
von a, b , $\text{kgV}(a, b)$, wenn

1) $a|m, b|m$

2) $\forall m' : a|m', b|m' \Rightarrow m|m'$

Analog für mehr als zwei Elemente.

Bemerkung

1) ggT und kgV sind nur bis
auf Einheiten bestimmt

2) Falls d und d' ggT, so folgt $d|d'$, $d'|d$ also sind sie assoziiert

3) ggT und kgV müssen nicht existieren

4) Existiert $\text{ggT}(a,b)$, dann auch
$$\text{kgV}(a,b) = \frac{ab}{\text{ggT}(a,b)}$$

5) $\text{ggT}(a,b) = \text{kgV}(a,b)$ und ab sind assoziiert.

3.5.15 Satz Sei R faktoriell,

$$a = p_1^{s_1} \cdots p_k^{s_k}, \quad b = p_1^{r_1} \cdots p_k^{r_k}$$

Darstellungen als Produkt von Primfaktoren.

Dann existieren $\text{ggT}(a,b)$, $\text{kgV}(a,b)$

und

$$\text{ggT}(a,b) = \prod p_i^{\min(s_i, r_i)}$$

$$\text{kgV}(a,b) = \prod p_i^{\max(s_i, r_i)}$$

Beweis Übung.

3.6 Hauptidealringe

3.6.1 Def

Ein Ideal I , das von einem Element erzeugt wird, $I = \langle a \rangle$, heißt Hauptideal.

Ein nullteilerfreier Ring, in dem alle Ideale Hauptideale sind, heißt Hauptidealring.

Bsp $\mathbb{Z}$ ist Hauptidealring.

3.6.2 Bemerkung

Hauptidealringe sind noethersch.

3.6.3 Satz

In einem Hauptidealring sind irreduzible Elemente prim.

Beweis: Sei p irreduzibel, $p \mid ab$. Es gilt $\langle p \rangle \subset \langle p, a \rangle$, $\langle p \rangle \subset \langle p, b \rangle$. Wäre $\langle p, a \rangle = R = \langle 1 \rangle = \langle p, b \rangle$, so gäbe es r, s mit
$$r_1 a + s_1 p = 1 = r_2 b + s_2 p$$

$$\Rightarrow 1 = (r_1 a + s_1 p)(r_2 b + s_2 p) =$$

$$r_1 r_2 ab + r_1 s_2 ap + r_2 s_1 bp + s_1 s_2 p^2$$

$\in \langle p \rangle$, da $ab \in \langle p \rangle \nRightarrow$ da p keine Einheit.

Also ist $\langle p, a \rangle \subsetneq R$.

Da R Hauptidealring ist, $\exists$

$d: \langle p, a \rangle = \langle d \rangle \subsetneq R$. Damit

$d \notin R^*$. Dann $\exists c, e:$

$p = c \cdot d$, $a = e \cdot d$. Da p irreduzibel

ist, folgt $c \in R^* \Rightarrow$

$$a = e d = e c^{-1} c d = e c^{-1} p$$

$\in \langle p \rangle$ also p/a .

Damit ist p prim. $\square$

3.6.4 Korollar

Hauptidealringe sind faktoriell.

Beweis: Hauptidealringe sind noethersch
wegen 3.6.2 und nullteilerfrei n. V.

Da wegen 3.6.3 irreduzible

Elemente prim sind, folgt mit Satz 3.5, 13, daß Hauptidealringe faktoriell sind. $\square$

3.6.5 Satz

Sei R ein Hauptidealring, $a_1, \dots, a_r \in R$

$$1) \quad \langle a_1, \dots, a_r \rangle = \langle \text{ggT}(a_1, \dots, a_r) \rangle$$

insbesondere gibt es eine Darstellung

$$\text{ggT}(a_1, \dots, a_r) = x_1 a_1 + \dots + x_r a_r$$

$$2) \quad \langle a_1 \rangle \cap \dots \cap \langle a_r \rangle = \langle \text{kgV}(a_1, \dots, a_r) \rangle$$

Beweis:

1) Da R Hauptidealring ist, ist

$$\langle a_1, \dots, a_r \rangle = \langle d \rangle \text{ für ein } d.$$

Es gilt $a_i \in \langle d \rangle \forall i \Rightarrow d \mid a_i \forall i$

Außerdem $d \in \langle a_1, \dots, a_r \rangle \Rightarrow$

$$\exists x_i \in R: d = x_1 a_1 + \dots + x_r a_r.$$

Sei d' ein Teiler von $a_i \forall i$,

dann gilt d' teilt $x_1 a_1 + \dots + x_r a_r = d$.

Damit ist $d = \text{ggT}(a_1, \dots, a_r)$.

2) Der Schnitt ist ein Ideal,

daher $\exists m: \langle a_1 \rangle \cap \dots \cap \langle a_r \rangle = \langle m \rangle$.

$$\Rightarrow m \in \langle a_i \rangle \forall i \Rightarrow a_i | m \forall i.$$

gibt $a_i | m' \forall i$ für ein m' , so

$$\text{folgt } m' \in \langle a_i \rangle \forall i \Rightarrow m' \in$$

$$\langle a_1 \rangle \cap \dots \cap \langle a_r \rangle = \langle m \rangle \Rightarrow m | m'$$

$$\Rightarrow m = \text{kgV}(a_1, \dots, a_r).$$

□

Bsp:

$$1) \text{ In } \mathbb{Z} \text{ ist } \langle 6, 15 \rangle = \langle 3 \rangle = \langle \text{ggT}(6, 15) \rangle$$

$$\langle 6 \rangle \cap \langle 15 \rangle = \langle 30 \rangle = \langle \text{kgV}(6, 15) \rangle$$

2) $\mathbb{C}[x, y]$ ist kein Hauptidealring.

$\langle x, y \rangle$ kann nicht von einem

Polynom erzeugt werden.

$\mathbb{C}[x, y]$ ist faktoriell (ohne Beweis)

also existiert $\text{ggT}(x, y) = 1$.

Aber $\langle x, y \rangle \neq \langle 1 \rangle = \mathbb{C}[x, y]$.

3.6.6 Lemma Sei R Hauptidealring,

$a \in R \setminus (R^* \cup \{0\})$. Dann ist

$\langle a \rangle$ maximal $\Leftrightarrow a$ irreduzibel

Beweis: " $\Rightarrow$ " Lemma 3.5.8

(R nullteilerfrei u. V.).

" $\Leftarrow$ " Sei a irreduzibel, sei

$$\langle a \rangle \subset \langle b \rangle \subset R \Rightarrow a \in \langle b \rangle$$

$$\Rightarrow \exists c: a = bc \Rightarrow b \in R^*$$

$$\text{oder } c \in R^*$$

$$1. \text{ Fall: } b \in R^* \Rightarrow \langle b \rangle = R$$

$$2. \text{ Fall: } c \in R^* \Rightarrow \langle a \rangle = \langle b \rangle$$

$$\Rightarrow \langle a \rangle \text{ ist maximal.}$$

□

3.7 Euklidische Ringe

3.7.1 Def Ein nullteilerfreier Ring

heißt euklidisch, wenn

$$\exists v: R \setminus \{0\} \rightarrow \mathbb{N},$$

$$\forall a, b \in R \setminus \{0\} \text{ mit } v(a) \geq v(b)$$

$$\exists q, r \in R:$$

$$1) a = qb + r$$

$$2) r = 0 \text{ oder } v(r) < v(b).$$

1) heißt dann Division mit Rest,

v heißt euklidische Norm.

Bsp

1) $\mathbb{Z}$ ist euklidisch mit $v: a \mapsto |a|$

2) $K[x]$ ist euklidisch mit $v = \deg$.

Bsp für eine Polynomdivision:

$$\begin{array}{r} (x^4 - 1) : (x^2 + 2x + 1) = x^2 - 2x + 3 \\ -(x^4 + 2x^3 + x^2) \\ \hline -2x^3 - x^2 - 1 \\ -(-2x^3 - 4x^2 - 2x) \\ \hline 3x^2 + 2x - 1 \\ -(3x^2 + 6x + 3) \\ \hline -4x - 4 \quad \text{Rest} \end{array}$$

$$\underbrace{(x^4 - 1)}_a = \underbrace{(x^2 - 2x + 3)}_q \cdot \underbrace{(x^2 + 2x + 1)}_b + \underbrace{(-4x - 4)}_r$$

Dabei gilt $\deg r < \deg b$.

Für das Verfahren benötigen wir, daß K ein Körper ist, denn man muß durch Leitkoeffizienten teilen.

3.7.2 Satz

Euklidische Ringe sind Hauptidealringe.

Beweis: $I = \langle 0 \rangle$ ist von 0 erzeugt.

Sei $I \neq \langle 0 \rangle$. Wähle $m \in I$ mit minimalem v .

Beh: $I = \langle m \rangle$

" $\supset$ " klar

" $\subset$ " Sei $b \in I$. Division mit Rest mit m liefert $b = q \cdot m + r$ mit $v(r) < v(m)$ oder $r = 0$

$$\Rightarrow r = b - qm \in I$$

Da m minimales v hatte,

$$\text{folgt } r = 0 \Rightarrow b = qm \Rightarrow$$

$$b \in \langle m \rangle.$$

□

Bsp

$$R = \mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

der Ring der ganzen Gaußschen Zahlen

Setze $v: R \setminus \{0\} \rightarrow \mathbb{N}$:

$$a+bi \mapsto a^2+b^2 = |a+bi|^2$$

Beh: v ist euklidische Norm.

Seien $a+bi, c+di \in \mathbb{Z}[i]$,

betrachte $\frac{a+bi}{c+di} =: x+iy$ mit

$$x = \frac{ac+bd}{c^2+d^2}, \quad y = \frac{bc-ad}{c^2+d^2} \in \mathbb{Q}.$$

Wähle $p, q \in \mathbb{Z}$ mit $|p-x| \leq \frac{1}{2}$,
 $|q-y| \leq \frac{1}{2}$.

Dann ist $|x+iy - (p+qi)|^2 =$

$$(x-p)^2 + (y-q)^2 \leq \frac{1}{4} + \frac{1}{4} < 1$$

$$\Rightarrow \left| \frac{a+bi}{c+di} - (p+qi) \right|^2 < 1 \Rightarrow$$

$$|a+bi - (p+qi)(c+di)|^2 < |c+di|^2$$

Setze $a+bi - (p+qi)(c+di)$ als

Rest, dann erfüllt $(\mathbb{Z}[i], v)$

Def 3.7.1.

Damit ist $\mathbb{Z}[i]$ Hauptidealring und faktoriell.

Bsp $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ ist Hauptidealring,
aber nicht euklidisch (ohne Beweis).

3.7.3 Satz (Euklidischer Algorithmus)

Sei R mit $v: R \setminus \{0\} \rightarrow \mathbb{N}$ euklidisch.

Seien $a, b \in R \setminus \{0\}$ mit $v(a) \geq v(b)$

1. Schritt: $a_1 := a, b_1 := b$

2. Schritt: Berechne eine Division mit

$$\text{Rest} \quad a_1 = q_1 b_1 + r_1$$

Wenn $r_1 = 0$ dann ist

$$\text{ggT}(a, b) = b_1, \text{ stop.}$$

Sonst setze $a_2 := b_1, b_2 := r_1$

und wiederhole Schritt 2 mit diesen.

Rückwärtseinsetzen liefert eine

$$\text{Darstellung} \quad \text{ggT}(a, b) = xa + yb.$$

Beweis wie in $\mathbb{Z}$.

Bsp: Wir berechnen in $\mathbb{Z}[i]$ den

ggT von $3+4i$ und $-1+12i$

$$\frac{-1+12i}{3+4i} = \frac{(-1+12i)(3-4i)}{9+16} = \frac{45+40i}{25}$$

$$\left| 2 - \frac{45}{25} \right| = \left| \frac{5}{25} \right| = \left| \frac{1}{5} \right| \leq \frac{1}{2}$$

$$\left| 2 - \frac{40}{25} \right| = \left| \frac{10}{25} \right| = \left| \frac{2}{5} \right| \leq \frac{1}{2}$$

$$\Rightarrow (-1+12i) = (2+2i)(3+4i) + r$$

$$\text{mit } r = (-1+12i) - (2+2i)(3+4i) =$$

$$(-1+12i) - (-2+14i) = 1-2i$$

$1-2i \neq 0$, weiter:

$$\frac{3+4i}{1-2i} = \frac{(3+4i)(1+2i)}{5} = \frac{-5+10i}{5} = -1+2i$$

$$\Rightarrow (3+4i) = (1+2i)(1-2i) + 0$$

$$\Rightarrow \text{ggT}(3+4i, -1+12i) = 1-2i$$

Dies ist nur eindeutig bis auf
Einheiten $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.

Andere ggT sind $-1+2i, 2+i, -2-i$.

3.8 Der Chinesische Restsatz

3.8.1 Def Sei R ein kommutativer Ring mit 1 , I_1, I_2 Ideale in R .
Wir definieren die Summe

$$I_1 + I_2 = \{a + b \mid a \in I_1, b \in I_2\}$$

und das Produkt

$$I_1 \cdot I_2 = \langle ab \mid a \in I_1, b \in I_2 \rangle,$$

das sind jeweils Ideale in R .

3.8.2 Def

I_1, I_2 heißen koprim : $\Leftrightarrow$

$$I_1 + I_2 = \langle 1 \rangle$$

Bsp

1) Für Hauptideale $I_1 = \langle a \rangle, I_2 = \langle b \rangle$
gilt $I_1 + I_2 = \langle a, b \rangle$
 $I_1 \cdot I_2 = \langle a \cdot b \rangle$

2) Sei R ein Hauptidealring.
 $\langle a \rangle, \langle b \rangle$ sind koprim $\Leftrightarrow$

$$\text{ggT}(a, b) = 1 \quad (\text{Satz 3.6.5}) \Leftrightarrow$$

$$\text{kgV}(a, b) = a \cdot b \quad \Leftrightarrow$$

$$\langle a \rangle \cdot \langle b \rangle = \langle ab \rangle = \langle \text{kgV}(a, b) \rangle \\ = \langle a \rangle \cap \langle b \rangle$$

3.8.3 Satz (Chinesischer Restsatz)

Sei R ein kommutativer Ring
mit 1, $I_1, \dots, I_r$ paarweise kopprime
Ideale. Dann ist

$$\varphi: R \longrightarrow R/I_1 \times \dots \times R/I_r$$

$$a \mapsto ([a], \dots, [a]) = \\ (a + I_1, \dots, a + I_r)$$

surjektiv, $\text{Ker } \varphi = I_1 \cap \dots \cap I_r = I_1 \cdot \dots \cdot I_r$.

Inbesondere

$$R / I_1 \cap \dots \cap I_r \cong R/I_1 \times \dots \times R/I_r$$

Erinnerung Satz 1.8, Chinesischer
Restsatz für $\mathbb{Z}$:

$n_1, \dots, n_r$ paarweise teilerfremd

$\Leftrightarrow \langle n_1 \rangle, \dots, \langle n_r \rangle$ paarweise
koprim

Dann ist $x \equiv a_1 \pmod{n_1}, \dots, x \equiv a_r \pmod{n_r}$
für $a_1, \dots, a_r \in \mathbb{Z}$ lösbar und die
Lösung ist eindeutig mod $n_1 \cdots n_r$

$$\begin{aligned} \varphi: \mathbb{Z} &\longrightarrow \mathbb{Z}/\langle n_1 \rangle \times \cdots \times \mathbb{Z}/\langle n_r \rangle \\ a &\longmapsto ([a], \dots, [a]) \\ &= (a_1, \dots, a_r) \end{aligned}$$

φ surjektiv $\Rightarrow \exists$ Lösung $a \in \mathbb{Z}$.

Eindeutigkeit mod $n_1 \cdots n_r \Leftrightarrow$

$$\mathbb{Z}/\langle n_1 \cdots n_r \rangle \cong \mathbb{Z}/\langle n_1 \rangle \times \cdots \times \mathbb{Z}/\langle n_r \rangle$$

ist Isomorphismus. Hier $\langle n_1 \rangle \cap \cdots \cap \langle n_r \rangle = \langle n_1 \cdots n_r \rangle$.

Beweis: Sei $a_i + I_i \in \mathbb{R}/I_i, \forall i$,

wir suchen $a \in \mathbb{R}$ mit

$$a + I_i = a_i + I_i \quad \forall i.$$

N.V. $\exists s_{ij} \in I_i, t_{ij} \in I_j:$

$$s_{ij} + t_{ij} = 1$$

$$\text{Betrachte } k_j = \prod_{i \neq j} s_{ij} = \prod_{i \neq j} (1 - t_{ij}).$$

Es gilt $k_j \in I_i, \forall i \neq j,$

$$k_j \in 1 + I_j.$$

Setze $a = \sum_{j=1}^r a_j k_j$, dann ist

$$\begin{aligned} a + I_j &= \sum_{k=1}^r a_k k_k + I_j = a_j k_j + I_j \\ &= (a_j + I_j) (k_j + I_j) = (a_j + I_j) (1 + I_j) = \\ & a_j + I_j \end{aligned}$$

$\Rightarrow \varphi$ ist surjektiv.

$$\text{Ker } \varphi = I_1 \cap \dots \cap I_r \text{ klar.}$$

$$\text{Noch zz: } I_1 \cap \dots \cap I_r = I_1 \cdot \dots \cdot I_r$$

" $\supset$ " klar

" $\subset$ " Induktion nach r .

$$\text{IA: } r=2: \quad s_{12} + t_{12} = 1, \quad s_{12} \in I_1, \\ t_{12} \in I_2.$$

$$\text{Sei } k \in I_1 \cap I_2 \Rightarrow$$

$$\begin{aligned} k \cdot 1 &= k(s_{12} + t_{12}) = k \cdot s_{12} + k \cdot t_{12} \\ &\in I_1 \cdot I_2 \end{aligned}$$

IV : es gelte $I_1 \cap \dots \cap I_{r-1} = I_1 \circ \dots \circ I_{r-1}$.

IS : $r \geq 2$; $s_{ir} \in I_i$, $t_{ir} \in I_r$:

$s_{ir} + t_{ir} = 1$. Dann ist

$$1 = \prod_{i=1}^{r-1} (s_{ir} + t_{ir})$$

$$= \underbrace{s_{1r} \dots s_{r-1,r}}_{\in I_1 \circ \dots \circ I_{r-1}} + \underbrace{t_{1r} \dots + t_{2r} \dots}_{\in I_r}$$

$\Rightarrow I_1 \circ \dots \circ I_{r-1}, I_r$ sind koprim

Mit den IA erhalten wir

$$(I_1 \circ \dots \circ I_{r-1}) \cdot I_r = (I_1 \circ \dots \circ I_{r-1}) \cap I_r$$

$$\stackrel{IV}{=} (I_1 \cap \dots \cap I_{r-1}) \cap I_r$$

□

Bsp $R = K[x]$, $u_1, \dots, u_n \in K$

paarweise verschieden. Setze

$f_i = x - u_i \in K[x]$, die f_i sind
paarweise teilerfremd.

Für $c_1, \dots, c_n \in K$ gibt es mit
dem chinesischen Restsatz daher
ein $g \in K[x]$:

$$g \equiv c_i \pmod{(x-u_i)} \Leftrightarrow$$

$$g(u_i) - c_i = 0 \Leftrightarrow g(u_i) = c_i.$$

g ist dabei eindeutig mod $f = \prod f_i$,
dividiere g mit Rest durch f und
erhalte den Rest g' mit
 $\deg(g') < n$, $g'(u_i) = c_i \forall i$.

Da $K[x]$ euklidisch ist, können
wir die s_{ij} , t_{ij} aus dem Beweis
des chinesischen Restsatzes bestimmen
und damit ist der Beweis
konstruktiv wie in $\mathbb{Z}$.

$$\text{Wir setzen } \hat{f}_i = \prod_{j \neq i} f_j = \prod_{j \neq i} (x - u_j)$$

Dann ist

$$\hat{f}_i \cdot \prod_{j \neq i} \frac{1}{u_i - u_j} = \prod_{j \neq i} \frac{x - u_j}{u_i - u_j} = \begin{cases} 1 \pmod{x - u_i} \\ 0 \pmod{x - u_j} \end{cases}$$

Damit gilt

$$g' = \sum_{i=1}^n c_i \prod_{j \neq i} \frac{x - u_j}{u_i - u_j}.$$

Dieses Polynom löst das Lagrange'sche Interpolationsproblem:

3.8.4 Satz (Lagrangescher Interpolationssatz)

Seien $u_1, \dots, u_n \in K$ paarweise verschieden,

$c_1, \dots, c_n \in K$, dann

$\exists! g \in K[x]$, $\deg g < n$,

$g(u_i) = c_i \quad \forall i$.

3.9 Übersicht

nullteilerfreie
Ringe

$$\frac{K[x, y, z, w]}{(2xy - zw)} \\ \mathbb{Z}[\sqrt{-3}]$$

Noethersch,
nicht faktoriell:
 $\mathbb{Z}[i\sqrt{5}]$

Faktoriell,
nicht
noethersch:
 $K[x_1, x_2, \dots]$

U

Faktorielle
Ringe

$$K[x_1, \dots, x_n] \\ \mathbb{Z}[x]$$

Noethersche
Ringe

$$K[x_1, \dots, x_n]$$

U

($\langle 2, x \rangle$ ist
kein Hauptideal)

(ohne Beweis:
Satz von Gauß:
 R faktoriell $\Rightarrow$
 $R[x]$ faktoriell)

Hauptidealringe

$$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$$

U

(ohne Beweis)

euklidische Ringe

$$\mathbb{Z}, \mathbb{Z}[i], K[x]$$

4. Die prime Restklassengruppe und Anwendungen

4.1 Die prime Restklassengruppe

4.1.1 Satz

Sei R ein endlicher Ring, R_N die Menge der Nullteiler, dann ist

$$R = R^* \cup R_N.$$

Beweis:

" $\supset$ " klar.

" $\subset$ " Sei $x \in R$, $x \notin R_N$.

Betrachte $\varphi: R \rightarrow R: y \mapsto x \cdot y$

Beh: φ ist injektiv.

$$\text{Sei } \varphi(y_1) = \varphi(y_2) \Rightarrow x \cdot y_1 = x \cdot y_2$$

$$\Rightarrow x \cdot (y_1 - y_2) = 0 \stackrel{x \notin R_N}{\Rightarrow}$$

$$y_1 - y_2 = 0 \Rightarrow y_1 = y_2$$

Da R endlich folgt, daß φ auch surjektiv ist.

Für $1 \in R$ $\exists$ Urbild $y \in R:$

$$\varphi(y) = 1 = x \cdot y \Rightarrow x \in R^* \quad \square$$

Bsp $\mathbb{Z}_6^* = \{1, 5\}, (\mathbb{Z}_6)_N = \{0, 2, 3, 4\}$

Bem: $\bar{a} \in \mathbb{Z}_n$ ist Einheit $(\Leftrightarrow)$

$\exists b: \bar{a}\bar{b} = \bar{1} \in \mathbb{Z}_n \Leftrightarrow \exists k:$

$ab - 1 = k \cdot n \xrightarrow{\text{Bézout (1.7)}} \text{ggT}(a, n) = 1$

4.1.2 Def $\mathbb{Z}_n^* = \{ \bar{a} \mid \text{ggT}(a, n) = 1 \}$

heißt die prime Restklassengruppe,
ihre Elemente prime Restklassen.

4.1.3 Korollar

Sei $n = p_1^{r_1} \cdots p_k^{r_k} \in \mathbb{Z}$ die Zerlegung
in Primfaktoren, so ist

$$\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{r_1}}^* \times \cdots \times \mathbb{Z}_{p_k^{r_k}}^*$$

Beweis mit dem chinesischen
Restsatz 3.7.3.

4.1.4 Def $\varphi: \mathbb{N} \rightarrow \mathbb{Z}$,

$$\varphi(n) := \#\{r \in \mathbb{Z} \mid 1 \leq r \leq n, \text{ggT}(r, n) = 1\}$$

$$= |\mathbb{Z}_n^*| = \text{Ordnung der primen Restklassengruppe}$$

heißt Eulersche φ -Funktion.

4.1.5 Satz (Fermat-Euler)

Seien $a, n \in \mathbb{Z}$, $n \geq 1$, $\text{ggT}(a, n) = 1$.

Dann gilt $a^{\varphi(n)} \equiv 1 \pmod{n}$

Beweis: $a \in \mathbb{Z}_n^*$, $\varphi(n) = |\mathbb{Z}_n^*|$,
die Ordnung von a teilt die
Gruppenordnung (2.3.9, Korollar
von Lagrange) $\Rightarrow \overline{a}^{\varphi(n)} = \overline{1}$. $\square$

4.1.6 Korollar

Sei p prim, $p \nmid a$

$$\Rightarrow a^{p-1} \equiv 1 \pmod{p}$$

Beweis: $\varphi(p) = p-1$ $\square$

4.1.7 Satz (Kleiner Satz von Fermat)

Sei p eine Primzahl, $a \in \mathbb{Z}$

$$\Rightarrow a^p \equiv a \pmod{p}$$

Beweis: Falls $p \mid a$ ist $a^p \equiv 0 \equiv a$.

Falls $p \nmid a$ ist $a^{p-1} \equiv 1 \Rightarrow$

$$a^p \equiv a. \quad \square$$

4.1.8 Satz

Sei $n = p_1^{r_1} \cdots p_k^{r_k} \in \mathbb{Z}$ die

Zerlegung in Primfaktoren.

$$\text{Dann ist } \varphi(n) = \prod_{i=1}^k \varphi(p_i^{r_i})$$

$$= \prod_{i=1}^k p_i^{r_i-1} (p_i - 1)$$

Beweis:

$$\varphi(p^r) = \# \{a \mid 1 \leq a \leq p^r, \text{ggT}(a, p^r) = 1\}$$

$$= p^r - \#\{\text{Vielfache von } p \text{ zwischen } 1 \text{ und } p^r\}$$

$$= p^r - p^{r-1} = p^{r-1} (p - 1).$$

Damit folgt die zweite Gleichheit,
die erste folgt aus dem chinesischen

Restsatz 3.7.3 bzw. 4.3.

□

4.1.9 Korollar

Sei $G = \langle g \rangle$ eine zyklische Gruppe.
Sei $|G| = n$, $d \mid n$. Dann gibt
es $\varphi(d)$ Elemente der Ordnung
 d in G , $\{g^{r \cdot \frac{n}{d}} \mid 1 \leq r \leq d, \text{ggT}(r, d) = 1\}$.

Insbesondere gibt es $\varphi(n)$ Elemente
der Ordnung n , also Erzeuger.

Folgt aus dem Satz über Untergruppen
zyklischer Gruppen, 2.3.13 (4).

Bsp.

$(\mathbb{Z}_{12}, +)$

Element	0	1	2	3	4	5	6	7	8	9	10	11
Ordnung	1	12	6	4	3	12	2	12	3	4	6	12

$$\varphi(12) = \varphi(4) \cdot \varphi(3) = 2(2-1) \cdot (3-1) = 4$$

Erzeuger von $\mathbb{Z}_{12}$: 1, 5, 7, 11

$$\varphi(6) = \varphi(2) \cdot \varphi(3) = 2,$$

Elemente der Ordnung 6:

$$\left(1 \cdot \frac{12}{6}\right) \cdot 1 = 2, \left(5 \cdot \frac{12}{6}\right) \cdot 1 = 10,$$

$$\text{denn } \{1, 5\} = \{r \mid 1 \leq r \leq 6, \text{ggT}(r, 6) = 1\}$$

$\varphi(2) = 1$, Element der Ordnung 2:

$$\left(1 \cdot \frac{12}{2}\right) \cdot 1 = 6$$

4.1.10 Korollar

Sei $n \in \mathbb{N}$.

$$\sum_{d|n} \varphi(d) = n.$$

Beweis: Sei G die zyklische Gruppe der Ordnung n . Jedes Element hat als Ordnung einen Teiler d von n , für jeden Teiler d gibt es $\varphi(d)$ Elemente dieser Ordnung. Daher ist $\sum_{d|n} \varphi(d)$ die Anzahl der Elemente von G . $\square$

4.1.11 Satz

Für $p \geq 3$ prim und $r \in \mathbb{N}_{>0}$ ist
 $(\mathbb{Z}_{p^r})^*$ zyklisch.

Zur Vorbereitung:

4.1.12 Lemma

$(\mathbb{Z}_p)^*$ ist zyklisch.

Beweis: Sei $n = |\mathbb{Z}_p^*| = p-1$.

Für jeden Teiler $d|n$
sei $\Psi(d)$ die Anzahl der Elemente
in $\mathbb{Z}_p^*$, die Ordnung d haben.

Wähle d mit $\Psi(d) \neq 0$.

$\Rightarrow \exists a \in \mathbb{Z}_p^*$, $\text{ord}(a) = d$

$\Rightarrow \langle 1, a, \dots, a^{d-1} \rangle \subset \mathbb{Z}_p^*$

ist eine zyklische Untergruppe,
alle ihre Elemente x erfüllen $x^d = 1$

$\Rightarrow$ Das Polynom $x^d - 1 \in \mathbb{Z}_p[x]$

hat mindestens d Nullstellen $\Rightarrow$
das Polynom $x^d - 1$ hat genau d
Nullstellen $\Rightarrow$ alle Elemente in
 $\mathbb{Z}_p^*$ der Ordnung d liegen in $\langle a \rangle$

$$\Rightarrow \psi(d) \leq \varphi(d).$$

$$\Rightarrow n = \sum_{d|n} \psi(d) \leq \sum_{d|n} \varphi(d) \stackrel{4.1.10}{=} n$$

$$\Rightarrow \psi(d) = \varphi(d) \quad \forall d$$

$$\Rightarrow \psi(n) = \varphi(n) \neq 0 \Rightarrow \exists b \in \mathbb{Z}_p^*,$$
$$\text{ord}(b) = n \Rightarrow \mathbb{Z}_p^* = \langle b \rangle \text{ ist}$$

zyklisch. $\square$

4.1.13 Lemma

Sei G eine Gruppe, $x, y \in G$

mit $xy = yx$ und $\langle x \rangle \cap \langle y \rangle = \{e\}$.

Dann gilt

$$\text{ord}(xy) = \text{kgV}(\text{ord}(x), \text{ord}(y)).$$

Beweis:

Sei $\text{ord}(x) = n$, $\text{ord}(y) = m$, $k = \text{kgV}(m, n)$.

$$\text{Es gilt } (xy)^k = x^k y^k = e$$

$$\Rightarrow \text{ord}(xy) \mid k.$$

$$\text{Sei } l \text{ so, da\ss } (xy)^l = e \\ \Rightarrow x^l y^l = e \Rightarrow x^l = \left(\frac{1}{y}\right)^l \\ \in \langle x \rangle \cap \langle y \rangle = \{e\} \Rightarrow$$

$$x^l = e \text{ und } \left(\frac{1}{y}\right)^l = e \Rightarrow y^l = e \\ \Rightarrow n \mid l \text{ und } m \mid l \\ \Rightarrow k \mid l \Rightarrow k \mid \text{ord}(xy) \\ \Rightarrow \text{ord}(xy) = k. \quad \square$$

4.1, 14 Lemma

$$a \equiv b \pmod{p^r} \Rightarrow a^p \equiv b^p \pmod{p^{r+1}}$$

$$\text{Beweis: } a = b + kp^r \Rightarrow$$

$$a^p = (b + kp^r)^p =$$

$$\sum_{j=0}^p \binom{p}{j} b^{p-j} (kp^r)^j = b^p \pmod{p^{r+1}}$$

$$\text{da } \binom{p}{1} = p. \quad \square$$

Bem Ist p prim und $0 < j < p$,
 so gilt $p \mid \binom{p}{j}$, denn p
 teilt den Zähler von $\frac{p!}{j!(p-j)!} = \binom{p}{j}$
 aber nicht den Nenner.

4.1.15 Lemma

Sei $p \geq 3$ prim und $r \geq 2$. Dann:
 $a \equiv 1 + p^{r-1} \pmod{p^r} \Rightarrow a^p \equiv 1 + p^r \pmod{p^{r+1}}$

Beweis:

$$a^p \stackrel{4.1.14}{\equiv} (1 + p^{r-1})^p = \sum_{j=0}^p \binom{p}{j} p^{(r-1) \cdot j}$$

$$= 1 + p \cdot p^{r-1} + \sum_{j=2}^p \binom{p}{j} p^{(r-1) \cdot j}$$

$$\equiv 1 + p^r \pmod{p^{r+1}} \quad \square$$

Beweis von Satz 4.1.11:

Der Fall $r = 1$ ist Lemma 4.1.12.

Sei $r \geq 2$. Es gilt

$$|\mathbb{Z}_{p^r}^*| = p^{r-1} \cdot (p-1).$$

Wir konstruieren Elemente

$$\bar{x}, \bar{y} \in \mathbb{Z}_{p^r}^* \quad \text{mit}$$

$$\text{ord}(\bar{x}) = p^{r-1}, \quad \text{ord}(\bar{y}) = p-1,$$

dann folgt mit Lemma 4.1.13
 (da $\text{ggT}(p^{r-1}, p-1) = 1$ und die
 Elemente in $\langle \bar{x} \rangle$ und in $\langle \bar{y} \rangle$
 als Ordnungen Teiler von p^{r-1} bzw.
 $p-1$ haben) $\text{ord}(\bar{x}\bar{y}) = p^{r-1} \cdot (p-1)$
 und $\langle \bar{x}\bar{y} \rangle = \mathbb{Z}_{p^r}^*$, also ist
 $\mathbb{Z}_{p^r}^*$ zyklisch.

Sei $\langle \bar{b} \rangle = \mathbb{Z}_p^*$ und

$d = \text{ord}(\bar{b})$ in $\mathbb{Z}_{p^r}^*$. Da

dann auch $\bar{b}^d = 1$ in $\mathbb{Z}_p^*$

folgt $(p-1) \mid d$.

Für $\bar{y} = \bar{b}^{\frac{d}{p-1}}$ folgt mit
 dem Satz über Untergruppen
 zyklischer Gruppen 2.3.13 (3)

$$\text{ord}(\bar{y}) = \text{ord}\left(\bar{b}^{\frac{d}{p-1}}\right) = \frac{\text{ord}(\bar{b})}{\text{ggT}(\text{ord}(\bar{b}), \frac{d}{p-1})} = \frac{d}{\text{ggT}(d, \frac{d}{p-1})} = \frac{d}{\frac{d}{p-1}} = p-1.$$

Setze $x = 1 + p$. Dann gilt

$$x \equiv 1 + p \pmod{p^2} \quad \begin{matrix} 4.1.15 \\ \Rightarrow \end{matrix}$$

$$x^p \equiv 1 + p^2 \pmod{p^3} \quad \begin{matrix} 4.15 \\ \Rightarrow \end{matrix}$$

$$x^{p^2} \equiv 1 + p^3 \pmod{p^4} \Rightarrow \dots \Rightarrow$$

$$x^{p^{r-2}} \equiv 1 + p^{r-1} \pmod{p^r}$$

$$\Rightarrow x^{p^{r-2}} = 1 + p^{r-1} + kp^r$$

$$\Rightarrow x^{p^{r-1}} = (1 + p^{r-1} + kp^r)^p =$$

$$\begin{aligned}
& \sum_{j=0}^p \binom{p}{j} (p^{r-1} + kp^r)^j \\
&= 1 + p \cdot (p^{r-1} + kp^r) + \sum_{j=2}^p \binom{p}{j} (p^{r-1} + kp^r)^j \\
&= 1 + p^r \pmod{p^r} \\
&\equiv 1 \pmod{p^r}
\end{aligned}$$

$$\begin{aligned}
&\Rightarrow \bar{y}^{p^{r-1}} = \overline{1} \text{ und } \bar{y}^{p^{r-2}} \neq \overline{1} \\
&\Rightarrow \text{ord}(\bar{y}) = p^{r-1}.
\end{aligned}$$

□

4.2 Anwendungen

4.2.1 Algorithmus (Primzahltest)

Sei $n \in \mathbb{N}$.

1) Wähle $a \in \mathbb{Z}$, bestimme $\text{ggT}(a, n)$ mit dem euklidischen Algorithmus.

Falls $\text{ggT}(a, n) \neq 1 \Rightarrow$
 n nicht prim.

2) Ist $\text{ggT}(a, n) = 1$, teste ob
 $a^n \equiv a \pmod{n}$. Falls nicht

$\Rightarrow n$ nicht prim

(kleiner Satz von Fermat)

Sonst keine Aussage, zurück zu 1).

Der Algorithmus terminiert nicht, falls n prim ist.

Man erkennt nur Nicht-Primzahlen, mit mehr Durchläufen erhöht sich die Wahrscheinlichkeit, daß eine Zahl, die nicht als Nicht-Prim

erkannt wird, tatsächlich prim ist.

4.2.2 Def n heißt Fermatsche Pseudoprimzahl zur Basis a , falls n nicht prim ist, aber $a^n \equiv a \pmod{n}$.

Bsp: $2^{341} \equiv 2 \pmod{341}$,
aber $341 = 11 \cdot 31$ ist keine Primzahl,
sondern eine Pseudoprimzahl zur
Basis 2.

Verwenden wir die Basis 3, so
erhalten wir $3^{341} \equiv 168 \not\equiv 3 \pmod{341}$,
so können wir schließen, daß
341 keine Primzahl ist.

4.2.3 Das RSA-Verfahren (Rivest, Shamir, Adleman)

Ein Verschlüsselungsverfahren, das
darauf beruht, daß Zahlen
schwer zu faktorisieren sind.

Alice möchte von Bob verschlüsselte
Nachrichten empfangen können.

Vorbereitung:

I Bob:

1. Wähle eine große Zahl N und kodiere Nachrichten in Zahlen $0 \leq m < N$.

II Alice:

2. Wähle 2 Primzahlen p, q mit $pq > N$, berechne $n = pq$ und $\varphi(n) = (p-1) \cdot (q-1)$.
3. Wähle $e \in \mathbb{N}$ mit $\text{ggT}(e, \varphi(n)) = 1$.
4. Berechne das Inverse von e mod $\varphi(n)$, also $0 < d < \varphi(n)$ mit $ed \equiv 1 \pmod{\varphi(n)}$.
5. $p, q, \varphi(n)$ kann vergessen werden.
6. (n, e) ist öffentlicher Schlüssel. Alice gibt diese Daten Bob.
 d ist Alices privater Schlüssel. Sie hält diese Zahl geheim.

Nachrichtenübertragung und Entschlüsselung

III. Bob möchte an Alice eine Nachricht senden, z.B. die Zahl m .

Er verschlüsselt mit Alices öffentlichem Schlüssel:

1. Berechne

$$C := m^e \bmod n$$

2. Sende C an Alice.

IV. Alice:

Berechne $\tilde{m} := C^d \bmod n$

mit dem geheimen Schlüssel d .

Dann gilt

$$\tilde{m} \equiv C^d \equiv (m^e)^d \equiv m^{ed} \equiv$$

$$m^{1+k \cdot \varphi(n)} \equiv m \cdot (m^{\varphi(n)})^k \equiv$$

$$m \bmod n$$

Da $m < N < n$ läßt sich m dadurch eindeutig zurück-

gewinnen.

Bem:

Um zu entschlüsseln braucht man d ,
also $\varphi(n)$, also die Faktorisierung
 pq von n .

Bsp:

$$n = 7 \cdot 11 = 77, \quad \varphi(n) = 6 \cdot 10 = 60$$

$$e = 13,$$

$$1 = \text{ggT}(13, 60) = (-23) \cdot 13 + 5 \cdot 60,$$

$$\text{also } d = -23 = 37.$$

Bob verschlüsselt $m=31$, also

$$\begin{aligned} m^e \bmod n &= 31^{13} \bmod 77 \\ &\equiv 3 \bmod 77. \end{aligned}$$

Bob sendet an Alice $\colon 3$.

Alice entschlüsselt:

$$3^d = 3^{37} \equiv 31 \bmod 77.$$

