Elementare Zahlentheorie

Prof. Dr. L. Kramer – WWU Münster, Sommersemester 2009
Vorlesungsmitschrift von Christian Schulte zu Berge
27. Juli 2009

Inhaltsverzeichnis

Vorwort

Dieses Skript entstand als Mitschrift in der Vorlesung „Elementare Zahlentheorie“, gelesen im Sommersemester 2009 von Prof. Dr. L. Kramer an der Universität Münster.

Es besteht keine Garantie auf Richtigkeit oder Vollständigkeit des Skriptes. Diese Version der Mitschrift ist zur Veröffentlichung bestimmt und darf unverändert im Original-pdf gerne weiterverbreitet werden. Sie ist noch in der Erstellungsphase und so gibt es noch laufend Ergänzungen und Korrekturen. Die stets aktuelle Version ist auf meiner Homepage `www.cszb.net` zu finden.

Die Nummerierung der einzelnen Definitionen und Sätze entspricht in den ersten Kapiteln *nicht* der die Prof. Kramer in der Vorlesung verwendet hat, da dort einige Definitionen und Sätze keine Nummern hatten. Um die Referenzierung innerhalb des Skriptes eindeutig zu machen, habe ich jedoch jeder Definition und jedem Satz/Lemma eine eindeutige fortlaufende Nummer gegeben.

Falls Fehler gefunden werden oder Fragen auftauchen, bitte einfach eine kurze Mail an `skript@cszb.net` schreiben.

Christian Schulte zu Berge

Kapitel 1

Primzerlegung

1.1 Grundlagen

1.5 Satz: *(Euklid)*
Es gibt unendlich viele Primzahlen.

Beweis:
Seien $p_1 < p_2 < \cdots < p_r$ Primzahlen. Betrachte $n = p_1 \cdot p_r + 1 \geq 2$. Setze $q := p(n)$, dann gilt $q \mid n$ und $\forall i \in 1, \ldots, r : q \nmid p_i$, denn sonst hätten wir $q \mid 1$. Insbesondere ist also $q \neq p_1, \ldots, p_r$ eine Primzahl (vgl. Lemma 4). □

Bemerkung:
Der Beweis liefert ein Verfahren zur Konstruktion von neuen Primzahlen aus $p_1, \ldots, p_r$.

Bemerkung:
Ist $n \in \mathbb{Z}, n \geq 2$ und gilt $p(n) > \sqrt{n}$, so ist $n \in \mathbb{P}$.

Beweis:
Schreibe $n = p(n) \cdot m$. Angenommen $p(n) < n$, dann gilt $1 < m < n$ und $p(n) \leq p(m) \leq m$ und damit $p(n)^2 \leq p(m) \cdot p(n) \leq m \cdot p(n) = n$. □

1.6 Satz: *Teilen mit Rest*
Sei $a, b \in \mathbb{Z}, b \neq 0$. Dann gibt es ganze Zahlen $r, s \in \mathbb{Z}$ mit

$$a = b \cdot s + r, \quad 0 \leq r < |b|$$

Die Zahlen r, s sind eindeutig bestimmt.

Beweis:

Eindeutigkeit:
Angenommen es gebe $a = bs + r = bs' + r'$ mit $0 \leq r, r' < |b|$. Ohne Einschränkung sei $r' \geq r$, dann gilt:

$$\begin{aligned} b(s - s') &= r' - r \geq 0, \quad 0 \leq r - r' < |b| \\ \Rightarrow |b| \cdot |s - s'| &= \underbrace{|r' - r|}_{<|b|} \\ \Rightarrow r &= r', s = s' \end{aligned}$$

Existenz:
Setze $S = \{k \in \mathbb{Z} \mid k \cdot |b| \leq a\}$, dann gilt $-|a| \in S \Rightarrow S \neq \emptyset$. Weiter hat S eine obere Schranke $|a|$. Also ist S nicht leer und beschränkt, hat also ein maximales Element $s := \max S$.

Es folgt, dass $s \cdot |b| \leq a \wedge (s+q) \cdot |b| > a$

$$\Rightarrow \exists r \in \mathbb{N} : a = s \cdot |b| + r, \quad 0 \leq r < |b|$$

Für $b \geq 0$, können wir die Betragsstriche weglassen und die Behauptung ist gezeigt. Für $b < 0$ setzen wir ohne Einschränkung $s := (-s)$.

□

1.2 Hauptsatz der Arithmetik

Das nächste Ziel ist der Hauptsatz der Arithmetik *(1.8)*: Jede natürliche Zahl ≥ 2 hat eine eindeutige Primfaktorzerlegung.

1.7 Lemma:
Sei $n \in \mathbb{Z}, n \geq 2$. Dann gibt es Primzahlen $p_1, \ldots, p_r \in \mathbb{P}$ mit $n = p_1 \cdots p_r$.

Beweis: Induktion über n:

Induktionsanfang $n = 2$:
klar.

Induktionsvoraussetzung:
Die Behauptung gilt für beliebiges aber festes n

Induktionsschritt:
Für $n \geq 3$ betrachte $p(n) \in \mathbb{P} \Rightarrow n = p(n) \cdot m$. Ist $n = p(n) \in \mathbb{P}$, so gilt die Behauptung. Ist $p(n) < n \Rightarrow 1 < m < n$. Nach der Induktionsvoraussetzung hat m eine Darstellung $m = q_1 \cdots q_s \Rightarrow n = p(n) \cdot q_1 \cdots q_s$.

□

1.8 Theorem: Hauptsatz der Arithmethik
Sei $n \in \mathbb{Z}, n \geq 2$. Dann gibt es eindeutige Primzahlen $p_1, \ldots, p_r \in \mathbb{P}$ mit $n = p_1 \cdots p_r$ und $p_1 \leq \cdots \leq p_r$.

Beweis:
Die Existenz haben wir bereits gezeigt, zu zeigen bleibt die Eindeutigkeit

Angenommen, es gebe ein Gegenbeispiel, dann gibt es nach dem Wohlordnungsprinzip ein kleinstes Gegenbeispiel $n \geq 2$, also:

$$n = p_1 \cdots p_r = q_1 \cdots q_s$$

mit $p_j, q_j \in \mathbb{P}, p_1 \leq \cdots \leq p_r, q_1 \leq \cdots \leq q_s$ und nicht $\forall j : p_j = q_j$. Das kleinste Gegenbeispiel ist offensichtlich keine Primzahl, also $r, s \geq 2$.

Ist $p_1 = q_1$, so gilt $p_2 \cdots p_r = q_2 \cdots q_s < n$ und wir hätten ein kleineres Gegenbeispiel gefunden. $\Rightarrow$ Widerspruch!

Also gilt $p_1 \neq q_1$, sei o.E. $q_1 > p_1$.
Betrachte:

$$(q_1 - p_1) \cdot q_2 \cdots q_s =: n' = n - p_1 \cdot q_2 \cdots q_s < n$$

Es folgt, dass $p_1 \mid n'$. Da $1 < n' < n$ hat n' eine eindeutige Zerlegung. Da $p_1 < q_1 \leq q_j$ für $1 \leq j \leq s$ gilt $p_1 \nmid q_j$. Also ist p_1 ein Primteiler von $q_1 - p_1 \Rightarrow p_1 \mid q_1 \Rightarrow$ Widerspruch.

Also kann es kein (kleinstes) Gegenbeispiel geben und die Primfaktorzerlegung ist eindeutig. □

1.9 Korollar:
Jede ganze Zahl $n \neq 0, \pm 1$ hat eine eindeutige Darstellung

$$n = \varepsilon \cdot p_1 \cdots p_r$$

mit $p_j \in \mathbb{P}, p_1 \leq \cdots \leq p_r, \varepsilon = \pm 1$.

1.10 Korollar:
Sei $a, b \in \mathbb{Z}, p \in \mathbb{P}$. Gilt $p \mid a \cdot b$, dann gilt $p \mid a \vee p \mid b$.

Beweis:
Ist $ab = 0$, so ist nichts zu zeigen. Sonst schreibe $a = \alpha p_1 \cdot p_r$ und $b = \beta q_1 \cdots q_s$ mit $\alpha, \beta \in \{-1, 1\}, p_j, q_j \in \mathbb{P}$. Da $p \mid ab$, folgt aus dem Hauptsatz, dass $p = p_j \vee p = q_j$ für ein j gilt. □

Notation:
Für $n \neq 0, n \in \mathbb{Z}$ und $p \in \mathbb{P}$ setze:

$$\nu_p(n) := \max\left\{k \in N : p^k \mid n\right\}$$

Bemerkung:
Mit dieser Schreibweise gilt:

$$\begin{aligned} n &= \varepsilon \cdot p_1^{l_1} \cdots p_r^{l_r}, \quad p_1 < \cdots < p_r, \quad l_1, \ldots, l_r \geq 1 \\ &= \varepsilon \cdot p_1^{\nu_{p_1}(n)} \cdots p_r^{\nu_{p_r}(n)} \\ &= \varepsilon \cdot \prod_{p \in \mathbb{P}} p^{\nu_p(n)} \end{aligned}$$

Das unendliche Produkt rechts ist in Wirklichkeit endlich, weil $\nu_p(n) = 0$ für fast alle $p \in \mathbb{P}$.

1.11 Lemma:
Sei $0 \neq a, b \in \mathbb{Z}$. Dann gilt

$$a \mid b \Leftrightarrow \forall p \in \mathbb{P} : \nu_p(a) \leq \nu_p(b)$$

Beweis:
Für $b = \pm 1$ ist das klar, sonst betrachte Primfaktorzerlegung $a \mid b \Leftrightarrow \exists am = b$ □

1.12 Definition: (Anzahl der Teiler)
Für $n \in \mathbb{Z}, n \geq 1$ sei $\tau(n)$ die *Anzahl der unterschiedlichen positiven Teiler* von n.

Beispiel:

$$\begin{aligned} \tau(1) &= 1 \\ \tau(2) &= 2 \\ \tau(5) &= 2 \\ \tau(6) &= 4 \end{aligned}$$

Bemerkung:

$$\tau(n) = 2 \Leftrightarrow n \in \mathbb{P}$$

1.13 Satz:
Für $n \in \mathbb{Z}, n \geq 1$ gilt

$$\tau(n) = \prod_{p \in \mathbb{P}} (1 + \nu_p(n))$$

Beweis:
Folgt direkt aus dem Lemma zuvor. □

Beobachtung:
Sind $n, m \geq 1$ teilerfremd, so folgt $\forall p \in \mathbb{P} : p \mid m \Rightarrow p \nmid n$. Also gilt dann

1.14 Definition: (Summe aller positiven Teiler)
Für $n \in \mathbb{Z}, n \geq 1$ sei $\sigma(n)$ die *Summe aller positiven Teiler* von n. Es gilt $\sigma(n) = 1 + n$, genau dann wenn $n \in \mathbb{P}$.

Beispiel:

$$\begin{aligned}\sigma(1) &= 1\\ \sigma(2) &= 1 + 2 = 3\\ \sigma(4) &= 1 + 2 + 4 = 7\end{aligned}$$

Bemerkung:
Die positiven Teiler m von n sind von der Form $m = \prod_{p\in\mathbb{P}} p^{a_p}$ mit $0 \leq a_p \leq \nu_p(n)$, also folgt

$$\begin{aligned}\sigma(n) &= \sum_{a_p=0}^{\nu_p(n)} \prod_{p\in\mathbb{P}} p^{a_p}\\ &= \prod_{p\in\mathbb{P}} \sum_{a_p=0}^{\nu_p(n)} p^{a_p}\\ &= \prod_{p\in\mathbb{P}} \frac{1 - p^{\nu_p(n)+1}}{1-p}\end{aligned}$$

An der Formel sehen wir wieder: falls $m, n \geq 1$ teilerfremd, so gilt

$$\tau(n \cdot m) = \tau(m) \cdot \tau(n)$$

1.15 Definition: (Vollkommenheit)
Im Altertum hat man sich für volkommene Zahlen interessiert: $n \in \mathbb{Z}, n \geq 1$ heißt *vollkommen*, falls n die Summe aller positiven Teiler echt kleiner n ist.

Bemerkung:

$$n \text{ vollkommen } \Leftrightarrow \sigma(n) = 2n$$

1.16 Satz:
Sei $n \in \mathbb{Z}, n \geq 2$ gerade. Dann ist äquivalent:

(i) $n = 2^{k-1}(2^k - 1)$ mit $2^k - 1 \in \mathbb{P}$

(ii) n ist vollkommen

Beweis:

(i) $\Rightarrow$ (ii): (Euklid)
Setze $n = 2^{k-1}(2^k - 1), k \geq 2$, dann gilt:

$$\sigma(n) = \sigma(2^{k-1}(2^k-1)) = \sigma(2^{k-1}) \cdot \sigma(2^k - 1) = \sum_{r=0}^{k-1} 2^r \cdot 2^k = \frac{2^k - 1}{2-1} \cdot 2^k = 2n$$

(ii) $\Rightarrow$ (i): (Euler)
Sei n gerade und vollkommen, dann gilt $n = 2^{k-1} \cdot m, k \geq 2, m$ ungerade.

$$2n = 2^k \cdot m = \sigma(n) = \sigma(2^{k-1}) \cdot \sigma(m) = (2^k - 1) \cdot \sigma(m)$$

Es folgt $2^k \mid \sigma(m)$, schreibe $\sigma(m) = 2^k \cdot l$

Es gilt $l = 1$, denn wäre $l > 1$, dann wäre

$$2^k \cdot m = (2^k - 1) \cdot 2 \cdot l \Rightarrow \sigma(m) \geq 1 + l + l(2^k - 1) > 2^k \cdot 1$$

Widerspruch!

Also: $l = 1, \sigma(m) = 2^k \Rightarrow m = 2^k - 1$ und $\sigma(m) = 1 + m \Rightarrow m \in \mathbb{P}$.

□

Bemerkung:
Primzahlen der Form $p = 2^k - 1$ heißen Mersennesche Primzahlen. Im Moment sind 46 Mersennesche Primzahlen bekannt. Ob es unendlich viele gibt ist unbekannt.

[Anm. des Verf.: Am 4.6.2009 wurde die 47. Mersennsche Primzahl gefunden.]

Ob es *ungerade* vollkommene Zahlen gibt, ist ebenfalls unbekannt.

1.17 Satz:
Ist $2^k - 1 \in \mathbb{P}$, so ist auch $k \in \mathbb{P}$.

Beweis:
Sei $k = r \cdot s, r, s \geq 2$, dann gilt:

$$2^k - 1 = 2^{rs} - 1 = \underbrace{(2^r - 1)}_{\geq 2} \underbrace{\sum_{j=0}^{s-1} 2^{rj}}_{\geq 2} \quad \Rightarrow \quad 2^k - 1 \notin \mathbb{P}$$

□

Beispiel:

$$\begin{aligned} 2^2 - 1 &= 3 \\ 2^3 - 1 &= 7 \\ &\vdots \\ 2^5 - 1 &= 31 \\ 2^{11} - 1 &= 2047 = 23 \cdot 89 \end{aligned}$$

1.3 Größter gemeinsame Teiler

1.18 Definition: (größter gemeinsamer Teiler)
Für $a, b \in \mathbb{Z}, a \neq 0 \vee b \neq 0$ ist

$$\text{ggT}(a,b) := \max\{d \in \mathbb{Z} : d \mid a, b\} =: (a,b)$$

der *größte gemeinsame Teiler* von a und b

Es gilt:

$$\begin{aligned} \text{ggT}(a,0) &= |a| \\ \text{ggT}(a,b) &\geq 1 \\ \text{ggT}(a,1) &= 1 \end{aligned}$$

1.19 Lemma:
Ist $b \neq 0$ und $a = mb + c$, so gilt $\text{ggT}(a,b) = \text{ggT}(b,c)$.

Beweis:

$$d \mid a, b \Rightarrow d \mid c \quad \wedge \quad d \mid b, c \Rightarrow d \mid a$$

□

1.20 Algorithmus: *Euklidischer Algorithmus*
Euklid: „Wenn b aber a nicht misst und man nimmt bei a, b abwechselnd immer das Kleinere vom Größeren weg, dann muss schließlich eine Zahl übrig bleiben, die die vorangehende misst."

Allgemein sei $a, b \neq 0$. Setze $r_0 := a, r_1 := b$.

$$\begin{aligned} r_0 &= s_0 \cdot r_1 + r_2 \quad 0 \leq r_2 < |r_1| \\ r_1 &= s_1 \cdot r_2 + r_3 \quad 0 \leq r_3 < r_2 \\ &\vdots \\ r_k &= s_k \cdot r_{k+1} + r_{k+2} \\ r_{k+1} &= s_{k+1} \cdot r_{k+2} + 0 \end{aligned}$$

Es ist $\text{ggT}(r_0, r_1) = \text{ggT}(r_1, r_2) = \ldots = \text{ggT}(r_{k+1}, r_{k+2}) = r_{k+2}$

Beispiel:
Berechne $\text{ggT}(343, 280) =: d$

$$\begin{aligned} 343 &= 1 \cdot 280 + 63 \\ 280 &= 4 \cdot 63 + 28 \\ 63 &= 2 \cdot 28 + 7 \\ 28 &= 4 \cdot 7 + 0 \end{aligned}$$

Also ist $\text{ggT}(343, 280) = 7$.

Bemerkung:
Das Euklidische Verfahren funktioniert sogar ohne Multiplikation. Pseudocode für ggT:

```
1 ggT(a,b) {
2     while a != 0 {
3         if (a > b)
4             a = a-b;
5         else
6             b = b-a;
```

```
7           }
8       return b;
9   }
```

Bemerkung:
Verfolgt man die Rechnungen im Euklidischen Algorithmus rückwärts, sieht man:

$$\begin{aligned} \text{ggT}(a,b) = r_{k+2} &= r_k - s_k \cdot r_{k+1} \\ r_{k+1} &= r_{k-1} - s_{k-1} \cdot r_k \\ &\vdots \end{aligned}$$

führt auf die Gleichung $ax + by = \text{ggT}(a,b)$ für $x, y \in \mathbb{Z}$.

1.21 Satz: *Formel von Bézout*
Sind $a, b \in \mathbb{Z}, a \neq 0 \vee b \neq 0$, so gibt es $x, y \in \mathbb{Z}$, mit $ax + by = \text{ggT}(a,b)$.

1.22 Korollar:
Jeder Teiler von $a, b (a, b \neq 0)$ teilt auch $\text{ggT}(a,b)$.

Beweis:

$$d \mid a, b \Rightarrow ax + by = \text{ggT}(a,b)$$

□

1.23 Korollar:
Zwei Zahlen $a, b \in \mathbb{Z}$ sind genau dann teilerfremd, wenn es $x, y \in \mathbb{Z}$ gibt mit $ax + by = 1$.

1.24 Korollar:
Sind $a, d \in \mathbb{Z}$ teilerfremd und gilt $d \mid a \cdot b$, so folgt $d \mid b$.

Beweis:
Schreibe $1 = ax + dy \Rightarrow b = abx + bdy \Rightarrow d \mid abx + bdy = b$ □

1.25 Korollar:
Sind $a, b \in \mathbb{Z}$ teilerfremd und gilt $a \mid m$ und $b \mid m$, so gilt $ab \mid m$.

Beweis:
Schreibe $m = s \cdot a, b \mid m = sa \Rightarrow b \mid s \Rightarrow s = rb \Rightarrow m = r \cdot a \cdot b$ □

1.4 Ganzzahlige Lösungen von $ax + by = c$

Wir betrachten jetzt Gleichungen der Art $ax + by = c$, wobei $a, b, c \in \mathbb{Z}$. Gesucht sind *ganzzahlige* Lösungen $x, y \in \mathbb{Z}$. Man nennt solche Gleichungen *lineare diophantische Gleichungen* (nach Diophantos von Alexandria, Mathematiker aus der Antike).

Geometrisch ist $ax+by = c$ eine Geradengleichung in der Ebene. Wir suchen die Lösungen mit ganzzahligen Koordinaten.

1.26 Lemma:
Sei $a, b \in \mathbb{Z}, a \neq 0 \vee b \neq 0$. Dann hat die Gleichung $ax + by = c$ genau dann Lösungen in $x, y \in \mathbb{Z}^2$, wenn $\text{ggT}(a, b) \mid c$.

Beweis:

„⇒“ Sei $d := \text{ggT}(a, b)$. Ist $d \mid c$, so finden wir nach Bézouts Lemma $x', y' \in \mathbb{Z}$ mit $ax' + by' = d$. Schreibe $c = d \cdot r \Rightarrow a(x'r) + b(y'r) = dr = c$.

„⇐“ Falls (x, y) eine Lösung ist, $ax + by = c$, so folgt $d \mid a, b \Rightarrow d \mid ax + by = c$.

□

Beispiel:

- $15x + 12y = 4$ hat keine ganzzahlige Lösung, da $\text{ggT}(12, 15) = 3 \nmid 4$.
- $3x + 7y = 4$ hat Lösungen, da $\text{ggT}(3, 7) = 1 \mid 4$.

Um nun *alle* ganzzahligen Lösungen zu finden, betrachten wir die Gleichungen $ax + by = 0$.

1.27 Lemma:
Sei $a, b \in \mathbb{Z}$ teilerfremd. Die ganzzahligen Lösungen von $ax + by = 0$ sind genau die Zahlen $(x, y) = (-bt, at)$, wobei $t \in \mathbb{Z}$ beliebig.

Beweis:

„⇒“ Ist (x, y) eine Lösung, so gilt $ax = -by \Rightarrow a \mid by$. Da $\text{ggT}(a, b) = 1$, folgt $a \mid y$. Schreibe $y = a \cdot t$ für ein $t \in \mathbb{Z} \Rightarrow ax = -bat$. Für $a \neq 0$ ist offensichtlich $x = -bt$. Für $a = 0$ folgt direkt $b = \pm 1$ also die Behauptung.

„⇐“ klar.

□

1.28 Theorem:
Sei $a, b \in \mathbb{Z}, a \neq 0 \vee b \neq 0$. Die lineare diophantische Gleichung $ax + by = c$ hat genau dann Lösungen $(x, y) \in \mathbb{Z}^2$, wenn $\text{ggT}(a, b) \mid c$ gilt.

Ist (x_0, y_0) eine solche Lösung, schreibe $d := \text{ggT}(a, b)$ sowie $a = a'd, b = b'd$. Die übrigen Lösungen (x, y) sind dann genau die Zahlenpaare $(x, y) = (x_0 - tb', y_0 + ta')$ für $t \in \mathbb{Z}$.

Beweis:
Das Kriterium für die Existenz von Lösungen haben wir bereits in Lemma *(1.26)* bewiesen.

Zum zweiten Teil: Sei (x_0, y_0) eine Lösung (die man z.B. mit dem euklidischen Algorithmus findet) und $(x, y) \in \mathbb{Z}^2$. Dann gilt:

$$\begin{aligned} ax + by = x &\iff a(x_0 - x) + b(y_0 - y) = 0 \\ &\overset{d \neq 0}{\iff} a'(x_0 - x) + b'(y_0 - y) = 0 \end{aligned}$$

Nun sind a', b' teilerfremd. Nach Lemma *(1.27)* sind damit die Zahlen $x_0 - y, y_0 - y$ von der Form $x_0 - x = b't$ und $y_0 - y = -a't$ für $t \in \mathbb{Z}$. □

Bemerkung:

- Der Beweis liefert ein konstruktives Verfahren zur Lösungssuche.
- Für konkrete Alltagslösungen hat man manchmal Zusatzbedingungen wie Positivität von $(x.y)$.

Frage:
Was ist mit lin. diophantischen Gleichungen mit mehr als 2 Variablen?

1.29 Definition: (Größter gemeinsamer Teiler für mehr als 2 Zahlen)
Für $a_1, \ldots, a_n \in \mathbb{Z}$ sei

$$\mathrm{ggT}(a_1, \ldots, a_n) := \max\{d \in \mathbb{Z} : d \mid a_1, \ldots, a_n\}$$

(Dabei sei $(a_1, \ldots, a_n) \neq (0, \ldots, 0)$). Offensichtlich gilt $\mathrm{ggT}(a_1, \ldots, a_n) = \mathrm{ggT}(\mathrm{ggT}(a_1, \ldots, a_{n-1}), a_n)$.

1.30 Satz: *Lemma von Bézout in Variation*
Sei $(0, \ldots, 0) \neq (a_1, \ldots, a_n) \in \mathbb{Z}^n$. Sei $d := \mathrm{ggT}(a_1, \ldots, a_n)$. Dann gibt es $x_1, \ldots, x_n \in \mathbb{Z}$, sodass

$$a_1x_1 + \ldots + a_nx_n = d$$

Beweis:
Wir führen eine vollständige Induktion über $n \in \mathbb{N}$:

Induktionsanfang: $n = 0, 1$**:** klar.

Induktionsschritt: $n \to n + 1$**:**

$$a := \mathrm{ggT}(a_1, \ldots, a_n) = x_1'a_1 + \ldots + x_n'a_n$$

$$\mathrm{ggT}(a_1, \ldots, a_{n+1}) = \mathrm{ggT}(a, a_{n+1}) = az + a_{n+1}x_{n+1} = (zx_1')a_1 + \ldots + (zx_n')a_n + a_{n+1}x_{n+1}$$

□

1.31 Korollar:
Sie $(a_1, \ldots, a_n) \in \mathbb{Z}^n, (a_1, \ldots, a_n) \neq (0, \ldots, 0)$. Die lin. diophantische Gleichung $a_1x_1 + \ldots + a_nx_n = c, c \in \mathbb{Z}$ hat genau dann ganzzahlige Lösungen, wenn gilt:

$$\mathrm{ggT}(a_1, \ldots, a_n) \mid c$$

Beweis:
Sei $d := \mathrm{ggT}(a_1, \ldots, a_n) \Rightarrow d \mid a_1x_1 + \ldots + a_nx_n = c$, falls $(x_1, \ldots x_n)$ Lösung.
Umgekehrt schreibe $d = a_1x_1' + \ldots + a_nx_n', c = r \cdot d \Rightarrow c = a_1(rx_1') + \ldots + a_n(rx_n')$ □

Bemerkung:
Wie löst man diese Gleichung praktisch?

$$a_1x_1 + \ldots + a_nx_n = c, \quad n \geq 3 \tag{1}$$

betrachte das Gleichungssystem

$$a_1x_1 + \ldots + a_{n-2}x_{n-2} + ay = c, \quad a = \mathrm{ggT}(a_{n-1}, a_n) \tag{2a}$$

$$a_{n-1}x_{n-1} + a_nx_n = ay \tag{2b}$$

Offensichtlich ist jede Lösung von (1) auch Lösung von (2a) und (2b). Die Gleichung (2b) ist für jedes $y \in \mathbb{Z}$ lösbar. Gleichung (2a) hat Lösung genau dann wenn $\mathrm{ggT}(a_1, \ldots, a_{n-2}, a) \mid c$.

Lösungsverfahren:
Löse (2a) als Gleichung in den Unbekannten $(x_1, \ldots, x_{n-2}, y)$, bestimme alle Lösungen von (2a). Für jede dieser Lösungen bestimme alle Lösungen der Glechung (2b) als Gleichung in $(x_{n-2}, x - n)$ zum vorher berechneten y.

1.5 Kongruenzen

1.32 Definition: (Kogruenz modulo m)
Sei $m \in \mathbb{Z}$ fest. Falls für $a, b \in \mathbb{Z}$ gilt, dass $m \mid a - b$, so schreibe $a \equiv b \bmod m$ oder $a \equiv b\ (m)$ und lies: „*a ist kongruent zu b modulo m*“.

Beispiel:

$$5 \equiv 7 \bmod 2$$
$$a \equiv 0 \bmod 2 \Leftrightarrow a \text{ gerade}$$
$$a \equiv b \bmod 0 \Leftrightarrow a = b$$

Bemerkung:
Offensichtlich gehlten folgende Regeln:

- $a \equiv 0 \bmod m \Leftrightarrow m \mid a \Leftrightarrow a$ ist Vielfaches von m
- $\forall a \in \mathbb{Z} : a \equiv a \bmod m$
- $\forall a, b \in \mathbb{Z} : a \equiv b \bmod m \Leftrightarrow b \equiv a \bmod m$
- $\forall a, b, c \in \mathbb{Z} : (a \equiv b \bmod m) \wedge (b \equiv c \bmod m) \Rightarrow a \equiv c \bmod m$

Damit ist Kongruenz mod m offensichtlich eine Äquivalenzrelation auf den ganzen Zahlen.

Ist $m \neq 0$, so gibt es zu jedem $a \in \mathbb{Z}$ genau ein $a_0 \in \mathbb{Z}$ mit $0 \leq a_0 < |m|$ und $a \equiv a_0 \bmod m$. Man nennt a_0 manchmal das *kleinste Residuum mod m* von a.

1.33 Satz:
Sei $m \in \mathbb{Z}$ fest. Kongruenz mod m ist verträglich mit Addition, Subtraktion und Multiplikation, d.h. falls $a \equiv a' \bmod m \wedge b \equiv b' \bmod m$, dann gilt auch:

$$a + r \cdot b \equiv a' + r \cdot b' \bmod m$$
$$a \cdot b \equiv a' \cdot b' \bmod m$$

Beweis:

$$\begin{aligned} a = a' + km \wedge b = b' + lm &\Rightarrow a + rb = a'rb' + m(k + rl) \\ &\Rightarrow a + rb \equiv a' + rb' \bmod m \\ a \cdot b = a'b' + (a'l + kb' + kl) &\Rightarrow a \cdot b \equiv a' \cdot b' \bmod m \end{aligned}$$

□

Bemerkung:
Vorsicht, beim Kürzen muss man aufpassen:

$$2 \cdot 3 \equiv 0 \bmod 6 \quad \text{aber} \quad 2, 3 \not\equiv 0 \bmod 6$$

1.34 Anwendung: Teilbarkeitsregeln:
Eine Zahl ist genau dann durch 9 teilbar, wenn ihre Quersumme durch 9 teilbar ist.

Sei $a \in \mathbb{Z}, a = \sum_{a=0}^{N} a_i 10^i$ in Dezimaldarstellung, also insbesondere, $0 \leq a_i < 10$. Die Quersumme ist $\sum_{i=0}^{N} a_i$. Es gilt:

$$10 = 9 + 1 \equiv 1 \bmod 9 \overset{(19)}{\Rightarrow} 10^i \equiv 1^i \bmod 9$$

Es folgt mit Satz *(1.33)*, dass auch $a \equiv \sum_{i=0}^{N} a_j \bmod 9$, also

$$a \text{ durch } 9 \text{ teilbar } \Leftrightarrow a \equiv 0 \bmod 9 \Leftrightarrow \sum_{i=0}^{N} a_i \equiv 0 \bmod 9$$

Genauso zeigt man die Teilbarkeitsregel für $m = 3$.

Beispiel:
Früher wurde das zur Kontrolle von Rechnungen benutzt:

$$\begin{aligned} 1152 \cdot 889 \overset{?}{=} 1024328 \quad &\Longrightarrow \quad 1152 \cdot 889 \equiv 1024328 \bmod 9 \\ &\overset{\text{Quersumme}}{\Longrightarrow} \quad 9 \cdot 26 \equiv 20 \bmod 9 \\ &\Longrightarrow \quad 0 \equiv 2 \bmod 9 \end{aligned}$$

Dies ist offensichtlich falsch.

Bemerkung:
Teilbarkeit durch 11:
Es gilt $10 = 11 - 1 \equiv -1 \bmod 11$, also bilde alternierende Quersumme:

$$a \text{ durch } 11 \text{ teilbar } \Leftrightarrow a \equiv \sum_{i=0}^{N} (-1)^i a_i \bmod 11$$

1.35 Satz:
Sind $m, c \in \mathbb{Z}$ teilerfremd, so folgt aus $a \cdot c \equiv b \cdot c \bmod m$, dass $a \equiv b \bmod m$. Ein c, das zu m teilerfremd ist, darf mal also kürzen.

Beweis:

$$m \mid (a-b)c \Rightarrow m \mid a - b \Rightarrow a \equiv b \bmod m$$

□

Beispiel:

$$4x \equiv 1 \bmod 15 \;\Leftrightarrow\; 4x \equiv 1 + 15 \bmod 15 \;\Rightarrow\; x \equiv 4 \bmod 15$$

Bemerkung:
Mit dieser Methode lassen sich lineare diophantische Gleichungen lösen. Für $b \neq 0$ genügt es x zu kennen.

$$ax + by = c \;\Leftrightarrow\; ax \equiv c \bmod b$$

denn eine Lösung der Kongruenz rechts liefert eine Lösung der Gleichung links.

Beispiel:

$$\begin{aligned} 9x + 16y = 35 \quad &\Leftrightarrow \quad 16y \equiv 35 \bmod 9 \\ &\Leftrightarrow \quad 7y \equiv 35 \bmod 9 \\ &\overset{(1.35)}{\Leftrightarrow} \quad y \equiv 5 \bmod 9 \\ &\Leftrightarrow \quad y = 5 + 9t \end{aligned}$$

1.36 Definition: (Lineare Kongruenz)
Eine Gleichung der Form $ax \equiv b \bmod m$ heißt *lineare Kongruenz*. Gesucht sind (ganzzahlige) Lösungen $x \in \mathbb{Z}$. Eine lineare Kongruenz lässt sich immer umschreiben in eine lineare diophantische Gleichung:

$$ax \equiv b \bmod m \Leftrightarrow ax - km = b$$

Bemerkung:
Das Theorem *(1.28)* liefert eine vollständige Antwort zur Lösbarkeit.

1.37 Theorem:
Sei $m > 0$ eine ganze Zahl. Die lineare Kongruenz $ax \equiv b \bmod m$ ist lösbar, genau dann wenn $\mathrm{ggT}(a, m) \mid b$.

Sei $d := \mathrm{ggT}(a, m)$. Schreibe $m = d \cdot m'$. Falls $d \mid b$ und falls x_0 eine Lösung der linearen Kongruenzen ist, so sind alle weiteren Lösungen von der Form $x = x_0 + tm', t \in \mathbb{Z}$.

Es gibt insbesondere genau d Lösungen x mit $0 \leq x < m$.

Beweis:
Umschreiben in die äquivalente lineare diophantische Gleichung $ax - km = b$ mit den beiden Unbekannten $x, k \in \mathbb{Z}$. Theorem *(1.28)* lässt sich darauf anwenden liefert die Behauptung. □

Die folgende Kürzungsregel ist sehr hilfreich:

1.38 Lemma:
Sei $d := \mathrm{ggT}(c, m)$, sei $m > 0$. Dann gilt

$$ac \equiv bc \bmod m \;\Leftrightarrow\; a \equiv b \bmod m'$$

Wobei $m = dm'$.

Beweis:

$$\begin{aligned} m \mid (a-b)c &\Rightarrow km = (a-b)c \quad \mid \text{setze } c'd = c \\ &\Rightarrow km' = (a-b)c' \quad \mid \mathrm{ggT}(m', c') = 1 \\ &\Rightarrow m' \mid a - b \end{aligned}$$

Umgekehrt:

$$m'l = a - b \Rightarrow m'lc = c(a-b) \Rightarrow m \mid c(a-b)$$

□

Beispiel:

$$\begin{aligned} 6x \equiv 15 \bmod 33 &\overset{(1.38)}{\Longleftrightarrow} 2x \equiv 5 \bmod 11 \\ &\Longleftrightarrow 2x \equiv 16 \bmod 11 \\ &\Longleftrightarrow x \equiv 8 \bmod 11 \\ &\Longleftrightarrow x = 8 + 11t \end{aligned}$$

Kapitel 2

Gruppen

2.1 Grundlagen

Manches in der Zahlentheorie wird einfacher vom abstrakten Standpunkt der Gruppen und Ringe aus betrachtet.

2.1 Definition: (Gruppe)
Sei G eine nicht leere Menge. Auf G sei eine Verknüpfung $\circ$ definiert, für die gilt:

- Assoziativität: $\forall a, b, c \in G : a \circ (b \circ c) = (a \circ b) \circ c$.
- Existenz eines neutralen Elementes: $\exists e \in G \; \forall g \in G : e \circ g = g = g \circ e$.
- Existenz eines inversen Elementes: $\forall g \in G \; \exists h \in G : g \circ h = e = h \circ g$.

Dann heißt $(G, \circ)$ *Gruppe*.

Bemerkung:
Neutrale Elemente sind immer eindeutig, denn seien e, e' neutrale Elemente, so folgt sofort:

$$e = ee' = e'$$

Inverse Elemente sind immer eindeutig, denn seien h, h' inverse Elemente zu g, so folgt sofort:

$$h = h \circ e = h \circ g \circ h' = e \circ h' = h'$$

2.2 Definition: (Monoid)
Sei G eine nicht leere Menge mit einer Verknüpfung $\circ$, für die gilt:

- Assoziativität: $\forall a, b, c \in G : a \circ (b \circ c) = (a \circ b) \circ c$.
- Existenz eines neutralen Elementes: $\exists e \in G \; \forall g \in G : e \circ g = g = g \circ e$.

Dann heißt $(G, \circ)$ *Monoid* oder *Halbgruppe*.

2.3 Definition: (abelsche Gruppe)
Sei $(G, \circ)$ eine Gruppe und gelte für $\circ$ zusätzlich

- Kommutativität: $\forall a, b \in G : a \circ b = b \circ a$.

so heißt $(G, \circ)$ *abelsche Gruppe*.

Beispiel:

- $(\mathbb{Z}, +)$ ist eine abelsche Gruppe.
- $(\mathbb{Q} - \{0\}, \cdot)$ ist eine abelsche Gruppe.
- $(\mathbb{N}, +)$ ist ein Monoid.
- $(\mathbb{R}^3, \cdot)$ ist eine nicht abelsche Gruppe.

2.4 Definition: (Untergruppe)
Sei $(G, \circ)$ eine Gruppe. Eine Teilmenge $H \subseteq G$ heit *Untergruppe*, falls H bezüglich $\circ$ eingeschränkt auf H selbst wieder eine Gruppe ist. Es also gilt:

(i) $e \in H$

(ii) $\forall a, b \in H : a \circ b \in H$.

(iii) $\forall g \in H : g^{-1} \in H$

Bemerkung:
Eine äquivalente Definition ist gegeben durch:

(i) $H \neq \emptyset$

(ii) $\forall g, h \in H : g \circ h^{-1} \in H$

Beispiel:
Für $m \in \mathbb{Z}$ ist $m\mathbb{Z} := \{mk \mid k \in \mathbb{Z}\}$ eine Untergruppe bezüglich $+$ von $\mathbb{Z}$.

2.5 Satz:
Die Untergruppen von $(\mathbb{Z}, +)$ sind genau die Untergruppen $m\mathbb{Z}$ mit $m \in \mathbb{N}$.

Beweis:
Sei $H \subseteq \mathbb{Z}$ eine Untergruppe.

Fall 1: $H = \{0\} \Rightarrow H = 0\mathbb{Z}$.

Fall 2: Sei $H \neq \{0\}$, dann gibt es ein $h \in H$, mit $h > 0$. Sei $m := \min\{h \in H \mid h > 0\}$. Für ein $h \in H$ gibt es dann $k \in \mathbb{Z}$, sodass $h = km + k_0$, wobei $0 \leq k_0 < m$.
Da $m \in H$ folgt, dass $km = m + \ldots + m \in H$ für $k \geq 0$ bzw. $km = (-m) + \ldots + (-m) \in H$ für $k < 0$. Also ist $k_0 = h - km \in H$.

Aus der Minimalität von m folgt $k_0 = 0$, also ist $h = km \in m\mathbb{Z}$.

□

Was haben Untergruppen von $(\mathbb{Z}, +)$ mit Kongruenzen zu tun?

$$a \equiv b \bmod m \Leftrightarrow m \mid (a - b) \Leftrightarrow a - b \in m\mathbb{Z}$$

Schreibweise: $a + m\mathbb{Z} := \{a + mk \mid k \in \mathbb{Z}\} \subseteq \mathbb{Z}$. Solche Mengen heißen *Nebenklassen* der Untergruppe $m\mathbb{Z}$

$$a \equiv b \bmod m \Leftrightarrow a \in b + m\mathbb{Z} \Leftrightarrow b \in a + m\mathbb{Z} \Leftrightarrow a + m\mathbb{Z} = b + m\mathbb{Z}$$

2.2 Linksnebenklassen und ihre Eigenschaften

2.6 Definition: (Linksnebenklassen)
Sei $(G, \cdot)$ eine Gruppe und $H \subseteq G$ eine Untergruppe, sei $g \in G$. Die Menge $gH := \{g \cdot h \mid h \in H\}$ heißt *Linksnebenklasse* von g in H. Es gilt $gH \subseteq G$.

Bemerkung:
Man kann auch *Rechtsnebenklassen* $Hg := \{hg \mid h \in H\} \subseteq G$ definieren. Ist G nicht kommutativ, so ist im Allgemeinen $gH \neq Hg$.

2.7 Satz:

(i) Die Abbildung $H \to gH, h \mapsto gh$, ($g \in G$ fest) ist eine Bijektion der Untergruppe $H \subseteq G$ auf die Nebenklasse $gH \subseteq G$. Insbesondere haben alle Linksnebenklassen gleich viele Elemente.

(ii) $g = g \cdot 1 \in gH$

(iii) $gH = H \Leftrightarrow g \in H$.

(iv) $g' \in gH \Leftrightarrow g'H = gH$.

Beweis:

(i) Betrachte $gH \to H, x \mapsto g^{-1}x$, so gilt für $x = gh, h \in H$, dass

$$gh \mapsto g^{-1}gh = h$$

Ist also Umkehrabbildung.

(ii) klar

(iii) „$\Leftarrow$“: $g \in H \Rightarrow gH \subseteq H$. Ist $h \in H$, so ist $h = gg^{-1}h \in gH \Rightarrow gH \supseteq H \Rightarrow gH = H$.
„$\Rightarrow$“: Ist $gH = H$, so folgt aus *(2.7.2)*, dass $g \in gH = H$.

(iv) Ist $g' \in gH \Rightarrow g = g \cdot h$ für ein $h \in H \Rightarrow g'H = ghH \overset{(2.7.3)}{=} gH$.
Ist $g'H = gH \overset{(2.7.2)}{\Rightarrow} g' \in g'H = gH$.

□

2.8 Definition: (Menge aller Linksnebenklassen)
Sei G eine Gruppe, $H \subseteq G$ Untergruppe. Die *Menge aller Linksnebenklassen* von H in G ist

$$G/H := \{gH \mid g \in G\}$$

Lies: „G modulo H“. Die Anzahl der Linksnebenklassen von H in G ist der *Index* von H in G:

$$[G : H] := \#G/H$$

2.9 Lemma:
G ist die disjunkte Vereinigung der H-Linksnebenklassen, d.h.

$$G = \bigcup \{gH \mid g \in G\}$$

und

$$gH \cap g'H \neq \emptyset \Rightarrow gH = g'H$$

Beweis:

$$g \in G \overset{(2.7.2)}{\Rightarrow} g \in gH \Rightarrow g \in \bigcup \{g'H \mid g' \in G\}$$

$$\tilde{g} \in gH \cap g'H \overset{(2.7.4)}{\Rightarrow} \tilde{g}H = gH \wedge \tilde{g}H = g'H \Rightarrow gH = g'H$$

□

2.10 Korollar: *Satz von Lagrange*
Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Dann ist G endlich genau dann, wenn H und $[G : H]$ endlich sind. In diesem Falle gilt:

$$\#G = \#H \cdot [G : H]$$

Beweis:

$$\sum_{gH \in G/H} \underbrace{\left(\sum_{x \in gH} 1 \right)}_{=\#gH} = [G : H] \cdot \#H$$

Nach Lemma *(2.9)* ist $\#G = \sum_{gH \in G/H} \left(\sum_{x \in gH} 1 \right)$. Wenn also H und $[G : H]$ endlich sind, gilt die Formel und G ist endlich.

Wenn G endlich ist, so ist auch die Teilmenge H endlich und G/H ist (als Menge von Teilmengen) selbst auch endlich. □

2.11 Korollar:
Ist G eine endliche Gruppe, $H \subseteq G$ Untergruppe, so gilt $\#H \mid \#G$

Bemerkung:
Die Anzahl der Elemente von G nennt man die *Ordnung* von G.

Bemerkung:
Die Anzahl der Links- und Rechtsnebenklassen von $H \subseteq G$ sind gleich, der Satz von Lagrange gilt auch für Rechtsnebenklassen.

Beweis:
Übungsaufgabe. □

Beispiel:
Wir betrachten die Gruppe $(\mathbb{Z}, +) = (G, \cdot)$ und deren Untergruppe $H = m\mathbb{Z}, m \in \mathbb{Z}$ fest.

- $m = 0, 0\mathbb{Z} = \{0\} \Rightarrow [\mathbb{Z} : \{0\}] = \infty$
- $m > 0$, dann ist $a + m\mathbb{Z} = \{b \in \mathbb{Z} \mid b \equiv a \bmod m$ eine typische Nebenklasse. Es gibt genau ein $a_0 \in \mathbb{Z}$ mit $a_0 \equiv a \bmod m$ und $0 \leq a_0 < m$ (vgl. 1.18). Folglich sind die Linksnebenklassen von $m\mathbb{Z}$ genau die folgenden: $m\mathbb{Z}, 1 + m\mathbb{Z}, \ldots, (m-1) + m\mathbb{Z}$, also m Stück. Also ist $[\mathbb{Z} : m\mathbb{Z}] = m$.

  Beachte: Endlicher Index, obwohl $\mathbb{Z}, m\mathbb{Z}$ unendlich ist.

2.3 Kongruenzrelationen

2.12 Definition: (Kongruenzrelation)
Sei G eine Gruppe. Eine *Kongruenzrelation* auf G ist eine Äquivalenzrelation "$\equiv$„, die mit der Verknüpfung verträglich ist, d.h. es soll gelten:

$$a \equiv a' \wedge b \equiv b' \Rightarrow a \cdot b \equiv a' \cdot b'$$

Setze $\bar{a} = \{g \in G \mid g \equiv a\}$ *Kongruenzklasse* von $a \in G$.

Beispiel:
Sei $(\mathbb{Z}, +) = (G, \cdot)$, dann ist $x \equiv y :\Leftrightarrow m \mid x - y$ eine Kongruenzrelation auf G.

2.13 Satz:
Sei $\equiv$ eine Kongruenzrelation auf der Gruppe G. Wir definieren $\bar{a} \cdot \bar{b} := \overline{a \cdot b}$. Dann gilt:

(i) Mit dieser Verknüpfung ist die Menge aller Kongruenzklassen eine Gruppe.

(ii) Die Kongruenzklasse $H := \{g \in G \mid g \equiv 1\} = \bar{1} \subseteq G$ ist eine Untergruppe von G.

(iii) Für alle $g \in G$ gilt $gH = Hg$.

(iv) Es gilt: $a \equiv b \Leftrightarrow a^{-1}b \in H$.

Beweis:

(i)
$$[a \equiv a' \wedge b \equiv b'] \Leftrightarrow \left[\bar{a} = \bar{a}' \wedge \bar{b} = \bar{b}'\right] \Rightarrow \left[\overline{a' \cdot b'} = \overline{a \cdot b}\right]$$

Diese Verknüpfung ist also wohldefiniert. Weiter gilt:

$$(\bar{a} \cdot \bar{b}) \cdot \bar{c} = \overline{ab} \cdot \bar{c} = \overline{abc} = \bar{a}(\bar{b} \cdot \bar{c})$$
$$\bar{1} \cdot \bar{a} = \overline{1 \cdot a} = \bar{a} = \bar{a} \cdot \bar{1}$$
$$\bar{a} \cdot \overline{a^{-1}} = \overline{a \cdot a^{-1}} = \bar{1} = \overline{a^{-1}} \cdot \bar{a}$$

Also sind alle Gruppenaxiome erfüllt.

(ii) Sei $H = \bar{1} \subseteq G$, $1 \equiv 1 \Rightarrow 1 \in \bar{1}$. Angenommen $g, k \in \bar{1}$, dann gilt:

$$g \equiv 1, h \equiv 1 \Rightarrow \bar{h} = \bar{1} \overset{\text{(i)}}{\Rightarrow} \overline{h^{-1}} = \bar{1} \Rightarrow h^{-1} \in \bar{1}$$

sowie
$$gh = 1 \cdot 1 = 1 \Rightarrow gh \in H$$

Also $H \subset G$ ist Untergruppe.

(iii)
$$a \in gH \Leftrightarrow g^{-1}a \in H \Leftrightarrow g^{-1}a \equiv 1 \Rightarrow a \equiv g$$
$$a \in Hg \Leftrightarrow ag^{-1} \in H \Leftrightarrow ag^{-1} \equiv 1 \Rightarrow a \equiv g$$

(iv)
$$a \equiv b \Leftrightarrow 1 \equiv a^{-1}b \Leftrightarrow a^{-1}b \in \bar{1} = H$$

□

2.14 Definition: (Normalteiler)
Eine Untergruppe $H \subseteq G$ heißt *normal* oder *Normalteiler*, falls für alle $a \in G$ gilt:

$$aH = Ha$$

Kurzschreibweise: $H \trianglelefteq G :\Leftrightarrow H$ ist Normalteiler in G.

Nicht jede Untergruppe ist normal (Übungsaufgabe), aber ist G abelsch, so ist jede Untergruppe normal.

2.15 Satz:
Sei G Gruppe und sei $H \trianglelefteq G$ normal. Dann ist $a \equiv b :\Leftrightarrow a^{-1}b \in H$ eine Kongruenzrelation auf G.

Beweis:

- $a \equiv a$
- $a \equiv b \Leftrightarrow b \equiv a$, denn $(b^{-1}a)^{-1} = a^{-1}b$
- $a \equiv b, b \equiv c \Rightarrow b^{-1}a \in H \wedge c^{-1}b \in H \Rightarrow (c^{-1}b)(b^{-1}a) = c^{-1}a \in H$

Also ist $\equiv$ eine Äquivalenzrelation.

Angenommen $a \equiv \tilde{a}, b \equiv \tilde{b}$, bleibt zu zeigen: $ab \equiv \tilde{a}\tilde{b}$

$$\left[\tilde{a}^{-1}a = h_1 \in H, \tilde{b}^{-1}b = h_2 \in H\right] \Rightarrow \left[a = \tilde{a}h_1 \wedge b = \tilde{b}h_2\right] \Rightarrow \left[ab = \tilde{a}h_1\tilde{b}h_2 = \tilde{a}\tilde{b}\underbrace{\tilde{b}^{-1}h_1\tilde{b}}_{=h_3 \in H}h_2\right]$$

Es ist $h_3 \in H$, denn $\tilde{b}H = H\tilde{b} \Rightarrow h_1\tilde{b} = \tilde{b}h_3 \Rightarrow \tilde{b}^{-1}h_1\tilde{b} = h_3 \in H \Rightarrow ab \equiv \tilde{a}\tilde{b}$. □

Fazit:
Kongruenzrelationen auf einer Gruppe G entsprechen Eins zu Eins Normalteilern in G.

Ist G abelsch, so entsprechen Kongruenzrelationen also genau den Untergruppen $H \subseteq G$. Insbesondere kennen wir damit alle Kongruenzrelationen auf $(\mathbb{Z}, +)$:

Ist $\equiv$ Kongruenzrelation auf $\mathbb{Z}$, so gibt es $m \in \mathbb{Z}$ so, dass $\equiv$ genau Kongruenz modulo m ist.

2.4 Homomorphismen

2.16 Definition: (Homomorphismus)
Seien $(G, \cdot)$ und $(K, \cdot)$ Gruppen. Eine Abbildung $\varphi : G \to K$ heißt *Homomorphismus*, falls für alle $g, h \in G$ gilt:

$$\varphi(gh) = \varphi(g)\varphi(h)$$

Bemerkung:
Es folgt:

$$1_K \cdot \varphi(1_G) = \varphi(1_G \cdot 1_G) = \varphi(1_G)\varphi(1_G) \quad \Longrightarrow \varphi(1_G) = 1_K$$
$$\varphi(gg^{-1}) = \varphi(1) = 1 = \varphi(g)\varphi(g^{-1}) \quad \Longrightarrow \quad \varphi(g^{-1}) = \varphi(g)^{-1}$$

2.17 Definition: (Mono-/Epi-/Isomorphismus)
Ein injektiver/surjektiver/bijektiver Homomorphismus heißt *Mono-/Epi-/Isomorphismus*.

Bemerkung:
Die Umkehrabbildung eines Isomorphismus ist selbst wieder ein Isomorphimus. Ist $\varphi : G \to K$ ein Isomorphismus, so schreibt man kurz: $\varphi : G \xrightarrow{\cong} K$.

Das Bild $\varphi(G) \subseteq K$ eines Homomorphismus ist immer eine Untergruppe. Ist G eine abelsche Gruppe, so ist auch $\varphi(G)$ eine abelsche Gruppe.

Beispiel:

1. Sei $(G, \cdot) = (K, \cdot) = (\mathbb{Z}, +)$. Setze $\varphi(x) := m \cdot x$ für ein festes $m \in \mathbb{Z}$. Dann gilt:

   $$\varphi(x + y) = m(x + y) = mx + my = \varphi(x) + \varphi(y)$$

   Also ist φ ein Homomorphismus. Weiter gilt:
   - φ ist Monomorphismus $\Leftrightarrow m \neq 0$.
   - φ ist Epimorphismus $\Leftrightarrow m = \pm 1$.
   - φ ist Monomorphismus $\Leftrightarrow m = \pm 1$.

2. Sei $G = (\mathbb{R}, +), (K, \cdot) = (\mathbb{R}_{>0}, \cdot), \exp : x \mapsto e^x$. Aus der Analysis kennen wir die Funktionalgleichung der Exponentialfunktion:

   $$e^{x+y} = e^x \cdot e^y$$

   Also ist exp ein Homomorphismus. Da exp sogar streng monoton steigend (also injektiv) und nach ganz $\mathbb{R}_{>0}$ abbildet, haben wir sogar einen Isomorphismus gefunden.

3. Sei G ein Gruppe und $H \trianglelefteq G$ ein Normalteiler mit zugehöriger Kongruenzrelation $\equiv$ auf G. Sei $g \in G$ mit Kongruenzklasse $\bar{g} := \{\tilde{g} \in G \mid \tilde{g} \equiv g\} = gH$. Definiere

$$P_H : G \to G/H,\ g \mapsto \bar{g} = gH$$

Nach Satz 2.9 ist G/H eine Gruppe mit Verknüpfung $\bar{g}\bar{h} = \overline{gh}$. Diese Gleichung sagt genau aus, dass P_H ein Homomorphismus (sogar Epimorphismus) ist.

4. Konkretes Beispiel zu 3.: Sei $(G, \cdot) = (\mathbb{Z}, +), H = m\mathbb{Z}$ für ein festes $m \in \mathbb{Z}$. Dann ist $\mathbb{Z}/m\mathbb{Z} =: \mathbb{Z}/m$ eine abelsche Gruppe, deren Elemente die Kongruenzklassen von ganzen Zahlen modulo m sind.

   Für $m = 0$ ist $\mathbb{Z}/0 \cong \mathbb{Z}$. Für $m \neq 0$ hat $\mathbb{Z}/m$ genau $|m|$ Elemente.

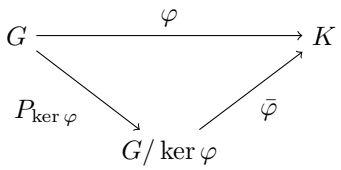
2.18 Definition: (Kern)
Sei $\varphi : G \to K$ ein Homomorphismus. Der *Kern* von φ ist

$$\ker(\varphi) := \{g \in G \mid \varphi(g) = 0\}$$

2.19 Satz: *Homomorphiesatz*
Sei $\varphi : G \to K$ ein Gruppenhomomorphismus. Dann ist $\ker\varphi \subseteq G$ ein Normalteiler in G. Die zugehörige Kongruenzrelation auf G ist gegeben durch:

$$g \equiv \tilde{g} \Leftrightarrow \varphi(g) = \varphi(\tilde{g})$$

Definiere $\bar{\varphi} : G/\ker\varphi \to K$ durch $\bar{\varphi}(\bar{g}) := \varphi(g)$. Dann ist $\bar{\varphi}$ ein Homomorphismus. Weiter gilt $\bar{\varphi} \circ P_{\ker\varphi} = \varphi$, d.h. das Diagramm



kommutiert. Ist $\psi : G/\ker\varphi \to K$ ein weiterer Homomorphismus mit $\psi \circ P_{\ker\varphi} = \varphi$, so gilt bereits $\psi = \bar{\varphi}$.

Beweis:
$\ker\varphi$ ist Normalteiler: $1 \in \ker\varphi,\ \varphi(g) = 1 = 1^{-1} = \varphi(g^{-1}),\ \varphi(g\tilde{g}) = \varphi(g)\varphi(\tilde{g}) \Rightarrow \ker\varphi$ ist Untergruppe von G.

Einfaches Argument: $g \equiv \tilde{g} :\Leftrightarrow \varphi(g) = \varphi(\tilde{g})$ ist offensichtlich Kongruenzrelation. Nach (2.9) ist $\bar{1} = \ker\varphi$ ein Normalteiler, der zu dieser Kongruenzklasse gerhört, $\bar{g} = g \cdot \ker\varphi$ Kongruenzklasse von g.

Wegen $\overline{g\tilde{g}} = \bar{g}\bar{\tilde{g}}$ folgt mit $\bar{\varphi}(\bar{g}) := \varphi(g)$, dass

$$\bar{\varphi}(\overline{g\tilde{g}}) = \bar{\varphi}(\bar{g} \cdot \bar{\tilde{g}}) = \varphi(g\tilde{g}) = \varphi(g)\varphi(\tilde{g}) = \bar{\varphi}(\bar{g})\bar{\varphi}(\bar{\tilde{g}})$$

also ist $\bar{\varphi}$ ein Homomorphismus (φ ist wohldefiniert, da: $\bar{g} = \bar{\tilde{g}} \Leftrightarrow \varphi(g) = \varphi(\tilde{g}) \Rightarrow \bar{\varphi}(\bar{g}) = \bar{\varphi}(\bar{\tilde{g}})$).

Weiter ist $P_{\ker\varphi}(g) = g \cdot \ker\varphi = \bar{g}$, also $\bar{\varphi} \circ P_{\ker\varphi}(g) = \bar{\varphi}(\bar{g}) = \varphi(g)$.

Ist ψ wie oben, so folgt:

$$\psi \circ P_{\ker\varphi}(g) = \psi(\bar{g}) = \varphi(g) = \bar{\varphi}(\bar{g}) \ \Rightarrow\ \psi = \bar{\varphi}$$

Schließlich ist $\bar{\varphi}$ injektiv, denn

$$\bar{\varphi}(\bar{g}) = \bar{\varphi}(\bar{\tilde{g}}) \Leftrightarrow \varphi(g) = \varphi(\tilde{g}) \Leftrightarrow g \equiv \tilde{g}$$

□

2.20 Korollar:
Ein Homomorphismus $\varphi : G \to K$ ist genau dann injektiv, wenn $\ker\varphi = \{1\}$.

Beweis:

$$\begin{aligned}\ker\varphi = \{1\} &\Leftrightarrow [\forall g, \tilde{g} \in G : g \equiv \tilde{g} \Leftrightarrow g = \tilde{g}] \\ &\Leftrightarrow [\forall g, \tilde{g} \in G : \varphi(g) = \varphi(\tilde{g}) \Leftrightarrow g = \tilde{g}] \\ &\Leftrightarrow \varphi \text{ injektiv}\end{aligned}$$

□

2.21 Korollar:
Falls $\varphi : G \to K$ ein Epimorphismus ist, so ist $\bar{\varphi} : G/\ker\varphi \to K$ ein Isomorphismus.

Beispiel:
Betrachte $m\mathbb{Z} \subseteq \mathbb{Z}$ für $m > 0$. Dies ist eine Untergruppe von $(\mathbb{Z}, +)$, setze:

$$\mathbb{Z}/m\mathbb{Z} =: \mathbb{Z}/m\,(= \mathbb{Z}_m)$$

ist eine endliche abelsche Gruppe mit m Elementen. Die Elemente sind die Kongruenzklassen mod m. Die Verknüpfung auf $\mathbb{Z}/m$ ist $\bar{a} + \bar{b} := \overline{a+b}$.

Ist z.B. $m = 2$, dann ist $\mathbb{Z}/2 = \{\bar{0}, \bar{1}\}$ mit $\bar{0} = 2\mathbb{Z} = \{$ gerade Zahl $\}, \bar{1} = 1 + 2\mathbb{Z} = \{$ ungerade Zahl $\}$.

Ist $m = 3$, dann ist $\mathbb{Z}/3 = \{\bar{0}, \bar{1}, \bar{2}\}$.

2.5 Zyklische Gruppen

2.22 Definition: (Zyklische Gruppen)
Sei $(G, \cdot)$ eine Gruppe und $a \in G$. Für $m \in \mathbb{Z}$ setze

$$a^m := \begin{cases} \underbrace{a \cdot a \cdots a}_{m\text{-mal}} & m > 0 \\ 1 & m = 0 \\ \underbrace{(a \cdot a \cdots a)}_{m\text{-mal}}^{-1} & m < 0 \end{cases}$$

Für alle $k, l \in \mathbb{Z}$ gilt mit dieser Konvention: $a^k \cdot a^l = a^{k+l}$.

Setze $\langle a \rangle := \{a^k \mid k \in \mathbb{Z}\}$, dann ist $\langle a \rangle \subset G$ eine Untergruppe von G. Man nennt sie die von a erzeugte *zyklische Untergruppe*.

Bemerkung:
Wählt man die Verknüpfung auf G additiv so schreibt man $n \cdot a$ statt a^n. Dies ist aber nur eine Änderung der Schreibweise.

2.23 Lemma:
Sei $a \in G$, setze $\alpha(k) := a^k$ für $k \in \mathbb{Z}$. Dann ist $\alpha : \mathbb{Z} \to G$ ein Gruppenhomomorphismus von $(\mathbb{Z}, +)$ nach $(G, \cdot)$.

2.24 Definition: (Ordnung)
Sei G eine Gruppe, sei $a \in G$. Die *Ordnung* von a ist definiert als

$$o(a) := \begin{cases} \infty & \text{falls } a^k \neq 1 \text{ für alle } k > 0 \\ \min\{k \geq 1 \mid a^k = 1\} & \text{sonst} \end{cases}$$

2.25 Satz:
Sei G eine Gruppe, $a \in G$. Dann gilt:

(i) $o(a) = \infty \Leftrightarrow \alpha : \mathbb{Z} \to G$ ist ein Isomorphismus auf $\langle a \rangle$.

(ii) $o(a) = m < \infty \Leftrightarrow \#\langle a \rangle = m$. Dann ist $\bar{\alpha} : \mathbb{Z}/m \to \langle a \rangle$ aus dem Homomorphiesatz ein Isomorphismus.

Ist $o(a) = m < \infty$, so ist $o(a) = \#\langle a \rangle$. Mit dem Satz von Lagrange folgt: Ist $\#G < \infty$ und $a \in G$, so gilt

$$o(a) \mid \#G$$

Beweis:

(i)

$$\alpha(k) = a^k = a \Leftrightarrow \alpha(-k) = 1$$

Also:

$$\begin{aligned} \alpha(k) \neq 1 \text{für alle } k \geq 1 &\Leftrightarrow \alpha(k) \neq 1 \text{für alle } k \neq 0 \\ &\Leftrightarrow \ker \alpha = \{0\} \\ &\Leftrightarrow \alpha \text{ ist Monomorphismus} \\ &\Leftrightarrow \alpha \text{ ist Isomorphismus von } (\mathbb{Z}, +) \text{ und } \alpha(\mathbb{Z}) = \langle a \rangle \end{aligned}$$

(ii) Nach (i) gilt $o(a) = \infty \Leftrightarrow \alpha$ injektiv, also $o(a) < \infty \Leftrightarrow \alpha$ nicht injektiv $\Leftrightarrow \ker \alpha \neq \{0\}$. Nach 2.5 ist $\ker \alpha = m\mathbb{Z}$ für ein $m > 0$. Nach 2.13 ist $\alpha(\mathbb{Z})$ insomorph zu $\mathbb{Z}/\ker \alpha = \mathbb{Z}/m$. weiter gilt $\alpha(m) = a^m = 1$ für $0 < t < m$ ist $\alpha(t) \neq 1$, also $o(a) = m$.

Es ist $o(a) = \#\langle a \rangle, \langle a \rangle \subseteq G$ ist Untergruppe. Nach 2.8 folgt, dass $o(a) = \#\langle a \rangle \mid \#G$. □

Fazit:
Jede unendliche zyklische Gruppe ist isomorph zu $(\mathbb{Z}, +)$. Jede endliche zyklische Gruppe G ist isomorph zu $\mathbb{Z}/m$ für ein $m \geq 1$, mit $\#G = m$.

2.26 Satz:
Sei G eine endliche zyklische Gruppe der Ordnung $\#G = m$, etwa $\langle a \rangle = G$ für ein $a \in G$. Sei $H \subseteq G$ eine Untergruppe. Dann gibt es $r, s \in \mathbb{N}$ mit $m = rs$ mit $\#H = s$ und $H = \langle a^r \rangle$. Insbesondere ist H auch zyklisch.

Beweis:
Betrachte $\alpha : \mathbb{Z} \to G, \alpha(k) = a^k$. Setze $\tilde{H} = \{k \in \mathbb{Z} \mid \alpha(k) \in H\}$. Dann ist $\tilde{H} \subset \mathbb{Z}$ selbst wieder eine Untergruppe, denn $\tilde{0} \in \tilde{H}$ und $k, l \in \tilde{H} \Rightarrow k \pm l \in \tilde{H}$.

Nach 2.5 gibt es $r \geq 1$ mit $\tilde{H} = r\mathbb{Z}$. Da $\ker \alpha \subseteq \tilde{H}$ also $m\mathbb{Z} \subseteq r\mathbb{Z} \Rightarrow r \mid m$. Schreibe $m = rs$.

$$H = \alpha(\tilde{H}) = \left\{a^{k \cdot r} \mid k \in \mathbb{Z}\right\} = \langle a^r \rangle$$

Für $0 < t < s$ ist $\alpha(rt) = a^{rt} \neq 1$, also $\#H = s$

□

2.27 Korollar:
Jede Untergruppe einer zyklischen Gruppe ist zyklisch.

Beweis:
Für endliche zyklische Gruppen folgt dies direkt aus dem vorigen Satz *(2.26)*. Eine unendliche zyklische Gruppe ist isomorph zu $(\mathbb{Z}, +)$, die Untergruppen $m\mathbb{Z} \subseteq \mathbb{Z}$ sind offensichtlich zyklisch *(2.5)*. □

2.28 Korollar:
Ist G endlich und zyklisch, $\#G = m$, so gibt es zu jedem Teiler s von m genau eine Untergruppe $H \subseteq G$ mit $\#H = s$.

Beweis:
Schreibe $G = \langle a \rangle$ und $m = rs$. Für $\langle a^r \rangle$ gilt $\#\langle a^r \rangle = s$. Der vorige Beweis zeigt umgekehrt, dass jede Untergruppe H mit $\#H = s$ genau $H = \langle a^r \rangle$ ist. □

2.29 Satz:
Ist G zyklisch der Ordnung $m < \infty$ und ist $G = \langle a \rangle$, so gilt für $b = a^r$, dass $\langle b \rangle = \langle a \rangle = G$ genau dann, wenn $\mathrm{ggT}(r, m) = 1$.

Beweis:

$$\langle b \rangle = \langle a \rangle \Rightarrow \exists s \in \mathbb{Z} : b^s = a \Rightarrow a^{rs} = a = a^1 \Rightarrow rs \equiv 1 \bmod m$$

Nach Bézout *(1.21)* folgt $rs + xm = 1 \Rightarrow \mathrm{ggT}(m, r) = 1$.
Ist umgekehrt $\mathrm{ggT}(m, r) = 1$, so gibt es nach *(1.21)* ein $s \in \mathbb{Z}$ mit $rs \equiv 1 \bmod m$, also

$$\underbrace{a^{rs}}_{=b^s} = a^1 \Rightarrow a \in \langle b \rangle \Rightarrow \underbrace{\langle a \rangle}_{=G} \subseteq \langle b \rangle$$

□

2.30 Definition: (Eulersche φ-Funktion)
Für $m \in \mathbb{Z}, m > 1$ sei

$$\varphi(m) := \#\{d \in \mathbb{Z} \mid 1 \leq d \leq m, \mathrm{ggT}(d.m) = 1\}$$

Ist G zyklisch der Ordnung m, so ist

$$\#\{b \in G \mid \langle b \rangle = G\} = \varphi(m)$$

Beispiel:

m	1	2	3	4	5	6	7	8
$\varphi(m)$	1	1	2	2	4	2	6	4

2.31 Satz:
Für jedes $m \geq 1$ gilt:

$$\sum_{d|m, d \geq 1} \varphi(d) = m$$

Beweis:
Zu jedem Teiler d von m gibt es genau eine Untergruppe $H_d \subseteq G, G \cong \mathbb{Z}/m$. Jedes H_d hat genau $\varphi(d)$ Erzeuger. Jedes $g \in G$ liegt in genau einem H_d, nämlich $H_d = \langle g \rangle$. Also ist

$$\sum_{d|m, d \geq 1} \varphi(d) = \#G = m$$

□

2.32 Korollar:
Sei G eine endliche abelsche Gruppe, $m = \#G$. Falls es zu jedem Teiler d von m höchstens eine Untergruppe $H \subseteq G$ gibt mit $\#H = d$, so ist G zyklisch.

Beweis:
Es gilt

$$m = \#G = \# \dot{\bigcup_{d|m, d\geq 1}} \{g \in G \mid o(g) = d\}$$

Weiter ist $\{g \in G \mid o(a) = d\} \leq \varphi(d)$ nach den Annahmen über G. Also folgt

$$m = \#G \leq \sum_{d|m, d\geq 1} \varphi(d) = m$$

Also gilt schon Gleichheit. Insbesondere ist $\{g \in G \mid o(g) = m\} \neq \emptyset$. Für $g \in G$ mit $o(g) = m = \#G$ folgt aber $\langle g \rangle = G$. □

Kapitel 3

Ringe

3.1 Grundlagen

3.1 Definition: (Ring)
Ein (kommutativer) *Ring* $(R, +, \cdot)$ besteht aus einer (nicht leeren) Menge R mit zwei Verknüpfungen $+, \cdot : R \times R \to R$ mit folgenden Eigenschaften:

(i) $(R, +)$ ist abelsche Gruppe

(ii) Die Multiplikation ist assoziativ, kommutativ und hat ein neutrales Element

(iii) Es gilt das Distributivgesetz $(a + b) \cdot c = ac + bc$.

Beispiel:
$(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ sind Ringe.
Aber $(\mathbb{N}, +, \cdot)$ ist kein Ring, da die inversen Elemente der Addition fehlen.

Bemerkung:
Das neutrale Element in $(\mathbb{R}, +)$ wird mit 0 bezeichnet, das neutrale Element in $(\mathbb{R}, \cdot)$ mit 1. Beide neutralen Elemente sind eindeutig bestimmt (vgl. 2.1).

Aus den Axiomen folgt unter anderem:

- $\forall r \in \mathbb{R} : r \cdot 0 = r \cdot (0 + 0) = r \cdot 0 + r \cdot 0 \overset{\text{kürzen}}{\Longrightarrow} 0 = r \cdot 0$

Aber Vorsicht: beim Multiplizieren in Ringen darf man nicht immer kürzen

extremes Beispiel:
$R := \{0\}$ mit $0 + 0 = 0 \cdot 0 = 0$ ist ein Ring. Hier gilt sogar $1 = 0$.

3.2 Definition: (Einheit)
Eine Element $r \in R$ heißt *Einheit*, wenn es ein Element $s \in R$ gibt mit $r \cdot s = 1$, d.h. r hat ein multiplikatives Inverses in R. Wir bezeichnen die Menge aller Einheiten in R

$$R^* := \{r \in R \mid r \text{ ist Einheit}\}$$

als die *Einheitengruppe von R*. Es gilt stets $1 \in R^* \Rightarrow R^* \neq \emptyset$ und R^* ist eine abelsche Gruppe.

Beispiel:
$\mathbb{Z}^* = \{\pm 1\}, \quad \mathbb{Q}^* = \mathbb{Q} - \{0\}, \quad \mathbb{R}^* = \mathbb{R}^* - \{0\}, \ \ldots$

3.3 Definition: (Körper)
Ein Ring R mit $R^* = R - \{0\}$ heißt *Körper*. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Körper, $\mathbb{Z}$ ist kein Körper.

3.4 Definition: (Kongruenzrelation)
Sei R ein Ring. Eine *Kongruenzrelation* auf R ist eine Äquivalenzrelation $\equiv$ mit folgenden zusätzlichen Eigenschaften:

$$(a \equiv a' \wedge b \equiv b') \Rightarrow (a + b \equiv a' + b' \wedge ab \equiv a'b')$$

Beispiel:
Nach 1.19 ist Kongruenz modulo m eine Kongruenzrelation auf $(\mathbb{Z}, +, \cdot)$.

3.5 Satz:
Sei R ein Ring mit Kongruenzrelation $\equiv$. Für $a \in R$ setze $\bar{a} := \{r \in R \mid a \equiv r\}$, und sei $I := \{r \in R \mid r \equiv 0\} = \bar{0} \subseteq R$. Dann gilt:

(i) $\bar{a} = a + I$ (Linksnebenklasse von a nach I in der Gruppe $(R, +)$

(ii) $R/I := \{\bar{a} \mid a \in R\}$ ist ein Ring mit Verknüpfungen $\bar{a} + \bar{b} = \overline{a + b}$ und $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$

(iii) $\forall i \in I, r \in R : i \cdot r \in I$

Beweis:
Nach 2.9 ist $I \subseteq R$ eine Untergruppe von $(R, +)$, also gilt (i).
Da die Kongruenzrelation $\equiv$ mit Addition und Multiplikation verträglich ist, erhalten wir Verknüpfungen wie in (ii). Nach 2.9 ist $(R/I, +)$ eine abelsche Gruppe. Die Multiplikation hat alle Eigenschaften, die wir brauchen, z.B. Distributivgesetz:

$$(\bar{a} + \bar{b}) \cdot \bar{c} = \overline{(a + b) \cdot c} = \overline{ac + bc} = \bar{a} \cdot \bar{c} + \bar{b} \cdot \bar{c}$$

Behauptung (iii) gilt, denn

$$i \in I \Leftrightarrow i \equiv 0 \Rightarrow r \cdot i = r \cdot 0 = 0 \Rightarrow ri \in I$$

□

3.2 Kongruenzrelationen

3.6 Definition: (Ideal)
Ist R ein Ring, $I \subseteq R$ Untergruppe von $(R, +)$ mit der Eigenschaft, $i \in I, r \in R \Rightarrow ir \in I$, so heißt I *Ideal* im Ring R, schreibe $I \trianglelefteq R$.

Die Kongruenzklasse der Null ist also immer ein Ideal.

Beispiel:
$I \subset \mathbb{Z}$ Untergruppe, dann ist $I = m\mathbb{Z}$ also insbesondere auch ein Ideal:

$$i \in I \Leftrightarrow \exists k \in \mathbb{Z} : i = mk \qquad r \in \mathbb{Z} \Rightarrow ir = mkr \in I$$

3.7 Satz:
Sei $I \trianglelefteq R$ ein Ideal. Definiere

$$r \equiv s :\Leftrightarrow r - s \in I$$

Dann ist „$\equiv$“ eine Kongruenzrelation auf dem Ring R.

Beweis:
Es ist $r \equiv s$ genau dann wenn es ein $i \in I$ gibt mit $r = s + i$. Also

$$(a \equiv a' \wedge b \equiv b') \Rightarrow \exists i, j \in I : (a' = a + i \wedge b' = b + i)$$

Weiter gilt:

$$a' + b' = a + b + (i + j) \equiv a + b, \quad a' \cdot b' = a \cdot b + a \cdot j + b \cdot i + ij = ab + \underbrace{(aj + bi + ij)}_{\in I} \equiv a \cdot b$$

(Wir rechnen nicht nach, dass „$\equiv$“ eine Äquivalenzrelation ist.) □

Fazit:
Wir haben durch die beiden vorigen Sätze eine 1-1-Entsprechung zwischen Idealen in R und Kongruenzrelationen auf R.

Beispiel:

1. Sei R ein Ring, $a \in R$. Setze
$$(a) := Ra = \{ra \mid r \in R\}$$
Dann heißt (a) das von a erzeugte Hauptideal.

2. Sei $R = \mathbb{Z}, a \in \mathbb{Z}$. Dann ist $(a) = a\mathbb{Z} \trianglelefteq \mathbb{Z}$ ein Ideal. Die zugehörige Kongruenzrelation ist Kongruenz modulo a. Der Ring der Kongruenzklassen ist
$$\mathbb{Z}/a := \mathbb{Z}/a\mathbb{Z} = \{r + a\mathbb{Z} \mid r \in \mathbb{Z}\}$$
Für $a \neq 0$ ist $\mathbb{Z}/a$ ein endlicher Ring mit $|a|$ Elementen.

3. Sei $R = \mathbb{Z}/m, m > 1$. Ist $I \trianglelefteq \mathbb{Z}/m$, so ist insbesondere $I \subseteq \mathbb{Z}/m$ Untergruppe. Nach (2.26) gibt es dann ein $\bar{r} \in \mathbb{Z}/m$ mit
$$\begin{aligned} I = \langle \bar{r} \rangle &= \{k\bar{r} \mid k \in \mathbb{Z}\} \\ &= \{\overline{kr} \mid k \in \mathbb{Z}\} \\ &= \{\bar{k} \cdot \bar{r} \mid \bar{k} \in \mathbb{Z}/m\} = (\bar{r}) \end{aligned}$$
Alle Ideale in $\mathbb{Z}/m$ sind also von dieser Gestalt.

Beweis:

1. Es ist $r \cdot a + s \cdot a = (r + s) \cdot a \wedge r \cdot a + (-r) \cdot a = 0$ also ist $((a), +)$ eine Gruppe. Außerdem gilt für alle $s \in R$, dass $s(r \cdot a) = (s \cdot r)a \in (a)$.

□

3.8 Satz:
Die Einheitengruppe von $\mathbb{Z}/m$ ist
$$(\mathbb{Z}/m)^* = \{\bar{a} \mid a \in \mathbb{Z}, \mathrm{ggT}(a, m) = 1\}$$

Beweis:
Sei $\bar{a} \in \mathbb{Z}/m$ Einheit, dann gibt es nach Definition ein $b \in \mathbb{Z}$ mit
$$\begin{aligned} \bar{a} \cdot \bar{b} = \bar{1} \quad &\iff \quad a \cdot b \equiv 1 \bmod m \\ &\iff \quad \exists x \in \mathbb{Z} : a \cdot b + m \cdot x = 1 \\ &\overset{\text{Bézout}}{\iff} \quad \mathrm{ggT}(a, m) = 1 \end{aligned}$$

□

3.9 Satz:
Insbesondere ist $\mathbb{Z}/m$ ein Körper, genau dann wenn m eine Primzahl ist.

Beweis:

$$\begin{aligned}
\mathbb{Z}/m \text{ Körper} &\overset{\text{Def}}{\iff} \mathbb{Z}/m^* = \mathbb{Z}/m - \{\bar{0}\} \\
&\iff \forall a \in \mathbb{Z} : a \in m\mathbb{Z} \veebar \operatorname{ggT}(a,m) = 1 \\
&\iff \pm 1, \pm m \text{ sind die einzigen Teiler von } m
\end{aligned}$$

□

Beobachtung:
Ist G eine endliche Gruppe und $g \in G$, so gilt $g^{\#G} = 1$. Denn: $o(g) =: l \mid \#G$ nach (2.25) und damit $\#G = k \cdot l \Rightarrow g^{\#G} = (g^l)^k = 1^k = 1$.

3.10 Satz: *(Euler)*
Ist $a, m \in \mathbb{Z}, m \geq 1$ und $\operatorname{ggT}(a,m) = 1$, so gilt $a^{\varphi(m)} \equiv 1 \bmod m$.

Beweis:
Wir rechnen in $\mathbb{Z}/m$. Es ist $\#\mathbb{Z}/m^* = \varphi(m)$, denn $\varphi(m) = \#\{a \in \mathbb{Z} \mid 0 \leq a \leq m, \operatorname{ggT}(a.m) = 1\}$. Nach Voraussetzung ist $\bar{a} \in \mathbb{Z}/m^*$, also $(\bar{a})^{\varphi(m)} = \bar{1}$. □

3.11 Korollar: *kleiner Satz von Fermat*
Ist $p \in \mathbb{P}$ und $a \in \mathbb{Z}$, so gilt $a^p \equiv a \bmod p$. Falls zusätzlich $p \nmid a$, so gilt $a^{p-1} \equiv 1 \bmod p$.

Beweis:
Nach dem Satz von Euler *(3.10)* gilt $a^{\varphi(p)} \equiv 1 \bmod p$ falls $p \nmid a$. Nun ist $\varphi(p) = p - 1$, da $p \in \mathbb{P}$, also $p \nmid a \Rightarrow a^{p-1} \equiv 1 \bmod p \Rightarrow a^p \equiv a \bmod p$ falls $p \nmid a$.
Falls $p \mid a$, so gilt $a \equiv 0 \bmod p \Rightarrow a^p \equiv 0 \bmod p \wedge a^p \equiv a \bmod p$. □

Beispiel: (Fermat)
Für alle $p \in \mathbb{P}$ gilt $p \mid 2^p - 2$ (Spezialfall für $a = 2$).

3.12 Satz: *Satz von Wilson*
Sei $m \in \mathbb{Z}, m \geq 2$. Es gilt $(m-1)! \equiv -1 \bmod m$ genau dann, wenn $m \in \mathbb{P}$.

Beweis:
Wir rechnen wieder in $\mathbb{Z}/m$. Ist $m \notin \mathbb{P}$, etwa $m = s \cdot t$ mit $s, t \geq 2$, dann folgt $\bar{s} \cdot \bar{t} = \bar{m} = \bar{0}$ in $\mathbb{Z}/m$, aber $\bar{s}, \bar{t} \not\equiv 0 \bmod m$, also $\bar{1} \cdot \bar{2} \cdots \overline{(m-1)} = \bar{0} \neq \bar{-1}$
Ist $m \in \mathbb{P}$, so ist $\mathbb{Z}/m$ ein Körper.

Vorüberlegung: In einem Körper hat die Gleichung $x^2 = 1$ genau die Lösungen ± 1, denn $x^2 = 1 \Leftrightarrow x^2 - 1 = 0 \Leftrightarrow (x-1)(x+1) = 0 \Leftrightarrow x = 1 \vee x = -1$.

Für $\bar{a} \in \mathbb{Z}/m, \bar{a} \neq \bar{0}, \bar{\pm 1}$ ist also $\bar{a}^{-1} \neq \bar{a}$. Es folgt $\bar{2} \cdot \bar{3} \cdots \overline{(m-2)} = \bar{1}$, da sich jedes Element mit seinem Inversen in $\mathbb{Z}/m$ kürzt. Also ist

$$\bar{1} \cdot \bar{2} \cdots \overline{(m-2)} \cdot \overline{(m-1)} \equiv \overline{m-1} \equiv \overline{-1} \bmod m$$

□

3.13 Definition: (Ringhomomorphismus)
Seien R, S Ringe und $\varphi : R \to S$ eine Abbildung. Wir nennen φ einen *(Ring-)Homomorphismus*, wenn gilt:

(i) $\forall a, b \in R : \varphi(a+b) = \varphi(a) + \varphi(b)$

(ii) $\forall a, b \in R : \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

(iii) $\varphi(1) = 1$

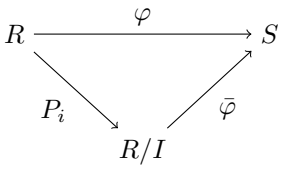
Beispiel:
Die Abbildung $\mathbb{Z} \to \mathbb{Z}/m, r \mapsto r + m\mathbb{Z} = \bar{r}$ ist ein Ringhomomorphismus.

Bemerkung:
Ähnlich wie bei Gruppen spricht man von Mono-/Epi-/Isomorphismen, wenn φ injektiv/surjektiv/bijektiv ist.

3.14 Satz: *Homomorphisatz für Ringe*
Seien R, S Ringe und $\varphi : R \to S$ ein Homomorphismus. Dann gilt:

(i) $\ker \varphi = \{r \in R \mid \varphi(r) = 0\} =: I$ ist ein Ideal, der Kern von φ.

(ii) Es gibt einen Homomorphismus $\bar{\varphi} : R/I \to S$ mit $\varphi(r) = \bar{\varphi}(\bar{r})$, d.h. das Diagramm



kommutiert

Dabei ist die Menge der Kongruenzklassen R/I selbst wieder ein Ring.

Beweis:
Definiere $r \equiv r'$ für $r, r' \in R$, falls $\varphi(r) = \varphi(r')$. Das ist offensichtlich eine Kongruenzrelation, da φ ein Homomorphismus ist. $I = \{r \in R \mid r \equiv 0\} = \{r \in R \mid \varphi(r) = 0\} = \ker \varphi$ ist also ein Ideal.
Definiere $\bar{\varphi} : R/S \to S$ durch $\bar{\varphi}(\bar{r}) := \varphi(r)$, dann gilt

$$\bar{\varphi}(\bar{r} + \bar{r}') = \bar{\varphi}(\overline{r + r'}) = \varphi(r + r') = \varphi(r) + \varphi(r') = \bar{\varphi}(\bar{r}) + \bar{\varphi}(\bar{r}')$$

Multiplikation analog, sowie $\bar{\varphi}(\bar{1}) = \varphi(1) = 1$.
Zudem ist $\bar{\varphi}$ eindeutig, denn angenommen es gäbe ein weitere $\psi : R/I \to S$ mit $\psi \circ P_I = \varphi$, dann folgt direkt:

$$\psi(P_I(r)) = \psi(\bar{r}) = \varphi(r) = \bar{\varphi}(\bar{r}) \;\Rightarrow\; \psi = \bar{\varphi}$$

□

Bemerkung:
Wie bei Gruppen gilt:

- $\bar{\varphi}$ ist immer ein Monomorphismus
- φ ist Monomorphismus $\Leftrightarrow I = \ker \varphi = \{0\}$
- $\bar{\varphi}$ ist Isomorphismus $\Leftrightarrow \varphi$ ist Epimorphismus

3.3 Der Chinesische Restsatz

3.15 Definition: (Direkte Produkte)
Sind $R_1, \ldots, R_k$ Ringe, so ist auch das Produkt $R := R_1 \times \ldots \times R_k$ ein Ring mit den Verknüpfungen

$$(r_1, \ldots, r_k) + (s_1, \ldots, s_k) := (r_1 + s_1, \ldots, r_k + s_k)$$
$$(r_1, \ldots, r_k) \cdot (s_1, \ldots, s_k) := (r_1 \cdot s_1, \ldots, r_k \cdot s_k)$$

Die Abbildung $P_{r_j} : R_1 \times \ldots \times R_k \to R_j, (r_1, \ldots, r_k) \mapsto r_j$ ist ein Ringepimorphismus.

3.16 Lemma:
Sei R ein Ring mit Idealen $I_1, \ldots, I_k \trianglelefteq R$. Für alle $s \neq t$ gelte $I_s + I_t = R$. Dann gilt

$$I_1 \cdot I_2 \cdots I_k = I_1 \cap I_2 \cap \ldots \cap I_k$$

wobei: $I_s + I_t := \{i + j \mid i \in I_s, j \in I_t\}$ und $I_s \cdot I_t := \{i \cdot j \mid i \in I_s, j \in I_t\}$.

Beweis:
Wir beweisen per Induktion über $k \geq 2$:

Induktionsanfang: $k = 2$

Nach Voraussetzung ist $I_1 + I_2 = R$. $I_1 \cap I_2$ ist Ideal, also $I_1 \cap I_2(I_1 + I_2) \subseteq I_1 \cap I_2$.

Andererseits ist:

$$\begin{aligned} I_1 \cap I_2 &= I_1 \cap I_2(I_1 + I_2) \\ &= (I_1 \cap I_2)(I_1) + (I_1 \cap I_2)(I_2) \\ &\subseteq I_2 \cdot I_1 + I_1 \cdot I_2 \\ &\subseteq I_1 \cdot I_2 \end{aligned}$$

Da I_1 ein Ideal ist, gilt $I_1 I_2 \subseteq I_1$ genauso wie $I_1 I_2 \subseteq I_2$, also:

$$I_1 I_2 \subseteq I_1 \cap I_2 \Rightarrow I_1 \cap I_2 = I_1 I_2$$

Induktionsschritt: $k \geq 3$:

$$I_1 \cap \bigcap_{s=2}^{k} I_s \overset{\text{IV}}{=} I_1 \cap (I_2 \cdots I_k) = I_1 \cdots I_k$$

□

3.17 Satz: *Chinesischer Restsatz (algebraische Version)*
Sei R ein Ring mit Idealen $I_1, \ldots, I_k \trianglelefteq R$. Für $s \neq t$ gelte $R = I_s + I_t$. Dann ist die Abbildung

$$\varphi : R \to R/I_1 \times \ldots \times R/I_k, \quad r \mapsto (r + I_1, \ldots, r + I_k)$$

ein surjektiver Ringhomomorphismus mit

$$\ker \varphi = I := I_1 \cap \ldots \cap I_k = I_1 \cdots I_k$$

Beweis:
Durch Nachrechnen verifiziert man, dass φ ein Ringhomomorphismus ist.

$$\varphi(r) = 0 \Leftrightarrow r \in I_1, \ldots, r \in I_k \Leftrightarrow r \in I_1 \cap \ldots \cap I_k =: I$$

Bleibt zu zeigen, dass φ surjektiv ist:
Sei $J_s := \bigcap_{t \neq s} I_t$, dann gilt nach dem Lemma (3.16) $I_s + J_s = R$ für alle s. Sei $(r_1 + I_1, \ldots, r_k + I_k) \in R/I_1 \times \ldots \times R/I_k$, dann wähle $i_s \in I_s, j_s \in J_s$ so, dass $i_s + j_s = 1$ für $s = 1, \ldots, k$. Setze $r = r_1 j_1 + \ldots + r_k j_k$, dann folgt:

$$\begin{aligned} \varphi(r) &= \varphi(r_1 j_1 + \ldots + r_k j_k) = (r + I_1, \ldots, r + I_k) \\ r + I_1 &= r_1 j_1 + \ldots + r_k j_k + I_1 \\ &= r_1 1 - \underbrace{r_1 i_1}_{I_1} + \ldots + I_1 \qquad \text{für } s \geq 2 \text{ gilt } j_s \in I_1 \\ &= r_1 + \left(r_2 j_2 + \ldots + r_k j_k\right) + I_1 \\ &= r_1 + I_1 \end{aligned}$$

Also gilt $\varphi(r) = (r_1 + I_1, \ldots, r_k + I_k)$ und damit ist φ surjektiv. $\square$

3.18 Korollar:
Es existiert ein Ringisomorphismus

$$\bar{\varphi} : R/I \xrightarrow{\sim} R/I_1 \times \ldots \times R/I_k$$

3.19 Satz: *Chinesischer Restsatz (zahlentheoretische Version)*
Seien $m_1, \ldots, m_k \geq 0$ paarweise teilerfremd. Dann gibt es zu jedem k-Tupel $(a_1, \ldots, a_k)$ von ganzen Zahlen eine Zahl $z \in \mathbb{Z}$, die alle folgenden Kongruenzen erfüllt:

$$\begin{aligned} z &\equiv a_1 \bmod m_1 \\ &\vdots \\ z &\equiv a_k \bmod m_k \end{aligned}$$

Die Lösung z ist eindeutig modulo $m := m_1 \cdots m_k$, d.h.

$$z' \in \mathbb{Z} \text{ ist Lösung} \Leftrightarrow z \equiv z' \bmod m$$

Beweis:
Wir führen diesen Spezialfall auf den allgemeine algebraischen Chinesischen Restsatz (3.17) mit $R = \mathbb{Z}$ zurück:
Wir wählen $I_s := (m_s) = m_s\mathbb{Z}$. Da $\mathrm{ggT}(m_s, m_t) = 1$ für $s \neq t$ gibt es nach Bézout (1.21) $u, v \in \mathbb{Z}$ mit $um_s + rm_t = 1 \Rightarrow m_s\mathbb{Z} + m_t\mathbb{Z} = \mathbb{Z}$. Also exisitiert ein Epimorphismus

$$\varphi : \mathbb{Z} \to \mathbb{Z}/m_1 \times \ldots \times \mathbb{Z}/m_k$$

Zu $a_1 + I_1, \ldots, a_k + I_k$ gibt es also $z \in \mathbb{Z}$ mit $\varphi(z) = (a_1 + I_1, \ldots, a_k + I_k)$, d.h. $z \equiv a_s \bmod m_s$ für $s = 1, \ldots, k$.
Es gilt $m_1\mathbb{Z} \cap \ldots \cap m_k\mathbb{Z} = (m_1 \cdots m_k)\mathbb{Z} = m\mathbb{Z} = \ker\varphi$, d.h. $\mathbb{Z}/m \simeq \mathbb{Z}/M_1 \times \ldots \times \mathbb{Z}/m_k$. $\square$

Beispiel:
Betrachten wir:

$$z \equiv 1 \bmod 3 \tag{3.19.1}$$
$$z \equiv 2 \bmod 5 \tag{3.19.2}$$
$$z \equiv 3 \bmod 7 \tag{3.19.3}$$

$3, 5, 7$ sind paarweise teilerfremd, also ist $m = 3 \cdot 5 \cdot 7 = 105$.

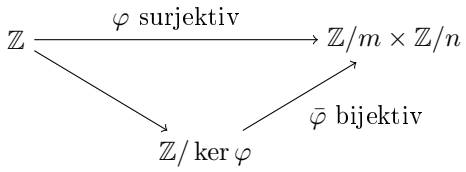
$$\begin{aligned}
&(3.19.1) \Rightarrow z = 1 + 3l_1 \\
&(3.19.2) \Rightarrow 1 + 3l_1 \equiv 2 \bmod 5 \quad &\Leftrightarrow\ & 3l_1 \equiv 1 \bmod 5 \\
&&& 3l_1 \equiv 6 \bmod 5 \\
&&& l_1 \equiv 2 \bmod 5 \Rightarrow l_1 = 2 + 5l_2 \\
&&\Rightarrow\ & z = 1 + 3l_1 = 1 + 3(2 + 5l_2) = z + 15l_2 \\
&(3.19.3) \Rightarrow 7 + 15l_2 \equiv 3 \bmod 7 \quad &\Leftrightarrow\ & 15l_2 \equiv 3 \bmod 7 \\
&&& 5l_2 \equiv 1 \bmod 7 \\
&&& 5l_2 \equiv 15 \bmod 7 \\
&&& l_2 \equiv 3 \bmod 7 \Rightarrow l_2 = 3 + 7l_3 \\
&&\Rightarrow\ & z = 7 + 15l_2 = 7 + 15(3 + 7l_3) = 52 + 105l_3
\end{aligned}$$

Bemerkung:
Sei $R = \mathbb{Z}$ und $m_1, \ldots, m_k$ mit $\text{ggT}(m_s, m_t) = 1$ für alle $s \neq t$. Dann ist $\varphi : \mathbb{Z} \to \mathbb{Z}/m_1 \times \ldots \times \mathbb{Z}/m_k, z \mapsto (z + m_1\mathbb{Z}, \ldots, z + m_k\mathbb{Z})$ surjektiv.

3.20 Korollar:
Sind $m, n \in \mathbb{N}$ mit $\text{ggT}(m, n) = 1$, so gilt

$$\mathbb{Z}/(m \cdot n) \cong \mathbb{Z}/m \times \mathbb{Z}/n$$

Beweis:
Betrachte $\varphi : \mathbb{Z} \to \mathbb{Z}/m \times \mathbb{Z}/n, z \mapsto (z + m\mathbb{Z}, z + n\mathbb{Z})$. Nach dem chinesischen Restsatz *(3.17)* ist φ ein Epimorphismus. Der Homomorphiesatz liefert



Es gilt $\ker \varphi = mn\mathbb{Z}$ □

Bemerkung:
In einem direkten Produkt $R \times S$ von Ringen R, S gilt: (r, s) ist Einheit genau dann, wenn r und s Einheiten sind, d.h.

$$(R \times S)^* = R^* \times S^*$$

3.21 Korollar:
Ist $m, n \in \mathbb{N}$ mit $\text{ggT}(m, n) = 1$, so gilt

$$(\mathbb{Z}/mn)^* \cong (\mathbb{Z}/m)^* \times (\mathbb{Z}/n)^*$$

Bemerkung:
Wir haben benutzt: sind G, H Gruppen, so ist auch $G \times H$ eine Gruppe mit Verknüpfung

$$(g_1, h_1) \cdot (g_2, h_2) := (g_1 g_2, h_1 h_2)$$

3.22 Satz:
Sind $m_1, \ldots, m_k \in \mathbb{N}$ paarweise teilerfremd, so gilt für die Eulersche φ-Funktion:

$$\varphi(m_1 \cdots m_k) = \varphi(m_1) \cdots \varphi(m_k)$$

Beweis:
Nach dem chinesischen Restsatz *(3.17)* gilt:

$$\mathbb{Z}/(m_1 \cdots m_k) \cong \mathbb{Z}/m_1 \times \ldots \times \mathbb{Z}/m_k$$

Mit vollständiger Induktion folgt

$$(\mathbb{Z}/(m_1 \cdots m_k))^* \cong (\mathbb{Z}/m_1)^* \times \ldots \times (\mathbb{Z}/m_k)^*$$

Die Eulersche φ-Funktion zählt aber gerade die Einheiten, also $\varphi(k) = \#(\mathbb{Z}/k)^*$, und so folgt die Behauptung. □

Um $\varphi(n)$ zu berechnen, muss man also φ von Primzahlpotenzen berechnen können.

3.23 Lemma:
Ist $p \in \mathbb{P}, k \geq 1$, so gilt $\varphi(p^k) = p^{k-1}(p-1) = p^k(1-\frac{1}{p})$ für die Eulersche φ-Funktion.

Beweis:
Es gilt $\varphi(p^k) = \#(\mathbb{Z}/p^k)^*$ und $\bar{a} \in \mathbb{Z}/p^k$ Einheit genau dann wenn $\mathrm{ggT}(a, p^k) = 1 \Leftrightarrow p \nmid a$. Die Nichteinheiten in $\mathbb{Z}/p^k$ sind genau $\bar{0}, \bar{p}, 2\bar{p}, \ldots, \overline{p^k - p}$, das heißt es gibt p^{k-1} Nichteinheiten. Der Rest besteht aus Einheiten, also

$$\#(\mathbb{Z}/p^k)^* = p^k - p^{k-1} = p^{k-1}(p-1)$$

□

3.24 Satz:
Ist $n \in \mathbb{N}, n \geq 1$ mit Primfaktorzerlegung (vgl. *(1.8)*)

$$n = \prod_{p \in \mathbb{P}} p^{\nu_p(n)} = \prod_{p \in \mathbb{P}, p|n} p^{\nu_p(n)}$$

so gilt für die Eulersche φ-Funktion

$$\varphi(n) = \prod_{p \in \mathbb{P}, p|n} p^{\nu_p(n)} \left(1 - \frac{1}{p}\right) = n \cdot \prod_{p \in \mathbb{P}, p|n} \left(1 - \frac{1}{p}\right)$$

Beweis:
voriges Lemma + Satz *(3.22)*. □

Bemerkung:
Eulers φ-Funktion nimmt *nicht* jeden Wert an, z.B. gibt es kein $n \in \mathbb{N}$ mit $\varphi(n) = 5$. Manche Werte nimmt sie mehrfach an, z.B. $\varphi(4) = 2 = \varphi(3)$. Erst 1999 konnte K. Ford folgendes beweisen: Zu jedem $k \geq 2$ gibt es ein l, sodass

$$\#\{n \in \mathbb{N} \mid \varphi(n) = l\} = k$$

Ein offenes Problem ist weiterhin, ob es ein l gibt mit $\#\{n \in \mathbb{N} \mid \varphi(n) = l\} = 1$.

Für große Zahlen m (etwas 200 Dezimalstellen) ist es mit heutigen Rechnern sehr langwierig Primfaktoren bzw. $\varphi(m)$ zu berechnen.

3.25 Lemma:
Seien $p, q \in \mathbb{P}$ Primzahlen, $p \neq q$. Sei $m := pq$ und sei $e \geq 1$ teilerfremd zu $\varphi(m) = \varphi(pq) = (p-1)(q-1)$, d.h. $\mathrm{ggT}(e, (p-1)(q-1)) = 1$. Sei $d \geq 1$ mit $e \cdot d \equiv 1 \bmod \varphi(m)$ (Lemma von Bezout). Dann gilt für alle $z \in \mathbb{Z}$

$$z^{ed} \equiv z \bmod m$$

Beweis:
Fermats kleiner Satz (2.6) + Chinesischer Restsatz.

Es gilt $\mathbb{Z}/pq \cong \mathbb{Z}/p \times \mathbb{Z}/q$. Wir zeigen in $\mathbb{Z}/pq$, dass $\bar{z}^{ed} = \bar{z}$ für alle $\bar{z} \in \mathbb{Z}/pq$:
Mit dem Isomorphismus schreibe $\bar{z} = (\bar{x}, \bar{y}), \bar{x} \in \mathbb{Z}/p, \bar{y} \in \mathbb{Z}/q$, dann gilt:

$$\bar{z}^{ed} = (\bar{x}, \bar{y})^{ed} = (\bar{x}^{ed}, \bar{y}^{ed}) \overset{!}{=} (\bar{x}, \bar{y})$$

Es gilt $ed = 1 + k \underbrace{\varphi(pq)}_{=(p-1)(q-1)}$. Nach dem keinen Fermat gilt

$$x^{1+k(p-1)(q-1)} \equiv x \bmod p$$

denn: $x \not\equiv 0 \bmod p \Rightarrow x^{p-1} \equiv 0 \bmod p \Rightarrow x^{1+k(p-1)(q-1)} \equiv x \bmod p$ und $x \equiv 0 \bmod p \Rightarrow x^{1+k(p-1)(q-1)} \equiv x \bmod p$ trivial.

Völlig analog folgt $y^{1+k(p-1)(q-1)} \equiv y \bmod q$. Insgesamt also

$$\forall(\bar{x}, \bar{y}) \in \mathbb{Z}/p \times \mathbb{Z}/q : (\bar{x}^{ed}, \bar{y}^{ed}) = (\bar{x}, \bar{y})$$

□

3.4 Das RSA-Verfahren

Ziel:
Jeder kann mir einen verschlüsselten Text schicken, den nur ich wieder entschlüsseln kann. Den Text verschlüsseln kann dagegen jeder, das Verfahren ist öffentlich zugänglich.

Vorbereitung:
Wähle zufällig zwei große Primzahlen $p \neq q$ ($\sim$100 Dezimalstellen). Berechne $m = p \cdot q$. Wähle eine Zahl $e \geq 1$ mit $\mathrm{ggT}(e, \varphi(m)) = \mathrm{ggT}(e, (p-1)(q-1)) = 1$. Bestimme $d \geq 1$ mit $ed \equiv 1 \bmod \varphi(m) = (p-1)(q-1)$.

Die Zahlen e und m werden veröffentlicht. Lösche $p, q, \varphi(m)$ und halte d geheim. Das Alphabet der Nachricht besteht aus $0, \ldots, m-1$.

Sei der Klartext gegeben als $(k_1, \ldots, k_t), 0 \leq k_j < m$. Dieser wird durch $k_j \mapsto k_j^e =: l_j$ verschlüsselt, sodass man den Geheimtext $(l_1, \ldots, k_t)$ erhält, der an den Empfänger durch einen unsicheren Kanal übertragen werden kann. Dieser entschlüsselt die Nachricht durch $l_j \mapsto l_j^d \bmod m$.

Es gilt

$$k_j \mapsto k_j^e = l_j \mapsto l_j^d = k_j^{ed} \equiv k_j \bmod m$$

Man erhält also wieder den ursprünglichen Klartext.

Die Sicherheit beruht darauf, dass es sehr aufwändig ist, d zu berechnen.

Bemerkung:
Das Verfahren ist recht rechenintensiv und wird daher oft zur Übertragung von Schlüssel für andere (symmetrische) Verschlüsselungsverfahren benutzt.

Es gibt RSA-Verfahren mit ≥ 3 Primzahlen, die Mathematik dahinter bleibt aber genau die gleiche.

Bemerkung:
Eine andere Anwendung der Euler-Formel sind Aufgaben der Art: Bestimmen Sie die letzten beiden Ziffern von 7^{355}. Es geht also darum $7^{355} \bmod 100$ zu berechnen. Da 100 und 7 Teilerfremd sind, gilt:

$$7^{\varphi(100)} \equiv 1 \bmod 100, \quad \varphi(100) = \varphi(2^2 \cdot 5^2) = 40$$

Weiter ist $355 = 320 + 35$, also $7^{355} \equiv 7^{35} \bmod 100$. Betrachte $7^2 = 50 - 1 \Rightarrow 7^4 = (50-1)^2 \equiv 1 \bmod 100$, also

$$7^{35} = 7^{32+3} \equiv 7^3 \bmod 100$$

$$\begin{aligned} 7^3 = (10-3)^3 &\equiv (-3)^3 + 10 \cdot (-3)^2 \binom{3}{1} \bmod 100 \\ &\equiv -27 + 270 \bmod 100 \\ &\equiv 43 \bmod 100 \end{aligned}$$

Also hat 7^{355} die beiden letzten Ziffern 43.

Kürzer:
Wie oben gilt: $7^4 \equiv 1 \bmod 100$ und $355 = 4 \cdot 88 + 3 \Rightarrow 7^{355} \equiv 7^3 \bmod 100$ ohne Formel von Euler.

3.5 Kongruenz von Polynomen

3.26 Satz: *Abspalten von Nullstellen*
Sei K ein Körper, sei $f(X) = a_0 + a_1X + \ldots + a_nX^n$ ein *Polynom über K* (d.h. $a_j \in K$) mit Leitkoeffizienten $a_n \neq 0$ und $n \geq 1$.

Falls $r \in K$ eine Nullstelle von f ist, d.h. $f(r) = 0$, so gibt es ein weiteres Polynom $g(X) = b_0 + \ldots + b_{n-1}X^{n-1}$ über K mit

$$f(X) = (X - r)g(X)$$

Beweis:
Betrachten wir zunächst den Fall $n = 1$: Sei $f(X) = a_1X + a_0 = \left(X + \frac{a_0}{a_1}\right) \cdot \underbrace{a_1}_{:=g}$.

Sei nun $n \geq 2$:
Vorüberlegung:
Es gilt für $j \geq 1$:

$$\frac{X^j - 1}{X - 1} = \sum_{i=0}^{j-1} X^i$$

Sei $r \neq 0$ dann folgt

$$\frac{X^j - r^j}{X - r} \cdot \frac{r}{r^j} = \frac{\left(\frac{X}{r}\right)^j - 1}{\frac{X}{r} - 1} = \sum_{i=0}^{j-1} \left(\frac{X}{r}\right)^i$$

umsortieren:

$$(*) \qquad X^j - r^j = (X - r) \sum_{i=0}^{j-1} X^i r^{j-i-1}$$

(gilt auch für $r = 0$).
Damit folgt nun:

$$\begin{aligned} f(X) &= f(X) - f(r) \\ &= \sum_{i=1}^{n} (X^i - r^i)a_i \\ &\overset{(*)}{=} (X - r) \cdot g(X) \end{aligned}$$

□

3.27 Korollar:
Ist K ein Körper, $f(X) = a_nX^n + \ldots + a_0$ ein Polynom über K. Dann hat f höchstens n Nullstellen in K.

Bemerkung:
Der Beweis benutzt, dass K ein Körper ist und so jedes Element ein multiplikatives Inverse besitzt. Für Ringe ist die Aussage i.A. falsch:

Betrachten wir zum Beispiel $f(X) = X^2 - 1$ in $\mathbb{Z}/8$, dann sind die Nullstellen gegeben durch $\pm\bar{1}, \pm\bar{3}$. Das sind insbesondere vier verschiedene Nullstellen.

3.28 Zwei Anwendungen von Satz *(1.21)*
Sei $p \in \mathbb{P}$ eine Primzahl, sei

$$f(X) = (X-1)(X-2)\cdots(X-(p-1)) = X^{p-1} + \ldots + (-1)^{p-1}(p-1)!$$

Sei $g(X) = X^{p-1} - 1$ und $f(X) - g(X) = \sum_{j=O}^{p-2} b_j X^j$.

Betrachte auch $\bar{f}(X) = (X-\bar{1})\cdots(X-\overline{p-1})$ und $\bar{g}(X) = X^{p-1} - \bar{1}$ über $\mathbb{Z}/p$. Für alle $\bar{a} \in (\mathbb{Z}/p)^*$ gilt:

$$\bar{f}(\bar{a}) = \bar{g}(\bar{a}) = \bar{0} \Rightarrow \bar{f}(X) - \bar{g}(X) \text{ hat } p-1 \text{ verschiedene Nullstellen}$$

Aber: $\bar{f} - \bar{g}$ hat Grad $p-2$ als folgt aus *(1.21)*, dass bereits $\bar{f}(X) - \bar{g}(X) = 0 = \text{const}$ gelten muss, also $b_j \equiv 0 \bmod p$.

Nun ist $b_0 = (-1)^{p-1}(p-1)! + 1 \equiv 0 \bmod p$.

(i) Es folgt (eine Richtung) vom Satz von Wilson *(3.12)*: $(p-1)! \equiv -1 \bmod p$ (für $p \neq 2$ ist $(-1)^{p-1} = 1$, für $p = 2$ stimmts auch).

(ii)
Satz von Wolstenholme:
Ist $p \in \mathbb{P}, p \geq 5$, so gilt:

$$\sum_{j=1}^{p-1} \frac{(p-1)!}{j} \equiv 0 \bmod p^2$$

Beweis:
Für $p \geq 3$ ist b_1 der Koeffizient des linearen Termes von $f(X)$, also

$$b_1 = \sum_{j=1}^{p-1} \frac{(p-1)!}{j}(-1)^{p-2} = -\sum_{j=1}^{p-1} \frac{(p-1)!}{j}$$

Klar: das ist durch p teilbar. Warum aber auch durch p^2:

$$\begin{aligned} f(p) = (p-1)! \quad &= \quad p^{p-1} + \ldots + b_1 p + (-1)^{p-1}(p-1)! \\ &\overset{p\geq 5}{\Longrightarrow} \quad 0 = p^{p-1} + \ldots + b_2 p^2 + b_1 p \\ &\Longrightarrow \quad 0 \equiv b_2 p^2 + b_1 p \bmod p^3 \\ &\overset{p|b}{\Longrightarrow} \quad 0 \equiv b_1 p \bmod p^3 \\ &\Longrightarrow \quad p^2 \mid b_1 \end{aligned}$$

□

Bemerkung:
Wolstenholmes Satz wird oft notiert als:

$$\sum_{j=1}^{p-1} \frac{1}{j} \equiv 0 \bmod p^2$$

Das ist folgendermaßen gemeint: Für $1 \leq j \leq p-1$ ist $\text{ggT}(j, p^2) = 1$. Also gibt es Zahlen $\hat{j}$ mit $\hat{j} \cdot j \equiv 1 \bmod p^2 \Rightarrow \hat{j} = \frac{1}{j}$. *Behauptung:*

$$\sum_{j=1}^{p-1} \hat{j} \equiv 0 \bmod p^2$$

Es gilt: $\mathrm{ggT}((p-1)!, p^2) = 1$, mod p^2 darf mal also $(p-1)!$ kürzen.

$$\sum_{j=1}^{p-1} \frac{(p-1)!}{j} \equiv \sum_{j=1}^{p-1} \hat{j} \cdot (p-1)! \equiv 0 \bmod p^2$$

3.29 Satz:
Sei K ein Körper, sei $S \subseteq K^*$ eine *endliche* Untergruppe der multiplikativen Gruppe $(K^*, \cdot)$. Dann ist S eine zyklische Gruppe, d.h. es gibt $s_0 \in S$ mit

$$S = \{s_0, s_0^2, s_0^3, \ldots, s_0^m = 1\}$$

Beweis:
Wir wenden das Kriterium *(2.32)* an und zeigen: zu jeden Teiler d von $m := \#S$ gibt es höchstens eine Untergruppe $H \subseteq S$ mit $\#H = d$. Satz *(2.32)* sagt, dass S dann zyklisch ist.

Sei also $H \subseteq S$ eine Untergruppe mit $\#H = d \mid m$. Für alle $h \in H$ gilt $h^d = 1$, also gilt

$$H \subseteq \left\{x \in K \mid x^d = 1\right\}$$

Es kann aber höchstens d verschiedene $x \in K$ geben mit $x^d = 1$ nach Satz *(1.21)*. Es folgt $H = \left\{x \in K \mid x^d = 1\right\}$. Die rechte Seite legt H eindeutig fest. Also lässt sich *(2.32)* anwenden. □

3.30 Korollar:
Ist $p \in \mathbb{P}$, so ist die Einheitengruppe $(\mathbb{Z}/p)^*$ zyklisch der Ordnung $p-1$.

Kapitel 4

Einheitengruppen und quadratische Reste

4.1 Einheitswurzeln und diskreter Logarithmus

4.1 Definition: (Einheitswurzel)
Sei K ein Körper, $n \geq 1$. Die Nullstellen von $X^n - 1$ heißen n-te *Einheitswurzeln*. Die Menge

$$\mu_n(K) := \{x \in K \mid x^n - 1 = 0\}$$

ist eine endliche zyklische Gruppe (bezüglich Multiplikation) deren Ordnung ein Teiler von n ist (nach *(3.29)*).

Ist $m := \#\mu_n(K)$, so gibt es also ein $u \in \mu_n(K)$ mit $\mu_n(K) = \{u, u^2, \ldots, u^{m-1}\}$. Man nennt u eine *primitive n-te Einheitswurzel*. Mit anderen Worten: $u^m = 1, u^k \neq 1$ für $1 \leq k < m$.

Beispiel:
Sei $K = \mathbb{Q}$, dann ist

$$\mu_2(\mathbb{Q}) = \{-1, 1\} = \mu_4(\mathbb{Q})$$

-1 ist primitive 2-te Einheitswurzel.

Sei $K = \mathbb{C}$, dann ist

$$\mu_4(\mathbb{C}) = \{\pm 1, \pm i\}$$

mit $i = \sqrt{-1}$. $\pm i$ sind primitive 4-te Einheitswurzeln.

Sei $K = \mathbb{Z}/5$, dann ist

$$\mu_3(\mathbb{Z}/5) = \{1\}$$

da 3 und $5 - 1 = 4$ teilerfremd sind.

Sei $K = \mathbb{Z}/p$, dann ist

$$\mu_{p-1}(\mathbb{Z}/p) = (\mathbb{Z}/p)^*$$

etwa $\mu_4(\mathbb{Z}/5) = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ mit den primitiven 4-ten Einheitswurzeln $\pm\bar{2} = \pm\bar{3}$

4.2 Definition: (diskreter Logarithmus)
Sei $u \in \mathbb{Z}/p$ eine primitive $(p-1)$-te Einheitswurzel, d.h. u erzeugt $(\mathbb{Z}/p)^*$ multiplikativ. Die Abbildung

$$\mathrm{ind}_u : \big((\mathbb{Z}/p)^*, \cdot\big) \to \big(\mathbb{Z}/(p-1), +\big), \quad u^k \mapsto k + (p-1)\mathbb{Z}$$

ist ein Gruppenisomorphismus und heißt *diskreter Logarithmus*.

Klar: $\mathrm{ind}_u(a \cdot b) = \mathrm{ind}_u(a) + \mathrm{ind}_u(b)$ und $\mathrm{ind}_u(\bar{1}) = \bar{0}$.

4.3 Satz:
Sei $p \in \mathbb{P}, m \geq 1$ ganze Zahl, teilerfremd zu p, also $p \nmid m$, Die Kongruenz $X^m \equiv a \bmod p$ ist genau dann lösbar, wenn $a^{(p-1)/d} \equiv 1 \bmod p$, wobei $d := \mathrm{ggT}(m, p-1)$. Die Anzahl der Lösungen in $\mathbb{Z}/p$ ist dann genau d.

Beweis:
Wir rechnen in der zyklischen Gruppe $(\mathbb{Z}/p)^*$. Sei $u \in \mathbb{Z}/p$ eine primitive $(p-1)$-te Einheitswurzel. Schreibe $\bar{a} = u^s$. Das geht, denn $\bar{a} \in (\mathbb{Z}/p)^*$ und u primitive $(p-1)$-te Einheitswurzel.

Ansatz:

$$\begin{aligned} x = u^t \text{ Lösung} &\iff x^m = \bar{a} \\ &\iff u^{t\cdot m} = u^s \\ &\overset{(4.2)}{\iff} t \cdot m \equiv s \bmod p-1 \end{aligned}$$

Diese Kongruenz ist lösbar genau dann, wenn $d := \mathrm{ggT}(m, p-1) \mid s$ (vgl. *(1.37)*).

$$\begin{aligned} \Leftrightarrow s \equiv 0 \bmod d &\overset{(1.38)}{\iff} s \cdot \left(\frac{p-1}{d}\right) \equiv 0 \bmod p-1 \\ &\overset{(4.2)}{\iff} u^{s\cdot\left(\frac{p-1}{d}\right)} \equiv 1 \bmod p \\ &\iff a'^{s\cdot\left(\frac{p-1}{d}\right)} \equiv 1 \bmod p \end{aligned}$$

Nach *(1.37)* ist d die Anzahl der Lösungen. □

Beispiel:
Wir wollen den vorigen Satz anwenden und $X^m \equiv a \bmod p$ berechnen. Sei $m = 3, p = 3$. Dann ist $d = \mathrm{ggT}(3-1, 3) = 1$. Lösbar, wenn

$$a^{\frac{p-1}{d}} = a^2 \equiv 1 \bmod 3$$

Für alle a teilerfremd zu 3 gilt aber $a^2 \equiv 2 \bmod 3$. Die Kongruenz $X^3 \equiv a \bmod 3$ ist also für alle zu 3 teilerfremden Zahlen a eindeutig in $\mathbb{Z}/3$ lösbar.

Sei $p = 7, m = 3$ und $d = \mathrm{ggT}(7-1, 3) = 3$.

$$\begin{aligned} \text{Lösbar für } a &\Leftrightarrow a^{\frac{7-1}{3}} = a^2 \equiv 1 \bmod 7 \\ &\Leftrightarrow a \equiv \pm 1 \bmod 7 \end{aligned}$$

Für $\bar{a} = \bar{1}$ ist $X = \{\bar{1}, \bar{2}, \bar{4}\}$, für $a = -\bar{1}$ ist $X = \{-\bar{1}, \bar{3}, \bar{5}\}$.

4.4 Satz:
Sei $p \in \mathbb{P}$ ungerade, $p = 2l + 1$. Für alle zu p teilerfremden a (d.h. $p \nmid a$) gilt entweder

$$a^l \equiv 1 \bmod p$$

oder

$$a^l \equiv -1 \bmod p$$

Im ersten Fall ist $X^2 \equiv a \bmod p$ lösbar, im zweiten Fall nicht.

Beweis:
Wende Satz *(4.3)* an mit $m = 2, d = ggT(p-1, 2) = 2$. Also ist $X^2 \equiv a \bmod p$ lösbar $\Leftrightarrow a^{\frac{p-1}{2}} = a^l \equiv 1 \bmod p$. Für alle $\bar{a} \in (\mathbb{Z}/p)^*$ gilt

$$\bar{a}^{p-1} = \bar{1} \Rightarrow \bar{a}^{2l} = \bar{1} \Rightarrow \left(\overline{a^l}\right)^2 = 1 \Rightarrow \overline{a^l} = \pm\bar{1}$$

□

Bemerkung:
Der Fall $p = 2$ ist uninteressant, denn $X^2 \equiv a \bmod 2$ hat genau eine Lösung in $\mathbb{Z}/2$.

4.5 Korollar:
Ist $p \in \mathbb{P}$ ungerade, so ist die Kongruenz $X^2 \equiv -1 \bmod p$ lösbar, genau dann, wenn $p \equiv 1 \bmod 4$.

Beweis:
$p = 2l + 1, a = -1$

$$\begin{aligned} a^l = (-a)^l \overset{!}{\equiv} 1 \bmod p \quad &\Leftrightarrow \quad l \text{ gerade} \\ &\Leftrightarrow \quad p \equiv 1 \bmod 4 \end{aligned}$$

□

Bemerkung:
Ist n ungerade, so gilt entweder $n \equiv 1 \bmod 4$ oder $n \equiv -1 \bmod 4$.

4.2 Quadratische Reste

4.6 Definition: (Quadratischer Rest, Legendre-Symbol)
Sei $p \in \mathbb{P}$ ungerade. Eine ganze zu p teilerfremde Zahl a heißt *quadratischer Rest mod p*, wenn $X^2 \equiv a \bmod p$ lösbar ist. Sonst heißt sie quadratischer Nicht-Rest

Sei $p \in \mathbb{P}, p \neq 2, a \in \mathbb{Z}$. Das *Legendre-Symbol* $(\frac{a}{p})$ „a nach p“ ist definiert als

$$(\frac{a}{p}) := \begin{cases} 1 & a \text{ ist QR mod } p \\ -1 & a \text{ ist QNR mod } p \\ 0 & \text{falls } p \mid a \end{cases}$$

4.7 Satz:
Sei $p \in \mathbb{P}$ ungerade. Der Wert von $(\frac{a}{p})$ hängt nur von der Kongruenzklasse von a mod p ab, d.h. $(\frac{a+p}{p}) = (\frac{a}{p})$. Die Abbildung

$$\big((\mathbb{Z}/p)^*, \cdot\big) \to \big(\{\pm 1\}, \cdot\big), \quad \bar{a} \mapsto (\frac{a}{p})$$

ist ein Gruppenhomomorphismus

Beweis:
Die erste Behauptung folgt aus der Definition vom Legendre-Symbol.
Sei $u \in (\mathbb{Z}/p)^*$ eine primitive $(p-1)$-te Einheitswurzel, $\bar{a} = u^s$ für $\bar{a} \in (\mathbb{Z}/p)^*$. $\bar{a}$ ist ein Quadrat genau dann wenn $s \equiv 0 \bmod 2$ gilt, d.h. $(\frac{a}{p}) = (-1)^s = (-1)^{\mathrm{ind}_u(\bar{a})}$. Es folgt, dass die Abbildung multiplikativ ist, d.h. $\bar{a} \cdot \bar{b} \mapsto (\frac{a}{p}) \cdot (\frac{b}{p})$. □

Eigenschaften des Legendre-Symbols:
Es gilt:

$$(\tfrac{a+k\cdot p}{p}) = (\tfrac{a}{p})$$

$$(\tfrac{1}{p}) = 1$$

$$(\tfrac{a^2}{p}) = 1$$

$$(\tfrac{-1}{p}) = \begin{cases} 1 & \text{falls } p \equiv 1 \bmod 4 \\ -1 & \text{falls } p \equiv 3 \bmod 4 \end{cases} = (-1)^{\frac{p-1}{2}}$$

$$(\tfrac{a\cdot b}{p}) = (\tfrac{a}{p}) \cdot (\tfrac{b}{p}) \text{ für alle } a, b \in \mathbb{Z}$$

$$\text{Euler-Kriterium: } (\tfrac{a}{p}) \equiv a^{\frac{p-1}{2}} \bmod p \text{ für alle } a \in \mathbb{Z}$$

4.8 Lemma: *Gauß'sches Lemma*
Sei $p \in \mathbb{P}$ ungerade, $p = 2l + 1$. Wähle $v_1, \ldots, v_l \in \mathbb{Z}/p$ so, dass $\left(\mathbb{Z}/p\right)^* = \{\pm v_1, \ldots, \pm v_l\}$ (zum Beispiel $v_j = \bar{j}$ mod p. Sei $a \in \mathbb{Z}$ teilerfremd zu p. Dann gibt es zu jedem $j = 1, \ldots, l$ ein $\varepsilon_j(a) = \pm 1$, sodass gilt:

$$v_j \bar{a} \equiv v_i \cdot \varepsilon_j(a) \bmod p$$

Dann gilt:

$$(\frac{a}{p}) = \varepsilon_1(a) \cdots \varepsilon_p(a)$$

Beweis:
Da a teilerfremd zu p ist, gilt $\bar{a} \in \left(\mathbb{Z}/p\right)^*$. Da $v_j \in \left(\mathbb{Z}/p\right)^*$ ist $\bar{a} \cdot v_j \in \left(\mathbb{Z}/p\right)^* = \{\pm v_1, \ldots, \pm v_l\}$. Es gibt folglich ein i mit $\bar{a} \cdot v_j = \pm v_i$, welches $\varepsilon_j(a)$ eindeutig festlegt. Zudem gilt:

$$\begin{aligned}(\bar{a}v_1)(\bar{a}v_2)\cdots(\bar{a}v_l) &= \bar{a}^l(v_1 \cdots v_l) \\ &= \varepsilon_1(a)\cdots\varepsilon_j(a)\cdot(v_1\cdots v_l)\end{aligned}$$

Es folgt:

$$\begin{aligned}\bar{a}^l = \varepsilon_1(a)\cdots\varepsilon_l(a) \quad &\Rightarrow \quad \underbrace{\varepsilon_1(a)\cdots\varepsilon_l(a)}_{\pm 1} \equiv a^{\frac{p-1}{2}} \bmod p \\ &\overset{\text{Euler Kriterium Satz 4}}{\Rightarrow} \quad \varepsilon_1(a)\cdots\varepsilon_l(a) \equiv (\frac{a}{p}) \bmod p \\ &\Rightarrow \quad \underbrace{\varepsilon_1(a)\cdots\varepsilon_l(a)}_{\pm 1} - \underbrace{(\frac{a}{p})}_{\pm 1} \equiv 0 \bmod p \\ &\Rightarrow \quad \varepsilon_a(1)\cdots\varepsilon_l(a) = (\frac{a}{p})\end{aligned}$$

□

4.9 Theorem: Quadratische Reziprozität (Gauß)
Seien $p, q \in \mathbb{P}$ ungerade und verschieden. Dann gilt:

$$(\frac{p}{q}) \cdot (\frac{q}{p}) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

Beweis:
Sei $p = 2l + 1, q = 2m + 1$ und damit $l = \frac{p-1}{2}, m = \frac{q-1}{2}$. Wir betrachten das Gauß'sche Lemma *(4.8)* mit $v_j := \bar{j}$.

1. **Beh.:** $(\frac{q}{p}) = (-1)^{\#L}$, wobei $L := \{(j,k) \mid 1 \le j \le l, 1 \le k \le m, 1 \le pk - qj \le l\}$.
   Bew.:
   Sei $q \cdot j \equiv \varepsilon_j(q) \cdot i \bmod p$ für $1 \le q \le l$, dann gilt:

$$\begin{aligned}\varepsilon_j(q) = -1 \Leftrightarrow q \cdot j + i &= p \cdot k \text{ für ein } k \in \mathbb{Z} \\ &\Rightarrow k = \frac{1}{p}(q \cdot j + i) \le \frac{1}{p}(q+1)l < \frac{q+1}{2} = m + 1 \\ &\Rightarrow 1 \le k \le m \\ &\Rightarrow i = pk - qj \in \{1, \ldots, l\} \\ &\Rightarrow (j,k) \in L\end{aligned}$$

   Ist umgekehrt $(j,k) \in L$, setze $i := pk - qj \Rightarrow qj \equiv -i \bmod p = \varepsilon_j(q) = -1$. Insgesamt folgt:

$$(\frac{q}{p}) \overset{(4.8)}{=} \varepsilon_1(q)\cdots\varepsilon_l(q) = (-1)^{\#L}$$

   Ganz genauso folgt:

$$(\frac{p}{q}) = (-1)^{\#M}$$

   mit $M := \{(j,k) \mid 1 \le j \le l, 1 \le k \le m, -m \le pk - qj \le -1\}$

2. Setze $A := \{(j,k) \mid 1 \le j \le l, 1 \le k \le m\} \supseteq L \cup M$. Klar: $L \cap M = \emptyset$. Weiter ist $pk - qj \neq 0$ für $(j,k) \in A$, denn $pk \equiv 0 \bmod p$ aber $qj \not\equiv 0 \bmod p$, denn $p \neq q, j \in \{1, \ldots, l\}$ teilerfremd zu p.
Es folgt $L \cup M = \{(i,j) \in A \mid -m \le pk - qj \le l\}$

Betrachte nun die Abbildung

$$\rho : A \to A, \quad (j,k) \mapsto (J', k') = (l + 1 - j, m + 1 - k)$$

welche quasi eine Drehung um 180° beschreibt. Offensichtlich gilt dann $\rho = \mathrm{id}_A \Rightarrow \rho$ bijektiv.

Setze $U := \{(j,k) \in A \mid pk - qj < m\}$ und $V := \{(j,k) \mid pk - qj > l\}$. Es folgt $A = U \cup V \cup L \cup M$ disjunkt. Nun gilt $\rho(U) = V$ und $\rho(V) = U$, denn durch Einsetzen verifiziert man:

$$qj' - pk' - m = -(qj - pk + l)$$

Es folgt:

$$(-1)^{\#A} = (-1)^{l \cdot m} = \underbrace{(-1)^{\#U} \cdot (-1)^{\#V}}_{=1} \cdot (-1)^{\#M} \cdot (-1)^{\#L} \overset{a)}{=} (\frac{q}{p}) \cdot (\frac{p}{q})$$

□

4.10 Satz: *(2. Ergänzungsatz zur Quadratischen Reziprozität)*
Sei $p \in P$ ungerade. Dann ist

$$(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv \pm 1 (\mod 8) \\ -1 & p \equiv \pm 3 (\mod 8) \end{cases}$$

Beweis:
Schreibe $p = 2l + 1, l = 4k + s$ mit $0 \le s \le 3$. Wende Gauß' Lemma 8 an mit $v_j = \bar{j} \quad j = 1, \ldots, l$.

$\underbrace{\varepsilon_j(2)}_{\pm 1} \cdot \bar{i} = 2 \cdot \bar{j} \quad 1 \le i \le l$

1. Fall $0 \le s \le 1$

$$\varepsilon_j(2) = \begin{cases} 1 & 1 \le j \le 2k \\ -1 & 2k < j \le l \end{cases} \overset{\text{Lemma 8}}{\Rightarrow} (\frac{2}{p}) = (-1)^{l-2k} = (-1)^l = (-1)^s = (-1)^{\frac{s(s+1)}{2}}$$

2. Fall $2 \le s \le 3$

$$\varepsilon_j(2) = \begin{cases} 1 & 1 \le j \le 2k+1 \\ -1 & 2k+1 < j \le l \end{cases} \overset{\text{Lemma 8}}{\Rightarrow} (\frac{2}{p}) = (-1)^{l-2k-1} = (-1)^{l-1} = (-1)^{s+1} = (-1)^{\frac{s(s+1)}{2}}$$

Nun ist $\frac{p^2-1}{8} = \frac{(2l+1)^2-1}{8} = \frac{l^2+l}{2} = \frac{l(l+1)}{2} \equiv \frac{s(s+1)}{2} (\mod 2)$ □

Bemerkung:
Der 1. Ergänzungsatz zur Quadratischen Reziprozität ist *(4.5)*

$$(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$$

Formelsammlung:
Damit haben wir folgende Formelsammlung.

$$(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p \equiv 1 \bmod 4 \\ -1 & p \equiv 3 \bmod 4 \end{cases}$$

$$(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv \pm 1 \bmod 8 \\ -1 & p \equiv \pm 3 \bmod 8 \end{cases}$$

Sowie für $p \neq q$ beide ungerade.

$$(\frac{p}{q}) \cdot (\frac{q}{p}) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

Das Legendre-Symbol ist invers zu sich selbst falls es nicht verschwindet, deshalb

$$(\frac{p}{q}) = (\frac{q}{p}) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

Beispiel:

1. Was ist $(\frac{219}{383})$? $383 \in \mathbb{P}, 219 = 3 \cdot 73$.

$$\begin{aligned}
(\frac{219}{383}) &= (\frac{3}{383}) \cdot (\frac{73}{383}) \\
(\frac{3}{383}) &= (\frac{383}{3})(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = (\frac{-1}{3})(-1)^{\frac{3-1}{2} \cdot \frac{383-1}{2}} = -(\frac{-1}{3}) = 1 \\
(\frac{73}{383}) &= (\frac{383}{73}) \cdot \underbrace{(-1)^{\frac{72}{2} \cdot \frac{382}{2}}}_{=1} = (\frac{18}{73}) = (\frac{2}{73}) \cdot (\frac{3}{73})^2 \overset{(4.10)}{=} 1 \\
&\Rightarrow (\frac{219}{383}) = 1
\end{aligned}$$

   Das heißt $X^2 \equiv 219 \bmod 383$ ist lösbar.

2. Was ist $(\frac{3}{p})$ für $p \in \mathbb{P}, p \geq 5$?

$$(\frac{3}{p}) = (\frac{p}{3}) \cdot (-1)^{\frac{p-1}{2}}$$

   Wir müssen p mod 3 für das Legendre-Symbol verstehen und p mod 4 für den Exponenten. Wir schauen uns p mod 12 näher an:

$$\mathrm{ggT}(p, 12) = 1 \;\Leftrightarrow\; p \equiv \pm 1, \pm 5 \equiv 1, 5, 7, 11 \bmod 12$$

   1. Fall: $p \equiv 1 \,(\mathrm{mod}\ 12)$:

$$(\frac{p}{3}) = (\frac{1}{3}) = 1 \;\; (-1)^{\frac{p-1}{2}} = 1 \Rightarrow (\frac{3}{p}) = 1$$

   2. Fall: $p \equiv 5 \,(\mathrm{mod}\ 12)$:

$$(\frac{5}{3}) = (\frac{2}{3}) = -1 \quad (-1)^{\frac{4}{2}} = 1 \Rightarrow (\frac{3}{p}) = -1$$

   3. Fall: $p \equiv 7 \,(\mathrm{mod}\ 12)$:

$$(\frac{7}{3}) = (\frac{1}{3}) = 1 \quad (-1)^{\frac{p-1}{2}} = -1 \Rightarrow (\frac{3}{p}) = -1$$

   4. Fall: $p \equiv 11 \,(\mathrm{mod}\ 12)$:

$$(\frac{11}{3}) = (\frac{2}{3}) = -1 \quad (-1)^{\frac{11-1}{2}} = -1 \Rightarrow (\frac{3}{p}) = 1$$

   Insgesamt folgt:

$$(\frac{3}{p}) = \begin{cases} 1 & p \equiv \pm 1 \,(\mathrm{mod}\ 12) \\ -1 & p \equiv \pm 5 \,(\mathrm{mod}\ 12) \end{cases}$$

4.11 Definition: (Der diskrete Logarithmus)
$p \in \mathbb{P}, u \in \mathbb{Z}/p$ primitive $(p-1)$-te Einheitswurzel (d.h. $\{u, u^2, u^3, \ldots, u^{p-1}\} = (\mathbb{Z}/p)^*$)

$$\begin{aligned}
\mathrm{ind}_u : ((\mathbb{Z}/p)^*, \cdot) &\overset{\cong}{\to} (\mathbb{Z}/(p-1), +) \\
\mathrm{ind}_u(u^s) &= s + (p-1)\mathbb{Z}
\end{aligned}$$

Vergleiche *(4.2)*: Für $a \not\equiv 0 \bmod p$ ist $(\frac{a}{p}) = (-1)^{\mathrm{ind}_u(\bar{a})}$ (setze $\bar{a} = u^s$)

In der Praxis ist die Berechnung von $\mathrm{ind}_u(a)$ sehr aufwendig.

4.3 Diffie-Hellman Schlüsseltausch

Ziel:
Alice und Bob wollen sich auf einen Schlüssel einigen, ohne diesen durch einen unsicheren Kanal zu übertragen.

Methode:
Wähle $p \in \mathbb{P}, u \in (Z/p)^*$ primitive $(p-1)$-te Einheitswurzel. Wähle $\alpha, \beta \in \mathbb{Z}/(p-1)$ beliebig $(\alpha, \beta \neq 0)$. Setze $a = u^\alpha, b = u^\beta \Rightarrow a^\beta = u^{\alpha \cdot \beta} = b^\alpha$

mögliche Umsetzung:
Alice veröffentlicht $p, u, a = u^\alpha$ für ein zufälliges und geheimes $\alpha \in \mathbb{Z}/(p-1), \alpha \neq 0$.

Bob will eine Nachricht $(c_1, c_2, \ldots, c_k)$ an Alice senden, $c_i \in \mathbb{Z}/p$. Bob wählt $\beta \in \mathbb{Z}/(p-1), \beta \neq 0$. β bleibt geheim. Bob berechnet $b := u^\beta$. Bob sendet

$$(b, d_1, \ldots, d_k) \quad d_j := c_j a^\beta$$

Alice berechnet $d_j \cdot b^{-\alpha} = c_j \cdot a^\beta \cdot b^{-\alpha} = c_j (u^{\alpha \cdot \beta}) \cdot (u^{-\beta \cdot \alpha}) = c_j$.

Will ein Lauscher die Nachricht dekodieren, muss er $a^\beta = b^\alpha$ kennen. Bekannt sind u, a, b somit muss der Lauscher noch $\alpha = \mathrm{ind}_u a$ und $\beta = \mathrm{ind}_u b$.

Dazu muss man ind_u effektiv berechnen können. Das kostst viel Rechenzeit.

Bemerkung:
Dahinter steht das Diffie-Hellman-Problem: Ist G eine Gruppe, $g \in G, a, b \in \mathbb{Z}$, wie berechnet man $g^{a \cdot b}$ aus g^a und g^b

Kapitel 5

Mehr zu Ringen und Zahlen

In diesem Kapitel wollen wir uns die Dinge, die wir im ersten Kapitel gelernt haben, nochmal von einem allgemeineren Standpunkt aus anschauen.

5.1 Definition: (Integritätsbereich, Euklidischer Ring)

(i) Sei R ein Ring, $R \neq \{0\}$. Dann heißt R *Integritätsbereich*, wenn man kürzen darf, d.h. wenn aus $a \cdot b = 0$ stets folgt $a = 0$ oder $b = 0$.

Es folgt: Ist $a \neq 0$ und $ax = ay$, dann gilt bereits $x = y$, denn

$$ax = ay \Rightarrow a(x - y) = 0 \overset{a \neq 0}{\Rightarrow} x - y = 0 \Rightarrow x = y$$

(ii) Ein Integritätsbereich R heißt *Euklidischer Ring*, wenn man „mit Rest teilen kann", d.h. es gibt eine Abbildung $\delta : R \to \mathbb{N}$ mit folgender Eigenschaft: Ist $a, b \in R, b \neq 0$, so gibt es $r, s \in R$ mit

$$a = b \cdot s + r \quad \text{wobei} \quad \delta(r) < \delta(b)$$

Beispiel:

zu (i) $\mathbb{Z}$ ist ein Integritätsbereich. Jeder Körper ist ein Integritätsbereich, insbesondere also auch $\mathbb{Z}/p$ für $p \in \mathbb{P}$.

Ist $m \geq 2, m \notin \mathbb{P}$, so ist $\mathbb{Z}/m$ kein Integritätsbereich, denn sei $m = k \cdot l$ mit $k, l \geq 2$ so gilt in $\mathbb{Z}/m$ $\bar{k} \cdot \bar{l} = \bar{m} = \bar{0}$.

zu (ii) $\mathbb{Z}$ ist ein euklidischer Ring mit $\delta(k) := |k|$ oder auch mit $\delta(k) = k^2$.

Jeder Körper ist ein euklidischer Ring mit $\delta(x) := \begin{cases} 0 & \text{falls } x = 0 \\ 1 & \text{falls } x \neq 0 \end{cases}$

5.2 Definition: (Körper der komplexen Zahlen)

(i) Sei $\mathbb{C}$ der Körper der komplexen Zahlen. Jede komplexe Zahl z ist von der Form $z = x + iy$ mit $x, y \in \mathbb{R}$, $i = \sqrt{-1}$, d.h. $i^2 = -1$.

Wir definieren $N(z) = x^2 + y^2$ als *Norm* von $z = x + iy$.

Das komplexe Konjugieren ist definiert als $(x + iy)^* := x - iy$ (oft auch geschrieben als $\overline{x + iy}$). Es folgt direkt, dass $N(z) = z \cdot z^*$. Weiterhin gilt $N(z \cdot w) = N(z) \cdot N(w)$.

(ii) Der Ring der *Gauß'schen Zahlen* ist

$$\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}] = \{x + iy \mid x, y \in \mathbb{Z}\}$$

Offensichtlich ist $\mathbb{Z}[i]$ ein Ring. Da $\mathbb{C} \supset \mathbb{Z}[i]$ ein Integritätsbereich ist, ist auch $\mathbb{Z}[i]$ ein Integritätsbereich.

Satz: Die Gauß'schen Zahlen bilden einen euklidischen Ring mit

$$\delta(z) := N(z) = z \cdot z^*$$

Beweis:
Seien $a, b \in \mathbb{Z}[i], b \neq 0$. Betrachte die komplexe Zahl $z := a/b = \tilde{x} + i\tilde{y}, \tilde{x}, \tilde{y} \in \mathbb{R}$. Es existieren $x, y \in \mathbb{Z}$ so, dass $|x - \tilde{x}| \leq \frac{1}{2}, |y - \tilde{y}| \leq \frac{1}{2}$. Setze $s := x + iy$, dann ist

$$N(z - s) = (\tilde{x} - x)^2 + (y - \tilde{y})^2 \leq \frac{1}{2}$$

und damit:

$$\begin{aligned} N(a - b \cdot s) &= N(b \cdot a/b - b \cdot s) \\ &= N(b)N(a/b - s) \\ &\leq \frac{1}{2}N(b) \\ &< N(b) \end{aligned}$$

Also gilt $N(r) < N(b)$. □

5.3 Definition und Satz: (Hauptideal, Hauptidealring)
Ein Integritätsbereich R heißt *Hauptidealring*, wenn jedes Ideal $I \trianglelefteq R$ ein *Hauptideal* ist, d.h. jedes Ideal ist von einem Element erzeugt, also $I = aR =: (a)$ für ein $a \in R$.

Jeder euklidische Ring ist ein Hauptidealring.

Beweis: (vgl. *(2.5)*)
Sei $I \trianglelefteq R$ ein Ideal. Ist $I = \{0\} = 0R = (0)$.

Ist $I \neq \{0\}$, wähle $a \in I$ mit $a \neq 0$ und $\delta(a)$ minimal. Ist $b \in I$, so gibt es $r, s \in R$ mit $b = as + r$ und $\delta(r) < \delta(a)$. Da $b \in I$ und $as \in I$ muss auch $r \in I$ sein. Da $\delta(a)$ minimal war, folgt bereits dass

$$r = 0 \;\Rightarrow\; b = as \;\Rightarrow\; b \in aR = (a) \;\Rightarrow\; I = (a)$$

□

Beispiel:
Insbesondere sind $\mathbb{Z}, \mathbb{Z}[i]$ Hauptidealringe.

Hierarchie von Ringen:

$$\text{Körper} \subset \text{euklidische Ringe} \subset \text{Hauptidealringe} \subset \text{Integritätsbereiche} \subset \text{Ringe}$$

5.4 Definition und Satz: (Teilbarkeit)
Sei R ein Hauptidealring. Für $a, b \in R$ schreibe $a \mid b$ „a teilt b“ falls $b = a \cdot s$ für ein $s \in R$ gilt.
Äquivalent dazu: $b \in (a)$ oder $(b) \subseteq (a)$.

Die Rechenregeln für Teilbarkeit aus §1.3 gelten folgendermaßen:

(i) $\forall a \in R, u \in R^* : u \mid a,\ a \mid a,\ a \mid 0$

(ii) $\forall a, b, c \in R : (a \mid b \wedge b \mid c) \Rightarrow a \mid c$

(iii) $\forall a, b \in R : (a \mid b \wedge b \mid a) \Rightarrow b = a \cdot u$ für ein $u \in R^*$

(iv) $\forall a, b, c \in R : (a \mid b \wedge a \mid c) \Rightarrow a \mid bs + ct$ für alle $s, t \in R$

(v) Ist $a \neq 0$ so gilt $ab \mid ac \Rightarrow b \mid c$.

Beweis:
Genau wie in §1.3. □

5.5 Lemma:
Sei R ein Hauptidealring, sei $p \in R, p \neq 0, p \notin R^*$. Die folgenden Bedingungen sind äquivalent:

(i) $a \mid p \;\Rightarrow\; (a \in R^* \vee a = pu, u \in R^*)$

(ii) $p \mid a \cdot b \;\Rightarrow\; (p \mid a \vee p \mid b)$

Beweis:

„⇐“: Gelte (ii) und $a \mid p$ also $ab = p \Rightarrow p \mid ab \overset{\text{(ii)}}{\Rightarrow} (p \mid a \vee p \mid b)$. Im ersten Fall gilt $a = pu$ mit $u \in R^*$. Im zweiten Fall gilt $p \mid b$ und $b \mid p$, also $b = pu$ mit $u \in R^*$, also $p = a \cdot b = a \cdot p \cdot u \Rightarrow a \cdot u = 1 \Rightarrow a \in R^*$.

„⇒“: Gelte $p \mid a \cdot b$, betrachte $I := (a) + (p) \trianglelefteq R \Rightarrow I = (c)$ für ein $c \in R$. Dann ist auch $p \in (c)$ also $c \mid p$.
Ist $c \in R^*$, dann folgt $(c) = R = aR + pR, 1 = axpy \Rightarrow b = abx + pby \Rightarrow p \mid b$.
Ist $c = p \cdot u$ für $u \in R^*$, so folgt $(c) = (p) \Rightarrow (a) \subseteq (p) \Rightarrow p \mid a$.

□

5.6 Definition: (Primelement)
Sei R Hauptidealring, $p \in R, p \neq 0, p \notin R^*$ heißt *Primelement*, wenn es die beiden äquivalenten Bedingungen aus dem Lemma *(5.5)* erfüllt.

Beispiel:

- Sei $R = \mathbb{Z}$, dann sind die Primelemente in $\mathbb{Z}$ gerade die Primzahlen.
- Betrachten wir den Ring $R = \mathbb{Z}[i]$ der Gauß'schen Zahlen. Wegen $N(wz) = N(z)N(w)$ und $N(1) = 1$ folgt, dass alle Einheiten in $\mathbb{Z}[i]$ Norm $= 1$ haben. $N(x + iy) = x^2 + y^2 \Rightarrow$ Die Gauß'schen Zahlen der Norm sind genau ± 1 und $\pm i$. Also gilt $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.

  Beispiel für Primelemente: $5 \in \mathbb{P}$ aber $5 = 4 + 1 = (2 + i)(2 - i)$, also ist 5 *kein* Primelement in $\mathbb{Z}[i]$. Dagegen ist $2 + i$ ein Primelement, denn $N(2 + i) = 5 \in \mathbb{P}$ und 5 kein nichttriviales Produkt ist.

  Die Primelemente in $\mathbb{Z}[i]$ heißen Gauß'sche Primzahlen.

5.7 Satz:
Die Gauß'schen Primzahlen sind genau die Gauß'schen Zahlen folgender Art:

a) $z = \pm p, z = \pm ip$ mit $p \in \mathbb{P}, p \equiv 3 \bmod 4$

b) $z = x + iy$ mit $xy \neq 0$ und $x^2 + y^2 \in \mathbb{P}$

Beweis:
Zeige zuerst, dass beide Typen Gauß'sche Primzahlen sind:

a) Sei $p \in \mathbb{P}$. Angenommen $p = z \cdot w$ mit $z, w \in \mathbb{Z}[i] \setminus \mathbb{Z}[i]^*$.

$$N(p) = p^2 = \underbrace{N(z)}_{\geq 2} \cdot \underbrace{N(w)}_{\geq 2} \Rightarrow N(z) = N(w) = p$$

Sei $z = a + ib$, dann ist $N(z) = a^2 + b^2 \equiv 0, 1, 2 \bmod 4$ denn $a^2, b^2 \equiv 0, 1 \bmod 4$. Es folgt $p \equiv 1 \bmod 4$ oder $p = 2$.

b) Sei $z = x + iy, x^2 + y^2 \in \mathbb{P}$, dann folgt bereits $xy \neq 0$. Angenommen $z = v \cdot w$ für $z, w \in \mathbb{Z}[i]$ dann folgt bereits:

$$\underbrace{N(z)}_{\in \mathbb{P}} = N(v)N(w) \;\Rightarrow\; N(v) = 1 \vee N(w) = 1 \;\Rightarrow\; v \in \mathbb{Z}[i]^* \vee w \in \mathbb{Z}[i]^*$$

Also ist p eine Gauß'sche Primzahl

Gauß'sche Zahlen vom Typ a) oder b) sind also immer Gauß'sche Primzahlen. Bleibt die Umkehrung zu zeigen, sei jetzt $z \in \mathbb{Z}[i]$ eine Gauß'sche Primzahl.

$$N(z) = q_1 \cdot q_2 \cdots q_k \text{ Primfaktorzerlegung in } \mathbb{N}$$

Da $N(z) = z \cdot z^*$ gibt es ein j mit $z \mid q_j =: p$. Genauso folgt $z^* \mid p^* = p \Rightarrow z \cdot z^* \mid p^2 = N(z)$, also ist $N(z) = p$ oder $N(z) = p^2$.

a) $N(z) = p^2$. Da $z, z^* \mid p^2$ gilt auch $z, z^* \mid p$ also $p = z \cdot w$.

$$\underbrace{N(z)}_{=p^2} N(w) = p^2 = N(p)$$

Also muss w schon eine Einheit sein $\Rightarrow z = \pm p$ oder $z = \pm ip$. $p \neq 2$, denn $2 = (1+i)(1+i)$ ist keine Gauß'sche Primzahl.

Warum ist $p \not\equiv 1 \bmod 4$? Wenn $p \equiv 1 \bmod 4$ gilt $(\frac{-1}{p}) = 1$, das heißt es gibt $a \in \{1, \ldots, p-1\}$ mit $a^2 \equiv -1 \bmod p$

$$k \cdot p = a^2 + 1 = (a+i)(a-i) \;\Rightarrow\; p \mid (a+i)(a-i)$$

Wäre p eine Gauß'sche Primzahl, so würde folgen:

$$p \mid a + i, \quad a - i = p(s + it) = ps + oti \Rightarrow p \mid 1$$

Widerspruch. Also muss schon $p \equiv 3 \bmod 4$ gelten und wir sind bei Typ a).

b) $N(z) = p = x^2 + y^2$ wobei $z = x + iy \Rightarrow x \cdot y \neq 0$ wir sind also bei Typ b).

□

Beispiel:
7 oder $2 + i$ sind Gauß'sche Primzahlen.

5.8 Lemma: *Eindeutigkeit der Primfaktorzerlegung*
Sei R ein Hauptidealring (z.B. $R = \mathbb{Z}[i]$) und seien $p_1, \ldots, p_k, q_1, \ldots, q_l$ Primelemente in R mit

$$p_1 \cdots p_k = q_1 \cdots q_l$$

Dann ist $k = l$ und es gibt $u_j \in R^*$ so, dass $p_j u_j = q_{j'}$, wobei zu jedem j genau ein j' gehört. Die Zerlegung in Primelemente ist also bis auf Reihenfolge und Multiplikation mit Einheiten eindeutig.

Beweis:
Ohne Beschränkung der Allgemeinheit nehmen wir $k \leq l$ an und führen eine vollständige Induktion nach k.

Induktionsanfang: $k = 1$
$p_1 = q_1 \cdots q_l \Rightarrow$ es gibt ein j mit $p_1 \mid q_j \Rightarrow q_j = p_1 u_1, u_1 \in R^* \Rightarrow 1 = q_1 \cdots q_{j-1} u_1 q_{j+1} \cdots q_l$.
Dann muss aber schon $l = 1$ und $p_1 = q_1$ gelten, da die q_j keine Einheiten sind.

Induktionsschritt: $k \geq 2$
$p_1 \cdots p_k = q_1 \cdot q_l \Rightarrow p_1 \mid q_j$ für ein $1 \leq j \leq l \Rightarrow q_j = p_1 u_1$ mit $u_1 \in R^*$.
Wir kürzen p_1 und erhalten $p_2 \cdots p_k = q_1 \cdots q_{j-1} u_1 q_{j+1} \cdots q_l$. Mit der Induktionsvoraussetzung folgt nun schon direkt die Behauptung.

□

5.9 Theorem:
Sei R ein Hauptidealring (z.B. $R = \mathbb{Z}[i]$), sei $r \in R, r \neq 0, r \notin R^*$. Dann gibt es Primelemente $p_1, \ldots, p_k \in R$ mit $r = p_1 \cdots p_k$. Nach Lemma *(5.8)* ist diese Zerlegung eindeutig bis auf Reihenfolge und Einheiten.

Beweis:
Wir nehmen an, das wäre falsch. Sei $M \subseteq R$ die Menge aller Gegenbeispiele, d.h. $m \in M \Rightarrow m \neq 0, m \notin R^*$ und m ist *kein* Produkt von Primelementen und $m \in M$.
Dann ist m kein Primelement, also $m = a \cdot b$ mit $a, b \notin R^*$. Es folgt $a \in M$ oder $b \in M$, sonst wäre m kein Gegenbeispiel. Wir erhalten so rekursiv eine Folge $\left(m_j\right)_{j \geq 1}$ von Gegenbeispielen $m_1 := m, m_2 \mid m_1, m_3 \mid m_2, \ldots$ und damit:

$$\{0\} \neq Rm_1 \subsetneqq Rm_2 \subsetneqq Rm_3 \subsetneqq \cdots$$

Setze:

$$I := \bigcup_{k \geq 1} Rm_k = \bigcup_{k \geq 1} (m_k)$$

Dies ist ein Ideal, denn sei $a, b \in I$ dann folgt

$$a \in Rm_k, b \in Rm_l \overset{\text{O.E. } k \geq l}{\Longrightarrow} a, b \in Rm_l \Rightarrow a \pm b \in Rm_l \subseteq I, a \cdot b \in Rm_l \subseteq I$$

und für $r \in R$ gilt $r \cdot a \in Rm_k \subseteq I$.

Weil R ein Hauptidealring ist, gibt es $m_0 \in R$ mit $I = Rm_0 \Rightarrow m_0 \in Rm_k$ für ein k.

$$I = Rm_0 \subseteq Rm_k \subsetneqq Rm_{k+1} \subseteq I$$

Dies ist aber ein Widerspruch, also kann es keine Gegenbeispiele geben. □

Bemerkung:
Für $\mathbb{Z} = R$ ist Theorem *(5.9)* der „Hauptsatz der Arithmetik“ *(1.8)* (mit einem anderen Beweis!).

Theorem 9 liefert, dass jede Gauß'sche Zahl $z \neq 0, \pm 1, \pm i$ ein Produkt von Gauß'schen Primzahlen ist.

5.10 Zerlegung in Primzahlen:
Wie zerlegt man eine Gauß'sche Zahl in Gauß'sche Primzahlen?

Betrachte zunächst gewöhnliche Primzahlen $p \in \mathbb{P} \subset \mathbb{Z}[i]$, dann gibt es 3 Fälle:

(i) $p = 2 = 1^2 + 1^2 = (1+i)(1-i) = -i(1+i)^2$, dann ist $1 + i = -i(1-i)$ Gauß'sche Primzahl.

(ii) $p \equiv 3 \bmod 4 \Rightarrow p$ ist Gauß'sche Primzahl vgl. *(5.7)*.

(iii) $p \equiv 1 \bmod 4 \Rightarrow p = x^2 + y^2 = (x+iy)(x-iy), xy \neq 0, x \pm iy$ sind beides Gauß'sche Primzahlen. Betrachte $x + iy \neq u(x - iy)$ für alle $u \in \{\pm 1, \pm i\}$, die beiden Gauß'schen Primfaktoren sind verschieden.

Damit kann man jede Gauß'sche Zahl zerlegen.

Beispiel:
Betrachten wir $z = 3 - 5i$, dann gilt $N(z) = 3^2 + 5^2 = 34 = 2 \cdot 17$. Wenn wir eine Zerlegung $z = z_1 \cdots z_k$ in Gauß'sche Primzahlen haben, so folgt aus der Multiplikativität der Norm, dass auch $N(z) = N(z_1) \cdots N(Z_k)$, wobei die $N(z_i)$ selbst wieder Primzahlen oder Quadrate von Primzahlen sind.

Wie oben gesehen führt uns die 2 zu $1 + i$. Weiter: $17 = 1 + 16 \rightarrow 4 \pm i$. Ansatz $u = \pm 1, \pm i, \varepsilon = \pm 1$, dann bekommen wir $z = u(1+i)(4+\varepsilon i) \overset{!}{=} 3 - 5i \Rightarrow \varepsilon = -1, u = -i$.

Also ist die Gauß'sche Primfaktorzerlegung gegeben durch: $3 - 5i = (-i)(1+i)(4-i)$.

5.11 Theorem: (Fermat)
Sei $p \in \mathbb{P}$. Die Gleichung $X^2 + Y^2 = p$ hat genau dann ganzzahlige Lösungen, wenn $p \not\equiv 3 \bmod 4$.

Beweis:
Sei $x^2 + y^2 = p = (x + iy)(x - iy)$. Daraus folgt nach *(5.7)*, dass $p = 2$ oder $p \equiv 1 \bmod 4$.

Andererseits ist $2 = 1^2 + 1^2$ und wenn $p \equiv 1 \bmod 4$, dann gibt es eine Gauß'sche Primzahl $z = x + iy$ mit $zz^* = p = x^2 + y^2$. □

5.12 Korollar: *Zwei-Quadrate-Satz*
Sei $n \in \mathbb{Z}, n \geq 2$. Die Gleichung $X^2 + Y^2 = n$ ist genau dann ganzzahlig lösbar, wenn für alle Primfaktoren p von n gilt:

$$(p \in \mathbb{P}, p \mid n, p \equiv 3 \bmod 4) \Rightarrow \nu_p(n) \text{ ist gerade}$$

Dabei sei $n = \prod_{p \in \mathbb{P}} p^{\nu_p(n)}$ die Primfaktorzerlegung nach *(1.8)*.

Beweis:
Sei $S = \{x^2 + y^2 \mid x, y \in \mathbb{Z}\}$. Wir überlegen uns zunächst, dass diese Menge abgeschlossen unter Multiplikation ist, also $k, l \in S \Rightarrow k \cdot l \in S$ gilt:

Sei $k = N(a + ib) = a^2 + b^2$ und $l = N(c + id) = c^2 + d^2$, dann gilt

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

Ist $p \in \mathbb{P}, p \not\equiv 3 \bmod 4$ dann folgt mit *(5.11)* schon $p \in S$.

Sei nun $p \in \mathbb{P}$, dann ist $p^{2l} \in S$, denn $p^{2l} = \left(p^l\right)^2 + 0^2 \in S$. Ist also die Bedingung von Satz 12 für n erfüllt, so folgt $n \in S$ mit Schritt 1. Die Bedingung ist also hinreichend.

Angenommen, $n = x^2y^2 = (x+iy)(x-iy)$, dann setzen wir $z := x+iy$. Zerlege z in Gauß'sche Primzahlen

$$z = \underbrace{z_1 \cdots z_k}_{\text{Typ } (5.7.1)} \cdot \underbrace{w_1 \cdots w_l}_{\text{Typ } (5.7.1)}$$

Dann ist

$$\begin{aligned} zz^* = n &= (z_1 z_1^*) \cdots (z_k z_k^*) \cdot (w_1 w_1^*) \cdots (w_l w_l^*) \\ &= p_1^2 \cdots p_k^2 \cdot q_1 \cdots q_l \end{aligned}$$

mit $p_j \equiv 3 \bmod 4, q_j \not\equiv 3 \bmod 4$. Dann folgt aber schon, dass $\nu_p(n)$ gerade, falls $p \equiv 3 \bmod 4$. Also ist die Bedingung auch notwendig. □

Beispiel:
Sei $n = 98 = 2 \cdot 7^2$, dann lässt sich 98 als Summe von zwei Quadraten schreiben.

$n = 27 = 3^3$ lässt sich nicht als Summe von zwei Quadraten schreiben, da $\nu_3(27) = 3$.

5.13 Definition und Satz (Pythagoäische Tripel)
Ein Tripel (r, s, t) ganzer Zahlen heißt *Pythagoäisches Tripel*, falls $r^2 + s^2 = t^2$.

Ist (r, s, t) ein Pythagoräisches Tripel, so sind auch $(\pm r, \pm s, \pm t), (\pm s, \pm r, \pm t)$ und für $d \in \mathbb{Z}$ auch $(d \cdot r, d \cdot s, d \cdot t)$ Pythagoräische Tripel.

Ein Pythagoräisches Tripel heißt *reduziert*, wenn $\mathrm{ggT}(r, s) = 1$. Um alle Pythagoräischen Tripel aufzuzählen, genügt es die reduzierten Tripel aufzuzählen.

Beispiel:
$3^2 + 4^2 = 5^2$.

Angenommen, $z = x + iy \Rightarrow z^2 = (x^2 - y^2) + i(2xy)$, dann ist auch

$$N\left(z^2\right) = \left(x^2 - y^2\right)^2 + (3xy)^2 = N(z)^2 = (x + y)^2$$

Wir haben also ein Pythagoräisches Tripel $(x^2-y^2, 2xy, x^2+y^2)$ gefunden.

Satz:
Alle reduzierten Pythaogräischen Tripel sind von der Form $\big(x^2-y^2, 2xy, \pm(x^2+y^2)\big)$ oder $\big(2xy, x^2-y^2, \pm(x^2+y^2)\big)$ mit $x, y \in \mathbb{Z}$ teilerfremd, $x-y$ ungerade.

Beweis:

„⇒“: Sei (r,s,t) ein reduziertes Pythagoräisches Tripel, schreibe

$$r+is = \underbrace{z_1 \cdots z_k}_{\text{Typ } (5.7.1)} \cdot \underbrace{w_1 \cdots w_l}_{\text{Typ } (5.7.1)}$$

als Zerlegung in Gauß'sche Primzahlen, dann folgt wie oben:

$$\begin{aligned} t^2 &= (z_1 z_1^*) \cdots (z_k z_k^*) \cdot (w_1 w_1^*) \cdots (w_l w_l^*) \\ &= p_1^2 \cdots p_k^2 \cdot q_1 \cdots q_l \end{aligned}$$

mit $p_j, q_j \in \mathbb{P}$, $p_j \equiv 3 \bmod 4, q_j \not\equiv 3 \bmod 4$. Da t^2 ein Quadrat ist, gibt es zu jedem j ein $j' \neq j$ mit $q_j = q_{j'}$ und l ist gerade. Durch Umsortieren gilt $q_j = q_{j+\frac{l}{2}}$ für $j = 1, \ldots, \frac{l}{2}$.

Betrachte $v = w_1 \cdots w_{\frac{l}{2}}$ und $r+is = v^2 \cdot u \cdot \underbrace{z_1 \cdot z_k}_{\in \mathbb{N}}$ mit $u = \pm 1, \pm i$. Ohne Einschränkung sei $z_j = p_j$, dann folgt aber schon $p_1 \cdots p_k \mid r, s$. Da r, s teilerfremd muss daher schon $k = 0$ sein.

Also ist $r+is = u \cdot v^2 = u \cdots (x+iy)^2 = u(x^2-y^2+2ixy)$. Damit ist (r,s,t) von der gewünschten Form.

„⇐“: Sind $x, y \in \mathbb{Z}$ teilerfremd, $x-y$ ungerade, so ist $\big(x^2-y^2, 2xy, x^2+y^2\big)$ ein Pythagoräisches Tripel.

$$\mathrm{ggT}\big(x^2-y^2, 2xy\big) = \mathrm{ggT}\big(\underbrace{(x-y)}_{\text{ungerade}} \underbrace{(x+y)}_{\text{ungerade}}, 2xy\big) = 1$$

□

Nächstes Ziel ist der Satz von Lagrange: Jede natürliche Zahl ist Summe von vier Quadraten ganzer Zahlen, also $n = W^2 + X^2 + Y^2 + Z^2$.

5.14 Lemma:
Ist $p \in \mathbb{P}, p \equiv 3 \bmod 4$, so gibt es $x, y \in \{1, \ldots, p-1\}$, sowie $k < p$ mit $x^2 + y^2 + 1 = kp$.

Beweis:
Da $p \equiv 3 \bmod 4$ gilt $(\frac{-1}{p}) = -1 = (\frac{p-1}{p})$. Andererseits ist $(\frac{1}{p}) = 1$. Es gibt also $a \in \{1, \ldots, p-2\}$ so, dass $(\frac{a}{p}) = 1$ und $(\frac{a+1}{p}) = -1$. Es folgt $(\frac{-(a+1)}{p}) = 1$.

Es gibt also ein x mit $x^2 \equiv a \bmod p$ mit $|x| < \frac{p}{2}$ und ein y mit $y^2 \equiv -(a+1) \bmod p$ und $|y| < \frac{p}{2}$. Es folgt $x^2 + y^2 \equiv a - a - 1 \bmod p \Rightarrow x^2 + y^2 + 1 = kp$. Da $|x|, |y| < \frac{p}{2}$ folgt $kp = x^2 + y^2 + 1 < 2\frac{p^2}{4} + 1 < p^2$. Also ist $k < p$. □

5.15 Lemma: *Eulers Formel*
Es gilt:

$$\begin{aligned} \left(\sum_{j=1}^4 x_j^2\right)\left(\sum_{j=1}^4 y_j^2\right) = \left(\sum_{j=1}^4 x_j y_j\right)^2 &+ (-x_1y_2 + x_2y_1 - x_3y_4 + x_4y_3)^2 \\ &+ (-x_1y_3 + x_3y_1 - x_4y_2 + x_2y_4)^2 \\ &+ (-x_1y_4 + x_4y_1 - x_2y_3 + x_3y_2)^2 \end{aligned}$$

Beweis:
Ohne Beweis. □

5.16 Theorem: Lagrange
Jede natürliche Zahl n lässt sich als Summe der Quadrate von vier ganzen Zahlen schreiben, also $n = w^2 + x^2 + y^2 + z^2$.

Beweis:
Nach *(5.15)* genügt es den Fall $n = p \in \mathbb{P}$ zu betrachten: Wenn die Aussage für alle Primzahlen ≥ 2 stimmt, stimmt sie für alle Zahlen (für $0, 1$ ist die Behauptung offensichtlich korrekt).

Ist $p \in \mathbb{P}, p \not\equiv 3 \bmod 4$, so gibt es x, y mit $p = x^2 + y^2 + 0^2 + 0^2$ *(5.11)*.

Ist $p \equiv 3 \bmod 4$, so igibt es nach *(5.14)* jedenfalls x, y mit $x^2 + y^2 + 1^2 = mp$ mit $1 < m < p$. Wir wählen das *kleinste* $m \in \{1, \ldots, p-1\}$ so, dass es x_1, x_2, x_3, x_4 gibt mit $x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp$.

Beh.: $m = 1$

1. Schritt: Dieses minimale m ist ungerade, denn sonst $m = 2l \Rightarrow x_1^2 + x_2^2 + x_3^2 + x_4^2 = 2lp \equiv 0 \bmod 2$. Ohne Einschränkung folgt $x_1^2 + x_2^2 \equiv 0 \equiv x_3^2 x_4^2 \bmod 2$ und

$$lp = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 = \frac{x_1^2 + x_2^2 + x_3^2 + x_4^2}{2}$$

Aber $l \leq m$. Dies ist ein Widerspruch da m minimal gewählt war.

2. Schritt Das minimale m ist $m = 1$, denn wäre $m \geq 3$ ungerade mit $x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp$. Wähle y_j mit $y_j \equiv x_j \bmod m$ und $|y_j| \overset{m \text{ ungerade}}{<} \frac{m}{2}$. Also:

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv \underbrace{y_1^2 + y_2^2 + y_3^2 + y_4^2}_{= lm < m^2 \Rightarrow l < m} \equiv 0 \bmod m$$

Wäre $l = 0$, so hätten wir $x_j \equiv 0 \bmod m$ für $j = 1, 2, 3, 4 \Rightarrow m^2 \mid pm \Rightarrow p = m$. Dies ist ein Widerspruch, denn $m < p$.

Also $1 < l < m$. Nun sagt Eulers Formel

$$\underbrace{\left(\sum_{=1}^{4} x_j^2\right)}_{\text{Vielfaches von } m} \left(\sum_{j=1}^{4} y_j^2\right) = A^2 + B^2 + C^2 + D^2$$

und $m \mid A, B, C, D$, also

$$\begin{aligned} & (p \cdot m)(l \cdot m) = A^2 + B^2 + C^2 + D^2 \\ \Leftrightarrow \quad & p \cdot l = \left(\tfrac{A}{m}\right)^2 + \left(\tfrac{B}{m}\right)^2 + \left(\tfrac{C}{m}\right)^2 + \left(\tfrac{D}{m}\right)^2 \end{aligned}$$

aber $l < m$ und damit Widerspruch!

□

Bemerkung:
Fermat hat 1637 behauptet/vermutet: Für $n \geq 3$ hat die Gleichung $x^n + y^n = z^n$ keine nichttriviale Lösung durch ganze Zahlen, das heißt jede ganzzahlige Lösung (x, y, z) hat die Zusatzeigenschaft $xyz = 0$. Fermat hat das für $n = 4$ später bewiesen.

Euler hat den Fall $n = 3$ betrachtet. Viele Spezialfälle von n wurden im 19./20. Jahrhundert bewiesen. Gerd Faltings zeigte 1984, dass es für festes n höchstens endlich viele nichttriviale Lösungen gibt.

1999 bewies A. Wiles Fermats Vermutung.

Kapitel 6

Irrationale und transzendente Zahlen

Erinnerung:
Der Körper $\mathbb{Q} := \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0 \right\}$ besteht aus allen rationalen Brüchen. Aber $\mathbb{Q}$ ist nicht vollständig, es gibt Cauchy-Folgen in $\mathbb{Q}$, deren Grenzwert nicht in $\mathbb{Q}$ liegt.

Die Vervollständigung von $\mathbb{Q}$ ist der Körper $\mathbb{R}$ der reellen Zahlen. $\mathbb{Q} \subseteq \mathbb{R}$ ist dicht. $\mathbb{Q}$ ist abzählbar, $\mathbb{R}$ ist dagegen nicht abzählbar. Insbesondere ist $\mathbb{Q} \subsetneq \mathbb{R}$.

Die Zahlen in $\mathbb{R} \setminus \mathbb{Q}$ heißen irrationale Zahlen. Die Pythagoräer wussten schon: $\sqrt{2} \notin \mathbb{Q}$. Betrachte die Funktion $f(x) = x^2 - 2$. Es gilt $f(0) = -2, f(2) = 2$. Nach dem Zwischenwertsatz existiert ein $x \in [0, 2]$ mit $f(x) = 0$. Also gilt $\sqrt{2} \in \mathbb{R}$.

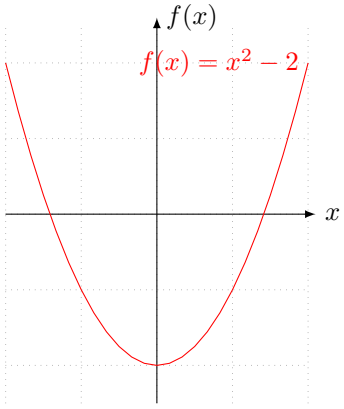


Abbildung 6.1: Funktion

Angenommen $\sqrt{2} \in \mathbb{Q}$, dann wäre $\sqrt{2} = \frac{a}{b}, a, b \in \mathbb{Z}, b \neq 0$. Ohne Einschränkung ist $\mathrm{ggT}(a, b) = 1$.

$$\frac{a^2}{b^2} = 2 \Rightarrow a^2 = 2b^2 \Rightarrow 2 \mid a^2 \Rightarrow 2 \mid a \Rightarrow 2^2 = 4 \mid a^2 \Rightarrow 2 \mid b^2 \Rightarrow 2 \mid b$$

Dies ist ein Widerspruch zu $\mathrm{ggT}(a, b) = 1$.

6.1 Definition: (algebraische Zahl, algebraischer Abschluss)
Ein nicht konstantes Polynom $f(X)$ heißt *normiert*, wenn der Leitkoeffizient 1 ist, d.h. wenn

$$f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0, \qquad n \geq 1$$

Eine reelle oder komplexe Zahl z heißt *algebraische Zahl*, wenn es ein normiertes Polynom $f(X)$ gibt mit $f(z) = 0$, dessen Koeffizienten $a_j \in \mathbb{Q}$ sind.

Die Menge aller algebraischen Zahlen in $\mathbb{C}$ ist $\overline{\mathbb{Q}}$ (sog. *algebraischer Abschluss* von $\mathbb{Q}$), $\overline{\mathbb{Q}} = \{z \in \mathbb{C} \mid z$ Nullstelle von norm. Polynom mit rationalen Koeffizienten$\}$.

Eine algebraische Zahl $z \in \mathbb{C}$ heißt *ganze algebraische Zahl*, wenn es ein normiertes Polynom $f(X)$ mit ganzzahligen Koeffizienten gibt mit $f(z) = 0$. Die Menge der ganzen algebraischen Zahlen ist $\mathcal{O} = \{z \in \mathbb{C} \mid z$ ganze alg. Zahl$\} \subseteq \overline{\mathbb{Q}}$.

$z \in \mathbb{C}$ heißt *transzendent*, wenn $z \in \mathbb{C} \setminus \overline{\mathbb{Q}}$.

Beispiel:
$\sqrt{2}$ ist algebraisch, denn $f(X) = X^2 - 2$.
$\sqrt{-1} = i$ ist algebraisch, denn $f(X) = X^2 + 1$.
$\frac{a}{b} \in \mathbb{Q}$ ist algebraisch, denn $f(X) = X - \frac{a}{b}$.
Aber e, π sind nicht algebraisch (wie wir später sehen werden).
$\sqrt{2}, \sqrt{3}, \sqrt{-1}, \ldots$ sind ganze algebraische Zahlen.

6.2 Satz:
Jede rationale, ganze algebraische Zahl ist eine ganze Zahl, also $\mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$.

Beweis:
Sei $\frac{a}{b} \in \mathbb{Q} \cap \mathcal{O}, \left(\frac{a}{b}\right)^n + \left(\frac{a}{b}\right)^{n-1} a_{n-1} + \ldots + a_0 = 0, a_j \in \mathbb{Z}$. Ohne Einschränkung sei $\mathrm{ggT}(a,b) = 1$. Betrachte $a^n + a^{n-1} \cdot b \cdot a_{n-1} + \ldots + b^n a_0 = 0$, dann folgt $a^n \equiv 0 \bmod b \Rightarrow b \mid a^n$. Ist $p \in \mathbb{P}$ Teiler von b so folgt $p \mid a$, ein Widerspruch zu $\mathrm{ggT}(a,b) = 1$. Dann muss aber schon $b = \pm 1$ gelten. □

6.3 Korollar:
Ist $r \in \mathbb{R}$ eine Nullstelle von einem ganzzahligen Polynom $X^n + a_{n-1}X^{n-1} + \ldots + a_0, n \geq 1, a_j \in \mathbb{Z}$, so folgt: $r \in \mathbb{Z}$ oder r ist irrational.

6.4 Korollar:
Ist $m \in \mathbb{N}$ kein Quadrat in $\mathbb{N}$, so ist $\sqrt{n}$ irrational. Insbesondere ist $\sqrt{p}$ irrational für alle $p \in \mathbb{P}$.

Beweis:
$X^2 - m$ hat keine Nullstelle in $\mathbb{Z}$ nach Annahme. Also sind die Nullstellen $\pm\sqrt{m}$ irrational. □

6.5 Definition: (transzendente Zahlen)
Die Zahlen in $\mathbb{C} \setminus \overline{\mathbb{Q}}$ heißen *transzendente Zahlen*.

$$\begin{array}{ccccc} \mathcal{O} & \subset & \overline{\mathbb{Q}} & \subset & \mathbb{C} \\ \cup & & \cup & & \cup \\ \mathbb{Z} & \subset & \mathbb{Q} & \subset & \mathbb{R} \end{array}$$

6.6 Definition: (Die Exponentialreihe)
Aus Analysis I wissen wir, dass für $z \in \mathbb{C}$

$$\exp(z) = \sum_{k=0}^{\infty} \frac{1}{k!} z^k$$

konvergiert für jedes $z \in \mathbb{C}$. Beachte: $\lim_{k\to\infty} \left(\frac{1}{k!} z^k\right) = 0$ für jedes $z \in \mathbb{C}$.
Die *Eulersche Zahl* ist $z := \exp(z) \approx 2{,}71\ldots$ Ziel: ist transzendent.

6.7 Definition und Lemma:
Sei $f(z) = \sum_{k=0}^{n} a_k z^k$ ein Polynom. Definiere neues Polynom $\hat{f}(z) := f(z) + f'(z) + f''(z) + \ldots = \sum_{k=0}^{n} f^{(k)}(z)$.
Setze $q(z) := \hat{f}(0) \cdot \exp(z) - \hat{f}(z)$. Dann gilt

$$|q(z)| \leq \exp(|z|) \cdot \sum_{k=0}^{n} |a_k| \cdot |z|^k$$

Beweis:
Es ist

$$\hat{f}(z) = \sum_{k=0}^{n} a_m \sum_{k=0}^{n} \frac{m!}{k!} z^k$$

Denn $g(z) = z^m, \hat{g}(z) = z^m + mz^{m-1} + \ldots + 1$. Also ist $\hat{f}(0) = \sum_{m=0}^{n} a_m \cdot m!$, insgesamt also

$$\begin{aligned} |q(z)| &= \left| \sum_{m=0}^{n} a_m \cdot m! \sum_{k=0}^{\infty} \frac{1}{k!} z^k - \sum_{m=0}^{n} a_m \cdot m! \sum_{k=0}^{m} \frac{1}{k!} z^k \right| \\ &= \left| \sum_{m=0}^{n} a_m \cdot \sum_{k=m+1}^{\infty} \frac{m!}{k!} z^k \right| \\ &= \left| \sum_{m=0}^{n} a_m \sum_{k=1}^{\infty} \frac{1}{k!} z^k z^m \right| \\ &\leq \sum_{m=0}^{n} |a_m| \cdot |z|^m \cdot \exp(m) \end{aligned}$$

□

6.8 Theorem:
Sei $g(z) = g_m z^m + g_{m-1} z^{m-1} + \ldots + g_0$ mit $m \geq 1, g_m, g_0 \neq 0, g_i \in \mathbb{Z}$. Dann gilt $g(e) \neq 0$ für $e = \exp(q)$.

Beweis:
Sei $g(z)$ wie oben fest gegeben. Sei $p \in \mathbb{P}$ eine Primzahl (später wählen wir p genauer). Betrachte

$$f(z) := \frac{1}{(p-1)!} z^{p-1} \prod_{j=1}^{m} (j - z)^p$$

(hängt von p und $m =$ Grad von g ab). f hat mit $z = 0$ eine Nullstelle der Ordnung $p - 1$, in $z - j$ eine Nullstelle der Ordnung p für $j = 1, \ldots, , m$. Es ist $\left(\frac{d}{dz}\right)^k f(0) = 0$ für $k = 0, \ldots, p-2$ und $\left(\frac{d}{dz}\right)^{p-1} f(0) = (m!)^p$. Weiter ist $\left(\frac{d}{dz}\right)^k f(j) = 0$ für $k = 0, \ldots, p-1$ und $\left(\frac{d}{dz}\right)^p f(j) \equiv 0 \bmod p$.
Folglich ist $\hat{f}(0) \equiv m! \bmod p$ und $\hat{f}(j) \equiv 0 \bmod p$ für $j = 1, \ldots, m$. Ist nun $p > m!, |g_0|$ so folgt

$$\sum_{j=0}^{m} g_j \hat{f}(j) \equiv g_0 \cdot (m!)^p \not\equiv 0 \bmod p$$

Insbesondere ist $\sum_{j=0}^{m} g_j \hat{f}(j)$ eine von 0 verschiedene ganze Zahl.

$$\begin{aligned} \hat{f}(0) \cdot g(\exp(0)) &= \hat{f}(0) \sum_{j=0}^{m} g_j \cdot \underbrace{e^j}_{\exp(j)} \\ &= \underbrace{\sum_{j=0}^{m} g_j \hat{f}(j)}_{\text{ganze Zahl} \neq 0} + \underbrace{\sum_{j=0}^{m} g_j q(j)}_{=:\varepsilon} \end{aligned}$$

Strategie: Wenn wir zeigen, dass $|\varepsilon| \leq \frac{1}{2}$, so ist die rechte Seite $e \neq 0$, also $g(e) \neq 0$. Nach *(6.7)* gilt $\varepsilon = \sum_{j=0}^{m} g_j q(j)$. Es genügt zu zeigen, dass die $g(j)$ sehr klein sind.

$$\begin{aligned} |q(j)| &\leq \exp(j) \sum_{k=0}^{n} |a_k| \cdot |z|^k \qquad \text{wobei } f(z) = \sum_{j=0}^{n} a_k z^k \\ \sum_{k=0}^{n} |a_k| \cdot |z|^k &\leq \frac{1}{(p-1)!} |l|^{p-1} \prod_{l=1}^{m} (j + l)^p \\ &= C \cdot \frac{A^{p-1}}{(p-1)!} \qquad \text{wobei } C, A \text{ nur von } m, l \text{ abhängen} \end{aligned}$$

Ist p hinreichend groß, wird dieser Ausdruck kleiner als jede positive reelle Zahl. Durch Wahl iner sehr froßen Primzahl p erreichen wir also, dass

$$\left|\sum_{j=0}^{m} g_j q(j)\right| \leq \frac{1}{2}$$

Es folgt $g(e) \neq 0$. □

6.9 Theorem: (Hermite 1873)
Die Eulersche Zahl e ist transzendent.

Beweis:
Sei $f(z) = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ mit $a_j \in \mathbb{Q}$. Angenommen $f(e) = 0$. Falls $a_0 = 0$, so teile durch e^k und wir erhalten ein neues Polynom mit rationalen Koeffizienten und konstantem Term $\neq 0$.

Weiter gibt es $0 \neq b \in \mathbb{Z}$ so, dass $a_j \cdot b \in \mathbb{Z}$ (z.B. kleinstes gemeinsames Vielfaches). So erhalten wir $g(z) = bz^n + a_{n-1}bz^{n-1} + \ldots + a_0 b, a_0 b \neq 0$. Mit *(6.8)* folgt, dass $g(e) \neq 0$. □

6.10 Definition und Satz:
Für $w_0, \ldots, w_k \in \mathbb{C}$ sei $\langle w_0, \ldots, w_k\rangle := \mathbb{Z} \cdot w_0 + \ldots + \mathbb{Z} \cdot w_k$. Das ist eine abelsche Gruppe (Untergruppe von $(\mathbb{C}, +)$).

Sei $u \in \mathbb{C}$, dann ist äquivalent:

(i) u ist ganze algebraische Zahl

(ii) Es gibt Zahlen $u_1, \ldots, u_k \in \mathbb{C}$ so, dass $u \cdot \langle 1, u_1, \ldots, u_k\rangle \subseteq \langle 1, u_1, \ldots, u_k\rangle$

Beweis:

(i)⇒(ii):
$u^n + a_{n-1}u^{n-1} + \ldots + a_0 = 0, aj \in \mathbb{Z} \Rightarrow u^n = -\big(a_0 + a_1 u + \ldots + a_{n-1}u^{n-1}\big)$. Betrachte $\langle 1, u, u^2, \ldots, u^{-1}\rangle =: M$. Es folgt $u^n \in M, u^k \in M$ für $k < u$ also $u \cdot M \subseteq M$.

(ii)⇒(i):
Sei $M := \langle 1, u_1, \ldots, u_k\rangle$ und gelte $u \cdot M \subseteq M$. Setze $u_0 := 1$. Es folgt

$$u \cdot u_0 = \sum_{j=0}^{k} c_{0j} \cdot u_j \cdots u \cdot u_s = \sum_{j=0}^{k} c_{sj} u_j \text{ mit } c_{sj} \in \mathbb{Z}$$

Wir erhalten also das lineare Gleichungssystem:

$$\sum_{j=0}^{k} (\delta_{sj} u u_j - c_{sj} u_j) = 0 \qquad (\mathbb{I}u - C) \begin{pmatrix} u_0 \\ \vdots \\ u_k \end{pmatrix} = 0$$

dabei ist $C = \big(c_{sj}\big)_{s,j=0}^{k}$ eine Matrix mit ganzzahligen Einträgen. Also ist $\det(\mathbb{I}u - C) = 0$. Das Polynom $\det(\mathbb{I}C - C) = g(x) = X^{k+1} + X^k g_k + \ldots + g_0$ mit $g_j \in \mathbb{Z}$ und $g(u) = 0$. Also ist u eine ganze algebraische Zahl.

□

6.11 Satz:
Die ganzen algebraischen Zahlen bilden einen Ring. Zu jeder algebraischen Zahl $u \in \overline{\mathbb{Q}}$ gibt es ein $a \in \mathbb{Z}, a \geq 1$ so, dass $a \cdot u$ eine ganze algebraische Zahl ist.

Beweis:
Sei $u, v \in \mathcal{O}$. Zu zeigen ist $u \pm v \in \mathcal{O}, u \cdot v \in \mathcal{O}$.

Nach *(6.10)* gibt es $M = \langle 1, u_1, \ldots, u_m \rangle, L = \langle 1, v_1, \ldots, v_l \rangle$ mit $uM \subseteq M, vL \subseteq L$. Es ist $M \cdot L = M \cdot L = \langle 1, u_1, \ldots u_m, v_1, \ldots, v_l, u_j v_k, \ldots \rangle$.

$$(u \pm v)M \cdot L \subseteq \underbrace{uM}_{\subseteq M} L \pm \underbrace{uL}_{\subseteq L} M \subseteq ML + LM = ML \overset{(6.10)}{\Rightarrow} u \pm v \in \mathcal{O}$$

$$(u \cdot v)ML = uM \cdot vL \subseteq M \cdot L \overset{(6.10)}{\Rightarrow} u \cdot v \in \mathcal{O}$$

Sei $u \in \overline{\mathbb{Q}}, u^n + a_{n-1}u^{n-1} + \ldots + a_0 = 0, a_j \in \mathbb{Q}$. Wähle $a \in \mathbb{Z}, a \geq 1$ sp, dass $aa_j \in \mathbb{Z}$ (a als Hauptnenner der a_j).

$$0 = a^n(u^n + \ldots, +a_0) = (\cdot + a_{\cdot -1}(\cdot^{-1} + \ldots + a_0 u)^n + \underbrace{aa_{n-1}}_{\in \mathbb{Z}}(a \cdot u)^{n-1} + \ldots + \underbrace{a^n a_0}_{\in \mathbb{Z}} \Rightarrow a \cdot u \in \mathcal{O}$$

□

Bemerkung:
(6.10) liefert eine Konstruktion des Polynoms, das $u \pm v$ oder $u \cdot v$ als Nullstelle hat.

Genauso zeigt man, dass $\overline{\mathbb{Q}}$ ein Ring ist. In *(6.10)* benutze statt $\langle 1, u_1, \ldots, u_k \rangle$ die abelsche Gruppe $\langle 1, u_1, \ldots, u_k \rangle_{\mathbb{Q}} := 1\mathbb{Q} + u_1\mathbb{Q} + \ldots + u_k\mathbb{Q}$. Damit kann man die Beweise von *(6.10)* und *(6.11)* wörtlich kopieren.

Tatsächlich ist $\overline{\mathbb{Q}}$ sogar ein Körper, der sogenannte *algebraische Abschluss* des Körpers $\mathbb{Q}$ ($\rightarrow$ Algebra I/II).

6.12 Erinnerung: Der Fundamentalsatz der Algebra
Der Fundamentalsatz der Algebra sagt, dass jedes nicht konstante Polynom in $\mathbb{C}$ eine Nullstelle hat (Beweis meist in Funktionentheorie).

Folgerung: Ist $f(z) = z^n + a_{n-1}z^{n-1} + \ldots + a_0, a_j \in \mathbb{C}, n \geq 1$. Mit *(3.26)* folgt $f(z) = (z - \alpha_1) \cdots (z - \alpha_n)$. Die α_i sind genau die komplexen Nullstellen von f.

6.13 Definition: (symmetrische Polynome)
Ein Polynom $f(t_1, \ldots, t_n)$ in n Variablen heißt *symmetrisch*, wenn es sich bei Permutation der Variablen nicht ändert.

Die *elementarsymmetischen Polynome* sind erklärt durch

$$(X - t_1)(X - t_2) \cdots (X - t_n) = X^n - \sigma_1(t_1, \ldots, t_n)X^{n-1} + \ldots + (-1)^n \sigma_n(t_1, \ldots, t_n)$$

mit

$$\begin{aligned} \sigma_1(t_1, \ldots, t_n) &= t_1 + \ldots + t_n \\ \sigma_2(t_1, \ldots, t_n) &= \sum_{j<k} t_j t_k \\ &\vdots \\ \sigma_n(t_1, \ldots, t_n) &= t_1 \cdots t_n \end{aligned}$$

Nach Konstruktion sind die $\sigma_k(t_1, \ldots, t_n)$ alle symmetrische Polynome. Die σ_k heißen *elementarsymmetrische Polynome*. Setzt man $t_n = 0$ in der Definition, so sieht man

$$\underbrace{\sigma_k(t_1, \ldots, t_{n-1})}_{k\text{-te elem. Pol. in } n-1 \text{ Variablen}} = \underbrace{\sigma_k(t_1, \ldots, t_{n-1}, 0)}_{k\text{-te elem. Pol. in } n \text{ Variablen}}$$

Beispiel:
$f(t_1, t_2) = t_1 + t_2 + t_1 \cdot t_2$ ist symmetrisch, $f(t_1, t_2) = t_1 - t_2$ ist nicht symmetrisch.

6.14 Satz: *Satz über symmetrische Polynome*
Sei $f(t_1, \ldots, t_n)$ ein symmetrisches Polynom. Dann gibt es eon Polynom $g(s_1, \ldots, s_n)$ in n Variablen mit

$$f(t_1, \ldots, t_n) = g\big(\sigma_1(t_1, \ldots, t_n), \ldots, \sigma_n(t_1, \ldots, t_n)\big)$$

Wenn f rationale / ganzzahlige Koeffizienten hat, so auch g.

Bemerkung:
Wir führen eine Induktion nach n:

Induktionsanfang: $n = 1$
$\sigma_1(t_1) = t_1$. Wir sind fertig mit $g = f$.

Induktionsschritt: $n \to n + 1$
Wir definieren uns zunächst den *Grad*

$$d\big(t_1^{k_1}, \ldots, t_n^{k_n}\big) := k_1 + \ldots + k_n, \quad d(f_1 + \ldots + f_r) := \max\{d(f_1), \ldots, d(f_r)\}$$

und das *Gewicht*

$$w\big(t_1^{k_1}, \ldots, t_n^{k_n}\big) := k_1 + 2k_2 + \ldots + nk_n, \quad w(f_1 + \ldots + f_r) := \max\{w(f_1), \ldots, w(f_r)\}$$

wobei f_j Monome sind.

Wir erweitern unsere Induktionsbehauptung und beweisen nun: $f(t_1, \ldots, t_n) = g(\sigma_1, \ldots, \sigma_n)$ mit $d(f) \geq w(g)$. (Für $n = 1$ ist das auch ok).

Ist $d(f) = 0$, so ist $f = \text{const}$, $g = f$ fertig. Wir führen eine zweite Indutkion nach $d(f) =: d$.

$f(t_1, \ldots, t_n, t_{n+1})$ ist gegeben

$$\underbrace{f(t_1, \ldots, t_n, 0)}_{\text{symm. in } t_1, \ldots, t_n} = g_1(\sigma_1, \ldots, \sigma_n) \qquad \text{(Induktionsannahme für } n\text{)}$$

Setze $f_1(t_1, \ldots, t_n, t_{n+1}) := f(t_1, \ldots, t_{n+1} - g_1\big(\sigma_1(t_1, \ldots, t_{n+1}), \ldots, \sigma_n(t_1, \ldots, t_{n+1})\big)$. $d(f_1) \leq d := d(f)$.

$f_1(t_1, \ldots, t_n, 0) = 0 \Rightarrow t_{n+1}$ lässt sich abspalten von $f_1 \Rightarrow$ *alle* t_j spalten ab, $f_1 = \underbrace{(t_1 \cdots t_{n+1})}_{=\sigma_{n+1}} \cdot f_2, d(f_2) <$ d, f_2 symmetrisch.

Es folgt $f_2(t_1, \ldots, t_{n+1}) = g_2(\sigma_1, \ldots, \sigma_{n+1})$. Setze $g_3(\sigma_1, \ldots, \sigma_{n+1}) = \sigma_{n+1} \cdot g_2(\sigma_1, \ldots, \sigma_{n+1}) = f_1(t_1, \ldots, t_{n+1})$.

Insgesamt:

$$f(t_1, \ldots, t_{n+1}) = g_1(\sigma_1, \ldots, \sigma_n) + g_3(\sigma_1, \ldots, \sigma_{n+1})$$

6.15 Theorem:
Sei α eine algebraische Zahl. Dann ist $\exp(\alpha) \neq -1$, mit anderen Worten: $e^\alpha + 1 \neq 0$.

Beweis:
Nach *(6.11)* existiert ein $a \in \mathbb{Z}, a > 0$ so, dass $a \cdot \alpha$ eine ganze algebraische Zahl ist, also Nullstelle eines Polynoms $g(X) = X^m + a_{m-1}X^{m-1} + \ldots + a_0$ mit $a_j \in \mathbb{Z}$. Nach dem Fundamentalsatz der Algebra zerfällt g in $\mathbb{C}$ als

$$g(X) = (X - a\alpha_1) \cdots (X - a\alpha_m)$$

wobei die $a\alpha_j$ die Nullstellen sind. Ohne Einschränkung sei $a\alpha = a\alpha_1$. Die $a\alpha_j$ sind alle ganze algebraische Zahlen. Erinnerung: $e^z := \exp(z)$ und es gilt $\exp(z)\exp(w) = \exp(z + w)$.

Wir beweisen, dass $\prod_{j=1}^{m}(e^0+e^{\alpha_j}) \neq 0$, denn daraus folgt, dass $\frac{e^0+e^{\alpha_j}}{1+e^{\alpha_j}} \neq 0$:
Sei $M := \{1,\ldots,m\}$, für $J \subseteq M$ betrachte $\beta_J := \sum_{j\in J}\alpha_j, \beta_\emptyset := 0$. Dies sind 2^m komplexe Zahlen und es gilt:

$$\prod_{j=1}^{m}\left(e^0+e^{\alpha_j}\right) = \sum_{j\in J} e^{\beta_j}$$

Beh.: Das Polynom $\prod_{j\in J}(X-a\beta_J)$ hat genau *ganzzahlige* Koeffizienten
Bew.: Die Koeffizienten dieses polynoms erhält man durch Einsetzen der $a\beta_J$ in die elementarsymmetrischen Polynome, sind also symmetrisch in den $a\beta_J$. Da $\beta_J = \sum_{j\in J}\alpha_j$ gilt, sind die Koeffizienten auch symmetrische Polynome in den α_j. Also sind die Koeffizienten dieses Polynoms Polynome in den elementarsymmetrischen Polynomen mit $a\alpha_j$ eingesetzt *(6.14)*. Nach Konstruktion ist aber $\sigma_k(a\alpha_1,\ldots,a\alpha_k) \in \mathbb{Z}$, da $g(X)$ $\mathbb{Z}$-Koeffizienten hat.
Die Koeffizienten von $\prod_{J\subseteq M}(X-\beta_J)$ sind also ganze Polynome in den $\sigma_k(\alpha_1,\ldots,\alpha_k) \in \mathbb{Z}^{J\subseteq M}$ und deswegen selber ganze Zahlen. Das Polynom $\prod_{J\subseteq M}(X-\beta_J)$ hat also $\mathbb{Q}$-Koeffizienten.

Nun sei $p \in \mathbb{P}$ eine (große) Primzahl, die Strategie ist ähnlich wie in *(6.8)*: Betrachte das Polynom

$$f(z) := \frac{1}{(p-1)!}\underbrace{(az)^{p-1}}_{\text{ganzz. Koeff.}}\prod_{\beta_j\neq 0}\underbrace{(az-a\beta_j)^p}_{\text{ganzz. Koeff.}}$$

Die Nullstellen von f sind 0 sowie der $\beta_J \neq 0$. $\left(\frac{d}{dz}\right)^k f(z)$ hat ganzzahlige Koeffizienten, falls $k \geq p$. Es gilt sogar: die Koeffizienten liegen in $p\mathbb{Z}$. $\left(\frac{d}{dz}\right)^k f(0) = 0$ für $k = 0,\ldots,p-2$.

$$\left(\frac{d}{dz}\right)^{p-1} f(0) = \underbrace{a^{p-1}\prod_{\beta_j\neq 0}(-a\beta_J)^p}_{\neq 0} \in \mathbb{Z}$$

Für p ausreichend groß ist $\left(\frac{d}{dz}\right)^{p-1} f(0) \not\equiv 0 \bmod p$

Setze $\hat{f} = f + f' + f'' + \ldots$, dann folgt

$$\hat{f}(0) \equiv a^{p-1}\prod_{\beta_J\neq 0}(-a\beta_J)^p \bmod p$$

und für genügend großes $p >> 0$ ist $\hat{f}(0) \not\equiv 0 \bmod p$. Weiter ist $(\frac{d}{dz})^k f(\beta_J) = 0$ für $k = 0,1,\ldots,p-1$ und für $\beta_J \neq 0$ $\hat{f}(\beta_J) = f^{(p)}(\beta_J) + f^{(p+1)}(\beta_J) + \ldots$. Nun gilt

$$\sum_{\beta_J\neq 0}\left(a\beta^J\right)^l = \sum_{J\subseteq M}\left(a\beta^J\right)^l \in \mathbb{Z}$$

da Polynom in den elementarsymmetrischen Funktionen $\sigma_k(a\alpha_1,\ldots,a\alpha_k)$, also $\sum_{\beta_J\neq 0}\hat{f}(\beta_J) \in p\mathbb{Z}$.
Insgesamt haben wir

$$\sum_{J\subseteq M}\hat{f}(\beta_J) = \underbrace{\sum_{J\subseteq M,\beta_J=0}\hat{f}(0)}_{C\cdot\hat{f}(0),C\geq 1} + \underbrace{\sum_{J\subseteq M\in\mathbb{Z},\beta_J\neq 0}\hat{f}(\beta_J)}_{\in p\mathbb{Z}}$$

mit $C\cdot\hat{f}(0) \not\equiv 0 \bmod p$ für $p >>= 0$. Es folgt:

$$\sum_{J\subseteq M}\hat{f}(\beta_J) \in \mathbb{Z}\setminus\{0\}$$

Nun schätzen wir wieder ab: Sei $q(z) := \hat{f}(0)\cdot\exp(z) - \hat{f}(z)$, dann erhalten wir:

$$\begin{aligned}\hat{f}(0)\sum_{J\subseteq M}e^{\beta_J} &= \sum_{J\subseteq M}q(\beta_J) + \sum_{J\subseteq M}\hat{f}(\beta_J)\\ &= \sum_{J\subseteq M}q(\beta_J) + C\cdot\hat{f}(0) + \sum_{\beta_J\neq 0}\hat{f}(\beta_J)\end{aligned}$$

Für $q(z)$ haben wir mit *(6.7)*

$$|q(z)| < \sum_{k=0}^{N} |c_k| \cdot |z|^k \quad \text{für } f(z) = \sum_{k=0}^{N} c_k z^k$$

Nun ist

$$\sum_{k=0}^{N} |c_k| \cdot |z|^k \leq \frac{1}{(p-1)!} a|z|^{p-1} \prod_{\beta_J \neq 0} \big(a|z| + a|\beta_J|\big)^p$$

also $\sum_{k=0}^{N} |c_k| \cdot |\beta_L|^k \leq \varepsilon$ für $\varepsilon > 0$ fest vorgegeben, $p >> 0$. Ist p also eine sehr große Primzahl, so ist $\left|\sum_{j \subseteq M} q(\beta_J)\right| < \frac{1}{2}$. Dann folgt:

$$\hat{f}(0) \cdot \underbrace{\sum_{J \subseteq M} e^{\beta_J}}_{= \prod_{j=1}^{m} (e^0 + e^{\alpha_j})} \neq 0$$

□

6.16 Theorem: (F. von Lindemann 1882)
Die Zahl $\pi \approx 3{,}14159$ ist transzendent.

Beweis:
$\sqrt{-1} = i$ ist algebraisch. Wenn π algebraisch wäre, so wäre auch $\pi \cdot i$ algebraisch, denn nach *(6.11)* ist $\overline{\mathbb{Q}}$ ein Ring. Es gilt aber $\exp(i\pi) = \cos\pi + i\sin\pi = -1$. Aber $\exp(\alpha) \neq -1$ für alle $\alpha \in \overline{\mathbb{Q}}$. □

6.17 Theorem:
Die „Quadratur des Kreises“ ist unmöglich, d.h. man kann *nicht* mit Zirkel und Lineal eine Strecke der Länge π konstruieren, wenn nur eine Strecke der Länge 1 gegeben ist.

Beweis:
In der Algebra I zeigt man: Alle Streckenlängen, die man konstruiert, sind algebraische Zahlen. Da $\pi \notin \overline{\mathbb{Q}}$, kann man π auch nicht konstruieren. □

Kapitel 7

Wiederholung

An dieser Stelle wollen wir die wichtigsten Erkenntnisse dieser Vorlesung nochmal zusammenfassen:

7.1 Teilbarkeit und ganze Zahlen

- Prinzip der vollständigen Induktion
- Primzahlen, Satz von Euklid *(1.5)*
- Teilen mit Rest
- Hauptsatz der Arithmetik *(1.8)*
- $\tau(n)$: Anzahl der positiven Teiler von n, $\sigma(n)$: Summe der positiven Teiler von n, multiplikativ für teilerfremde Zahlen.
- vollkommene Zahlen, Mersennesche Primzahlen (weitere Eigenschaften in der Übung)
- Euklidischer Algorithmus, ggT, Lemma von Bézout *(1.21)*
- Lineare Diophantische Gleichungen, Lösbarkeit
- Lineare Diophantische Gleichungen in ≥ 3 Variablen $\rightarrow$ Zurückführen auf 2 Variablen.
- Kongruenuzen $a \equiv b \bmod m \Leftrightarrow m \mid a - b$, Kürzungsregeln *(1.35)*, *(1.38)*
- Quersummenregeln für Teilbarkeit durch $3, 9, 11$.
- Lösen von linearen Diophantischen Gleichungen durch Kongruenzen: $ax + by = x \Leftrightarrow ax \equiv c \bmod b$.

7.2 Gruppen

- Begriff der Gruppe, Untergruppe, Nebenklasse
- Untergruppen von $(\mathbb{Z}, +)$ sind von der Form $m\mathbb{Z} := \{k \cdot m \mid k \in \mathbb{N}\}$ für $m \in \mathbb{N}$.
- Satz von Lagrange $\#G = \#H \cdot [G : H]$
- Kongruenzrelation auf Gruppen, Normalteiler (auf abelschen Gruppen äquivalent)
- Homomorphiesatz
- $\mathbb{Z}/m = \{\text{Kongruenzklassen in } \mathbb{Z} \bmod m\}, m > 0 \Rightarrow \#Z/m = m$.
- zyklische Gruppen (von einem Element erzeugt), Klassifikation aller zyklischen Gruppen (bis auf Isomorphie) in $\mathbb{Z}, \mathbb{Z}/m$.
- Untergruppen vonzyklischen Gruppen sind selbst wieder zyklisch
- Eulersche φ-Funktion *(2.30)*

7.3 Ringe

- Begriff des Rings, Körpers
- Kongruenzrelationen auf Ringen, Ideale (äquivalent)
- Menge der Kongruenzklassen ist wieder ein Ring $(\mathbb{Z}, +, \cdot) \to (\mathbb{Z}/m, +, \cdot)$
- Einheiten in Ringen, $(\mathbb{Z}/m)^* = \{\bar{a} \in \mathbb{Z}/m \mid \mathrm{ggT}(a, m) = 1\}, \varphi(m) = \#(\mathbb{Z}/m)^*$
- Satz von Euler *(3.10)*, Satz von Fermat *(3.11)*, (Beweis?)
- Satz von Wilson *(3.12)* (Beweis?)
- Chinesischer Restsatz: $(\mathrm{ggT}(m, n) = 1) \Rightarrow (\mathbb{Z}/mn \cong \mathbb{Z}/m \times \mathbb{Z}/n) \Rightarrow (\varphi(mn) = \varphi(m)\varphi(n))$
- Wenn man $\varphi(p^k) = p^{k-1}(p-1)$ berechnen kann, kann man $\varphi(m)$ für jedes $m \in \mathbb{N}$ berechnen:
- RSA-Verfahren *3.4* (beruht darauf, dass es sehr aufwändig ist, die Primfaktorzerlegung großer Zahlen zu bestimmen)

7.4 Einheiten und quadratische Reste

- primitive m-te Einheitswurzeln, diskreter Logarithmus, $\big((\mathbb{Z}/p)^*, \cdot\big) \cong \big(\mathbb{Z}/(p-1), +\big)$
- $\mathrm{ggT}(a, p) = 1, X^m \equiv a \bmod p$ lösbar $\Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \bmod p, d := \mathrm{ggT}(m, p-1)$
- Für den Fall $m = 2$ haben wir Quadratische Reste und das Legendre-Symbol *(4.6)* betrachtet.
- $\bar{a} \to (\frac{a}{p})$ ist Homomorphismus von $(\mathbb{Z}/m)^*$ nach $(\{\pm 1\}, \cdot)$
- Formelsammlung: Quadratische Reziprozität, $(\frac{2}{p}), (\frac{-1}{p})$
- Diffie-Hellamnn Schlüsselaustausch *4.3*

7.5 Mehr zu Ringen und Zahlen

- euklidische Ringe, Hauptidealringe, Integritätsbereiche
- Gaußsche Zahlen $\mathbb{Z}[i]$, Primelemente, Gaußsche-Primzahlen
- Existenz und Eindeutigkeit der Faktorisierung in Primelemente in Hauptidealringen
- Zwei-Quadrate-Satz, Vier-Quadrate-Satz, Pythagoräische Tripel

7.6 Irrationale und transzendente Zahlen

- rationale / irrationale Zahlen / algebraische Zahlen / transzendente Zahlen *(6.5)*
- $\sqrt{p}$ ist irrational, wenn $p \in \mathbb{P}$
- e, π sind irrational