

Ergänzungen zur LAG 1 WS 12-13

Dozent:
Prof. Dr. Felix Leinen

Mitschrift von:
Sven Bamberger, Maicon Hieronymus

L^AT_EXarbeit von:
Sven Bamberger

Zuletzt Aktualisiert:
21. Dezember 2012



Zusammenfassung:

Bei den „Ergänzungen zur LAG 1“ handelt es sich um den Baustein „Zahlentheorie und Ergänzungen zur Linearen Algebra“ des Pflichtmoduls „Lineare Algebra und Zahlentheorie“, der im Studiengang BSc Informatik im Laufe des 1. Studienjahres parallel zum Baustein „Lineare Algebra und Geometrie I“ (LAG 1) absolviert werden soll.

<http://www.mathematik.uni-mainz.de/arbeitsgruppen/gruppentheorie/leinen/w12-lag-plus/>

Raum: Mi 03-428

Uhrzeit: 08:00-10:00

Abgabe: Dienstags 10:00

Dieses Skript wurde erstellt, um sich besser auf die Klausur vorzubereiten und eine ordentliche und für alle Personen lesbare Mitschrift zu haben.

Dieses Dokument garantiert weder Richtigkeit noch Vollständigkeit, da es aus Mitschriften gefertigt wurde und dabei immer Fehler entstehen können. Falls ein Fehler enthalten ist, bitte melden oder selbst korrigieren und neu hochladen.

Hier kleine Notizen zu einzelne Besonderheiten dieses Dokumentes.

1. /* */ alles zwischen diesen Zeichen sind Kommentare und sollen zum tieferen Verständnis oder Besondere Fragestellungen darstellen. Dabei ist zu beachten, das die Notation nicht immer komplett korrekt ist. Es können also kleinere mathematische Fehler auftauchen, welche aber für das Verständnis relevant sind.

Inhaltsverzeichnis

I. Grundlagen	1
I.1. Abbildungen	1
I.2. Äquivalenzrelationen	5
II. Elementare Zahlentheorie	9
II.1. Teilbarkeit	9
II.2. Modulo Rechnen	12
II.3. Kryptographie	15
II.4. Primzahlen:	18
III. Algebraische Strukturen	21
III.1. Gruppen	21
III.2. Ringe	24
III.3. Polynomringe	26
III.4. Körperkonstruktionen	29
III.5. Endliche Körper	30

I. Grundlagen

I.1. Abbildungen

I.1.1. Idee:

Es seien A und B Mengen. Unter einer Abbildung f stellen wir uns einen Algorithmus vor, der aus jeder eingabe $a \in A$ ein eindeutig bestimmte Ausgabe $b \in B$ errechnet, b ist nur durch a (und f) festgelegt.

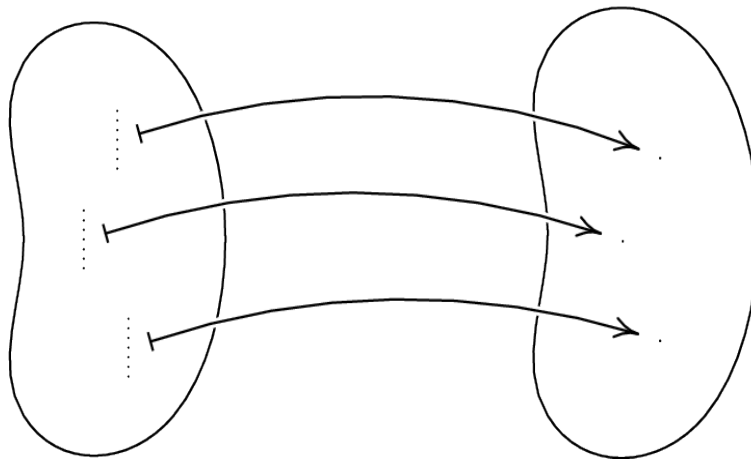


Abbildung I.1.: Eine einfache Abbildung

I.1.2. Definition:

Es seien A und B Mengen. Eine Abbildung f mit $f : A \rightarrow B$ sei eine Teilmenge f von $A \times B = \{(a, b) | a \in A, b \in B\}$ so, dass gilt:

- zu jedem $a \in A$ existiert ein $b \in B$ mit $(a, b) \in f$
- sind $(a, b_1), (a, b_2) \in f$, so gilt $b_1 = b_2$

f ist also das, was in der Schule im Fall reeller Funktionen als Graph der Funktion bezeichnet wurde. Anstatt $(a, b) \in f$ schreiben wir $b = f(a)$. Die Menge A heißt Definitionsbereich von f , die Menge B heißt Zielbereich von f . Ferner sei Bild $f = \{b \in B | \exists a \in A \text{ mit } f(a) = b\} = \{f(a) | a \in A\} = f(A)$ (Wertebereich)

I. Grundlagen

I.1.3. Beispiel:

1. Vorzeichenfunktion $sign. \mathbb{Z} \rightarrow \{-1, 0, 1\}$ $sign = \{(z, 1) | z < 0\} \cup \{(0, 0)\} \cup \{(z, 1) | z > 0\}$
2. Identität: Für jede Menge A sei $id_A : A \rightarrow A$ gegeben durch $id_A(b) = a \ \forall a \in A$

$$f : \mathbb{R} \rightarrow \mathbb{R}, f(a) = a^2 \ \forall a \in \mathbb{R}$$

$$g : \mathbb{R} \rightarrow \mathbb{R}, g(a) = 2a \ \forall a \in \mathbb{R}$$

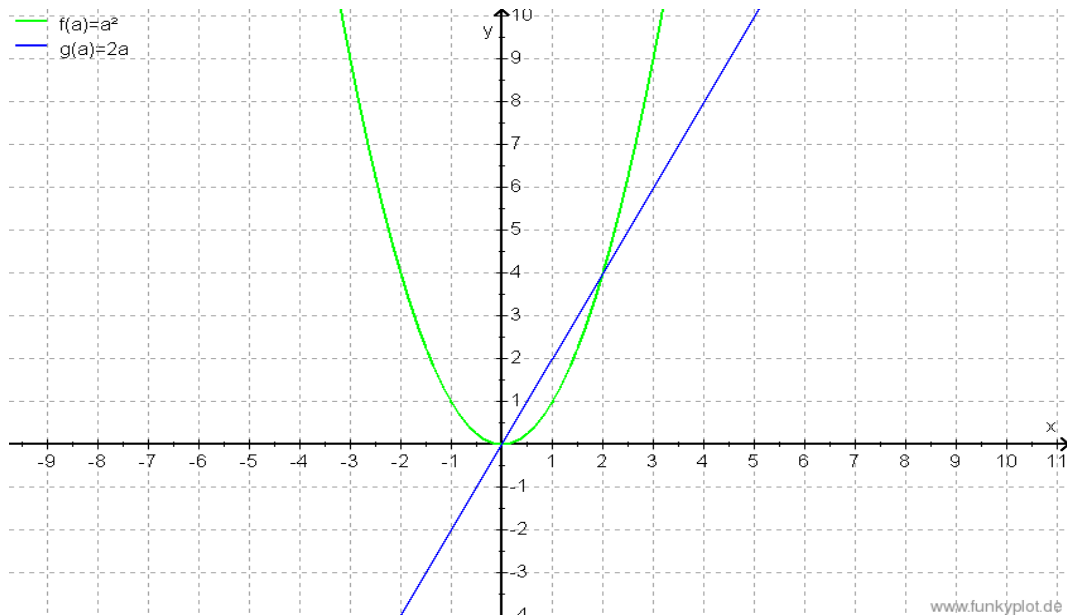


Abbildung I.2.: Ein Beispiel Graph

$$\text{Bild } f = \{b \in \mathbb{R} | b \geq 0\} \subsetneq \mathbb{R}$$

$$\text{Bild } g = \mathbb{R}$$

3. $g : \mathbb{Z} \rightarrow \mathbb{Z}, g(a) = \{2a | a \in \mathbb{Z}\} \subsetneq \mathbb{Z}$ (Kurzschreibweise: $(= 2\mathbb{Z})$)

I.1.4. Definition:

Eine Abbildung $f : A \rightarrow B$ heie:

- surjektiv, falls $\text{Bild } f = B$ ist d.h., falls $\forall b \in B$ ein $a \in A$ existiert mit $f(a) = b$
- injektiv, falls es zu jedem $b \in B$ hchstens ein $a \in A$ gibt mit $f(a) = b$.
d.h.
 - aus $f(a_1) = f(a_2)$ folgt $a_1 = a_2$
 - aus $a_1 \neq a_2$ folgt $f(a_1) \neq f(a_2)$
- bijektiv, falls f injektiv und surjektiv ist

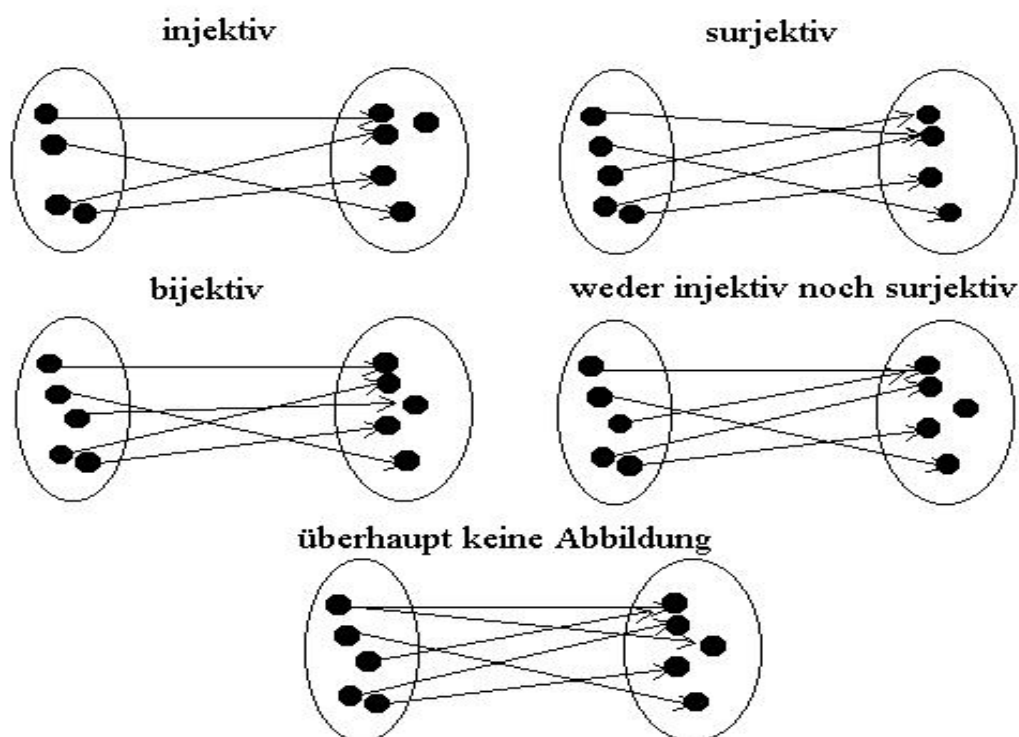


Abbildung I.3.: Mögliche Abbildungen auf einen Blick

I.1.5. Beispiel:

Sei $\mathbb{R}_{\geq 0} = \{a \in \mathbb{R} | a \geq 0\}$

1. $f : \mathbb{R} \rightarrow \mathbb{R}, f(a) = a^2$ nicht surjektiv, nicht injektiv ($-1 \notin \text{Bild } f$) ($(-1)^2 = 1^2$)
2. $f : \mathbb{R} \rightarrow \mathbb{R}_{\geq 0}, f(a) = a^2$ surjektiv, nicht injektiv
3. $f : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}, f(a) = a^2$ nicht surjektiv, injektiv
4. $f : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}_{\geq 0}, f(a) = a^2$ bijektiv

I.1.6. Definition**Komposition von Abbildungen**

Es seien $f : A \rightarrow B$ und $g : B \rightarrow C$ Abbildungen. Wir definieren $g \circ f : A \rightarrow C$ vermöge $(g \circ f)(a) = g(f(a))$
 $\forall a \in A$

I. Grundlagen

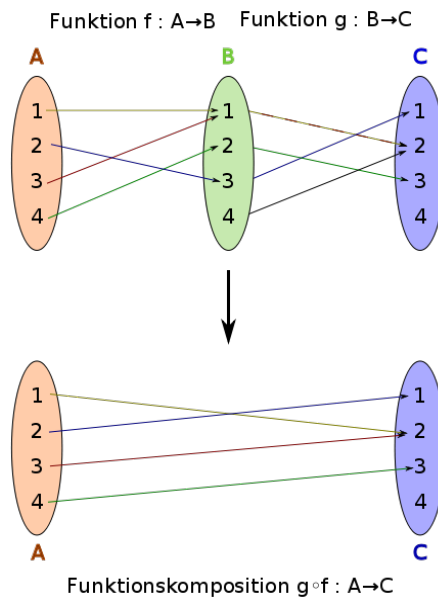


Abbildung I.4.: Eine mögliche Komposition

I.1.7. Beispiel

$$f, g: \mathbb{R} \rightarrow \mathbb{R}, f(x) = x^2, g(x) = 2x \quad \forall x \in \mathbb{R}$$

Dann:

$$(g \circ f)(x) = g(f(x)) = g(x^2) = 2x^2$$

$$(f \circ g)(x) = f(g(x)) = f(2x) = (2x)^2 = 4x^2$$

Es kommt auf die Reihenfolge von f und g an!

I.1.8. Satz

Seien $f: A \rightarrow B$ und $g: B \rightarrow A$ Abbildungen mit $g \circ f = id_A$. Dann ist f injektiv und g surjektiv.

Beweis:

f injektiv: Seien $a_1, a_2 \in A$ mit $f(a_1) = f(a_2)$ z.z. $a_1 = a_2$

$$\text{Dazu: } a_1 = id_A(a_1) = (g \circ f)(a_1) = g(f(a_1)) = g(f(a_2)) = (g \circ f)(a_2) = id_A(a_2) = a_2$$

g surjektiv: Sei $a \in A$ (=Zielbereich von g)

z.z. Es gibt ein $b \in B$ (=Definitionsbereich von g) mit $g(f(a)) = (g \circ f)(a) = id_A(a) = a$ wähle daher $b = f(a)$

$$/* f: A \rightarrow B \quad f \circ id_A: A \rightarrow B \quad f \circ id_A = f */$$

I.1.9. Definition:

In der Situation I.1.8 nennen wir g eine linksinverse von f und f eine rechtsinverse von g .

I.1.10. Definition:

Ist $f : A \rightarrow B$ bijektiv, so sei die zu f inverse Abbildung $f^{-1} : B \rightarrow A$ gegeben durch $f^{-1} = \{(b, a) \in B \times A \mid a, b \in f\}$

Warnung: Das klappt nur bei bijektiven Abbildungen f , da f^{-1} beidseitig invers zu f ist.

Hinweis: f^{-1} inverse der Abbildung f f^{-1} volles Urbild jedoch ist dies nicht zwangsläufig bijektiv

I.1.11. Definition:

Sei $f : A \rightarrow B$ und $Y \subseteq B$. Dann nennen wir $j(Y) = \{a \in A \mid f(a) \in Y\}$ das volle Urbild zu Y unter f .

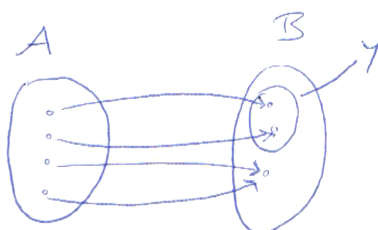


Abbildung I.5.: Eine Abbildung auf Untermengen

I.1.12. Beispiel:

In 1.5(1) war $f : \mathbb{R} \rightarrow \mathbb{R}$, $f(a) = a^2$. $f(\{0, 1, 4\}) = \{-2, -1, 0, 1, 2\}$

Beispiel: $g : \mathbb{Z} \rightarrow \mathbb{Z}$, $g(a) = a^2$
 $f^{-1}(\{0, 1, 2, 3, 4\}) = \{-2, -1, 0, 1, 2\}$

I.2. Äquivalenzrelationen

I.2.1. Bemerkung:

Es sei $f : A \rightarrow B$ eine Abbildung. Für jedes feste $b \in B$ nennen wir $f^{-1}(b) = \{a \in A \mid f(a) = b\}$ die Faser von b unter f . Offenbar sind je zwei Fasern disjunkt: $b_1 \neq b_2 \implies f^{-1}(b_1) \cap f^{-1}(b_2) = \emptyset$ ferner ist $A = \bigcup_{b \in B} f^{-1}(b)$.

Wir sprechen von einer disjunkten Zerlegung bzw. Partition von A . /* Faser $\hat{=}$ volles Urbild; disjunkt = Schnitt ist leer. */

I.2.2. Beispiel:

A = Menge aller Autos.

F = Menge aller Farbcodes von Autos.

$f : A \rightarrow F$ ordnet jedem Auto seinen Farbcode zu. Damit werde die Autos anhand ihrer Farbe (Faser von blaue (blaue Autos)) in unterschiedliche Schubladen gepackt, die Faser von f . Die Fasern sind disjunkt, da jedes Auto einen bestimmten Farbcode hat. Jedes Auto hat einen Farbcode, liegt also in einer Faser. Vermöge f können zwei Autos gleicher Farbe als „gleichwertig“ angesehen werden.

I. Grundlagen

I.2.3. Definition:

Eine Äquivalenzrelation auf einer Menge A sei eine Teilmenge von $A \times A$ mit folgenden Eigenschaften:

R ist reflexiv: für jedes $a \in A$ ist $(a, a) \in R$

R ist symmetrisch: ist $(a_1, a_2) \in R$, so auch $(a_2, a_1) \in R$

R ist transitiv: sind $(a_1, a_2), (a_2, a_3) \in R$, so auch $(a_1, a_3) \in R$

Anstatt $(a, b) \in R$ schreiben wir $a \sim_R b$ und sagen „a äquivalent b“.

I.2.4. Beispiel:

- a) zu Beispiel 2.2 ist $\mathbb{R} = \{(a, b) \in A \times A \mid f(a) = f(b)\}$ eine Äquivalenzrelation auf der Menge A aller Autos.
- b) Auf jeder Menge ist die Gleichheit „ $=$ “ von Elementen eine Äquivalenzrelation.
- c) Kongruenz von Dreiecken in der Zeichenebene \mathbb{R}^2 ist eine Äquivalenzrelation auf der Menge dieser Dreiecke.

Erinnerung

Äquivalenzrelation \sim auf M

- reflexiv $\forall a \in M, a \sim a$
- symmetrisch wenn $a \sim b$, dann $b \sim a$
- transitiv wenn $a \sim b \wedge b \sim c$, dann $a \sim c$

I.2.5. Definition:

Es sei \sim eine Äquivalenzrelation auf M . Für jede $a \in M$ sei $\{b \in M \mid a \sim b\} = [a] \stackrel{\text{wegen Symmetrie}}{=} \{b \in M \mid b \sim a\}$ die sogenannte Äquivalenzklasse zu a . Jedes $b \in [a]$ heie ein Vertreter von $[a]$.

Beachte: Reflexivität $\Rightarrow a$ Vertreter von $[a]$ (wegen Symmetrie).

I.2.6. Hauptsatz:

Es sei M eine feste Menge. Dann gilt:

- Die Äquivalenzrelationen auf M entsprechen genau den Partitionen von M .

Genauer:

- (a) Ist $M = \dot{\bigcup}_{i \in I} M_i$ ($\dot{\bigcup}$ = disjunkte Vereinigung) eine Partition von M , so ist eine Äquivalenzrelation \sim auf M gegeben durch: $a \sim b \Leftrightarrow$ es gibt ein $i \in I$ mit $a, b \in M_i$. Die Äquivalenzklassen zu \sim sind genau die Mengen $M_i (i \in I)$
- (b) Ist \sim eine Äquivalenzrelation auf M , so bilden die Äquivalenzklassen zu \sim eine Partition von M .

(c) Die durch (a) und (b) gegebenen Abbildungen sind bijektiv und gegenseitig invers.

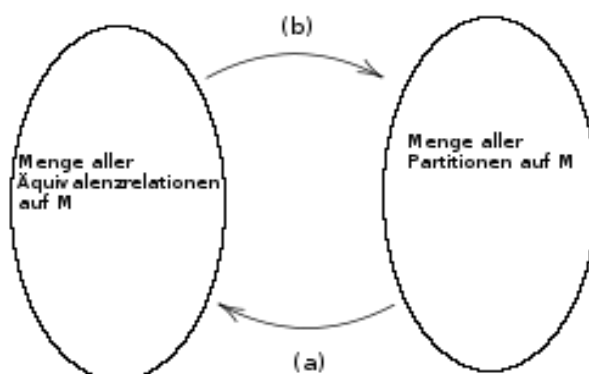


Abbildung I.6.: Eine bijektive und inverse Abbildung

Beweis:

(a)

reflexiv: Sei $a \in M$. Dann existiert ein $i \in I$ mit $a \in M_i \Rightarrow a \sim a$.

symmetrisch: Seien $a, b \in M$ mit $a \sim b \Rightarrow \exists i \in I : a, b \in M_i \Rightarrow b \sim a$.

transitiv: Seien $a, b, c \in M$ mit $a \sim b$ und $b \sim c \Rightarrow$ es gibt $i \in I$ mit $a, b \in M_i$ und es gibt $j \in J$ mit $b, c \in M_j$. Da $b \in M_i \wedge M_j$ und die Partition $M = \bigcup_{i \in I} M_i$ disjunkt ist, ist $i = j \Rightarrow a, c \in M_i = M_j$ und somit $a \sim c$. Nach Definition von \sim ist $[a] = M_i$ für das einzige $i \in I$ mit $a \in M_i$.

(b) Jeder $a \in M$ liegt in einer Äquivalenzklasse, z.B. in $[a]$. Also genügt es z.z.: Verschiedene Äquivalenzklassen zu \sim sind sogar disjunkt. Seien dazu $a, b \in M$ mit $[a] \cap [b] \neq \emptyset$ zeige $[a] = [b]$.
Wähle $c \in [a] \cap [b]$. Dann: $a \sim c$ und $c \sim b$ transitiv $\Rightarrow a \sim b \Rightarrow a \in [b]$ und $b \in [a]$.
Ist nun $x \in [a]$, so $x \sim a$ und $a \sim b$, somit $x \sim b$ und $x \in [b]$.
Fazit: $[a] \subseteq [b]$ Analog: $[b] \subseteq [a]$

(c) Die Abbildungen sind offensichtlich zueinander invers, daher bijektiv.

I.2.7. Bemerkung:

Gemäß 2.1 liefern die nicht leeren Fasern einer Abbildung $f : A \rightarrow B$ eine Partition von A , also eine Äquivalenzrelation auf A .

Umgekehrt kann zu jeder Partition $A = \bigcup_{i \in I} A_i$ von A eine Abbildung $g : A \rightarrow I$ definiert werden via $g(a) = i$ falls $a \in A_i$

Dann $A_i = g(i)$ und die Partition der A_i ist die Faser-Partition von g .

II. Elementare Zahlentheorie

II.1. Teilbarkeit

II.1.1. Definition:

Seien $a, b \in \mathbb{Z}$. Gibt es ein $s \in \mathbb{Z}$ mit $a = b \cdot s$, so sagen wir „ b teilt a “, schreiben $b|a$ und nennen b einen Teiler von a .

II.1.2. Bemerkung:

- aus $a|b$ und $a|c$ folgt stets $a|(b \pm c)$
 $(b = a \cdot x) \text{ und } c = a \cdot y \Rightarrow b \pm c = a(x \pm y)$
- aus $a|b$ und $c|d$ folgt stets $ac|bd$
 $(b = ax) \text{ und } d = c \cdot y \Rightarrow bd = (ac)(xy)$

II.1.3. Satz:

Sei $n \in \mathbb{N} \setminus \{0\}$ fest. eine Äquivalenzrelation \equiv_n auf \mathbb{Z} ist gegeben durch: $a \equiv_n b \Leftrightarrow n|(b - a)$ (sogenannte Kongruenz modulo n)

II.1.4. Beweis:

- **reflexiv:** Sei $a \in \mathbb{Z}$. Da $0 = n \cdot 0$, ist $n \mid 0 = (a - a)$
 $\Rightarrow a \equiv_n a$
- **symmetrisch:** Seien $a, b \in \mathbb{Z}$ mit $a \equiv_n b \Rightarrow n|(b - a)$
 $\Rightarrow n|(a - b) \Rightarrow bn \equiv_n a$
- **transitiv:** Seien $a, b \in \mathbb{Z}$ mit $a \equiv_n b$ und $b \equiv_n c$
 $\Rightarrow n|(b - a) \text{ und } n|(c - b)$
 $\Rightarrow^{1.2} n|(c - b) + (b - a) = c - a$
 $\Rightarrow a \equiv_n c$

II.1.5. Satz:

Die Äquivalenzklasse zu \equiv_n sind genau: $[0], [1], [2], \dots, [n-1]$ Insbesondere gilt die sogenannte Division mit Rest in \mathbb{Z} : zu gegebenen $a \in \mathbb{Z}, 0 < n \in \mathbb{N}$ existieren $q, r \in \mathbb{Z}$ mit $a = qn + r$ und $r \in \{0, \dots, n-1\}$ und q und r sind eindeutig bestimmt.

Beweis: Sei K eine Äquivalenzklasse zu \equiv_n . Wähle $r \in \mathbb{N}$ minimal bzgl. $r \in K$.

Beachte: K enthält eine natürliche Zahl. Ist $a \in K$ negativ, so addiere ein Vielfaches $q \cdot n$ von n sodass $a + qn > 0$. Dann ist $n|qn = (a + qn) - a$, also $a + qn \in K$.

Dann ist $r \in \{0, \dots, n - q\}$, dann wäre $r \geq n$, so $n|n = r - (r - n)$ also $r - n \in K$ natürliche Zahl $< r$. \nmid

Somit ist K eine der Äquivalenzklassen $[0], [1], \dots, [n-1]$

Sei nun $0 \leq r < s \leq n-1$

II. Elementare Zahlentheorie

Annahme: $[r] = [s] \Rightarrow r \equiv_n s, n | s - r \not\Rightarrow$ zu $0 < s - r < n$

Fazit: $[r] \neq [s]$

Damit $\mathbb{Z} = [0] \dot{\cup} [1] \dot{\cup} \dots \dot{\cup} [n-1]$

Ist $a \in \mathbb{Z}$, so $a \in [r]$ für ein $r \in \{0, \dots, n-1\} \Rightarrow n | a - r$

also: $a - r = qn$ für ein $q \in \mathbb{Z}, a = qn + r$

Eindeutigkeit von q und r:

Sei $q_1 n + r_1 = a = q_2 n + r_2$ mit $r_1, r_2 \in \{0, \dots, n-1\}$

Dann: $(q_1 - q_2)n = r_2 - r_1, n | r_2 - r_1, r_1 \equiv_n r_2 \Rightarrow r_1 = r_2$

Somit $(q_1 - q_2) \cdot n = 0 \Rightarrow^{n \neq 0} q_1 - q_2 = 0, q_1 = q_2 \quad \square$

II.1.6. Definition:

Eine natürliche Zahl $p \geq 2$ heißt Primzahl, wenn 1 und p die einzigen natürlichen Zahlen sind, die p teilen.

Also: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ...

Satz:

- a) Jede natürliche Zahl $n \geq 2$ ist ein Produkt von Primzahlen.
- b) Euklid: Es gibt unendlich viele Primzahlen

Beweis:

a) Wähle einen kleinsten Teiler > 1 von n . Dieser muß Primzahl sein, also $n = p \cdot b$ mit $b < n$. Zerlege nun b weiter.

b) Annahme p_1, \dots, p_s sind die einzigen Primzahlen.

Bild: $m = p_1 \cdot \dots \cdot p_s + 1$. Nach (a) muss einer der p_i Teiler von m sein.

Dann: $p_i | m$ und $p_i | p_1 \cdot \dots \cdot p_s \Rightarrow^{1.2} p_i | m - p_1 \cdot \dots \cdot p_s = 1 \not\Rightarrow$

II.1.7. Fundamentalsatz der Zahlentheorie

$0 \neq z \in \mathbb{Z}$ Dann hat z eine eindeutige Darstellung der Form $z = \varepsilon \cdot p_1 \cdot p_2 \cdot \dots \cdot p_s$ mit $\varepsilon \in \{\pm 1\}, p_1 \leq p_2 \leq \dots \leq p_s$ Primzahlen.

Beweis: o.E. $z \geq 0$ Induktion nach z . $z = 1$ Wähle $s = 0$

$Z \geq z$ Sei $z = p_1 \cdot \dots \cdot p_s = q_1 \cdot \dots \cdot q_t$ für gewisse Primzahlen p_i, q_j mit $p_1 \leq \dots \leq p_s, q_1 \leq \dots \leq q_t$.

z.Z.: $s = t$ und $p_i = q_i$ für $1 \leq i \leq s$.

$s \geq$ und $t \geq 1$

o.E. $p_1 \leq q_1$

Annahme: $p_1 \not\leq q_1 \leq q_2 \leq \dots \leq q_t$

Division mit Rest durch $p_1 \quad q_j = a_j p_1 + r_j$ mit $0 \leq r_j < p_1$ Da p_j Primzahl $\Rightarrow r_j > 0 \text{ für } 1 \leq j \leq t$.

Betrachte: $m = r_1 \cdot r_2 \cdot \dots \cdot r_t < p_1^t < q_1 \cdot q_2 \cdot \dots \cdot q_t = z$

Induktion $\Rightarrow m$ hat eindeutige Zerlegung im Produkt von Primzahlen Insbesondere $p_1 \nmid m$ (da $p_1 \nmid r_j \quad \forall j$)

Nun: $m = (q_1 - a_1 p_1)(q_2 - a_2 p_1) \cdot \dots \cdot (q_t - a_t p_1) = q_1 \cdot q_2 \cdot \dots \cdot q_t + p_1(\dots) \Rightarrow^{p_1 | 2} p_1 | m \not\Rightarrow$

Fazit: $p_1 = q_1$ und $p_2 \cdot \dots \cdot p_s = q_2 \cdot \dots \cdot q_t$

Induktion liefert $p_j = q_j$ für $2 \leq j \leq t = s$

II.1.8. Definition:

Für $a, b \in \mathbb{Z} \setminus \{0\}$ sei

- $ggT(a, b) = \max\{d \in \mathbb{Z} \mid d|a \wedge d|b\}$
- kleinster gemeinsamer Vielfaches $kgV(a, b) = \min\{c \in \mathbb{N} \mid a|c \wedge b|c\}$

II.1.9. Bemerkung:

Ist $a = \pm p_1^{\alpha_1} \dots p_s^{\alpha_s}$ und $b = \pm p_1^{\beta_1} \dots p_s^{\beta_s}$ mit Primzahlen $p_1 < p_2 < \dots < p_s$ und gewissen $\alpha_i \geq 0, \beta_i \geq 0$, so gilt $ggT(a, b) = p_1^{\gamma_1} \dots p_s^{\gamma_s}$ wo $\gamma_i = \min\{\alpha_i, \beta_i\}$
 $kgV(a, b) = p_1^{\delta_1} \dots p_s^{\delta_s}$ wo $\delta_i = \max\{\alpha_i, \beta_i\}$
 Insbesondere: $\gamma_i + \delta_i = \alpha_i + \beta_i$ und daher $|a \cdot b| = ggT(a, b) \cdot kgV(a, b)$

II.1.10. Euklidischer Algorithmus

Zur Bestimmung von $ggT(a, b)$

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

1. Setze $a_0 = |a|, a_1 = |b|$, o.E. $q_1 < q_0$
2. Wiederhole Division mit Rest:
 $q_{i-1} = q_i \cdot a_i + a_{i+1}$ wo $0 \leq a_{i+1} < a_i$
3. Ergibt sich erstmalig $a_{m+1} = 0$, so ist $a_m = ggT(a, b)$

Beispiel:

$$\begin{aligned} a &= 90, b = 84 \\ 90 &= a = 1 \cdot 84 + 6 \\ 84 &= 14 \cdot 6 + 0 \\ \Rightarrow 6 &= ggT(90, 84) \end{aligned}$$

II.1.11.

/* Fehlerhafte Nummerierung an der Tafel, oder in der Mitschrift. */

II.1.12. Satz

Der Euklidische Algorithmus terminiert und liefert den ggT

Beweis: Er terminiert, da $a_0 > a_1 > a_2 > \dots > a_m > a_{m+1} \geq 0$ in \mathbb{N}

Zwischenschritte: - Ist $a = q \cdot b + r$, so $ggT(a, b) = ggT(b, r)$

- Ist $d|a$ und $d|b$, so $d|a - q \cdot b = r \Rightarrow d|b$ und $d|r$
- Ist $d|b$ und $d|r$, so $d|q \cdot b + r = a \Rightarrow d|a$ und $d|b$

Daher ergibt sich in 1.10

$$ggT(a, b) = ggT(a_0, q_1) = ggT(a_1, q_2) = ggT(a_2, q_3) = \dots = ggT(a_{m-1}, q_m) \equiv a_m$$

/* $0 = a_{m+1}$, d.h. $a_{m-1} = q_m \cdot a_{m+1} = 0$ dem oben genannten \equiv */

II.1.13. Bemerkung:

Der Euklidische Algorithmus ist schnell.

II. Elementare Zahlentheorie

II.1.14. Erweiterter Euklidischer Algorithmus

Mit der Notation aus 1.10 berechnen wir zusätzlich für $0 \leq j \leq m$ ganze Zahlen v_i, v_j wie folgt:

- in Schritt 1 $u_0 = 1, v_0 = 0, u_1 = 0, v_1 = 1$

- in jedem Durchlauf der Schleife 2:

$$u_{i+1} = v_{i-1} - q_i \cdot u_i$$

$$v_{i+1} = v_{i-1} - q_i \cdot v_i$$

Dann gilt $\forall i: a_i = u_i \cdot a_0 + v_i \cdot a_1$

Insbesondere ist am Ende $a_m = u_m \cdot a_0 + v_m \cdot a_1 = ggT(a_0, a_1)$

Beweis: mit Induktion nach i :

$$\underline{i=0} \quad a_0 = 1 \cdot a_0 + 0 \cdot a_1 \quad \checkmark$$

$$\underline{i=1} \quad a_1 = 0 \cdot a_1 + 1 \cdot a_1 \quad \checkmark$$

$$\begin{aligned} \underline{1 \leq i \rightarrow i+1} \quad a_{i-1} &= a_{i-1} - q_i \cdot a_i \stackrel{Ind}{=} (u_{i-1} \cdot a_0 + v_{i-1} \cdot a_1) - q_i (u_i \cdot a_0 + v_i \cdot a_1) \\ &= a_0 \underbrace{(u_{i-1} - q_i \cdot u_i)}_{= u_i} + a_1 \underbrace{(v_{i-1} - q_i \cdot v_i)}_{= v_{i+1}} \quad \square \end{aligned}$$

II.1.15. Folgerung:

Zu beliebigen $a, b \in \mathbb{Z} \setminus \{0\}$ existieren $\underbrace{u, v \in \mathbb{Z}}_{\text{sogenannte Bezout-Koeffizienten}}$ mit $ggT(a, b) = u \cdot a + v \cdot b$.

II.1.16. Beispiel:

$$a_0 = 245, \quad a_1 = 112$$

a_i	q_i	u_i	v_i
245		1	0
112	2	0	1
21	5	1	-2
7	3	-5	11
0			

$$7 = ggT(a_0, a_1) = (-5) \cdot 245 + 11 \cdot 112$$

II.2. Modulo Rechnen

II.2.1. Motivation

Für ein festes $0 < n \in \mathbb{N}$ betrachten wir die Äquivalenzklassen zwischen Äquivalenzrelation \equiv_n . Es sei $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \dots, [n-1]\}$. Wir wollen eine Addition und Multiplikation auf $\mathbb{Z}/n\mathbb{Z}$ einführen, so wie wir das von der Uhr (für $n = 12$) gewöhnt sind.

$$[a] + [b] = [a + b] \quad \text{und} \quad [a] \cdot [b] = [a \cdot b] \quad \forall a, b \in \mathbb{Z}$$

Frage: Ist das möglich oder ergeben sich Widersprüche?

II.2.2. Satz

Die in 2.1 definierte Addition $+$ $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ und Multiplikation \cdot $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ sind wohldefiniert (widerspruchsfrei definiert), da das Ergebnis $[a] + [b]$ bzw. $[a] \cdot [b]$ nur von den Äquivalenzklassen $[a]$ und $[b]$ abhängt sind nicht von a und b selbst.

Beweis: Seien $[a_1] = [a_2], [b_1] = [b_2]$. Dann: $n|a_2 - a_1 \wedge n|b_2 - b_1$
 $\Rightarrow n|a_2 - a_1 + b_2 - b_1 = (a_2 + b_2) - (a_1 + b_1)$

$$\Rightarrow \underbrace{[a_2] + [b_2]}_{[a_2] + [b_2]} = \underbrace{[a_1 + b_1]}_{[a_1] + [b_1]}$$

Ebenso: $n|a_2(b_2 - b_1) + b_1(a_2 - a_1) = a_2b_2 - a_1b_1$

$$\Rightarrow \underbrace{[a_2b_2]}_{[a_2][b_2]} = \underbrace{[a_1b_1]}_{[a_1][b_1]}$$

II.2.3. Beispiel:

In $\mathbb{Z}/12\mathbb{Z}$ gilt: $[11]^2 = [11^2] = [121] = [1]$
 geschickter: $[11]^2 = [-1]^2 = [(-1)^2] = [1]$

Beachte: $[3] \cdot [4] = [3 \cdot 4] = [12] = [0]$ wobei $[3]$ und $[4]$ alleine gesehen jeweils $\neq 0$

Wenn klar ist, dass wir $\mathbb{Z}/n\mathbb{Z}$ rechnen für ein konstantes n , so lassen wir die Klammern i.d.R. weg.

WDH:

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &= \{[0], [1], \dots, [n-1]\} \quad a \equiv_n b \Leftrightarrow n|b - a \text{ für } a, b \in \mathbb{Z} \\ [a] + [b] &= [a + b] \\ [a] \cdot [b] &= [a \cdot b] \end{aligned}$$

II.2.4. Bemerkung:

Da $+$ und \cdot in $\mathbb{Z}/n\mathbb{Z}$ auf die entsprechenden Rechenoperationen in \mathbb{Z} zurückgeführt werden, erbt $\mathbb{Z}/n\mathbb{Z}$ die aus \mathbb{Z} bekannten Rechengesetze.

Beachte jedoch: Es kann Elemente $x \neq u \neq y$ in $\mathbb{Z}/n\mathbb{Z}$ geben mit $x \cdot y = 0$. (etwa $[2] \cdot [3] = [0]$ in $\mathbb{Z}/6\mathbb{Z}$)

Solche x, y heißen Nullteiler.

II.2.5. Definition:

Wir nennen $x \in \mathbb{Z}/n\mathbb{Z}$ invertierbar, falls es in $y \in \mathbb{Z}/n\mathbb{Z}$ gibt mit $x \cdot y = 1$. Mit $(\mathbb{Z}/n\mathbb{Z})^x$ bezeichnen die Menge aller invertierbaren Elemente in $\mathbb{Z}/n\mathbb{Z}$.

II.2.6. Satz:

$n \geq 1$ ist fest. Für $a \in \mathbb{Z}$ sind äquivalent:

1. $[a]$ ist invertierbar in $\mathbb{Z}/n\mathbb{Z}$
2. $\text{ggT}(a, n) = 1$

Beweis:

II. Elementare Zahlentheorie

- (1) \Rightarrow (2): Sei $[a] \cdot [b] = [1]$, $n|ab - 1, n \cdot v = ab - 1$ für ein $v \in \mathbb{Z}$
 $\cdot \Rightarrow 1 = ab - nv$
 \cdot Ist q ein Teiler von a und n , so auch von 1.
 $\cdot \Rightarrow q = \pm 1, \text{ggT}(a, n) = 1$
- (1) \Rightarrow (2): Sei $1 = \text{ggT}(a, n) = a \cdot u + n \cdot v$ für gewisse $u, v \in \mathbb{Z}$
 $\cdot \Rightarrow n|nv = 1 - au \Rightarrow [1] = [a] \cdot [a] \quad \square$

II.2.7. Folgerung:

$(\mathbb{Z}/n\mathbb{Z})^x = \{[a] | 0 < a < n \text{ und } \text{ggT}(a, n) = 1\}$. Ist $n = p$ eine Primzahl, so ist jedes Element $\neq 0$ in $\mathbb{Z}/p\mathbb{Z}$ invertierbar.

Beachte:

Für $n = a \cdot b$ mit $0 < a \leq b < n$ wird dies falsch.

$$[a] \cdot [b] = [n] = [0]$$

Wäre nun $[c] \cdot [a] = [1]$, so $[c] \cdot [a] \cdot [b] = [1] \cdot [b] = [b]$ wobei $[c] \cdot [0] = [0]$

II.2.8. Definition:

$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^x| = \text{Anzahl der } a \in \{1, \dots, n-1\} \text{ mit } \text{ggT}(a, n) = 1$.
Das definiert die eulersche φ -Funktion $\varphi: \mathbb{N} \setminus \{0\} \rightarrow \mathbb{N}$

II.2.9. Satz: (Euler)

$n \geq 1$ **fest** . für jedes $x \in (\mathbb{Z}/n\mathbb{Z})^x$ gilt $x^{\varphi(n)} = 1$

Mit anderen Worten: Für jedes zu n teilerfremde $a \in \mathbb{Z}$ gilt $a^{\varphi(n)} \equiv_n 1$.

Insbesondere: Ist $n = p$ Primzahl, so $x^p = x \quad \forall x \in \mathbb{Z}/p\mathbb{Z}$. (da $\varphi(p) = p-1$)

Beweis:

Sei $(\mathbb{Z}/n\mathbb{Z})^x = \{x_1, x_2, \dots, x_{\varphi(n)}\}$

Für festes $z \in (\mathbb{Z}/n\mathbb{Z})^x$ definieren wir $\alpha_z: (\mathbb{Z}/n\mathbb{Z})^x \rightarrow (\mathbb{Z}/n\mathbb{Z})^x$ durch $\alpha_z(x) = x \cdot z \quad \forall x \in (\mathbb{Z}/n\mathbb{Z})^x$

(da: $x \cdot z \cdot z^{-1} \cdot x^{-1} = x \cdot 1 \cdot x^{-1} = 1 \Rightarrow xz \in (\mathbb{Z}/n\mathbb{Z})^x$) Da z invertierbar ist $z \cdot y = 1y \cdot z$ für ein $y \in (\mathbb{Z}/n\mathbb{Z})^x$

somit $\alpha_z \cdot \alpha_y = id = \alpha_y \cdot \alpha_z \Rightarrow \alpha_z$ bijektiv.

$\Rightarrow \alpha_z$ vertauscht die Elemente $x_1, x_2, \dots, x_{\varphi(n)}$

$$\text{Somit: } \underbrace{\prod_{i=1}^{\varphi(n)} x_i}_{=: d} = \prod_{i=1}^{\varphi(n)} \alpha_z(x_i) = \prod_{i=1}^{\varphi(n)} (x_i \cdot z) = \underbrace{\left(\prod_{i=1}^{\varphi(n)} x_i \right)}_{= d} \cdot z^{\varphi(n)}$$

Multiplikation mit d^{-1} liefert $1 = z^{\varphi(n)} \quad \square$

II.3. Kryptographie

II.3.1. Ziel:

Anna und Bruno wollen vertrauliche Nachrichten austauschen. Jedoch ist der Übertragungsweg unsicher. Sie wissen, dass der böse Lasko lauschen wird. Gibt es eine sichere Verschlüsselungsmethode?

II.3.2. Problem:

Alle klassischen Verfahren (z.B. Caesar-Verschlüsselung) arbeiten mit einem geheimen Schlüsselwort, welches von Anna und Bruno zuvor vereinbart werden muss. Insbesondere bei häufigem Wechsel des Schlüsselworts ist das schwierig, da persönliche Treffen in aller Regel zu aufwendig sind.

II.3.3. Erinnerung:

Sei $0 < a \in \mathbb{R}$ fest. Die Logarithmusfunktion $\log_a :]0, \infty[\rightarrow \mathbb{R}$ zu Basis a . ist die Inverse der Abbildung $a^\cdot : \mathbb{R} \rightarrow]0, \infty[$ speziell $a = e$ $x \rightarrow a^x$ für alle $x \in \mathbb{R}$ liefert $a^\cdot = \exp(\cdot)$ $a^x = y \leftrightarrow x = \log_a y$

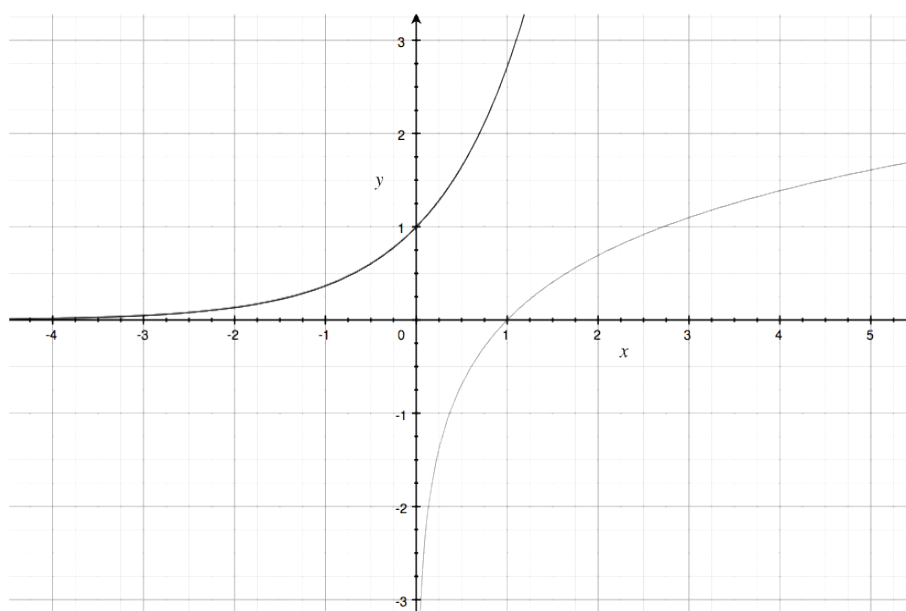


Abbildung II.1.: Es wurden $y_1 = e^x$ und $y_2 = \ln x$

II.3.4. Definition:

Es seien $2 \leq n \in \mathbb{N}$ und $0 < a < n$ fest gewählt. Gilt $a^k \equiv_n b$, so nennen wir k einen diskreten Logarithmus von b zur Basis a modulo n .

II.3.5. Beispiel:

$$n = 13 \quad a = 7$$

b	1	2	3	4	5	6	7	8	9	10	11	12
$\log_a b \bmod n$	12	11	8	10	3	7	1	9	4	2	5	6

II. Elementare Zahlentheorie

II.3.6. Idee:

- Die Abbildung $k \rightarrow a^k \bmod n$ ist relativ rasch zu berechnen (vgl. 3.7).
- Die Umkehrfunktion, des diskreten Logarithmus erlaubt mit heutigen Methoden keine systematische rasche Berechnung.

Wir nennen daher $k \rightarrow a^k \bmod n$ eine Einwegsfunktion.

II.3.7. Rasche Berechnung von $a^k \bmod n$

Sei $k = \varepsilon_0 \cdot 2^0 + \varepsilon_1 \cdot 2^1 + \dots + \varepsilon_s \cdot 2^s$ mit $\varepsilon_i \in \{0, 1\} = \sum_{j=0}^s \varepsilon_j 2^j$ die eindeutige Binärdarstellung von k .

Dann gilt:

$$a^k = a^{\sum_{j=0}^s \varepsilon_j 2^j} = \prod_{j=0}^s a^{\varepsilon_j 2^j} = \prod_{j=0}^s (a^{2^j})^{\varepsilon_j} = \prod_{\varepsilon_j=1}^s a^{2^j}$$

Wir berechnen daher die $a^{2^j} \bmod n$ durch sukzessives Quadrieren und sofortiges Reduzieren modulo n .

Beispiel:

Berechne $3^{48} \bmod 23$: Dazu: $48 = 32 + 16 = 2^5 + 2^4 = (110000)_2$

j	0	1	2	3	4	5
$3^{2^j} \bmod_{23}$	3	9	$81 \equiv 12$	$144 \equiv 6$	$36 \equiv 13$	$169 \equiv 9$

Fazit:

Anstelle von 48 Multiplikationen genügen 6 Multiplikationen.

Schlüsseltauschalgorithmus (Diffie-Hellmann)

- Anna & Bruno vereinbaren öffentlich eine Primzahl p und eine Basis $a \in \{2, \dots, p-2\}$
- Anna & Bruno wählen jeder für sich eine persönliche Geheimzahl k_A bzw. k_B .
- Beide berechnen insgeheim $a^{k_A} \bmod p = b_A$ bzw. $a^{k_B} \bmod p = b_B$
- Anna sendet b_A an Bruno, Bruno sendet b_B an Anna (öffentlich)
- Nun können beide für sich den Rest $a^{k_A k_B} \bmod p$ berechnen.

Da

$$a^{k_A k_B} = (a^{k_B})^{k_A} \equiv_p b_A^{k_B} \leftarrow \text{Bruno!}$$

$$(a^{k_B})^{k_A} \equiv_p b_B^{k_A} \leftarrow \text{Anna!}$$

Damit haben beide die Geheimzahl $a^{k_A k_B} \bmod p$ vereinbart

- Carlo kennt das ganze System, er kennt a, p, b_A, b_B und kann trotzdem nicht $a^{k_A k_B} \bmod p$ berechnen.

II.3.8. Definition:

Es sei T eine Menge an Teilnehmern in einem Netzwerk.

Ein System öffentlicher Schlüssel sei eine Familie $\{f_t, g_t | t \in T\}$ von Abbildungen derart, dass gilt:

- f_t ist eine öffentlich bekannte Einwegsfunktion
- g_t ist eine nur dem Teilnehmer t bekannte Inverse zu f_t

II.3.9. Definition:

T = Menge der Teilnehmer $\{f_t, g_t | t \in T\}$ wo f_t Einwegsfunktion mit Inverser g_t
System öffentlicher Schlüssel

II.3.10. Vorteile:

- Gibt es ein solches System, in dem jeder Teilnehmer seinen Schlüssel f_t, g_t selbst bestimmen kann, so entfällt der Schlüsseltausch.
- Neue Teilnehmer können jederzeit hinzustoßen.
- Spontane Kommunikation wird möglich
- n Teilnehmer benötigen lediglich $2 \cdot n$ Schlüssel. (anstelle $\frac{n(n-1)}{2}$ Schlüssel für Paare von Teilnehmern)

II.3.11. RSA-Verfahren

1. Schlüsselerzeugung

- Teilnehmer t wählt zwei große PRIMzahlen $p_t \neq q_t$ und bildet $n_t = p_t \cdot q_t$. Dann berechnet t die Eulersche φ -Funktion $\varphi(n_t)$
 Dies ist ganz einfach:
 Die einzigen Teiler $d \in \{1, \dots, n_t-1\}$ mit $\text{ggT}(d, n_t) \neq 1$ von n_t zwischen 1 und $n_t - 1$ sind von der Form $p_t \cdot a$ (a geeignet ($1 \leq a \leq q_t - 1$)) oder $q_t \cdot b$ (b geeignet ($1 \leq b \leq p_t - 1$))
 \Rightarrow Es gibt genau $(q_t - 1) + (p_t - 1)$ solche d .
 $\Rightarrow \varphi(n_t) = |\{c | 0 < c < n_t, \text{ggT}(c_t, n_t) = 1\}| = (n_t - 1) - (q_t - 1) - (p_t - 1) = (p_t - 1)(q_t - 1)$
- Nun wählt t eine Zahl $k_t \in \{2, \dots, \varphi(n_t) - 1\}$ teilerfremd zu $\varphi(n_t)$ (z.B. eine Primzahl $> \varphi(n_t)$) reduziert modulo $\varphi(n_t)$
- Mit dem erweiterten Euklid-Algorithmus bestimmt t Zahlen l_t und v_t so dass $1 = k_t \cdot l_t + \varphi(n_t) \cdot v_t$
- t vernichtet vorraussichtlich $p_t, q_t, \varphi(n_t), v_t$
- als öffentlichen Schlüssel gibt t das Paar (k_t, n_t) heraus i als Geheimschlüssel verbleibt l_t bei t .

2. Die Sicherheit des Verfahrens beruht darauf, dass es für große p_t, q_t keinen raschen, systematischen Weg gibt, um aus n_t heraus p_t, q_t oder $\varphi(n_t)$ zu bestimmen.

3. Kryptographie mittels RSA

Anna will Bruno eine Nachricht senden. Der Klartext sei eine große ganze Zahl. $x \in \{2, \dots, n_B - 2\}$ (alle ASCII-Zeichen einer Nachricht können in einer einzigen großen Zahl zusammengefasst werden).

- Anna verschlüsselt den öffentlichen Schlüssel (k_b, n_b) von Bruno
- Bruno berechnet $z \equiv y^{l_B} \pmod{n_B}$
- Nach Satz von Euler (2.9) gilt:
 $z \equiv y^{l_B} \equiv x^{k_B l_B + v_t \varphi(n_B)} \equiv x^1 \equiv x \pmod{n_B}$
- Es ist extrem unwahrscheinlich dass $\text{ggT}(x, n_B) \neq 1$ ist, da Anna sonst eine Zerlegung von n_B gefunden hätte.
- Carlo ist machtlos, da er aus y, k_B, n_B nicht auf x kommen kann, obwohl er das Verfahren genau versteht.

II.3.12. elektronische Unterschrift

Bruno will Anna einen unterschriebenen = authentifizierten Geheimauftrag x senden. Er sendet $y \equiv x^{k_A} \pmod{n_A}$ und zugleich $z \equiv y^{l_B} \pmod{n_B}$. Jeder kann verifizieren, dass die verschlüsselte Nachricht von Bruno stammt, indem er y mit $z^{k_B} \pmod{n_B}$ vergleicht. Denn nur Bruno war in der Lage, z aus y heraus zu berechnen.

II.4. Primzahlen:

II.4.1. Motivation:

Wie wir gesehen haben, spielt die Bestimmung großer Primzahlen eine wichtige Rolle.

II.4.2.

- (a) die Verteilung der Primzahlen in \mathbb{N} ist sehr unregelmäßig. Zu jeder Zahl $s \geq 2$ gibt es s aufeinanderfolgende Zahlen, die nicht prim sind.

Beweis: Wähle $t = s + 1$ und betrachte $t!, t! + 2, t! + 3, \dots, t! + t$. Offenbar ist $k | t! + k$ für $2 \leq k \leq t$.

- (b) Die Verteilung der Primzahlen in \mathbb{N} ist sehr regelmäßig: Bezeichne mit $\pi(x)$ die Anzahl der Primzahlen $\leq x$. Dann nähert sich $\pi(x)$ für wachsende x immer nahe der Funktion $x \rightarrow \frac{x}{\ln(x)}$ an.

Genauer: $\lim_{x \rightarrow \infty} \frac{x}{\ln(x)} = 1$ (ohne Beweis)

II.4.3. Bemerkung:

Wie viele Primzahlen gibt es zwischen 10^{199} und 10^{200} ?

Wie in 4.2 (b): Ungefähr

$$\frac{1}{\ln 10} \left(\frac{10^{200}}{200} - \frac{10^{199}}{199} \right) \approx \frac{1}{2,3} \cdot 10^{199} \left(\frac{1790}{4 \cdot 10^4} \right)$$

Die Anzahl der Atome auf der Erde $\approx 10^{51}$

Wir können es gar nicht schaffen, diese Primzahlen alle auszurechnen.

II.4.4. Satz (Fermat-Test)

Genau dann ist $n \geq 2$ eine Primzahl, wenn gilt

$$a^{n-1} \equiv_n 1 \quad \forall a \leq \sqrt{n}$$

Beweis: „ \Rightarrow “ Satz von Euler

(n Primzahl $\Rightarrow \varphi(n) = n - 1$)

„ \Leftarrow “

Sei n keine Primzahl, etwa $n = a \cdot b$ mit $2 \leq a \leq \sqrt{n}$

Dann $a \nmid a^{n-1} \Rightarrow n \nmid a^{n-1} - 1$, d.h. $a^{n-1} \not\equiv_n 1$

II.4.5. Problem:

Für ein einzelnes a ist die Gleichung $a^{n-1} \equiv_n 1$ schnell geprüft:

Es dauert jedoch viel zu lang, das für alle $a \leq \sqrt{n}$ zu tun.

II.4.6. Probabilistischer Fermat-Test (Ausweg)

Sei $n \geq 3$ ungerade. Ist n eine Primzahl?

- Wähle $a \in \{2, \dots, n-2\}$ zufällig
- Bestimme $d = \text{ggT}(a, n)$. Ist $d > 1$, so STOP \leadsto Ausgabe keine Primzahl
- Andernfalls berechne $a^{n-1} \bmod n$
 - Ist $a^{n-1} \not\equiv_n 1$, so STOP \leadsto Ausgabe: Keine Primzahl
 - Ist $a^{n-1} \equiv_n 1$, so gehe zurück auf LOS.

Idee:

Entweder stellt sich nach kurzer Zeit heraus, dass n keine Primzahl, oder n ist mit hoher Wahrscheinlichkeit eine Primzahl

II.4.7. Beispiel:

Ist $341 = 11 \cdot 31$ eine Primzahl?

1. Runde $a = 2$ $\text{ggT}(2, 341) = 1$ zeige $2^{340} \equiv_{341} 1$

Nun: $1023 = 11 \cdot 93 \Rightarrow 11 | 2^{10} - 1 | 2^{340} - 1$

Ferne: $31 | 2^5 - 1 | 2^{340} - 1$

$\Rightarrow 341 = 11 \cdot 31 | 2^{340} - 1$ mit $\text{ggT}(11, 31) = 1$

\leadsto 1. Runde liefert keine Information.

2. Runde $a = 3$ $\text{ggT}(341, 3) = 1$ Berechne $3^{340} \bmod 341$

$$340 = 2^2 \cdot 85 = 2^2(64 + 16 + 4 + 1) = 2^8 + 2^6 + 2^4 + 2^2$$

2^k	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8
$3^{2^k} \bmod 341$	9	81	$6561 \equiv 82$	$6724 \equiv -96$	$9216 \equiv 9$	81	82	-98

$$\Rightarrow 3^{340} \equiv_{341} (-96)^2 \cdot 81^2 \equiv_{341} 9 \cdot 82 = 738 \not\equiv_{341} 1$$

Fazit: $a = 3$ zeigt uns, dass 341 keine Primzahl ist. Wir nennen $a = 3$ einen Zeugen für 341. $a = 2$ war kein Zeuge.

Beachte: Der Test liefert keine Zerlegung von $n = 341$.

II.4.8. Bemerkung

Es gibt Nicht-Primzahlen, für die kein Zeuge existiert. Die kleinste solche ist $561 = 3 \cdot 11 \cdot 17$
 n Primzahl $\Leftrightarrow a^{n-1} \equiv_n 1 \quad \forall 2 \leq a \leq n-2$

II.4.9. Miller-Rabin-Test

Sei $n \geq 3$ ungerade. Dann ist $n-1 = 2^v \cdot m$ für ein $v \geq 1$ und m ungerade. Es folgt: $a^{n-1} - 1 = (a^{2^{v-1} \cdot m})^2 - 1^2 = (a^{2^{v-1} \cdot m} + 1) \cdot (a^{2^{v-1} \cdot m} - 1) = \text{usw.} = (a^{2^{v-1} \cdot m} + 1) \cdot (a^{2^{v-2} \cdot m}) \cdot (a^m + 1)(a^m - 1)$

Ist n Primzahl, so muss n eine der Klammern rechts teilen. Wir nennen daher n eine starke Pseudoprimzahl zur Basis a , wenn n eine der Klammern teilt.

Klar: n starke Pseudoprimzahl zu jeder Basis $a \in \{2, \dots, n-2\} \Leftrightarrow n$ Primzahl

Beim probabilistischen Miller-Rabin-Test wird in gleicher Weise beim probabilistischen Fermat-Test für diverse Basen geprüft, ob n starke Pseudoprimzahl zur Basis a ist.

II.4.10. Beispiel:

$$n = 561, a = 2, \text{ggT}(a, n) = 1$$

$$2^{560} - 1 = (2^{280} + 1)(2^{240} + 1)(2^{70} + 1)(2^{35} + 1)(2^{35} - 1)$$

Teste, ob 561 eine der Klammern teilt.

$$35 = 32 + 2 + 1 = 2^5 + 2^1 + 2^0$$

k	0	1	2	3	4	5
$2^{2^k} \bmod 561$	2	4	16	256	$65536 \equiv -101$	$10201 \equiv 103$

$$\Rightarrow 2^{35} \equiv 103 \cdot 4 \cdot 2 \equiv 8824 \equiv 263 \not\equiv \pm 1 \pmod{561}$$

$$2^{70} \equiv 263^2 = 69169 \equiv 166 \not\equiv \pm 1 \pmod{561}$$

$$2^{140} \equiv 27556 \equiv 67 \not\equiv \pm 1 \pmod{561}$$

$$2^{280} \equiv 67^2 \equiv 4489 \equiv 1 \not\equiv -1 \pmod{561}$$

$\Rightarrow 561$ keine Primzahl

II.4.11. Satz:

Ist $n > 9$ ungerade und keine Primzahl, ist die Anzahl der Basen $a \in \{2, \dots, n-2\}$ bzgl. derer n eine starke Pseudoprimzahl ist, $\leq \frac{\varphi(n)}{4} < \frac{n}{4}$ (ohne Beweis)

Somit sind min. $\frac{3}{4}$ aller Basen Zeugen für n , und die Wahrscheinlichkeit, dass bei zufällig gewählten a das n starke Pseudoprimzahl ist, ist $< \frac{1}{4}$.

Indem wir 20 Runden durchlaufen, können wir die Wahrscheinlichkeit, dass n immer noch als mögliche Primzahl gehandelt wird, auf $< \frac{1}{4^{20}} \approx \frac{1}{10^{13}}$ senken.

Wir können diese Wahrscheinlichkeit unter jede Grenze senken, also z.B. unter die Wahrscheinlichkeit, dass bei der Rechnung ein zufälliger Computerfehler eintritt.

III. Algebraische Strukturen

III.1. Gruppen

III.1.1. Definition:

Eine Gruppe G sei eine Menge mit einer Verknüpfung $* : G \times G \rightarrow G$ derart, dass gilt:

- (1) **Assoziativität:** $(a * b) * c = a * (b * c)$
- (2) **Neutrales Element:** $\exists e \in G \mid a * e = a = e * a \quad \forall a \in G$
(e ist eindeutig: „ $e_1 = e_1 * e_2 = e_2$ “)
- (3) **Inverse:** Zu jedem $a \in G$ existiert ein $b \in G$ mit $a * b = e = b * a$
(das b wird als a^{-1} bezeichnet, da es eindeutig von a abhängt:
„ $b_1 = b_1 * e = b_1 (* a * b_2) = (b_1 * a) * b_2 = e * b_2 = b_2$ “)

Beachte: (1) und (2) sind Eigenschaften für einen Monoid

G heie zustzlich kommutativ, falls gilt: $a * b = b * a \quad \forall a, b \in G$

III.1.2. Beispiel:

- (a) \mathbb{N} mit $+$ ist Monoid, aber keine Gruppe
 $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ bzgl. $+$ sind Gruppen.
 $\mathbb{Z}/n\mathbb{Z}$ bzgl. $+$ ist eine Gruppe (vererbt von \mathbb{Z})
 $\mathbb{Z} \setminus \{0\}$ bzgl. \cdot ist Monoid
 $(\mathbb{Z}/n\mathbb{Z}) \setminus \{0\}$ bzgl. \cdot ist Gruppe $\Leftrightarrow n$ ist eine Primzahl
 Diese Regeln sind Kommutativ
- (b) Sei Ω eine Menge. Dann ist $\text{Abb}(\Omega, \Omega) = \{f \mid f : \Omega \rightarrow \Omega\}$ bzgl. Komposition von Abbildungen immer im Monoid. Die Menge $\text{Sym}(\Omega) = \{f \in \text{Abb}(\Omega, \Omega) \mid f \text{ bijektiv}\}$ ist eine Gruppe bzgl. Komposition. „symmetrische Gruppe“ $\text{Sym}(\Omega)$ ist nicht kommutativ, sofern $|\Omega| \geq 3$

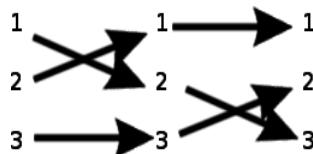


Abbildung III.1.: Fadendiagramm mit der Funktion 1 auf 3

III. Algebraische Strukturen

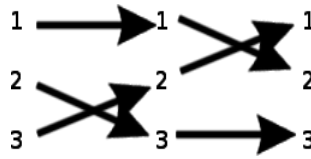


Abbildung III.2.: Fadendiagramm mit der Funktion 1 auf 2

In folgenden lassen wir $*$ weg.

III.1.3. Lemma:

Sei G eine Gruppe und $a, b, c \in G$:

- (a) $(ab)^{-1} = b^{-1}a^{-1}$ und $(a^{-1})^{-1} = a$, $e^{-1} = e$
- (b) Setzt man $a^0 = e$, $a^n = a(a^{n-1})$ und $a^{-n} = (a^{-1})^n \quad \forall n \geq 1$ so gelten die üblichen Potenzgesetze.

Kurzregeln:

- aus $ab = ac$ folgt stets $b = c$ (Multiplikation mit a^{-1} von links)
- aus $ab = cb$ folgt stets $a = c$ (Multiplikation mit b^{-1} von rechts)

III.1.4. Definition:

Eine Untergruppe U der Gruppe G sei eine Teilmenge von G , die bzgl. der Verknüpfung (Multiplikation) in U selbst eine Gruppe bildet. d.h. es muss gelten:

- $e \in U$
- U ist gegen Multiplikation abgeschlossen und gegen Inversion. (Dies ist gewährleistet, falls für alle $a, b \in U$ gilt $ab^{-1} \in U$)

Schreibe: $U \leq G$

III.1.5. Beispiel:

- (a) $\mathbb{Z} \leq \mathbb{Q}$ bzgl. $+$
- (b) $\{a^2 | a \in (\mathbb{Z}/n\mathbb{Z})^x\} \leq (\mathbb{Z}/n\mathbb{Z})^x$ (bzgl. \cdot) da $1^2 = 1$, $a^2b^2 = aabb$, $abab = (ab)^2$,
 $(a^2)^{-1} = (a^{-1})^2$

III.1.6. Satz von Lagrange

Sei G endliche Gruppe und $U \leq G$. Dann $|U| \mid |G|$.

Beweis:

Die Rechtsmultiplikation mit festen $g \in G$ ist eine bijektive Abbildung $G \rightarrow G$ / $*$ $x \rightarrow x \cdot g$ (die Inverse ist Rechtsmultiplikativ mit g^{-1})

Daher gilt $|U| = |U \cdot g|$, $U \cdot g = \{u \cdot g | u \in U\}$ für jedes (feste) $g \in G$

$$\mathbb{Z} = \bigcup_{k=0}^{n-1} (k + n\mathbb{Z})$$

$$G = \bigcup_{g \in G} U \cdot g, \text{ da } g = e \cdot g \in U \cdot g$$

Zeige: Die Ug (g geeignet) bilden eine Partition von G . (dann:

$$|G| = \left| \bigcup_{g \text{ geeignet}} Ug \right| = \sum_{g \text{ geeignet}} |Ug| = \sum_{g \text{ geeignet}} |U| = m \cdot |U| \text{ wo } m = \text{Anzahl der } Ug \text{ (} g \text{ geeignet)}$$

Dazu sei $x \in Ug_1 \cap Ug_2$ Zeige: $Ug_1 = Ug_2$

Dann $u_1g_1 \cdot x = u_2g_2$ mit $u_1, u_2 \in U$ geeignet

$$\Rightarrow U \cdot u_1g_1 = U \cdot u_2g_2$$

$$\Leftrightarrow Ug_1 = Ug_2$$

III.1.7. Folgerung:

In jeder endlichen Gruppe G gilt: $g^{|G|} = e \ \forall g \in G$ (vgl. Satz von Euler (II.2.6), wo $(\mathbb{Z}/n\mathbb{Z})^x = \varphi(n)$ war)

Beweis:

Betrachte $U = \{g^z | z \in \mathbb{Z}\} \leq G$ für festes g aus G .

Zeige: $g^{|U|} = e$ (dann $g^{|G|} = (g^{|U|})^m = e$ für $|G| = |U| \cdot m$ gemäß 1.6)

Kopiere hierzu den Beweis des Satzes von Euler und verwende, dass U kommutativ ist.

III.1.8. Definition:

Ein Gruppenhomomorphismus $\varphi : G \rightarrow H$ (wobei G, H Gruppen sind) Sei eine Abbildung mit $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) \ \forall a, b \in G$

III.1.9. Satz:

(a) $\varphi(e) = e \quad \varphi(a^{-1}) = (\varphi(a))^{-1} \quad \forall a \in G \checkmark$

(b) Bild $q \leq H \checkmark$

(c) Die Fasern von φ sind genau die Menge Ug ($g \in G$)
 wo $N = \{u \in G | \varphi(u) = e\} =: \text{Kern } \varphi$
 und $Ng = \{ug | u \in N\}$

(d) N ist ein Normalteiler von G , d.h.

- $N \leq G$ und

- $g^{-1}ug \in N$ für jedes $u \in N$ und $g \in G$

Beweis:

(c): Sei $g \in G$ fest. Betrachte $\varphi(g) \in \text{Bild } \varphi$

Sei $a \in G$ mit $\varphi(a) = \varphi(g)$

Dann:

$$e = \varphi(a)\varphi(g)^{-1} = \varphi(a \cdot g^{-1}) \text{ und } a \cdot g^{-1} \in \text{Kern } \varphi = N$$

$$a \cdot g^{-1} = u \in N \text{ für ein } u$$

$$\Rightarrow a = u \cdot g \in Ng$$

III. Algebraische Strukturen

Dies zeigt: Faser zu $\varphi(g)$ ist in Ng enthalten.

Sei umgekehrt $a \in Ng$, also $a = u \cdot g$ für ein $u \in N = \text{Kern}\varphi$

$$\Rightarrow \varphi(a) = \varphi(u \cdot g) = \varphi(u) \cdot \varphi(g) = e \cdot \varphi(g) = \varphi(g)$$

$\Rightarrow a$ in Faser zu $\varphi(g)$

(d):

- Nach (a) ist $e \in N$. Ferner gilt für $a, b \in N$:

$$\varphi(ab^{-1}) = \varphi(a) \cdot \varphi(b)^{-1} = e \cdot e^{-1} = e$$

$$\Rightarrow ab^{-1} \in N = \text{Kern}\varphi$$

- Für $u \in \text{Kern}\varphi$ und $g \in G$ gilt

$$\varphi(g^{-1}ug) = \varphi(g)^{-1} \cdot \underbrace{\varphi(g) \cdot \varphi(g)}_{=e} = \varphi(g)^{-1} \cdot \varphi(g) = e$$

$$\Rightarrow g^{-1}ug \in N$$

III.1.10. Bemerkung

Sei $\varphi: G \rightarrow H$ ein Gruppenhomomorphismus. Nach II.1.9(c) ist eine Projektion gegeben durch:

$$Ng \longleftrightarrow \varphi(g)$$

$$\{Ng | g \in G\} \xleftrightarrow{\tilde{\varphi}} \text{Bild}\varphi$$

Vermöge $\tilde{\varphi}$ übertragen wir die Gruppenstruktur von $\text{Bild}\varphi$ auf $\{Ng | g \in G\} =: G/N$

Wie funktioniert die Multiplikation in G/N ?

$$(Ng_1) \cdot (Ng_2) \xleftrightarrow{\tilde{\varphi}} \varphi(g_1) \cdot \varphi(g_2) = \varphi(g_1g_2) \xleftrightarrow{\tilde{\varphi}} N(g_1g_2)$$

Also: $(Ng_1) \cdot (Ng_2) = N(g_1g_2) \quad \forall g_1, g_2 \in G$

Ebenso: Ne ist das neutrale Element in G/N

$N(g^{-1})$ ist das Inverse zu Ng .

Das entspricht genau der Addition auf $\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z} + k | k \in \mathbb{Z}\}$

III.2. Ringe

III.2.1. Definition:

Ein Ring R sei eine Menge mit Verknüpfungen $+$ und \cdot , derart dass gilt:

1. R ist eine kommutative Gruppe bzgl. $+$

(neutrales Element: 0)

(Inverse zu $a \in R$ bzgl. $+$: $-a$)

2. \cdot ist assoziativ: $a(bc) = (ab)c \quad \forall a, b, c \in R$

3. Distributivgesetze:

$$a(b+c) = ab+ac \quad \forall a, b, c \in R$$

$$(a+b)c = ac+bc \quad \forall a, b, c \in R$$

Gibt es ein neutrales Element bzgl. \cdot in R , so heißt R Ring mit Eins.

Ist \cdot kommutativ, so heißt R ein kommutativer Ring.

Ist $R \setminus \{0\}$ bzgl. \cdot eine kommutative Gruppe, so nennt man R einen Körper.

III.2.2. Beispiel:

- (a) \mathbb{Z} und $\mathbb{Z}/n\mathbb{Z}$ sind kommutative Ringe mit Eins.
 $\mathbb{Z}/n\mathbb{Z}$ ist Körper $\Leftrightarrow n$ Primzahl (II.2.7)
 \mathbb{Q} und \mathbb{R} sind Körper.
- (b) Die Menge aller $(n \times n)$ -Matrizen mit Einträge aus einem Ring ist ein nicht kommutativer Ring (sofern $n \geq 2$ und $R \neq \{0\}$)
- (c) In jedem Ring mit Eins bilden die invertierbaren Elemente eine Gruppe.

III.2.3. Lemma:

- (a) Ist R ein Ring, so gilt stest
 $a \cdot 0 = 0 = 0 \cdot a$ und
 $(-a) \cdot b = -(ab) = a(-b) \quad \forall a, b \in R$
- (b) Jeder Körper ist nullteilerfrei, d.h., aus $a \cdot b = 0 \Rightarrow a = 0$ oder $b = 0$.

Beweis:

- (a) $a \cdot 0 + a \cdot 0 = a(0 + 0) = a \cdot 0 = a \cdot 0 + 0$
 $\xRightarrow{\mathbb{R}^+ \text{Gruppe}} a \cdot 0 = 0$
 $ab + a(-b) = a(b + (-b)) = a \cdot 0 = 0$
 $\Rightarrow a(-b) = -(ab)$
- (b) Ist $a \cdot b = 0$ und ist $a \neq 0$, so
 $a^{-1}(a \cdot b) = (a^{-1}a)b = 1 \cdot b = b$ wobei $a^{-1} = a^{-1} \cdot 0 = 0$

III.2.4. Definition:

Ringhomomorphismus: $\varphi : R \rightarrow S$
 Sei ein Gruppenhomomorphismus bzgl. + mit $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) \quad \forall a, b \in R$
 Setze wieder $\text{Kern}\varphi = \{a \in R \mid \varphi(a) = 0\}$

III.2.5. Bemerkung:

In gleicher Weise wie bei Gruppen gilt dann:

- (a) Bild φ ist ein Unterring von S .
- (b) $\text{Kern}\varphi$ ist ein sogenanntes Ideal von R , d.h., es gilt:
- $\text{Kern}\varphi$ ist Untergruppe von R^+
 - magnetische Eigenschaft: $a \cdot r \in \text{Kern}\varphi \wedge r \cdot a \in \text{Kern}\varphi \quad \forall a \in \text{Kern}\varphi$ und $r \in R$
 - die Fasern von φ sind genau die Mengen $(\text{Kern}\varphi) + a \quad (a \in R)$
- Wir haben also wieder eine Bijektion

$$(\text{Kern}\varphi) + a \xleftrightarrow{\tilde{\varphi}} \varphi(a)$$

$$R \setminus \text{Kern}\varphi = \{ \text{Kern}\varphi + a \mid a \in R \} \longleftrightarrow \text{Bild}\varphi$$

Wieder kann $R \setminus \text{Kern}\varphi$ vermöge $\tilde{\varphi}$ zu einem Ring gemacht werden.

$$I := \text{Kern}\varphi$$

$$(I + a) + (I + b) = I + (a + b)$$

$$(I + a) \cdot (I + b) = I + (ab) \quad \forall a, b \in R$$

III.3. Polynomringe

Stets sei R ein kommutativer Ring mit Eins.

III.3.1. Definition:

Ein Polynom f (keine Funktion!) aus R sein ein formaler Ausdruck der Form:

$$f = c_0 + c_1 x + c_2 x^2 + \dots + c_n x^n \text{ mit } n \in \mathbb{N}, c_0, \dots, c_n \in R$$

Dabei sei x ein Symbol, die sogenannte Variable, die bei Bedarf jeden festen Wert aus R annehmen kann.

Wir rechnen daher mit Polynomen so, als wäre x ein Element aus R :

Ist $g = d_0 + d_1 x + \dots + d_m x^m$ ein weiteres Polynom mit $d_h \in R$, so sei

$$f + g := (c_0 + d_0) + (c_1 + d_1)x + \dots + (c_n + d_n)x^n$$

$\Rightarrow \sum_{l=0}^{n+m} (\sum_{j+k=l} c_j d_k) x^l$ (hierbei sei $c_j = 0$ für $j > n$ $d_h = 0$ für $h > m$) Es bezeichne $R[x]$ ein kommutativer Ring mit Eins mit Koeffizienten aus R .

III.3.2. Satz:

Bzgl. der in III.3.1 definierten Addition und Multiplikation ist $R[x]$ ein kommutativer Ring mit Eins.
Beweis:

Da sich x wie ein Element aus R verhält.

III.3.3. Warnung:

In $R[x]$ gilt das sogenannte Prinzip des Koeffizientenvergleichs, d.h.

$$\sum_{k=0}^n c_k x^k = \sum_{k=0}^b d_k x^k \Leftrightarrow c_k = d_k \quad \forall k$$

zu jedem $f = \sum_{k=0}^n c_k x^k \in R[x]$ gibt es eine zugehörige Abbildung $\tilde{f}: R \rightarrow R$ $\tilde{f}(a) = \sum_{k=0}^n c_k a^k \quad \forall a \in R$

\tilde{f} verhält sich anders wie f , denn die \tilde{f} erfüllen im allgemeinen nicht das Prinzip der Koeffizientenvergleichs.
Beweis:

$R = \mathbb{Z}/p\mathbb{Z}$ wo p Primzahl. Es gilt $a^p = a \quad \forall a \in R$ aber $x^p \neq x$

(Die Abbildung ist gleich bei unterschiedlichen Polynomen.)

III.3.4. Definition:

Sei $0 \neq f = \sum_{k=0}^n c_k x^k$ mit $c_n \neq 0$. Dann sei $\text{grad } f = n$ Formel sei $\text{grad } 0 = -\infty$

III.3.5. Satz:

$$(a) \quad \begin{aligned} \text{grad } (f - g) &\leq \max(\text{grad } f, \text{grad } g) \\ \text{grad } (f \cdot g) &\leq (\text{grad } f) + (\text{grad } g) \quad \forall f, g \in R[x] \end{aligned}$$

(b) Ist R nullteilerfrei, so gilt stets $\text{grad}(fg) = (\text{grad } f + \text{grad } g)$ „Gradformel“

$R[x]$ wo R kommutativ mit Eins.

Jeder $f \in R[x]$ hat ein Grad.

Ist R nullteilerfrei, so: $\text{grad}(fg) = \text{grad } f + \text{grad } g$

In diesem Fall ist $R[x]$ selbst nullteilerfrei.

Ferner ist $(R[x])^x = R^x$ (invertierbare „konstante“
direkt aus Gradformel \uparrow = Grad 0)

In folgenden betrachten wir nur noch $K[x]$ wobei K ein Körper ist.

III.3.6. Division mit Rest:

Division mit Rest in $K[x]$:

Es seien $f, g \in K[x]$ mit $g \neq 0$. Dann existieren eindeutig bestimmte $q, r \in K[x]$ mit $f = q \cdot g + r$ wo $\text{grad } r < \text{grad } g$

Beweis

Eindeutigkeit: Sind $f = q_1 g + r_1 = q_2 g + r_2$ mit $\text{grad } r_i < \text{grad } g$, so $(q_1 - q_2)g = r_2 - r_1$ mit $\text{grad } \underbrace{r_2 - r_1}_{\text{grad } g + \text{grad}(q_1 - q_2)} \not\leq$

$$\begin{aligned} & \text{grad } g \\ \Rightarrow & \text{grad } q_1 - q_2 = -\infty \text{ und } q_1 = q_2, r_2 = r_1 \end{aligned}$$

Existenz: Ist $\text{grad } f < \text{grad } g$, so wähle $q = 0$ und $r = f \rightsquigarrow$ fertig. Sei nun $\underbrace{\text{grad } f}_{=n} \geq \text{grad } g = m$ Ferner seien a und b die Höchstkoeffizienten von f bzw. g , also

$$f = a \cdot x^n + \dots, g = b \cdot x^m + \dots$$

$$\text{Induktion nach } n: n = 0 \Rightarrow m = 0 \text{ und } f = \underbrace{(ab^{-1})}_q \cdot g + \underbrace{0}_r \quad \checkmark$$

$n > 0$ Betrachte $h = f - (ab^{-1})x^{n-m} - g \Rightarrow \text{grad } h < n$. Induktion liefert $h = \tilde{q}g + r$ mit $\text{grad } r < \text{grad } g$

$$\Rightarrow f = h + (ab^{-1})x^{n-m} = \underbrace{((ab^{-1})x^{n-m} + \tilde{q})}_{=q} g + r \text{ mit } \text{grad } r < \text{grad } g.$$

III.3.7. Bemerkung:

$K[x]$ verhält sich also ähnlich wie \mathbb{Z} . Beide sind kommutativ, nullteilerfreie Ringe mit eins, in denen eine Division mit Rest möglich ist. (wobei der Grad der Polynome in $K[x]$ die Rolle der Absolutbetrages in \mathbb{Z} übernimmt). So ein Rechenbereich heißt EUKLIDischer Ring

III.3.8. Satz:

In einem EUKLIDischen Ring S haben die Ideale genau die Form $a \cdot S = \{a \cdot s \mid s \in S\}$ (für jedes feste $a \in S$) (Insbesondere: Die Ideale in \mathbb{Z} sind genau die $n\mathbb{Z}$ ($n \in \mathbb{N}$))

Beweis: Klar: $a \cdot S$ Ideal (wegen Distributivgesetz) Sei I nun irgendein Ideal in S . Ist $I = \{0\}$, so $I = 0 \cdot S \rightsquigarrow$ fertig.

Sei nun $I \neq \{0\}$. Wähle $a \in I \setminus \{0\}$ kleinstmöglich bzgl. der Funktion, die die Größe der Elemente in S heißt.

Magnetische Eigenschaft $a \cdot S \subseteq I$

Zeige: $I \subseteq a \cdot S$

Sei dazu $b \in I$ beliebig. Division mit Rest: $b = q \cdot a + r$ wo r kleiner als a (sogar echt kleiner)

Dann: $r = b - aq \in I$

Nach Wahl von a muss $r = 0$ sein.

Somit: $b = a \cdot q \in a \cdot S$

III.3.9. Bemerkung:

Wir nennen ein Polynom $f \in K[x]$ normiert, falls sein Höchstkoeffizient $= 1$ ist. Ist $I \neq \{0\}$ ein Ideal in $K[x]$, so existiert genau ein normiertes $f \in K[x]$ mit $f \cdot K[x] = I$.

Beweis:

Existenz: nach III.3.8 ist $I = f \cdot K[x]$ für ein $f \in K[x]$

Ersetze f durch $a^{-1}f$ wo $a =$ Höchstkoeffizient von f .

Eindeutigkeit: Sei $f_1 \cdot K[x] = I = f_2 \cdot K[x]$ wo f_1, f_2 normiert

$\Rightarrow f_1 - f_2 \in I$ mit echt kleineren Grad als f_1 und f_2 .

Insbesondere: $f_1 - f_2 - f_1 \cdot q$ und $\underbrace{\text{grad}(f_1 - f_2)}_{< \text{grad} f_1} = \text{grad} f_1 + \text{grad} q$

$\Rightarrow \text{grad} q = -\infty, q = 0, f_1 - f_2 = 0$

Wir können nun alle unsere Argumente aus der elementaren Zahlentheorie von \mathbb{Z} auf $K[x]$ übertragen und erhalten analoge Sätze.

Dabei:

natürliche Zahlen \leftrightarrow normierte Polynome

Vorzeichen $\pm 1 \leftrightarrow a \in K^x$

Sind $f, g \in K[x]$, so sagen wir g teilt f (und schreiben $g|f$) falls $f = g \cdot h$ für ein $h \in K[x]$. Die Partition von $K[x]$ in die Nebenklassen.

$r + g \cdot K[x]$ (wo $\text{grad} r < \text{grad} g$) besteht aus den Äquivalenzklassen der Äquivalenzrelation \equiv_g wo

$$f_1 \equiv_g f_2 \Leftrightarrow g|f_2 - f_1 \Leftrightarrow f_2 - f_1 \in g \cdot K[x]$$

An die Stelle der Primzahlen aus \mathbb{Z} treten die sogenannte normierten irreduziblen Polynome:

III.3.10. Definition:

Ein Polynom $f \in K[x] \setminus K$ heie irreduzibel in $K[x]$, wenn es keine echte Zerlegung von f in $K[x]$ gibt, d.h. aus $f = g \cdot h$ mit $g, h \in K[x]$ folgt $g \in K^x$ oder $h \in K^x$

III.3.11. Satz:

Jedes Polynom $f \in K[x] \setminus \{0\}$ hat eine bis auf Reihenfolge der Faktoren eindeutige Zerlegung der Form $f = a \cdot p_1 \cdot p_2 \cdot \dots \cdot p_s$ wo $a \in K^x, p_1, \dots, p_s \in K[x]$ normiert und irreduzibel

Beweis: kopiere den Beweis des Hauptsatzes der Zahlentheorie.

III.3.12. Folgerung:

Es gibt unendlich viele normierte, irreduzible Polynome in $K[x]$ (wie II.1.6(b)).

III.3.13. Beispiel:

Irreduzible Polynomen in $(\mathbb{Z}/2\mathbb{Z})[x]$:

Grad 1: $x, x+1$ sind irreduzibel wegen der Gradformel

Grad 2: $x^2 = x \cdot x, x^2 + x = x(x+1), x^2 + 1 = (x+1)^2 \Rightarrow$ Reduzibel
 $x^2 + x + 1 \Rightarrow$ Irreduzibel.

Grad 3: $x^3 = x \cdot x^2, x^3 + x^2 = x^2(x+1), x^3 + x = x(x+1)^2, x^3 + x^2 + x + 1 = (x+1)^3, x^3 + x^2 + x = x(x^2 + x + 1), x^3 + 1 = (x+1)(x^2 + x + 1) \Rightarrow$ Reduzibel
 $x^3 + x + 1, x^3 + x^2 + 1 \Rightarrow$ Irreduzibel

III.3.14. Bemerkung

Es seien $f, g \in K[x] \setminus \{0\}$ und $f = a \cdot p_1^{\alpha_1} \cdot \dots \cdot p_s^{\alpha_s}$, $g = b \cdot p_1^{\beta_1} \cdot \dots \cdot p_s^{\beta_s}$ wo $\alpha_i, \beta_i \geq 0$ und wo p_i normiert und irreduzibel in $K[x]$

$ggT(f, g) = p_1^{\gamma_1} \cdot \dots \cdot p_s^{\gamma_s}$ wo $\gamma_i = \min\{\alpha_i, \beta_i\}$

$kgV(f, g) = p_1^{\delta_1} \cdot \dots \cdot p_s^{\delta_s}$ wo $\delta_i = \max\{\alpha_i, \beta_i\}$

Dann gilt: $f \cdot g = a \cdot b \cdot ggT(f, g) \cdot kgV(f, g)$

Ferner kann $ggT(f, g)$ wie bei den ganzen Zahlen mit dem EUKLID Algorithmus berechnet werden und der erweiterte EUKLID Algorithmus liefert BEZOUT-Koeffizienten $u, v \in K[x]$ mit $ggT(f, g) = u \cdot f + v \cdot g$

III.4. Körperkonstruktionen

Stest sei K ein Körper.

III.4.1. Definition und Bemerkung:

Sei $f \in K[x] \setminus K$ fest. Wir betrachten die Menge $\{g + f \cdot K[x] \mid g \in K[x]\} = K[x]/f \cdot K[x] = \{g + f \cdot K[x] \mid g \in K[x] \text{ mit } \text{grad } g < \text{grad } f\}$ Wie beim Übergang $\mathbb{Z} \leadsto \mathbb{Z}/n\mathbb{Z}$ wird $K[x]/f \cdot K[x]$ ein kommutativer Rint mit eins vermöge:

$\bar{g} + \bar{h} = \overline{g+h}$ und $\bar{g} \cdot \bar{h} = \overline{gh} \quad \forall g, h \in K[x]$ wo $\bar{g} = g + K[x]$

Da jede Nebenklasse \bar{g} genau einen Vertreter vom Grad $< \text{grad } f$ enthält.

Wird also nur mit Polynomen vom Grad $< \text{grad } f$ gerechnet und bei Überschreiten der Gradgrenze modulo f reduziert.

K ein fester Körper, $f \in K[x] \setminus K$ fest

$K[x]/fK[x] = \underbrace{\{g + fK[x] \mid g \in K[x], \text{grad } g < \text{grad } f\}}_{=\bar{g}}$

$$\bar{g} + \bar{h} = \overline{g+h}, \quad \bar{g} \cdot \bar{h} = \overline{gh} \quad \forall g, h \in K[x]/fK[x]$$

III.4.2. Beispiel:

Wähle $K = \mathbb{Z}/n\mathbb{Z}$, $f = x^3 + x + 1 \in K[x]$

$\Rightarrow K[x]/fK[x] = \{\bar{g} \mid g \in K[x] \text{ mit } \text{grad } g < 3\}$ enthält $2 \cdot 2 \cdot 2 = 8$ Elemente mit $\bar{f} = \bar{0}$, d.h. $x^3 = x + 1$ und f .

$\Rightarrow (x^2 + 1) \cdot (x^2 + x + 1) = x^4 + x^3 + x^2 + x + 1 = x^4 + x^3 + x + 1 \equiv x^4 = x^3 \cdot x \equiv x \cdot (x + 1) = x^2 + x$ und f

d.h. $(x^2 + 1) \cdot (x^2 + x + 1) = x^2 + x$ in $K[x]/fK[x]$

III.4.3. Satz:

Seien $f \in K[x] \setminus K$ und $g \in K[x] \setminus \{0\}$. Genau dann ist \bar{g} in $K[x]/fK[x]$ invertierbar, wenn $ggT(f, g) = 1$

Beweis: vgl. $\mathbb{Z}/z\mathbb{Z}$

III.4.4. Folgerung:

Genau dann ist $K[x]/fK[x]$ ein Körper, wenn f in $K[x]$ irreduzibel ist.

III.4.5. Bewertung:

Sei S ein kommutativer Ring mit Eins. Der Körper K sei ein Teilring von S mit $A_S = A_K$ Für S ist ein Ringhomomorphismus

festes $a \in S$.

III. Algebraische Strukturen

$$\begin{aligned}\varepsilon_a : K[x] &\longrightarrow S \\ f &\longrightarrow f(a) \\ f \text{ wird gegeben durch } &\sum_{i=0}^r c_i x^i \\ f(a) \text{ wird gegeben durch } &\sum_{i=0}^r c_i a^i\end{aligned}$$

Wir müssen a eine Nullstelle von f in S falls $f(a) = 0$

III.4.6. Satz:

Genau dann ist $a \in K$ Nullstelle von $f \in K[x]$, wenn gilt $x-a \mid f$ in $K[x]$. (d.h. $f = (x-a)g$ mit $g \in K[x]$).

Beweis: $f(a) = 0 \Leftrightarrow \varepsilon_a(f) = 0 \Leftrightarrow f \in \underbrace{\text{Kern } \varepsilon_a}_{\text{ist ein Ideal in } K[x]}$

Klar: $(x-a) \in \text{Kern } \varepsilon_a$, also $(x-a) K[x] \subseteq \text{Kern } \varepsilon_a$.

Ferner: $K \cap \text{Kern } \varepsilon_a = \{0\}$
 konstantes Polynome in $K[x] \Rightarrow \text{Kern } \varepsilon_a = (x-a) \cdot K[x]$
 $\Rightarrow x-a$ ist Polynom in $\text{Kern } \varepsilon_a \setminus \{0\}$ von kleinstmöglichem Grad.

III.4.7. Beispiel:

Fortsetzung von 4.2: $K = \mathbb{Z}/n\mathbb{Z}$, $f = x^3 + x + 1 \in K[x]$
 f ist irreduzibel in $K[x]$, da f keine Nullstelle in $\mathbb{Z}/2\mathbb{Z}$ hat.
 (und $\text{grad } f = 3$ ist)
 $K[x]/fK[x]$ ist ein Körper mit 8 Elementen.
 Beachte: $\mathbb{Z}/8\mathbb{Z}$ ist kein Körper.

III.4.8. Konstruktion:

Sei $f \in K[x]$ irreduzibel. Bilde $L = K[x]/fK[x]$. Wir betrachten K als Teilkörper von L via
 $c \in K \longleftrightarrow \bar{c} \in L$
 Dann ist $f \in K[x] \subseteq L[x]$ und \bar{x} ist Nullstelle von f in L .

Beweis: Sei $f = \sum_{i=0}^r c_i x^i \in K[x]$, also $c_i \in K$
 $= \sum_{i=0}^r \bar{c}_i x^i \in L[x]$
 $\Rightarrow f(\bar{x}) = \sum_{i=0}^r c_i x^i = \sum_{i=0}^r \bar{c}_i x^i = \bar{f} \stackrel{L=K[x]/fK[x]}{\underset{\downarrow}{=}} 0$
 $\in L$

III.5. Endliche Körper

III.5.1. Satz:

Zu jedem endlichen Körper L existiert eine Primzahl p so dass gilt:

- (a) $K = \underbrace{\{1 + 1 + \dots + 1\}}_{k\text{-mal}} \mid k \in \mathbb{N}$ ist ein Teilkörper von L isomorph zu $\mathbb{Z}/p\mathbb{Z}$.
- (b) L ist ein K -Vektorraum. Insbesondere gilt $|L| = p^n$ für $n = \dim_K L$

$$(c) \quad \underbrace{a + \dots + a}_{p \text{ mal für jedes } a \in L} = 0$$

Beweis:

$$(a) \text{ Betrachte: } \varphi: \mathbb{Z} \rightarrow L \\ z \mapsto \underbrace{1 + \dots + 1}_{z \text{ mal}}$$

Abbildungsverzeichnis

I.1. Eine einfache Abbildung	1
I.2. Ein Beispiel Graph	2
I.3. Mögliche Abbildungen auf einen Blick	3
I.4. Eine mögliche Komposition	4
I.5. Eine Abbildung auf Untermengen	5
I.6. Eine bijektive und inverse Abbildung	7
II.1. Es wurden $y_1 = e^x$ und $y_2 = \ln x$	15
III.1. Fadendiagramm mit der Funktion 1 auf 3	21
III.2. Fadendiagramm mit der Funktion 1 auf 2	22