1 Jonas B.

Logik (Kapitel 2)

- Wahre Aussage => Theorem/Lemma/Korrolar

Operatoren

- Konjugation => Logisches Und => $A \land B$ (Beide müssen wahr sein)
- Disjunktion => Logisches Oder => $A \lor B$ (Eines muss wahr sein)
- Implikation $A \to B$: (= Alternativ $\neg A \lor B$) Wenn A, so ist B.
- Zweiseitige Implikation (= Alternativ $(A \to B) \land (B \to A)$) $\Leftarrow (A \land B) \lor (\neg A \land \neg B)$
- Bindstärke: $\neg / \lor / \land / \to / \Leftrightarrow$ (Stark … Schwach)

A	B	$A \to B$
0	0	1
0	1	1
1	0	0
1	1	1

A	B	$A \Leftrightarrow B$
0	0	1
0	1	0
1	0	0
1	1	1

- Zwei Formeln sind äquivalent, gleiche Wahrheitstabelle $A \equiv B$
- Logische Konsequenz: $F \models G$ ($\leq$) (= G folgt aus F) (Wenn F wahr, dann auch G wahr)

Erfüllbarkeiten

- Tautologie (= Allgemeingültig) => Für alle Werte wahr / $F \lor \neg F \equiv T$
- Erfüllbar, wenn mind. 1 Wert wahr ist → Wenn es eine Interpretation gibt, für die Formel wahr ist
- Unerfüllbar, wenn alles falsch ist / $F \land \neg F \equiv \bot$
- Lemma 2.2: $F \to G$ ist T, wenn $F \models G$
- Menge U ist das Universum / Def. 2.11. k-ary Prädikat P on U ist eine Funktion $U^k \to \{0,1\}$, die jedem Element $\{x_1, x_2, \dots x_k\}$ einen Wahrheitswert zuschreibt

Quantoren

- $\forall x \; P(x) \to P(x)$ ist für alle x in U wahr / $\forall x\, P(x) \equiv T$
- $\exists x \; P(x) \to$ Es existiert ein x in P(x), welches wahr ist

$\exists y \forall x \Rightarrow \forall x \exists y$ ✓
$\forall x \exists y \not\Rightarrow \exists y \forall x$ ↯

Regeln

- Beisp. 2.15: $prime(x) := x > 1 \land \forall y \forall z \, ((yz = x) \to ((y = 1 \lor (z = 1)))$ / even & odd $\exists k \; n = 2k\underbrace{(+1)}_{odd}$
- $\forall x\, P(x) \land \forall x\, Q(x) \equiv \forall x\, (P(x) \land Q(x))$
- $\neg \forall x\, P(x) \equiv \exists x\, \neg P(x)$ // $\neg \exists x\, P(x) \equiv \forall x\, \neg P(x)$

Beweisstrategien

$\Rightarrow / \models$

- $S \Rightarrow T$ (= Wenn S ist wahr, dann auch T ist wahr)
  - ↳ Hier geht es um ein Statement bzw. mathematische Aussage
- $F \models G$ (= Hier geht es um Formeln)

Beweistypen

- Direkter Beweis: $S \Rightarrow T$ (Man hält S für wahr und zeigt daraus T)
- Indirekter Beweis: Man setzt S = falsch und leitet her t = falsch $\neg S \Rightarrow \neg T$
- Beweis über Umweg: $S \Rightarrow T$ $T \Rightarrow U$ (Bsp. $(A \to B) \land (B \to C) \models A \to C$
- Modus Ponens: Man zeigt, dass R = wahr und $R \Rightarrow S$ wahr, dann S wahr
- Fallunterscheidung: $R_1, \dots, R_k \Rightarrow S$
- Beweis mittels Widerspruch: Man kehrt Aussage um, und zeigt, dass diese falsch ist
- Existenzbeweis: Man gibt ein Beispiel, für das es richtig ist
- Pigeonhole Prinzip: Es gibt n Objekte auf m Menge, wobei $n > m$ ist
- Proof by contradiction: $\{F \lor G, \neg G\} \vdash F$

Logik (Kapitel 6) (Prädikatenlogik erweitert Aussagenlogik)

Beweissystem

- Beweissystem: • Menge mathematischer Aussagen S (= Formeln)
- $\Pi = (S, P, \tau, \phi)$ • Menge von Beweisen P (zur Verifikation) $\phi = S \times P \to \{0,1\}$
  • Funktion $\tau = S_K \to \{0,1\}$
- Korrektes B.S: Kein Beweis für falsche Aussage $\forall s \in S \; (\exists p \in P \; \phi(s,p) = 1 \to \tau(s) = 1)$
- Vollständiges BS: Für jede wahre Aussage gibt es Beweis $\forall s \in S \; (\tau(s) = 1 \to \exists p \in P \; \phi(s,p) = 1)$

Syntax Semantik

- Syntax: Definiert, welche Abfolge von Symbolen vom Alphabet erlaubt sind
- Semantik: Funktion σ, die Formel + Interpretation $\sigma(F, \mathcal{A}) / \mathcal{A}(F)$ Wahrheitswert gibt

Interpretation

- Interpretation $\mathcal{A}$: Wahl der Werte der Variabeln
- Passende Interpretation: Wenn alle Variabeln in S definiert sind
- Modell: Interpretation, wo Formel wahr ist $\mathcal{A} \models F$

Literal Atom

- Atom: Eine Variable mit Wahrheitswerten
- Literal: Atomare Formel oder die Negation davon

A	B	C	$(A \land \neg B) \lor (B \land \neg C)$
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	0

DNF (1): $(\neg A \land B \land \neg C) \lor (A \land \neg B \land \neg C) \lor (A \land \neg B \land C) \lor \dots$

CNF (0): $(A \lor B \lor C) \land (A \lor B \lor \neg C) \land (A \lor \neg B \lor \neg C) \land \dots$

Aussagenlogik

- Unsere Formeln sind die atomaren formeln

Normal form

- Konjunktive Normalform (CNF): $(X \lor Y \lor Z) \land \dots \land (A \lor B \lor C)$ (0)
- Disjunktive Normalform (DNF): $(X \land Y \land Z) \lor \dots \lor (A \land B \land C)$ (1)
- $\neg(F \lor G) \vdash \neg F \land \neg G$ // $F \land F \to G \vdash G$

Prädikatenlogik

Beinhalten nur Variabeln als Argument → $f^{(n)}$ ← ¬ Argument; ↗ Argument, z.B. Formeln

Syntax

- Syntax: Variabeln (G), Quantoren $\exists x \forall y$, Funktion $f(x)$, Prädikat $p(f(x))$
- Variable/Symbole → Terme → Formeln

Frei / Gebunden / Ersetzen

- Freie Variabeln: Wenn kein Quantor davorsteht z.B. x
- Gebundene Variabeln: In Verknüpfung mit Quantor z.B. $\exists x\ x$
- $\exists x\ f(x) \land f(x)$ sind nicht die selben Variabeln, man kann das zweite x durch anderes Symbol ersetzen $F[x/t]$ (x durch t ersetzt)

Struktur interpretation

- Struktur (=Interpretation): $\mathcal{A} = (U, \phi, \psi, \xi)$ U=Universum ($U^{\mathcal{A}}/f^{\mathcal{A}}/P^{\mathcal{A}}/z^{\mathcal{A}}=1$) Für Strukturinterpretation
  ϕ = ordnet jeder Funktion eine Bedeutung zu (z.B. $f(x,y) = x \geq y$)
  ψ = ordnet jedem Prädikat Bedeutung zu // ξ = ordnet Variable Wert zu
- Prenexform = Wenn alle Quantoren am Anfang vorkommen
  ↪ $\neg(\forall u\ P(u) \land \exists v\ P(v)) \Rightarrow \exists u \neg P(u) \lor \forall v \neg P(v)$
- $\neg\exists x \forall y\ (P(y,x) \Leftrightarrow \neg P(y,y))$ // $\{0,1\}^{\infty}$ unzählbar y. bit of x. Sequenz *

Regeln

- Lemma 6.6: 1.) $\neg(\forall x\ F) \equiv \exists x \neg F$ / 2.) $\neg(\exists x\ F) \equiv \forall x \neg F$ / 3.) $(\forall x\ F) \land (\forall x\ G) \equiv \forall x\ (F \land G)$
  4.) $(\exists x\ F) \lor (\exists x\ G) \equiv \exists x\ (F \lor G)$ / 5.) $\forall x \forall y F \equiv \forall y \forall x F$ / 6.) $\exists x \exists y F \equiv \exists y \exists x F$
  7.) $(\forall x F) \land H \equiv \forall x\ (F \land H)$ / 8.) $(\forall x F) \lor H \equiv \forall x\ (F \lor H)$ / 9.) $(\exists x F) \land H \equiv \exists x\ (F \land H)$
  10.) $(\exists x\ F) \lor H \equiv \exists x\ (F \lor H)$
- Lemma 6.2: 1.) $F \lor F \equiv F$ / 1.) $F \land F \equiv F$ / 2.) $F \land G \equiv G \land F$ / 3.) $(F \land G) \land H \equiv F \land (G \land H)$
  4.) $F \land (F \lor G) \equiv F$ / 5.) $F \land (G \lor H) \equiv (F \land G) \lor (F \land H)$ / 6.) $F \lor (G \land H) \equiv (F \lor G) \land (F \land H)$
  7.) $\neg\neg F \equiv F$ / 8.) $\neg(F \land G) \equiv \neg F \land \neg G$ / 9.) $F \lor \top \equiv \top$ / 10.) $F \lor \bot \equiv F$ / 10.) $F \land \bot \equiv \bot$
  11.) $F \lor \neg F \equiv \top$ / 11.) $F \land \neg F \equiv \bot$

Kalkül

Erlaubt es, neue Regeln aus bestehenden zu erstellen

- Besteht aus: Syntax, Semantik und Schlussregeln
- Schlussregel: $\{F_1, \dots, F_k\} \vdash_R G$ (=Schlussregel G erstellt durch Preconditions mit Regel R)
- Kalkül besitzt endliche Menge von Schlussregeln $K = \{R_1, \dots, R_k\}$
- Kalkül ist korrekt/widerspruchsfrei: $M \vdash_K F \Rightarrow M \models F$ (Wenn M gültig ist, ist auch F)
- Kalkül ist vollständig: $M \models F \Rightarrow M \vdash_K F$ (herleiten)
- Vollständig + nicht korrekt: $K := \{R\}$ mit $\emptyset \vdash_R F$ / unvollständig + korrekt: $\{F \land G\} \vdash F$

Resolutionskalkül

- Prüft, ob Menge von Formeln unerfüllbar sind
- Wenn $\neg F$ unerfüllbar ist, ist F Tautologie
- Formelmenge muss in CNF übergeben werden
- Resultierungsschritt umfasst nur eine Eliminierung
- Wenn $K(m) \vdash_{Res} \emptyset$, dann ist Menge m unerfüllbar
- Beispiel: $(A \to B) \to ((B \to C) \to (A \to C))$ ist Tautologie
  $\neg[(A \to B) \to ((B \to C) \to (A \to C))]$ ist unerfüllbar $\Rightarrow \emptyset$
  ↪ Tabelle → CNF
  $M = \{\{\neg A, B\}, \{\neg B, C\}, \{A\}, \{\neg C\}\}$ (= M ⇒ Klauselmenge) Klausel

$\{\neg A, C\}$

$\{C\}$

$\{\emptyset\}$

- Wenn man mehrere Formeln gegeben hat → $F_1 \land F_2 \land \dots \land F_K$

* There exists no index x, so dass no sequence in the enumeration, such that for all y, the yth bit on that sequence is equal to the negation of the yth bit on the yth sequence.

Jonas B.

Sets, Relations and functions

$x \in A$ mit $x \subseteq A$ $A = \{\emptyset\}$
$A \notin P(A)$ mit $x \in A$ mit $x \subseteq P(A)$ $A = \{\emptyset, 1\}$
$A \subseteq P(A)$ mit $x \notin P(A)$ $\Rightarrow A = \emptyset$

Syntax
- $x \in A$ (Element, Menge) (= x ist Element von A) / $x \notin A$ (= Kein Element von A)
- Mengen $A = B$ sind gleich, wenn $\forall x (x \in A \Leftrightarrow x \in B)$
- Kardinalität $|A|$ (= Anzahl Elemente in der Menge)
- Menge A mit Elementen a, b, c $\Rightarrow A = \{a, b, c\}$ (Reihenfolge egal)

Untermengen
- Mengen können selbst wieder Elemente einer Menge sein
- Untermenge $A \subseteq B$ // $\forall x (x \in A \rightarrow x \in B)$ // A ist Teilmenge von B
- Equivalenzcheck: $A = B \Leftrightarrow (A \subseteq B) \wedge (B \subseteq A)$ → A muss auch Menge sein

Leere Menge
- Leere Menge $\emptyset$ oder $\{\}$ // $\forall x (x \notin \emptyset)$
  - ↳ Leere Menge ist Teilmenge jeder anderen Menge
  - ↳ Leere Menge ist unique // $\emptyset \subseteq \emptyset'$ und $\emptyset' \subseteq \emptyset \Rightarrow \emptyset = \emptyset'$
  - ↳ Mit leerer Menge Mengen konstruieren: $A = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$ $|A| = 3$
  - ↳ $|\emptyset| = 0$ // $|\{\emptyset\}| = 1$ // $|\{\emptyset, \{\emptyset, \{\emptyset\}\}\}| = 2$

Potenzmenge
- Potenzmenge $P(A) := \{S \mid S \subseteq A\}$ ⇒ Menge aller möglichen Kombinationen
  - ↳ Kardinalität $2^{|A|}$ ↳ $A \subset P(A)$ ⇒ Menge aller möglichen Teilmengen (A ist Teilmenge von sich selbst)
  - ↳ $P(\{A, B, C\}) = \{\emptyset, \{A\}, \{B\}, \{C\}, \{A, B\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$ $|2^3 = 8|$
  - ↳ $P(\emptyset) = \{\emptyset\}$ // $P(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$ // $P(P(\emptyset)) = \{\emptyset, \{\emptyset\}\}$

$\boxed{\overline{D} \cap \overline{C} = \overline{D \cup C}}$

Operationen
- Vereinigung zweier Mengen: $A \cup B := \{x \mid x \in A \vee x \in B\}$ $(A \vee B)$ OR
- Schnitt zweier Mengen: $A \cap B := \{x \mid x \in A \wedge x \in B\}$ $(A \wedge B)$ AND
- Komplement $\overline{A} := \{x \in \text{Universum} \mid x \notin A\}$ u $\boxed{\overline{A \cap B} = \overline{A} \cup \overline{B}}$ $(\neg A)$ $\boxed{\overline{A \cup B} = \overline{A} \cap \overline{B}}$
- Differenz $B - A$ // $B \setminus A$: $B - A := \{x \in B \mid x \notin A\}$
- Kartesisches Produkt/Tupel: $A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$ $|A \times B| = |A| \cdot |B|$
  - ↳ Alle Paare, die man mit Element aus A/B machen kann → Reihenfolge wichtig ↳ 1. Element von A
  - ↳ $A = \{1, 2\}$ $B = \{3, 4\}$ $\Rightarrow A \times B = \{(1,3), (1,4), (2,3), (2,4)\}$

Relationen

ist Geschwister = ig = ikoie - id (ich selbst) ik oim ∩ ikoiv (= Echte Geschw.)

- Leere Relation $\emptyset$ z.B. $< \cap >$ = symmetrisch + transitiv

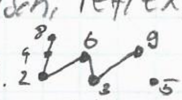
Definition
- $a \rho b$ (a ist in Relation mit b) $(a \to b) = \rho^1$ Matrix transponiert ≙ Inverses bilden
- Identitätsrelation $id = a \rho a$ $\rho^2 (a \to b \to c)$
- Kardinalität: 2^{n^2} (n = Anzahl Elemente)

Typen
- Inverses $\hat{\rho} := \forall a \forall b \; a \rho b \Leftrightarrow b \hat{\rho} a$ (Auch ρ^{-1}) (kehrt Frage um)
- Reflexiv: $a \rho a$ für jedes $a \in A$ der Relation (In Matrix, Diagonale = 1)
- Irreflexiv: $a \not\rho a$
- Symmetrisch: $\forall a \forall b \; a \rho b \Leftrightarrow b \rho a$ (Matrix ist symmetrisch)
- Antisymmetrisch: $\forall a \forall b \; (a \rho b \wedge b \rho a) \rightarrow a = b$ (Trifft nur zu, wenn $a = b$)
- Transitiv: $\forall a \forall b \; (a \rho b \wedge b \rho c) \rightarrow a \rho c$ $a \to b \to c$ $\rho^2 \subseteq \rho$ Komposition

Spezielle Relation
- Komposition: Verknüpfung zweier Relationen $a \rho b \wedge b \sigma c \Rightarrow a \rho \circ \sigma c \Rightarrow \rho \circ \sigma$
- Transitiver Abschluss/Hülle ρ^* = Alle Möglichkeiten etwas zu erreichen $a \rho^* b$ ↳ Man darf so viele Schritte machen, wie es geht

Äquivalenzrelation
- Äquivalenzrelation: symmetrisch, reflexiv, transitiv $[a]_\theta$
- Äquivalenzklasse ist Teilmenge, welche alle Elemente Kriterium erfüllen
- $[a]_\theta$ alle Elemente, die zu a äquivalent sind $:= \{b \in A \mid b \,\theta\, a\}$
- Partition: Menge aller Äquivalenzklassen (disjungt, keine Überschneidungen)

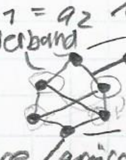
Ordnungsrelation
- Partielle Ordnung $(A; \preceq)$ Transitiv, antisymmetrisch, reflexiv (kein Zyklus) (= Poset)
- $a \prec b \Leftrightarrow a \preceq b \wedge a \neq b$ → z.B. $\leq$ → Hasse-Diagram

Hasse Diagramm
- Hasse-Diagramm: $a \prec b$ ⇒ B ist höher als A z.B.  (Teilbarkeiten)

Ordnung
- Totally-ordered: Wenn alle Elemente in der Menge vergleichbar sind $\forall a \forall b \; a \prec b \vee b \prec a$
- Well-ordered: Totally-ordered + jede Teilmenge hat mind. 1 Element

Lexikon
- Lexigrographische Ordnung: $(a_1, b_1) \leq_{lex} (a_2, b_2) :\Leftrightarrow a_1 < a_2 \vee (a_1 = a_2 \wedge b_1 \sqsubseteq b_2)$

Positionen
- Minimal/Maximales Element a: $\neg \exists b \;\; b \prec a \,/\, a \prec b$
- Kleinstes/Grösstes Element a: $a \preceq b$ // $a \succeq b$ für alle b
- Untere/obere Schranke a: $a \preceq b$ // $a \succeq b$ für alle b
- Kleinst unterste/grösst oberste Schranke: Wenn es keine kleinere/grössere Schranke gibt

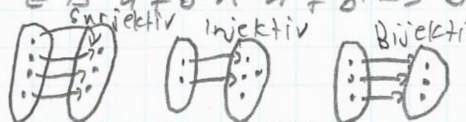
Nicht Verband  Maximale Elemente, Kein grösstes Element, Minimales Element + Kleinstes Element

- Meet: $a \wedge b$ wenn a/b grösst unterste Schranke haben
- Join: $a \vee b$ wenn a/b kleinst oberste Schranke haben
- Lattices (= Verband): Meet + Join → Jede zwei Elemente der gleichen Ebene müssen eine kleinst oberste Schranke und eine grösst unterste Schranke haben

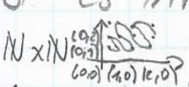
Funktionen

- $f: a \to b$ (=von Definitionsbereich in Bild/Wertebereich)
- f ist totally defined: $\forall a \in A\ \exists b \in B\ afb$
- f ist well defined: $\forall a \in A\ \exists b, b' \in B\ afb \wedge afb' \to b = b'$

Injektiv Surjektiv
- Injektiv: $a \neq b \Rightarrow f(a) \neq f(b)$
- Surjektiv: Für jedes a existiert ein b
- Bijektiv: Injectiv + Surjectiv
  - ↳ Für Bijektive-Funktionen gibt es Inverses f^{-1}



Zählbare / unzählbare Mengen



$\mathbb{Z} \cong \mathbb{N}$ $\{2,-1,0,1,2,3\}$

- Wenn zwei Mengen bijektiv sind → selbe Kardinalität $A \sim B \Leftrightarrow |A| = |B|$
- A ist zählbar wenn von der Kardinalität her $A \preceq \mathbb{N}$

Beispiel
- Zählbar: $\mathbb{Z}$ / $\{0,1\}^* := \{0,1,00,01,...\}^*$ / $\mathbb{N} \times \mathbb{N}$ $(= \mathbb{N}^2)$ / $A \times B$ / $\mathbb{Q}$ / A^* / $A_1 \cup A_2 \cup ...$ / A^n ← n Tuples / Java-Progr.
- Überabzählbar: $\{0,1\}^\infty$ (=Cantorscher Diagonalisierungsbeweis) / Menge Äquivalenzrelationen auf $\mathbb{N}$ / $\mathcal{P}(\mathbb{N})$ / $\mathbb{R}$

Zusatz ↳ There are uncomputable functions $\mathbb{N} \to \{0,1\}$

Regeln
- Theorem 3.4: $A \cap (B \cap C) = (A \cap B) \cap C$ / $A \cap (A \cup B) = A$ / $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
  $A \cap \bar{A} = \emptyset$ / $A \subseteq B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B$

Zahlentheorie

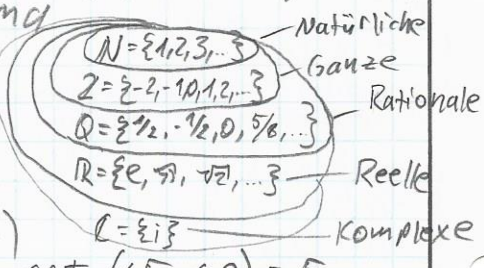
Gesetze
- Kommutativgesetz (=Vertauschungsgesetz) / $a+b = b+a$ // $b \cdot a = a \cdot b$
- Assoziativgesetz (=Verbindungsgesetz) / $(a+b)+c = a+(b+c)$ // $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- Distributivgesetz (=Verteilungsgesetz) / $a \cdot (b+c) = ab + ac$

Teilen
- Teilbar: $a | b$ $(= b/a)$ $(= a \neq 0)$ existiert ein $c = b/a$ (B=Vielfaches / A=Teiler)
  ↳ $4 | 12 \Leftrightarrow 4$ teilt $12 \Leftrightarrow 12 = 4 \cdot 3$
- Teilen mit Rest: $\frac{a}{d} = q + r$ (r = Rest)
- Rest a mod d

→ $ggT(6,12) = 6$ → $ggT(a,b) | a$ / $ggT(a,b) | b$

ggT
- Grösster gemeinsamer Teiler ($ggT(a,b) = d$): $d | a \wedge d | b \wedge \forall c\ ((c | a \wedge c | b) \to c | d)$
- Wenn $ggT(a,b) = 1$, dann ist a / b teilerfremd

Erweiterter euklidischer Algorithmus für ggT



- $ggT(65,40)$: $65 = 1 \cdot 40 + 25$ (1)
  $40 = 1 \cdot 25 + 15$ (2)
  $25 = 1 \cdot 15 + 10$ (3)
  $15 = 1 \cdot 10 + 5$ (4)
  $10 = 2 \cdot \boxed{5}$

$\boxed{5} \overset{(4)}{=} 15 - 10$
$\overset{(3)}{=} 15 - (25 - 15) = 2 \cdot 15 - 25$
$\overset{(2)}{=} 2 \cdot (40 - 25) - 25 = 2 \cdot 40 - 3 \cdot 25$
$\overset{(1)}{=} 2 \cdot 40 - 3 \cdot (65 - 40) = 5 \cdot 40 - 3 \cdot 65 \Rightarrow 65 \cdot (-3) + 40 \cdot (5) = 5$

$ggT(65,40) = 5$

- Primfaktorenzerlegung ist eindeutig

$\sqrt{2}$
- Beweis: $\sqrt{n}$ irrational: $\sqrt{n} = a/b$ / ^{2} // $n = \frac{a^2}{b^2}$ / $\cdot b$ / $n \cdot b^2 = a^2$ (ungerade, gerade - Anzahl an Primfaktoren)

kgV
- kleinster gemeinsames Vielfaches $kgV(a,b) = l := a | l \wedge b | l \wedge \forall m\ ((a | m \wedge b | m) \to l | m)$
- $gcd(a,b) \cdot lcm(a,b) = a \cdot b$

Mod
- Modulo: $a \equiv_m b := m | (a-b) := a \equiv b \mod (m) = a \bmod m = b \bmod m$ → $a \equiv_m b \Leftrightarrow \exists s\ a - b = m \cdot s$
- a und b müssen entweder gerade oder ungerade sein
- $a \equiv_2 b$ und $a \equiv_3 b \Rightarrow a \equiv_6 b$ / $a \equiv_m b \Rightarrow a \neq b$ / ungerade + ungerade = gerade

Gerades ungerade
- ungerade · ungerade = ungerade / gerade · ungerade = gerade / ungerade - gerade = ungerade

Rest
- $a \equiv_m R_m(a)$ / $a \equiv_m b \Leftrightarrow R_m(a) = R_m(b)$
- $R_m(a+b) = R_m(R_m(a) + R_m(b))$ / $R_m(a \cdot b) = R_m(R_m(a) \cdot R_m(b))$
- Mod(9) = $R_9(247) = R_9(2+4+7) = 4$ / $R_9(3158) = R_9(3+1+5+8) = 8$ / $R_9(247 \cdot 3158) = R_9(4 \cdot 8) = 5$

Multip. Inverses modulo
- Multiplikatives Inverses: $ax \equiv_m 1$ hat eindeutige Lösung, wenn $ggT(a,m) = 1$ → x = mod - Invers. Zahl
  ↳ $ax = k \cdot m + 1$ für jedes k ⇒ Berechnung: erweiterter Euklidischer Algorithmus
- Negativer Modulo $-25 \bmod 13 = 1 \Rightarrow -25 = -2 \cdot 13 + 1$ - Rest

Chin. Rest Satz
- Chinesischer Restsatz: $x \equiv_{m_1} a$, $x \equiv_{m_2} b$, $x \equiv_{m_3} c$ } Wenn $ggT(m_1, m_2, m_3)$ teilerfremd sind $= 1$, dann gibt es eine eindeutige Lösung

*Repräsentiert alle natürlichen Zahlen in binär

$\log_7(11) = x \Leftrightarrow 7^x = 11$

Jonas B.

Algebra

- Algebraische Struktur $\langle S; \Omega \rangle$ (S = (Träger)menge) (Ω = Liste von Operationen)

Monoid $\langle S; *, e \rangle$ → Beispiel: $(a^b)^c = a^{b^c}$ nicht assoziativ → $\mathbb{Z}, \mathbb{N}, \mathbb{Q}, \mathbb{R}, \mathbb{Z}_m$

$\langle \mathbb{Z}; +, 0 \rangle$
- Assoziativität bezüglich der Operation $* \Rightarrow (a*b)*c = a*(b*c)$
- Neutrales Element $e \Rightarrow a*e = a$ & $e*a = a$

Neutrales Beweis: - Rechts/Links neutrales Element $e*e' = e'$ / $e*e' = e$ (e = Links / e' = rechts) $\Rightarrow e' = e$

Gruppe $\langle G; *, \hat{\ }, e \rangle$ Beispiel: $\langle \mathbb{Z}; +, -, 0 \rangle$ & $\langle \mathbb{Z}_m; \oplus, \ominus, 0 \rangle$, $\mathbb{Z}_m = \langle \mathbb{Z}_m; \oplus \rangle$

Gruppe:
- Assoziativ + neutrales Element → Monoid, aber keine Gruppe $\langle \mathbb{N}_0; \oplus \rangle$
- Inverses Element $\hat{a} * a = e$ / $a * \hat{a} = e$

Invers Beweis: - Rechts/Links Inverses: (b = links) (c = rechts) $\Rightarrow b*a = e$ / $a*c = e$ / $\Rightarrow b = b*e = b*(a*c) = (b*a)*c = e*c = c$

Abelsche Gruppe $\langle G; * \rangle$ → $\hat{(\hat{a})} = a*e = a*(\hat{a}*\hat{\hat{a}}) = a*(\hat{a}*\hat{\hat{a}}) = (a*\hat{a})*\hat{\hat{a}} = \hat{\hat{a}} \Leftarrow a$

Abelsche:
- Wenn eine Gruppe oder Monoid zusätzlich noch kommutativ ist
- Assoziativ + neutrales Element + Inverses Element
- Kommutativität: $a*b = b*a$ → $|G| = 8 = \mathbb{Z}_8 = \mathbb{Z}_2 \times \mathbb{Z}_4 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

Regeln: - Lemma 5.3: (i) $\hat{(\hat{a})} = a$ / (ii) $\widehat{a*b} = \hat{a} * \hat{b}$ / (iii) $a*b = a*c \Rightarrow b = c$ / (iv) $b*a = c*a \Rightarrow b = c$

Homomorphismus:
- Homomorphismus zwischen zwei Gruppen: Strukturbewahrende Funktion/Abbildung
- Funktion ψ von Gruppe $\langle G; *, \hat{\ }, e \rangle$ zu $\langle H; *, \hat{\ }, e' \rangle$ ist ein Homomorphismus, wenn gilt: $\psi(a*b) = \psi(a) * \psi(b)$ z.B. $\det(a \cdot b) = \det(a) \cdot \det(b)$
- Homomorphismus ist bijektiv, dann Isomorphismus $a \cong b$
- Lemma 5.5.: (i) $\psi(e) = e'$ / (ii) $\psi(\hat{a}) = \widehat{\psi(a)}$ $\Rightarrow \psi(eg) = \psi(eg) \cdot \psi(g) \cdot \widehat{\psi(g)}$ $= \psi(e_G \cdot g) \ \psi(g)$

$\boxed{a \equiv_m b \Leftrightarrow m \mid a - b}$

Untergruppe:
- Untergruppe: $H \leq G$ (= H ist Untergruppe von G)
- Für alle Gruppen gibt es triviale Untergruppen: $\{e\}$ und G selbst
- Bsp: $\langle \mathbb{Z}_{12}, \oplus, \ominus, 0 \rangle$: $\{0\}$, $\{0, 6\}$, $\{0, 4, 8\}$, $\{0, 3, 6, 9\}$, $\{0, 2, 4, 6, 8, 10\}$, $\mathbb{Z}_{12}$

Ordnung einer Gruppe und Element:
- Ordnung eines Elements: Wieviel Mal muss ich a^n nehmen $= e$ / $ord(a) = a^m = e$
- Wenn $ord(a) = \infty$ hat die Gruppe unendlich Elemente
- $ord(e) = 1$ / Wenn $ord(a) = 2$ dann ist $a \cdot a = e$ und a ist selbst Invers
- Ordnung einer Gruppe ist die Anzahl der Elemente $|G|$
- Wenn $|G|$ endlich ist dann ist auch $\forall a \in G$ $ord(a)$ endlich

→ Gruppe 10 Elemente durch 1. Generator zufall $e(10) = 4$ = Anzahl Gen → $\{1, 3, 7, 9\}$

Zyklische Gruppe:
- Gruppe $G = \langle g \rangle$ ist zyklisch, wenn sie generiert werden kann durch Generator g
- Eine zyklische Gruppe kann mehrere Generatoren haben z.B. g und g^{-1} bzw $\hat{g}$ ($2^1 \bmod (10)$, $2^2 \bmod (10)$ ...)
- Gruppe $\langle \mathbb{Z}_n, \oplus \rangle$ ist zyklisch für jedes n, wann 1 ist Generator / Generator $ggT(g, n) = 1$
- $g^0 = e$ / $g^{|G|} = g$ / Hoch steht stellvertretend z.B. $\langle \mathbb{Z}_5; \oplus \rangle$ $g^1 = g$ $g^2 = g+g$ $g^3 = g+g+g$
- Theorem 5.7.) Zyklische Gruppe mit Ordnung $|G| = n$ ist isomorph zu $\langle \mathbb{Z}_n; \oplus \rangle$

Lagrange:
- Ordnungen von Untergruppen (Lagrange): $H \leq G \Leftrightarrow |H|$ dividiert $|G| \Leftrightarrow \frac{|G|}{|H|} = \mathbb{N}$
- Ordnung jedes Elements teilt die Gruppenordnung: $ord(a)$ teilt $|G| \Leftrightarrow \frac{|G|}{ord(a)} = \mathbb{N}$
- Wenn Ordnung einer Gruppe $|G|$ = prim, dann zyklisch, jedes Element ausser e Generator

$\mathbb{Z}_m^*$ und $\varphi(m)$:
- Bei $\mathbb{Z}_m$ haben nicht alle Zahlen Inversen, bei $\mathbb{Z}_m^*$ schon $\Rightarrow \mathbb{Z}_m^* = \{a \in \mathbb{Z}_m \mid ggT(a, m) = 1\}$
- Eulerfunktion $\varphi(m) = |\mathbb{Z}_m^*|$ z.B. $\mathbb{Z}_{18}^* = \{1, 5, 7, 11, 13, 17\}$ $\varphi(18) = 6$
- $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$ z.B. $\varphi(18) = \varphi(2) \cdot \varphi(9) = 1 \cdot 6 = 6$
- Wenn m Primzahl ist: $\varphi(p) = p - 1$ / $\varphi(p^e) = p^{e-1} \cdot (p-1)$ z.B. $\varphi(\underset{\text{Nicht prim}}{16}) = \varphi(2^4) = 2^3 \cdot 1 = 8$

Kleine Fermat:
- Für $m \geq 2$ und für alle a $ggT(a, p) = 1$ gilt: $a^{\varphi(m)} \equiv_m a$ / Für jede prim p und jedes a: $a^{p-1} \equiv_p 1$
- $\mathbb{Z}_m^*$ ist zyklisch, wenn $m = 2$, $m = 4$, $m = p^e$, $m = 2p^e$ (p ist ungerade prim & $e \geq 1$)

Ring $\langle R; +, -, 0, \cdot, 1 \rangle$ mit zwei Operationen z.B. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, $\mathbb{Z}_m = \langle \mathbb{Z}_m; \oplus, \odot \rangle$
- $\langle R; +, -, 0 \rangle$ muss kommutative Gruppe (abelsche Gruppe) sein
- $\langle R; \cdot, 1 \rangle$ ist ein Monoid
- Distributivität: $a(b+c) = ab + ac$ und $(b+c) \cdot a = ba + ca$
- Lemma 5.17: (i) $0a = a0 = 0$ / (ii) $(-a) \cdot b = -ab$ / (iii) $(-a) \cdot (-b) = ab$
- Lemma 5.18: (i) $a \mid b$ und $b \mid c \Rightarrow a \mid c \Rightarrow \mid$ ist transitiv / (ii) $a \mid b \Rightarrow a \mid b \cdot c$ $\forall c$ (iii) $a \mid b$ und $a \mid c \Rightarrow a \mid (b + c)$

→ $a \in \mathbb{Z}_m$ $ggT(a, m) = 1$ → A invertierbar ⟺ A Einheit

- Einheit (= Elemente, die invertierbar sind) $u \cdot u^{-1} = 1$ / Menge aller Einheiten R^*
- Beispiel: $\mathbb{Z} \Rightarrow \mathbb{Z}^* = \{-1, 1\}$ $(1 \cdot 1 = 1)$ / $\mathbb{R} \Rightarrow \mathbb{R}^* = \mathbb{R} - \{0\}$ / Gauss-Zahlen$^* = \{1, i, -1, -i\}$
- Nullteiler: $a \neq 0$, wenn $a \cdot b = 0$ ergibt und $b \neq 0$
- Beispiel: $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\} \Rightarrow$ In $\mathbb{Z}_m$ ist Element entweder Einheit oder Nullteiler

0: Nichts per Definition; 1: Einheit $1 \cdot 1 = 1$; 2, 3: Nullteiler $2 \cdot 3 = 0$, $3 \cdot 2 = 0$; 4: Nullteiler $4 \cdot 3 = 0$; 5: Einheit $5 \cdot 5 = 1$

Untergruppen von $\mathbb{Z}_7^*$ ← 1. Untergruppe

$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$ / $|\mathbb{Z}_7^*| = 6 \Rightarrow$ Grösse: 1, 2, 3

$1 = \{1\}$ / $2 = \{2, 2^2, 2^3\}$ / $3 = \{3, 3^2, 6, 3^4, 5, 1\}$ / $4 = \{4, 2, 1\}$ ....

Integritätsbereich z.B. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$

- Kommutativer Ring ohne Nullteiler, also z.B. nicht $\mathbb{Z}_{20}$: $5 \cdot 8 = 0$ ↯
- Integritätsbereich: $a | b \Rightarrow b = a \cdot c$ ist eindeutig ($c = b/a$) (Quotient ist eindeutig)

Polynomielle Ringe $\mathbb{Z}_{Grad}[x]$

- Hier gilt immer noch Modulo: $[2x^2 + 3x + 1] + [5x + 6] = 2x^2 + x$
- Für jeden Ring R, ist $R[x]$ ebenfalls ein Ring.
- Regeln: Lemma 5.22: (i) Wenn D Integritätsbereich ist, dann auch $D[x]$ / (ii) Einheit in $D^* = D^*[x]$

Körper z.B. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ aber nicht $\mathbb{Z}$ und $R[x]$ / $\mathbb{Z}_p$ ist Körper, nur wenn p = prim *

- Kommutativer Ring F, in welchem jedes nicht 0-Element eine Einheit ist
- $F^* = F - \{0\}$
- In diesem Körper kann man gut Gleichungssysteme lösen → Jede Zahl hat Inverses
- Integritätsbereich: Jeder Körper ist ein Integritätsbereich, da nicht 0-Elemente Einheit sind, somit keine Nullteiler
- Wenn Integritätsbereich endlich ist, ist er auch ein Körper (Theorem 5.25.)

Polynomielle Körper

- $F[x]$ ist monisch/normiert, wenn erster Koeffizient 1 ist z.B. $1x^2 + 3x + 5$
- Galois-Körper: $GF(Grad)[x]$ / $GF(5)[x] = \mathbb{Z}_5[x]$
- Reduzibel/irreduzibel für Faktorisierung: Reduzibel: Wenn man Polynom faktorisieren kann / Primfaktorenzerlegung / Hat Nullstellen
- Irreduzibel: Wenn es nicht in kleinere Polynome zerfällt
- Test: Grad kleiner-gleich 3: Schauen auf Nullstellen / Grösser als 3: Nullstelle: Reduzibel sonst → keine Aussage

$F[x]$:

- Polynomdivision: $GF(7)$ (mod 7) $= (x^3 + 2x^2 + 5x + 4) : (2x^2 + x + 1) = 4x + 6 + R(2x + 5)$
- ggT $([x^3 + 4x^2 + 5x + 2], [x^3 + 6x^2 + 11x])$, $GF(7)$: $(x+1) \cdot (x^2 + 3x + 2)$ $(x+3)(x^2 + 3x + 2)$ → ggT
  - $x^3 + 4x^2 + 1$ mod (5) → Nullstelle $= 2 \Rightarrow (x-2) \bmod (5) \Rightarrow (x+3)$

$$\begin{array}{l} -(x^3 + 4x^2 + 4x) \\ \hline 5x^2 + x + 4 \\ -(5x^2 + 6x + 6) \\ \hline 2x + 5 \end{array}$$

- Korrelar 5.30: Polynom mit Grad 3/3 ist irreduzibel, wenn es keine Nullstelle hat
- Theorem 5.31: Ein Polynom d. Grades hat maximal d Nullstellen

$F[x]_{mod}$:

- Polynome mit mod: $F[x]_{mod(x)} := \{a(x) \in F[x] \mid deg(a(x)) < d\}$ (Alle Polynome kleiner $m(x)$)
- Anzahl Elemente: $|F[x]_{m(x)}| = q^d$ (q = Anzahl Elemente von F (z.B. $\mathbb{Z}_5 = 5$) / d = Grad)
- Irreduz. = Körper: $F[x]_{m(x)}$ ist immer ein Ring, und wenn irreduzibel, dann auch Körper → keine Nullteiler
- $\mathbb{C}$: $\mathbb{R}[x]_{x^2+1}$ sind $\mathbb{C} \Rightarrow x^2 + 1 = b + ai$ / $R_{x^2+1}(x^2) = -1$ / Alle anderen Grad 2 isomorph zu $\mathbb{C}$ / Höhere faktorisierbar mit x^1/x^2
- Anzahl Körper: Theorem 5.39: Endlicher Körper mit q-Elementen existiert nur, wenn $prim^x = q$ existiert

Diffie Hellman	RSA
1. Festlegen Generator (Prim/Mod) 3 mod(17) = shared	1. Zwei sehr grosse Primzahlen p und q
2.1 Alice private Key 15 ⇒ 3^{15} mod(17) = 6 = shared Bob	2. Berechne $n = p \cdot q$
2.2 Bob private Key 13 ⇒ 3^{13} mod(17) = 12 = shared Alice	3. Berechne $\varphi(n) = (p-1) \cdot (q-1)$
3.1 Alice 12^{15} mod(17) = 10 / $3^{13^{15}}$ mod(17) = 10	4. Wähle e: $1 < e < \varphi(n)$ und ggT$(e, \varphi(n)) = 1$
3.2. Bob 6^{13} mod(17) = 10 / $3^{15^{13}}$ mod(17) = 10	5. e und n ⇒ öffentlicher Schlüssel
↳ Gruppe $\mathbb{Z}_p^*$ = zyklisch ← Diskretes Logarithmus	6. Bestimme $d \Rightarrow e \cdot d \equiv_{\varphi(n)} 1 \Rightarrow d \equiv_{\varphi(n)} e^{-1}$
↳ Kann auch andere zyklische Gruppe sein wo Problem	7. d, n ⇒ Privater Schlüssel

grosse Zahlen mod(n):

$R_{11}(4^{2015})$ / $R_{11}(4^{10}) = 1 \Rightarrow R_{11}(4^{R_{10}(2015)}) =$

$R_{11}(4^5) = R_{11}(2^{10}) = 1$ → Geht auch für $R_3(x)$

$R_9(106345) = R_9(1+6+3+4+5) = R_9(19) = R_9(1+9) = 1$

$a^{p-1} \equiv_p 1$ wenn a, p teilerfremd sind

8. Verschlüsseln von Plaintext m: $y = m^e \bmod (n)$
9. Entschlüsseln von y: $m = y^d \bmod (n)$

$\mathbb{Z}^*_{n \cdot m} \cong \mathbb{Z}^*_n \times \mathbb{Z}^*_m \Rightarrow$ ggT(a, nm) = ggT(a, n) ∧ ggT(a, m) (Isomorph, teilerfremd)

$\mathbb{Z}^*_{15} \cong \mathbb{Z}^*_3 \times \mathbb{Z}^*_5$ / $\mathbb{Z}^*_{20} \cong \mathbb{Z}^*_4 \times \mathbb{Z}^*_5$ / $\mathbb{Z}_3 \to \mathbb{Z}_4$ isomorph

$\mathbb{Z}^*_{20} = \mathbb{Z}^*_4 \times \mathbb{Z}^*_5$

Interpolation: Polynom d. Grades interpoliert mit $d+1$ Punkten

↳ Ein Polynom 2. Grades hat 3 Koeffizienten

↳ 3 Gleichungen $(ax^2 + bx + c)$, 3 Unbekannte

$A = \{0, 1, 2\} = (1, 3)$-Code C

↳ $|A|^1 = 3$ (= Anzahl Elemente) ↳ Wieviele Stellen wir in 1 Element haben

$C = \{(0,0,0), (0,1,2), (1,2,1)\}$

- Hamminggewicht oder Hammingdistanz: Anzahl an wie vielen Stellen sich zwei Elemente unterscheiden
- Minimaldistanz: Kleinste Hamminggewicht aller Elemente
  - $(0,0,0)$ & $(0,1,2) = 2$ / $(0,0,0)$ & $(1,2,1) = 3$
  - $(0,1,2)$ & $(1,2,1) = 3$ ./.
  - ↳ Minimaldistanz $= 2 = d$
- Theorem 5.41: Code C mit Minimumdistanz d kann t Fehler korrigieren $d \geq 2t + 1$
  - ↳ Code C $2 \geq 2t + 1$
  - ↳ 0 Fehler korrigieren

Endliche Körper:

Gibt es Körper mit 4 Elementen?

- Ja, da $prim^x = 4 \Leftrightarrow 2^2 = 4$
- $\mathbb{Z}_x[x]_{m(x)}$ ← Muss irreduzibel sein
- $\mathbb{Z}_2[x]_{x^2+x+1} = \{0, 1, x, x+1\}$
  - ↳ $2^2 = 4$ Elemente
- Nullstellen: $p(y) = x \cdot (y) + x$

$p(0) = x \cdot 0 + x = x$ / $p(1) = x + x = 2x \bmod (2) = 0$

$p(x) = x \cdot x + x = x^2 + x = (x^2 + x + 1) + R(1) = 1$

$p(x+1) = x \cdot (x+1) + x = x^2 + 2x = x^2 = (x^2 + x + 1) + R(x+1) = x + 1$

Primzahlen: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, ... (2 – Einzig gerade Primzahl)

$\sqrt[2]{4} = 4^{\frac{1}{2}}$

* Da $\mathbb{Z}_p^*$, $\mathbb{Z}_p - \{0\}$ ist und eine multiplikative Gruppe ist