Gruppen Ringe und Körper

Gruppen

Verknüpfung

Eine ist Verknüpfung eine Abbildung v : A × B → C

(x, y) → v(x, y)

und kann mit einem Operator x ★v y = v(x, y) oder kürzer x ★ y = v(x, y) geschrieben werden, wenn der Zusammenhang klar ist. Wenn A = B = C, so ist v eine Verknüpfung auf A.

Gruppen

Eine Verknüpfung ist eine Gruppe, wenn gilt:

1. Assoziativität: ∀x, y, z ∈ G : (x ★ y) ★ z = x ★ (y ★ z)

2. Neutrales Element: ∃e ∈ G : ∀x ∈ G : e ★ x = x ★ e = x

3. Inverse Elemente: ∀x ∈ G : ∃y ∈ G : x ★ y = y ★ x = e

Für eine kommutative Gruppe oder abelsche Gruppe gilt zusätzlich:

4. Kommutativität: ∀x, y ∈ G : x ★ y = y ★ x

Wenn (G, ★) eine Gruppe ist, so gilt:

(1) Das Element e ist eindeutig.

(2) Für jedes x ∈ G gibt es genau ein y ∈ G mit x ★ y = y ★ x = e

Multiplikative Interpretation

Gruppen werden als additive oder multiplikative Gruppen interpretiert

- In additiv interpretierten Gruppen wird oft + als Operator, 0 als neutrales Element e und −x für das inverse Element y zu x verwendet

- In multiplikativ interpretierten Gruppen wird oft · oder ∗ als Operator, 1 als neutrales Element e und x −1 für das inverse Element y zu x verwendet

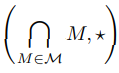
**Die generische Verknüpfung** ★ **wird ab hier multiplikativ interpretiert.**

Untergruppen

Wenn (G,★) eine Gruppe ist und H ⊆ G dann ist (H,★) eine Untergruppe von (G,★)

Außerdem muss gelten U ≠ ∅ und ∀x, y ∈ U : x ★ y−1 ∈ U.

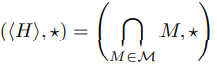
Sind (H, ★) und (L, ★) Untergruppen einer Gruppe (G, ★), so ist (H ∩ L, ★) ebenfalls eine Untergruppe von (G, ★). Ist ϻ ein Mengensystem von Untergruppen von G, so ist



ebenfalls eine Untergruppe von (G, ★).

Erzeugendensystem

Sei (G, ★) eine Gruppe und H ⊆ G eine Teilmenge. Seien im Mengensystem ϻ die Mengen aller alle Untergruppen (M, ★) von G, für die H ⊆ M gilt. Dann ist



die von H erzeugte Gruppe. Man sagt auch: H ist das Erzeugendensystem von <H>.

Zyklische Gruppen

Eine zyklische Gruppe (<a>, ★) ist eine von genau einem Element a erzeugte Gruppe. Ist <a> endlich, so ist die Anzahl der Elemente die Ordnung von a: ord(a) = |<a>|

Ist a ∈ G für eine Gruppe (G, ★), so gilt mit an = a ★ . . . ★ a, a0 = 1 und a−n = (a-1)n,  
dass <a> = { az | z ∈ Z)

Ringe und Körper

Ring

Wenn R eine Menge und + und · Verknüpfung auf R ist. Dann ist (R,+, ·) ein Ring, wenn

1. (R,+) eine kommutative Gruppe ist
2. · auf R assoziativ ist
3. Für alle a, b, c ∈ R die Distributivgesetze gelten

Das neutrale Element der Gruppe (R, +) wird mit 0 bezeichnet

Die Struktur wird Ring mit 1 genannt, wenn es ein neutrales Element 1 bezüglich der Verknüpfung · gibt

R ein kommutativer Ring, wenn die Verknüpfung · kommutativ ist

Menge der Polynome

Wenn (R, +, ·) kommutativer Ring mit 1 ist, dann ist R[x] Menge der Polynome über R

R[x] = { anxn + an−1xn−1 + . . . + a1x + a0 | n ∈ N0, a0, . . . , an ∈ R }

Grad das Polynom = n Monom = akxk

Ist (R, +, ·) ein kommutativer Ring mit 1, so sind die Polynome (R[x], +, ·) über R ebenfalls ein kommutativer Ring mit 1

Sei (R, +, ·) ein kommutativer Ring. Dann ist a ∈ R Teiler von b ∈ R, geschrieben a|b, wenn es ein k ∈ R gibt mit b = k · a

Sei n ∈ N und x ∈ Zn. Dann existiert genau dann ein y ∈ Zn mit x · y ≡ 1 mod n, wenn x = 1 oder x und n teilerfremd sind

Größter Gemeinsamer Teiler

Seien a, b ∈ Z. Der größte gemeinsame Teiler ggT(a, b) ist die größte natürliche Zahl, die a und b teilt

Für a, b, k ∈ N und a > k · b gilt ggT(a, b) = ggT(b, a − k · b)

Gaußklammer

Für a ∈ R sei die Gaußklammer b = ⌊a⌋c ∈ Z die größte ganze Zahl b ≤ a

Damit gilt also für a, b ∈ N auch ggT(a, b) = ggT(b, a− ⌊a/b⌋ b ). Der Wert a− ⌊a/b⌋ b ist der ganzzahlige Rest von a nach Division durch b und wird auch a modulo b genannt

Euklidische Algorithmus

Seien a0, a1 ∈ N und u0 = 1, u1 = 0, v0 = 0, v1 = 1. Für natürliche k sei iterativ

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Solange ak+1 > 0 gilt, ak = ggT(a0,a1) = uk · a0 + vk · a1

Das dargestellte Verfahren samt Berechnung einer Linearkombination ggT(a0, a1) = uka0 + vka1 wird auch als Erweiterter Euklidischer Algorithmus bezeichnet

Multiplikative Inverse

Sei n ∈ N, n > 1 und x ∈ Zn. Ist ggT(n, x) = 1 = u · n + v · x, so gilt für **y = v**, wenn v > 0 oder y = n + v, wenn v<0: **x · y ≡ 1 mod n** (also ist y die mult. Inverse von x)

Körper

(R, +, ·) als Körper bezeichnet, wenn

(R, +, ·) ein kommutativer Ring mit 1 ist

(R\{0}, ·) eine kommutative Gruppe ist

Genau dann, wenn n eine Primzahl ist, ist (Zn\{0}, ·) eine kommutative Gruppe

Zyklische Codes

Binärcode

Ein Binärcode ist eine injektive Abbildung c : M → ZN2 für ein N ∈ ℕ. Das Bild des Binärcodes sind die Codewörter mit N Bits

Hammingdistanz

Sei n ∈ ℕ und seien x, y ∈ Zn2 zwei Binärvektoren der Länge n. Dann bezeichnet die Hammingdistanz H(x, y) die Anzahl der unterschiedlichen Bits

Zyklisch

Ein Binärcode c : M → ZN2 ist zyklisch, wenn es zu jedem Codewort c(x) = y = (y1, . . . , yN ) zu einem x ∈ M auch die zyklische Drehung y0 = (y2, . . . , yN , y1) Codewort ist, also ein x0 ∈ M existiert, so dass c(x0) = y0

Linear

Ein Binärcode c : Z n 2 → Z N 2 ist linear, wenn für alle x (1), x(2) ∈ Z n 2 gilt:

c(x(1) + x(2)) = c(x(1)) + c(x(2))

Generatorpolynom

Ein Polynom p(x) ist ein Generatorpolynom eines Codes c :

Z2[x]/xn+1 → Z2[x]/xN +1

wenn der Code durch diese Polynommultiplikation darstellbar ist

c(q) = q · p

Diffie-Helmann-Schlüsselaustausch

(1) Einer der Kommunikationspartner wählt eine Primzahl p und einen Erzeuger α ∈ Zp\{0, 1}. Die Parameter (p, α) werden öffentlich an den anderen Partner übersendet

(2) Die zwei Kommunikationspartner wählen Zufallszahlen a und b, berechnen die Potenzen α a und α b in Zp und senden das Ergebnis öffentlich zum anderen Partner

(3) Jetzt werden die empfangenen Ergebnisse mit der eigenen Zufallszahl potenziert und die beiden erhalten (α a ) b bzw. (α b ) a in Zp

(4) Da (α a ) b = α a·b = (α b ) a gilt, haben beide Kommunikationspartner nun einen gemeinsamen Schlüssel α a·b für die weitere Kommunikation.

Perfect Forward Secrecy nutzt das um immer wieder neue Schlüssel auszutauschen.

Kleiner Satz von Fermat

Sei p eine Primzahl und a ∈ Zp. Dann gilt

ap ≡ a mod p

Ist a !≡ 0, so gelten die direkten Folgerungen

ap−1 ≡ 1 mod p und an(p−1) ≡ 1 mod p

für alle natürlichen Zahlen n ∈ N

Eulersche Phi-Funktion

bezeichnet die Anzahl der zu n teilerfremden ganzen Zahlen in 1, . . . , n

ϕ(n) = | {a ∈ N | 1 ≤ a ≤ n ∧ ggT(a, n) = 1 } |

Satz von Euler-Fermat

Sei n ∈ N und a ∈ Zn, dann ist

a ≡ aϕ(n)+1 mod n

Ist n = p · q für zwei Primzahlen p != q, so ist ϕ(n) = (p − 1)(q − 1) und es folgt

a ≡ a(p−1)(q−1)+1 mod n

RSA-Verfahren

(1) Wählen Sie zwei große unterschiedliche Primzahlen p und q.

(2) Berechnen Sie das Produkt n = pq

(3) Wähle einen zu (p − 1)(q − 1) teilerfremden öffentlichen Exponenten e ∈ N, das heißt ggT(e,(p − 1)(q − 1)) = 1

(4) Berechne den geheimen Exponenten d ∈ N mit der Eigenschaft e · d ≡ 1 mod (p − 1)(q − 1)

Dann ist kPUB = (e, n) der öffentliche Schlüssel und kSEC = (d, n) der zugehörige geheime Schlüssel dieses RSA-Verfahrens.