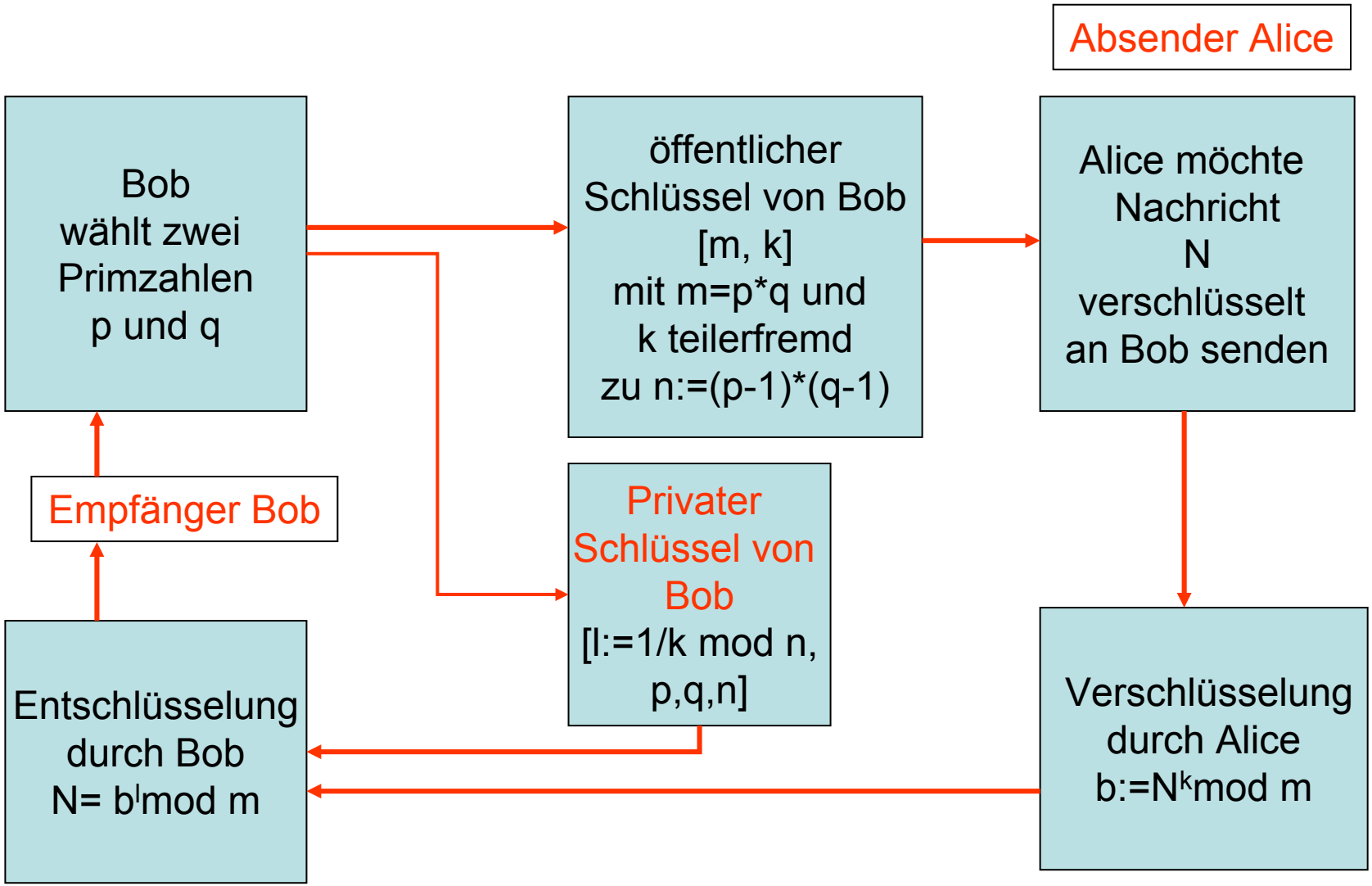
Algebraische Strukturen

Elliptische Kurven,
endlich erzeugte
abelsche Gruppen
und Einführung
in die Ringtheorie

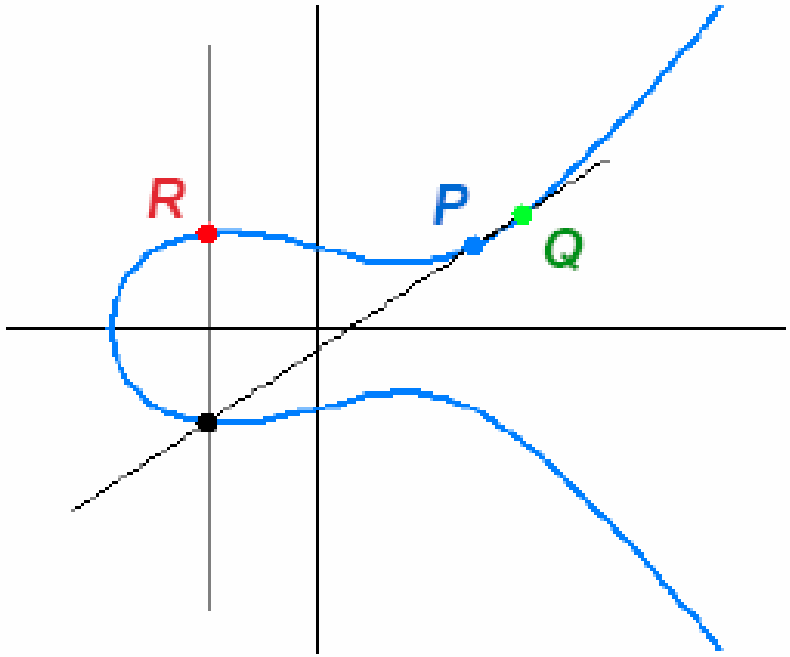
M.B. Wischnewsky
J. Zhao

26.01.2007

RSA-Verschlüsselungsverfahren



Elliptische Kurven in der Kryptographie



Punkte auf elliptischen Kurven können „addiert“ werden:

$R = P + Q$

$$\mathrm{E}(a, b) := y^2 = x^3 + a\,x + b$$

Geometrie der E(a,b)

- Die Kurve E(a,b) besitzt in jedem Punkt eine eindeutig bestimmte Tangente.
- Jede nicht-senkrechte Gerade, die eine solche elliptische Kurve in 2 Punkten schneidet, schneidet sie auch in einem dritten Punkt, wenn man den Berührungspunkt einer Tangente als doppelten Schnittpunkt zählt.
- Wenn die Punkte (x_1,y_1) und (x_2,y_2) rationale Koordinaten besitzen, so gilt das auch für den 3. Punkt (x_3,y_3).

Konstruierung der Gruppe E(a,b,Q)

Idee:

Als Verknüpfung definiert man hierfür eine Addition, welche die zwei Punkte (x_1,y_1) und (x_2,y_2) auf den Punkt $(x_3,-y_3)$ abbildet, also auf den an der x-Achse gespiegelten dritten Schnittpunkt.

(∞,∞) kann als Schnittpunkt einer senkrechten Geraden definiert werden.

Auf $E_{a,b}(\mathbb{Q})$ sei eine *Addition*

$$+ : \begin{cases} E_{a,b}(\mathbb{Q}) \times E_{a,b}(\mathbb{Q}) & \to E_{a,b}(\mathbb{Q}), \\ ((x_1, y_1), (x_2, y_2)) & \mapsto (x_1, y_1) + (x_2, y_2) \end{cases}$$

definiert durch:

(i) $(x, y) + (\infty, \infty) = (\infty, \infty) + (x, y) = (x, y)$ für alle $(x, y) \in E_{a,b}(\mathbb{Q})$.

(ii) Für $(x_1, y_1) \neq (\infty, \infty)$ und $(x_2, y_2) \neq (\infty, \infty)$ ist

$$(x_1, y_1) + (x_2, y_2) = \begin{cases} (\infty, \infty), & \text{für } (x_1, y_1) = (x_2, -y_2), \\ (x_3, y_3), & \text{für } (x_1, y_1) \neq (x_2, -y_2), \end{cases}$$

mit

$$x_3 = \lambda^2 - x_1 - x_2,$$

$$y_3 = \lambda(x_1 - x_3) - y_1 = \lambda(x_2 - x_3) - y_2,$$

$$\lambda = \begin{cases} \frac{(3x_1^2 + a)}{(2y_1)} & \text{für } (x_1, y_1) = (x_2, y_2), \\ \frac{(y_1 - y_2)}{(x_1 - x_2)} & \text{für } (x_1, y_1) \neq (x_2, y_2). \end{cases}$$

Die Menge $E_{a,b}(\mathbb{Q})$ bildet mit dieser Addition eine abelsche Gruppe (zum Beweis siehe etwa [Si1]). In dieser Gruppe ist (∞, ∞) das neutrale Element, das Inverse von (x, y) ist $(x, -y)$.

Das diskrete Logarithmusproblem

Definition. Es sei $(G, *)$ eine beliebige, kommutative endliche Gruppe. Dann betrachte das folgende Problem:

Gegeben $g, h \in G$, $ord(g) = n$, finde eine Zahl k, $0 \leq k \leq n-1$ mit $g * g * \cdots * g = h$ (k − Faktoren).

$g^k = h$ bzw. $kg = h$

Diese Zahl k heißt der **diskrete Logarithmus** von h zu Basis g. Notation: $k := \log_g h$.

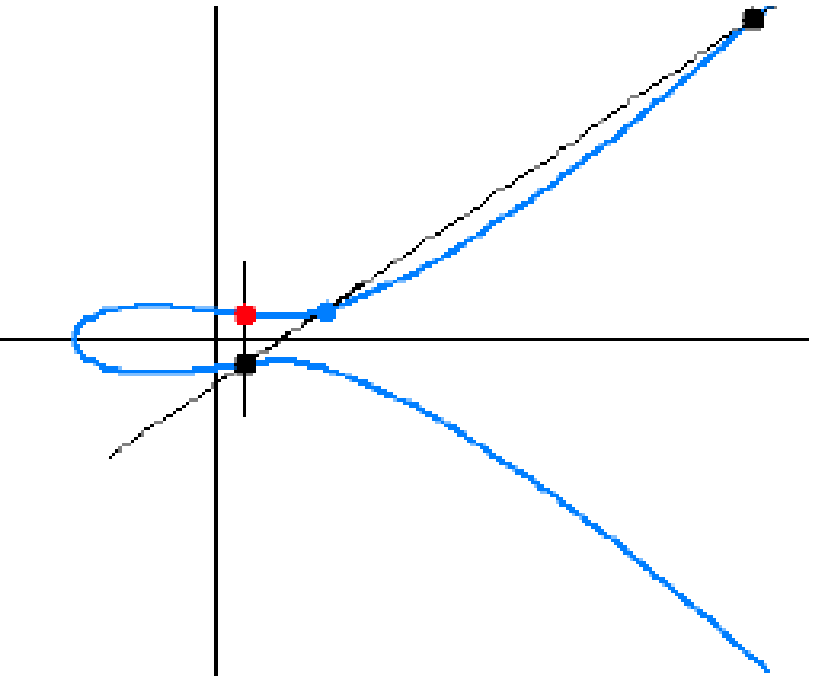
Wir schreiben auch $g^k := g * \cdots * g$ bzw.

$kg := g + g + \cdots + g$

falls die Gruppenoperation additiv geschrieben wird).

- Das **diskrete Logarithmusproblem** besteht darin aus den Angaben g und h die ganze Zahl k zu berechnen mit $g^k = h$.

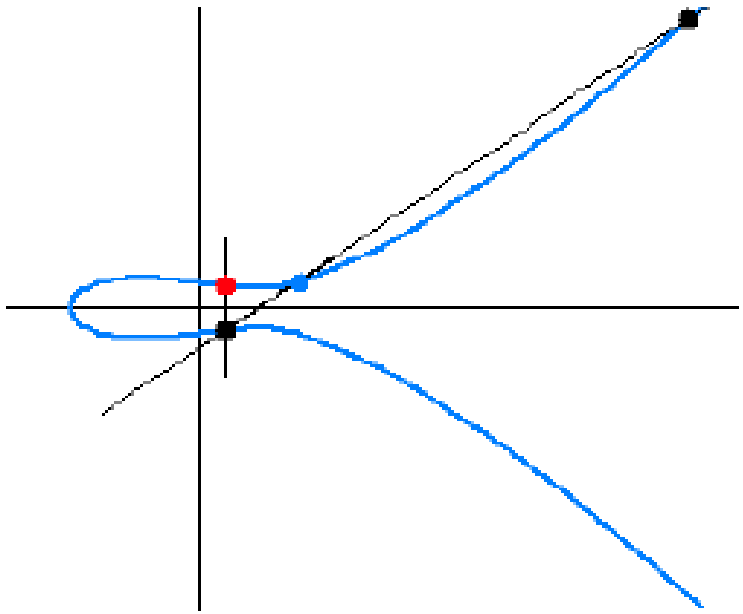
Elliptische Kurven in der Kryptographie
Das diskrete Logarithmusproblem



- Indem man einen Punkt ***P*** *n*-mal zu sich selbst addiert, erhält man den Punkt ***Q*** = *n* ***P***.
- Hat man umgekehrt nur das Ergebnis ***Q*** und den Basispunkt ***P*** vorgegeben, so besteht das diskrete Logarithmusproblem darin, den Faktor *n* zu berechnen.
- Diese Aufgabe ist bis heute nicht in kurzer Zeit lösbar.

Beispiel: ***Q*** = 6 ***P***

Elliptische Kurven in der Kryptographie

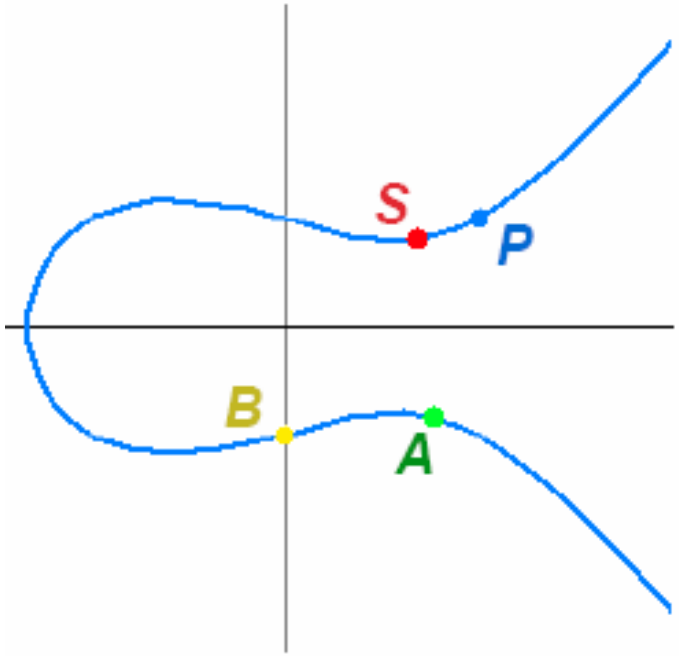


Indem man einen Punkt P n-mal zu sich selbst addiert, erhält man den Punkt Q= n P.

- Hat man umgekehrt nur das Ergebnis Q und den Basispunkt P vorgegeben, so besteht das diskrete Logarithmusproblem darin, den Faktor n zu berechnen.
- Diese Aufgabe ist bis heute nicht in kurzer Zeit lösbar.

Elliptische Kurven in der Kryptographie

Schlüsselaustausch nach Diffie-Hellman



- Alice und Bob einigen sich auf Punkt ***P***.
- Alice wählt *n* und schickt Bob ***A*** = *n* ***P***.
- Bob wählt *m* und schickt Alice ***B*** = *m* ***P***.
- Alice und Bob berechnen
  S = *n m* ***P*** = *n* ***B*** = *m* ***A***.
- Charly, der die beiden belauscht, kennt nur ***A***, ***B*** und ***P***, kann damit aber **nicht** den **geheimen Schlüssel *S*** bestimmen, denn dazu müsste er *n* oder *m* berechnen können.

Endlich erzeugte abelsche Gruppen

Hauptsatz 1

Elementarteilerversion

Es gibt ein $n \in \mathbb{N}$ dass $n_1, \ldots, n_k \in \mathbb{N}$

$$A \cong \mathbb{Z}^n \times \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z}$$

mit $2 \leq n_i$ und $n_i | n_{i+1}$ für jedes i.

Endlich erzeugte abelsche Gruppen

Hauptsatz 2

Zerlegung in Unzerlegbare

Es gibt paarweise verschiedene Primzahlen $p_1, \ldots, p_m$ und Werte $a_{i,j} \in \mathbb{N}$, so dass

$$\begin{aligned} A \cong \mathbb{Z}^n \times & \mathbb{Z}/p_1^{a_{1,1}}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_1^{a_{1,k_1}}\mathbb{Z} \\ & \times \\ & \mathbb{Z}/p_2^{a_{2,1}}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_2^{a_{2,k_2}}\mathbb{Z} \\ & \times \\ & \vdots \\ & \times \\ & \mathbb{Z}/p_m^{a_{m,1}}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_m^{a_{m,k_m}}\mathbb{Z}, \end{aligned}$$

mit $a_{i,l} \leq a_{i,l+1}$ für alle $l \in \{1, \ldots, k_i - 1\}$.

Mit Hilfe dieses Satzes kann man leicht alle endlichen abelschen Gruppen bis auf Isomorphie bestimmen.

Abelsche Gruppen der Ordnung

2	3	4	5	6	7
$\mathbb{Z}_2$	$\mathbb{Z}_3$	$\mathbb{Z}_4$ $\mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Z}_5$	$\mathbb{Z}_2 \times \mathbb{Z}_3$	$\mathbb{Z}_7$

8	9	10	11	12
$\mathbb{Z}_8$ $\mathbb{Z}_2 \times \mathbb{Z}_4$ $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Z}_9$ $\mathbb{Z}_3 \times \mathbb{Z}_3$	$\mathbb{Z}_2 \times \mathbb{Z}_5$	$\mathbb{Z}_{11}$	$\mathbb{Z}_3 \times \mathbb{Z}_4$ $\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

Chinesischer Restsatz

Beispiel

"Wie alt bist Du?" wird Daisy von Donald gefragt.

"So was fragt man eine Dame doch nicht" antwortet diese.

"Aber wenn Du mein Alter durch drei teilst, bleibt der Rest zwei."

"Und wenn man es durch fünf teilt?" "Dann bleibt wieder der Rest zwei.

Und jetzt sage ich Dir auch noch, dass bei Division durch sieben der Rest fünf bleibt.

Nun müßtest Du aber wissen, wie alt ich bin.

Chinesischer Restsatz

- X = 2 mod (3)
- X = 2 mod (5)
- X = 5 mod (7)

Chinesischer Restsatz

Eine **simultane Kongruenz** ganzer Zahlen ist ein System von linearen Kongruenzen

Satz:
Wenn $b_1, \ldots, b_k$ und $m_1, \ldots, m_k$ natürliche Zahlen sind mit $\mathrm{ggT}(m_i, m_j) = 1$ für alle $1 \leq i < j \leq k$, dann gibt es für $m = m_1 \cdot \ldots \cdot m_k$ genau ein $x \in \mathbb{Z}_m$ mit

$$x \equiv b_i \pmod{m_i} \qquad \text{für alle } i = 1, \ldots, k.$$

Chinesischer Restsatz

Lösungsverfahren

Es seien die paarweise teilerfremden Zahlen a_1, a_2,...,a_n gegeben. Um alle Zahlen x mit $x \equiv r_1 \bmod a_1$, $x \equiv r_2 \bmod a_2$, ...,$x \equiv r_n \bmod a_n$ zu finden, bestimme man die Zahl $a=a_1 \cdot a_2 \cdots a_n$ sowie die Zahlen $b_1:=a/a_1$, $b_2:=a/a_2$,...,$b_n:=a/a_n$. Dann bestimme man die Zahlen x_i in den Gleichungen $x_i \cdot b_i + y_i \cdot a_i = 1$ für i=1,...,n.

Dann gilt: $x=x_1 \cdot b_1 \cdot r_1 + \ldots + x_n \cdot b_n \cdot r_n + k \cdot a$

Chinesischer Restsatz

- AUFGABEN mit Maple
  Suche alle x mit
  a) $x \equiv 217 \bmod 373$ und $x \equiv 25 \bmod 251$
  b) $x \equiv 16 \bmod 88$ und $x \equiv 37 \bmod 55$
  c) $x \equiv 281 \bmod 389$ und $x \equiv 269 \bmod 457$
  d) $x \equiv 15 \bmod 88$ und $x \equiv 37 \bmod 55$

Ringe

Ringe

Definition Seien R eine Menge und +, * Verknüpfungen auf R .
R heißt Ring (mit Einselement), wenn gilt:

1. (R,+) ist abelsche Gruppe.
2. (R,*) ist Halbgruppe.
3. Es gelten $a*(b + c) = ab+ac$ und $(b+c)*a = ba + ca$
   für alle $a,b,c \in R$. (Distributivgesetze)
4. Es gibt ein Element $1 = 1_R \in R$ mit $1 \cdot a = a \cdot 1 = a$ für alle $a \in R$.

Der Ring heißt kommutativ, falls * **kommutativ** ist.

Im Folgenden sei R stets ein kommutativer Ring mit 1

Ringe

Wie allgemein üblich bei additiv notierter

Gruppenverknüpfung, bezeichnen wir das neutrale Element von $(R,+)$ mit **0** und

sprechen vom ***Nullelement*** oder der *Null* von R;

Das neutrale Element von $(R, \cdot)$

heißt ***Eins*** oder ***Einselement*** und wird in der Regel mit **1** bezeichnet,

zur besseren Unterscheidung manchmal auch

mit $\mathbf{1}_R$.

Ringe
Beispiele

1. Z ist kommutativer Ring mit Eins.
2. Der **Restklassenring Z_n** ist kommutativer Ring mit Eins.
3. Seien R ein kommutativer Ring mit 1und S eine nicht leere Menge,
   Abb(S,R) := { f: S → R Abbildung} .
   Abb(S,R) ist ein kommutativer Ring mit 1 mit den Verknüpfungen + und *

(f+g)(s):= f(s)+g(s) und (f*g)(s) := f(s)*g(s)

Ringe

Satz 1 (Vorzeichenregeln)**.** *Es seien R ein Ring und a, b Elemente von R. Dann*

gilt:

1. (a) $a0 = 0a = 0$*;*
2. (b) $a(-b) = (-a)b = -ab$*;*
3. (c) $(-a)(-b) = ab$*.*

Beweis klar

z.B. $a0+a0=a(0+0)=a0 \rightarrow a0 = 0$ (Addition mit –a0 auf beiden Seiten).

Ringe

Allgemein gilt für $x_i,\, y_j \in R$ $(1 \leq i \leq n,\ 1 \leq j \leq m,\ n, m \in \mathbb{N})$:

$$x_1 + \ldots + x_n = \sum_{i=1}^{n} x_i; \qquad x_1 \cdot \ldots \cdot x_n = \prod_{i=1}^{n} x_i \,.$$

Die leere Summe wird als 0, das leere Produkt als 1 definiert. letzteres natürlich nur, falls $1 \in R$ gilt. Wir erhalten dann:

$$\begin{aligned}
\left(\sum_{i=1}^{n} x_i\right)\left(\sum_{j=1}^{m} y_j\right) &= \sum_{i=1}^{n}\sum_{j=1}^{m} x_i y_j, \\
x^n &= \prod_{i=1}^{n} x, \\
x^{n+m} &= x^n \cdot x^m, \\
(x^n)^m = x^{nm}&, \\
(x+y)^n &= \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y_i
\end{aligned}$$

in kommutativen Ringen R mit 1.

Ringe

Definition.

- Das Element a des Ringes R heißt ein ***Nullteiler***, wenn es ein Element

  $b \in R$, $b \neq 0$, gibt mit $ab = 0$ oder $ba = 0$.

- Besitzt R keine von 0 verschiedenen Nullteiler, so heißt R ***nullteilerfrei***.

- Ist $R \neq 0$ ein nullteilerfreier, kommutativer Ring, dann heißt R ein ***Integritätsring*** (oder *Integritätsbereich*).

Ringe

Satz 2. *Ein kommutativer Ring R ist genau dann ein Integritätsring, wenn in*

ihm die Kürzungsregel

$$ab = ac,\ a \neq 0 \rightarrow b = c \text{ gilt.}$$

Beweis.

- „←“: Ist a ein Nullteiler, $ab = 0$ für $b \neq 0$, so ist die Kürzungsregel wegen $ab = a0$ sicherlich verletzt.
- „ →“: Für die Umkehrung hat man nur zu beachten, daß $a(b-c) = 0$, wenn $ab = ac$.

Beispiele für Integritätsringe

Satz Der Ring Z der ganzen Zahlen.ist ein Integritätsring

Satz Z_p, p Primzahl. Dann ist Z_p ein Integritätsring.

Beweis. Ist p Primzahl und $a \in Z$, $a \neq 0$ dann sind a und p teilerfremd, d.h ggT(a,p)=1. Dies ist äquivalent zu [a] ist invertierbar in Z_p. Sein [a]*[b]= [a]*[c] → [b] = [c] , denn aus

$[a]^{-1} *([a]*[b]) = [a]^{-1} *([a])*[c]) \rightarrow [b] = [c]$

Ringe

Definition: Die invertierbaren Elemente in dem Monoid

(R, *) heißen ***Einheiten*** von R.

Natürlich sind Einheiten niemals Nullteiler.

Die Menge aller Einheiten von R ist offensichtlich eine Gruppe bezüglich der Multiplikation von R, die

Einheitengruppe R* von R.

Beispiele:

- $Z^* = \{-1, 1\}$

Körper

Definition Ein **Körper** $(K,+,\cdot)$ besteht aus einer Menge K und zwei Verknüpfungen + und $\cdot$ auf K, für die gilt:

(a) $(K,+,\cdot)$ ist ein kommutativer Ring mit 1.

(b) Inverse Elemente: Zu jedem $a \in K$ mit $a \neq 0$ existiert ein $a^{-1} \in K$ mit

$$a^{-1} \cdot a = 1.$$

Satz. *Es sei $m \geq 2$. Dann sind die folgenden Eigenschaften äquivalent:*

(a) Z_m *ist ein Integritätsring.*

(b) Z_m *ist ein Körper.*

(c) *m ist Primzahl.*

Ohne Beweis: Da Z_m endlich ist, sind (a) und (b) äquivalent.

Ist m keine Primzahl, dann gibt es $a,b \in Z$ mit $1 < a, b < m$ und $m = ab$.

Bezeichnet can : $Z \rightarrow Z_m$ die natürliche Projektion, so hat man

$$\text{can}(a) \neq 0 \neq \text{can}(b),$$

aber $\text{can}(a)\,\text{can}(b) = \text{can}(m) = 0$; Z_m ist also kein Integritätsring.

Umgekehrt sei m Primzahl. Es gelte $\text{can}(a)\,\text{can}(b) = 0$ für $a,b \in Z$, also $\text{can}(ab) = 0$. Daraus folgt $ab \in Zm$. Da m Primzahl ist, folgt: m teilt a oder m teilt b*. Das bedeutet aber $\text{can}(a) = 0$ oder $\text{can}(b) = 0$. Z_m ist also Integritätsring.