Algebraische Strukturen

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

M.B. Wischnewsky
J. Zhao

30.01.2007

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 · 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

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

d.h. für die Einheitengruppe R* von R gilt

$$R^* = R\backslash\{0\}$$

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.*

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.

Körper

Beispiele

1. **Q** (die rationalen Zahlen), **R** (die rellen Zahlen).
2. Ist p eine Primzahl, so ist **Z**/p**Z** ein endlicher Körper.
   Z/2**Z** = {0,1} ist der kleinste Körper.

Primzahlen

Ein kurzer Überblick

„Primzahlen sind die Atome für die natürlichen Zahlen“

Die Mathematik ist die Königin der Wissenschaften, und die Zahlentheorie ist die Königin der Mathematik.

C.F. Gauß (1777-1855)

Primzahlentheorie in der Antike

- Es ist nicht genau bekannt, wann Menschen das erste Mal über Primzahlen nachdachten.
- Erstes Wissen über Primzahlen nachweisbar bei den antiken Griechen, genauer bei den Pythagoräern ca. 500-300 v.Chr.
- Um 300 v.Chr.: **Euklids Elemente Buch IX**: Der Beweis für die Existenz von unendlich vielen Primzahlen.
- 200 v.Chr.: Das **Sieb des Eratosthenes** (Algorithmus zur Bestimmung von Primzahlen bis zu einer Zahl x)

Das antike China

Die antiken Chinesen beschäftigten sich mit Primzahlen im Rahmen ihrer Zahlenmystik.

In der chinesischen Vorstellung waren ungerade Zahlen männlich und gerade weiblich. Ungerade Zahlen mit vielen Teilern galten als „unmännlich“. **Primzahlen galten** daher **als besonders männlich.**

Sieb des Eratosthenes

Beschreibung:

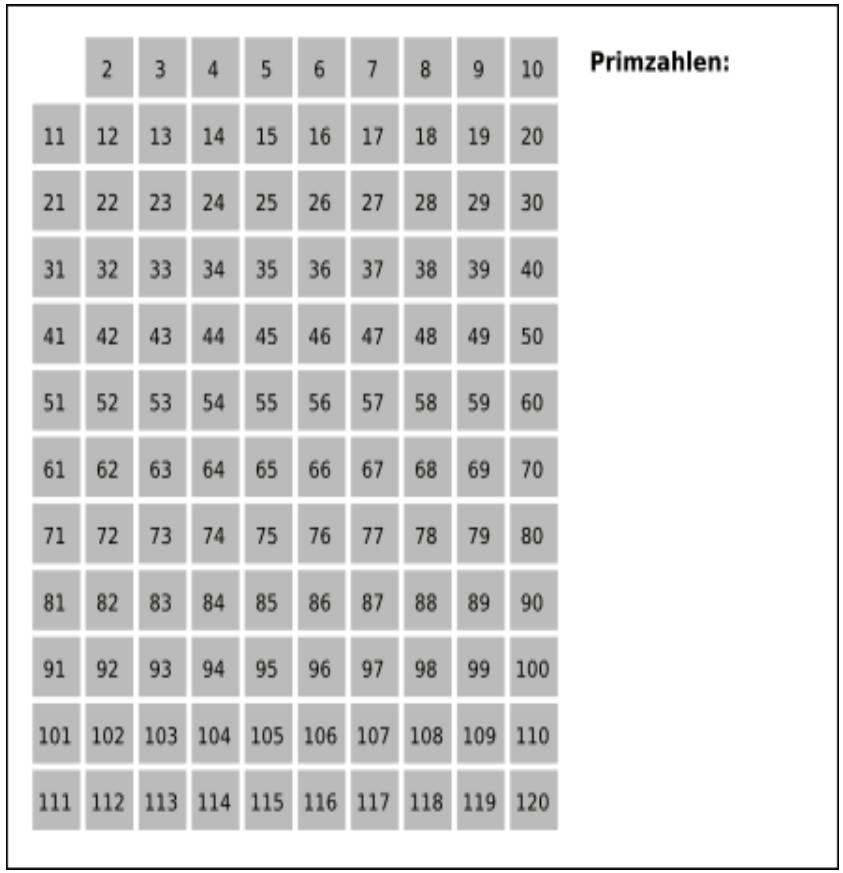
1. Initialisierung eines Zahlenfeldes von 2 bis einem Maximum m
2. n ist die jeweils zu verarbeitende Zahl.
   Sie wird mit 2 initialisiert.

3. Alle Vielfachen von n im Zahlenfeld werden markiert.
4. n wird auf die nächste unmarkierte Zahl gesetzt.

5. Schritte 3 und 4 werden solange wiederholt, bis $n>\sqrt{m}$

Abbruch bei Wurzel aus m, da alle Produkte aus n und kleineren Primzahlen bereits markiert.

Sieb des Eratosthenes



- Demonstration:

Es werden die Primzahlen zwischen 2 und 120 ermittelt. Erst werden alle Vielfache von 2 rot, dann von 3 grün, 5 blau und 7 gelb markiert. Damit ist die Grenze $\sqrt{120} \approx 10{,}95$ erreicht, denn die nächste freie Zahl ist 11.

Alle unmarkierten Plätze sind Primzahlen.

Das Sieb des Eratosthenes*

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

Die verbleibenden Zahlen sind nun alle Primzahlen zwischen 0 und 50

* sh. Vorlesung

Euklid von Alexandria

- Gelebt von ca. 330 bis ca. 275 v. Chr.
- „Die Elemente“ ein 13-bändiges Kompendium des damaligen Mathematik-Wissens

Es gibt unendlich viele Primzahlen.

Annahme: Es gibt nur endlich viel Primzahlen p_1, ..., p_n.

Betrachte nun n := p_1 * ... * p_n +1.

n ist nicht durch p_1, ..., p_n teilbar. Also muss n selbst Primzahl sein oder aus Primzahlen zusammen gesetzt sein, die von p_1, ..., p_n verschieden sind.

Widerspruch!

2 kleine Beispiele: 2*3+1=7

2*3*5*7*11*13+1=30031=59*509

Es gibt also unendlich viele Primzahlen.

Primzahltests

- **Probedivision**: eine Zahl n ist genau dann Primzahl, wenn sie keinen Teiler zwischen 1 und $\sqrt{n}$ hat. Man kann also versuchen, n durch alle kleineren Zahlen zu dividieren.
- Rechnet man (großzügig)
  1 Milliarde Divisionen pro Sekunde, so schafft man
  - pro Jahr etwa 3*10^16 Divisionen,
  - seit Entstehung der Welt also etwa 5*10^26 Divisionen.
- Man hätte in dieser Zeit also eine **53-stellige Zahl** testen können. In der Mathematik der Gegenwart untersucht man jedoch zum Teil Zahlen mit mehreren Millionen Stellen!

- Gibt es schnellere Verfahren?

Mersennesche Primzahlen

Definition Eine Primzahl P_m heißt Mersennesche Primzahl, wenn es eine Primzahl p gibt mit

$$P_m = 2^{p-1}$$

Bis ins Mittelalter glaubte man, dass für jede Primzahl p die Zahl = 2^{p-1} wieder prim ist. Man beachte aber, dass 2r-1 für eine zusammengesetzte Zahl r=st wegen:

2r-1=(2s-1)(2(t-1)s+2(t-2)s +...+2s+1) nicht prim ist.

#	p	Dezimalstellen von Pm	Entdeckung
5	13	4	**1456**
6	17	6	**1588**
7	19	6	**1588**
8	31	10	**1772**
9	61	19	**1883**
10	89	27	**1911**
11	107	33	**1914**
12	127	39	**1876**
13	521	157	**1952**
14	607	183	**1952**
15	1279	386	**1952**
16	2203	664	**1952**
17	2281	687	**1952**
18	3217	969	**1957**
19	4253	1281	**1961**
20	4423	1332	**1961**

#	p	Dezimalstellen von Pm	Entdeckung
30	132049	39751	**1983**
31	216091	65050	**1985**
32	756839	227832	**1992**
33	859433	258716	**1994**
34	1257787	378632	**1996**
35	1398269	420921	**1996**
36	2976221	895932	**1997**
37	3021377	909526	**1998**
38	6972593	2098960	**1999**
39	13466917	4053946	**2001**
40	20996011	6320430	**2003**
41	24036583	7235733	**2004**
42	25964951	7816230	**2005**
43	30402457	9152052	**2005**
44	32582657	9808358	**2006**

Die größte bekannte Primzahl bis 2006

- **44. bekannte Mersenne-Primzahl gefunden**
- Am **4. September** entdecken Dr. Curtis Cooper und Dr. Steven Boone, beide Professoren an der Central Missouri State Universität die 44. bekannte Mersenne Primzahl,

$$2^{32.582.657}-1.$$

- Diese Zahl hat **9808358 Dezimalstellen** und verpasst damit knapp das Preisgeld von 100000$.

- Der Electronic Frontier Foundation $100,000 Preis wird erst bei größer 10000000 Dezimalstellen (Quelle: www.Mersenne.org)

Die Goldbach-Vermutung

- Primzahlen sind durch eine *multiplikative* Eigenschaft defiiniert. Damit ist zunächst unklar, was passiert, wenn man Fragen über Primzahlen stellt, bei denen es um *Addition* geht. Das berühmteste offene Problem in diesem Zusammenhang ist zweifellos die *Goldbach-Vermutung*, benannt nach dem Mathematiker Goldbach aus dem 18. Jahrhundert:
- Stimmt es oder stimmt es nicht, dass jede gerade Zahl größer als 3 als Summe von zwei Primzahlen geschrieben werden kann?
  (Zum Beispiel ist 4 = 2 + 2, 6 = 3 + 3, 8 = 3 + 5, 10 = 5 + 5, 12 = 5 + 7, ...; geht das immer??) **Bemerkungen dazu:**

  - Das Problem scheint sehr schwierig zu sein, viele haben sich schon vergeblich daran versucht.
  - Wer es löst, wird schlagartig berühmt und reich.
  - Es gibt einen Roman zum Problem, der sehr lesenswert ist.

Konstruktion von Ringen

Unterringe

Definition Sei $(R,+,\cdot)$ ein Ring und $S \subset R$.
Dann ist $(S,+,\cdot)$ genau dann ein Ring, falls

(a) $(S, +)$ ist Untergruppe von $(R, +)$.

(b) $(S, \cdot)$ ist abgeschlossen:

$$a, b \in S \rightarrow a \cdot b \in S.$$

$(S,+,\cdot)$ heißt dann **Unterring** von $(R,+,\cdot)$.
In diesem Fall heißt
R **Oberring (Erweiterungsring)** von S.

Unterringe

Beispiel:

$(mZ,+,\cdot)$ ist Unterring in $(Z,+,\cdot)$, denn

(a) $(mZ, +)$ ist Untergruppe von $(Z, +)$.

(b) $(mZ, \cdot)$ ist abgeschlossen:

Seien $a, b \in mZ$:

Dann gibt es ganze Zahlen $q_1, q_2 \in Z$:

$a = q_1 m$, $b = q_2 m$

$\rightarrow a \cdot b = (q_1 m)(q_2 m) = (q_1 q_2)m \in mZ$.

Konstruktion von Ringen
Ideale

Es sei R ein Ring. $\mathfrak{a} \subseteq R$ *heißt* Linksideal *(bzw.* Rechtsideal*)*

von R, falls gilt:

(1) $\mathfrak{a}$ *ist Untergruppe von* $(R,+)$, *das heißt,* $\mathfrak{a} \neq \emptyset$ *und* $\mathfrak{a}+(-\mathfrak{a}) \subseteq \mathfrak{a}$.

(2) $\forall a \in \mathfrak{a}\ \forall x \in R\ :\ xa \in \mathfrak{a}$ *(bzw.* $ax \in \mathfrak{a}$*), das heißt,* $R\,\mathfrak{a} \subseteq \mathfrak{a}$ *(bzw.* $\mathfrak{a} \supseteq \mathfrak{a}\,R$*).*

$\mathfrak{a} \subseteq R$ *heißt* Ideal*, falls* $\mathfrak{a}$ *sowohl Links- als auch Rechtsideal ist.*

Konstruktion von Ringen
Ideale

Hilfssatz: Der Durchschnitt von Idealen ist wieder ein Ideal.

Definition: Sei A □ R eine Teilmenge,

(A) := ∩ { a ⊂ R; a ist ein Ideal und A ⊂ a}

heißt das **von A erzeugte Ideal in R**.

(A)Ist nach Definition das kleinste Ideal von R, dass A umfasst.
A Heißt Erzeugensystem von R, wenn R = (A).

Hilfssatz:

$Es\ sei\ \emptyset \neq A \subseteq R,$ R Ring. Dann besteht (A) aus allen endlichen Summen von Elementen der Form

$$n\,a,\ x\,a,\ a\,y,\ x\,a\,y\ \ mit\ a \in A,\ x, y \in R,\ n \in \mathbb{Z}.$$

Ideale

Satz: Es sei R ein Ring und A eine nichtleere Teilmenge von R

(1) $(A) = \left\{ \sum_{\text{endl.}} x_i \cdot a_i \cdot y_i \;\middle|\; x_i, y_i \in R,\ a_i \in A \right\}$ *für* $R \ni 1$;

(2) $(A) = \left\{ \sum_{\text{endl.}} x_i \cdot a_i + \sum_{\text{endl.}} m_j \cdot b_j \;\middle|\; x_i \in R,\ m_j \in \mathbb{Z},\ a_i, b_j \in A \right\}$
für R *kommutativ;*

(3) $(A) = \left\{ \sum_{\text{endl.}} x_i \cdot a_i \;\middle|\; x_i \in R,\ a_i \in A \right\}$ *für* R *kommutativ mit Eins.*

Hauptideale

Definition.

1) Ein Ideal a eines Ringes R heißt

- **Hauptideal**, falls a = (x) für ein x $\in$ R gilt.
- **endlich erzeugbar**, falls a = (A) mit A□R endlich gilt.
- Ein Integritätsring R heißt **Hauptidealring**, wenn jedes Ideal in R ein Hauptideal ist.

Beipiel **Z** ist ein Hauptidealring

Restklassenringe

Definition und Satz

Es sei R ein Ring mit Ideal $\mathfrak{a}$. Dann läßt sich $R/\mathfrak{a}$ mittels

$$(x+\mathfrak{a})+(y+\mathfrak{a}) =: (x+y)+\mathfrak{a}, (x+\mathfrak{a})(y+\mathfrak{a}) := xy+\mathfrak{a} \quad \forall x, y \in R$$

zu einem Ring machen, dem Faktorring $R/\mathfrak{a}$ oder Restklassenring R modulo $\mathfrak{a}$.

Restklassenringe
Bemerkungen

(1) Für $1 \in R$ ist $1 + \mathfrak{a}$ Einselement von $R/\mathfrak{a}$. R kommutativ $\Rightarrow$ $R/\mathfrak{a}$ kommutativ.

(2) Für $x - y \in \mathfrak{a}$ schreibt man $x \equiv y \bmod \mathfrak{a}$ ("kongruent"). Hierfür gelten die Regeln:

$$\left.\begin{array}{l} x \equiv y \bmod \mathfrak{a} \\ u \equiv v \bmod \mathfrak{a} \end{array}\right\} \Rightarrow x \dot{\pm} u \equiv y \dot{\pm} v \bmod \mathfrak{a}.$$

Für $R = \mathbb{Z}$ bedeutet die alte Schreibweise $x \equiv y \bmod n$ gerade $x \equiv y \bmod n\mathbb{Z}$, denn sämtliche Ideale von $\mathbb{Z}$ waren ja als Hauptideale nachgewiesen. Die spezielle Äquivalenzrelation $\equiv$ heißt Kongruenzrelation.

Ringhomorphismus

Definition. Es seien R; S zwei Ringe. Unter einem **Ringhomorphismus**

von R nach S versteht man eine Abbildung

$f : R \rightarrow S$ mit

$f(x + y) = f(x) + f(y)$;

$f(x \ y) = f(x) \ f(y) \ \forall x; y \in R$:

Homomorphiessatz

Bemerkungen

(1) Für Ringhomomorphismen f : R → S ist
f(R) Unterring von S;

$$\ker f = f^{-1}(0) \text{ Ideal in } R.$$

(2) Ist R ein Ring mit Ideal a, so ist

e: R →R/a : x → x+a

ein Ringepimorphismus, der sog.
kanonische Epimorphismus. Es ist ker(e) = a

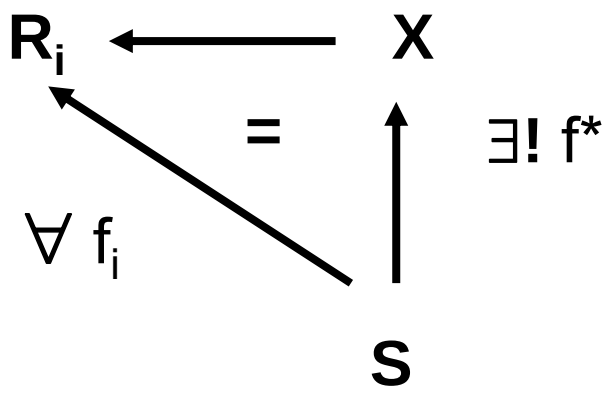
Homomorphiessatz: Für Ringhomomorphismen
f : R → S gilt: **R/a** ≅ **f(R**) mit a:= Ker(f)

Beweis analog zum Beweis für Gruppen

Produkt von Ringen*

- Sei $(\mathbf{R_i, i} \in I)$ eine Familie von Ringen.
- Ein Ring X zusammen mit einer Familie von Ringhomomorphismen p_i: X $\rightarrow R_i$ **heißt** Produkt **der** $(\mathbf{R_i, i} \in I)$, wenn folgendes gilt:
- Zu jedem Ring S und jeder Familie von Ringhomomorphismen
- **f_i : S $\rightarrow$ R_i existiert genau einen Ringhomom. f*: S $\rightarrow$ X mit**

$$\mathbf{p_i}^* \, f^* = f_i$$



* Definition analog zu Produkten von Mengen und Gruppen

Polynomringe

Sie sind die wichtigsten Ringe.

Definition Sei $(R,+,\cdot)$ ein Ring und $a_0, a_1, \ldots, a_n \in R$.

Dann nennen wir die Abbildung:

$$p : R \to R, \qquad x \mapsto \sum_{k=0}^{n} = a_k x^k$$

Polynom (¨über R).

Dabei ist $x^k := x \cdot x \cdot \ldots \cdot x$, k−mal. $a_0, \ldots, a_n$ heißen Koeffizienten von p.

Die Menge aller Polynome über R nennen wir **R[x].**

Polynomringe

Definition. Sei R ein Ring. Jedem Polynom P$\in$ R[X]. ordnen wir seinen **Grad**

grad(P) $\in$ N $\cup$ {$-\infty$ } zu durch die Vorschrift

$$\begin{aligned} \operatorname{grad} P &= n && \text{falls } P = a_n X^n + \ldots + a_0 \text{ mit } a_n \neq 0; \\ \operatorname{grad} P &= -\infty && \text{für } P \text{ das Nullpolynom.} \end{aligned}$$

Für ein von Null verschiedenes Polynom
$P = a_nX^n + \ldots + a_1X + a_0$ mit
n = grad P nennt man $a_n \in R\backslash 0$ seinen **Leitkoeffizienten**.
Ein Polynom heißt **normiert** genau dann, wenn sein Leitkoeffizient 1 ist.

Beispiel: $p(x) = 5x^3 - 1{,}3x + 6$ ist Polynom 3. Grades.

Polynomringe

Auf R[x] definieren wir eine Addititon und eine Multiplikation ”punktweise“

durch

$(p + q)(x) := p(x) + q(x)$

$(p \cdot q)(x) := p(x) \cdot q(x)$.

Satz ($R[x],+, \cdot)$ ist ein Ring, der **Polynomring über R**.

Polynomringe

Satz

Mit $p(x) = \sum_{k=0}^{n} a_k x^k, \qquad q(x) = \sum_{k=0}^{n} b_k x^k$ gilt:

$$(p+q)(x) = \sum_{k=0}^{n} (a_k + b_k) x^k$$

$$(p \cdot q)(x) = \sum_{k=0}^{n+n} \left(\sum_{\substack{i+j=k \\ 0 \le i,j \le n}} a_i b_j \right) x^k.$$

Polynomringe

Bemerkung: Sei R[X] der Polynomring einer Variablen X über R. dann gilt:

$$\text{grad}(f+g) \leq \max(\text{grad}(f), \text{grad}(g))$$

$$\text{grad}(f*g) \leq \text{grad}(f)+\text{grad}(g)$$

Polynomringe

Lemma. Ist R ein Integritätsring, so ist auch der Polynomring R[X] ein Integritätsring und es gilt grad(PQ) = grad P + gradQ. Weiter gilt:

$$R[X]^* = R^*$$

Beweis: Ist R nullteilerfrei, so ist offensichtlich der Leitkoeffizient von PQ das Produkt der Leitkoeffizienten von P und Q.

Teilbarkeit mit Rest in Polynomringen

Satz. *R sei ein kommutativer Ring, $g \in R[X]$, $g \neq 0$, und der Leitkoeffizient b von g sei eine Einheit in R.*

Dann gibt es zu jedem $f \in R[X]$ eindeutig bestimmte

Polynome $q, r \in R[X]$ mit

$$f = qg + r \text{ und } \operatorname{grad}(r) < \operatorname{grad}(g).$$

Euklidischer Algorithmus
Beispiel

Die algorithmische Bestimmung von *Quotient q* und *Rest r* lässt sich wie bei den ganzen Zahlen durchführen. Z.B. ist

$$
\begin{array}{rrrrrl}
(X^4 & +3X^3 & +2X^2 & -X & +4) & : (X^2-1) = X^2+3X+3 \ (=q) \\
-(X^4 & & -\ X^2) & & & \\
 & 3X^3 & +3X^2 & -X & +4 & \\
 & -(3X^3 & & -3X) & & \\
 & & 3X^2 & +2X & +4 & \\
 & & -(3X^2 & & -3) & \\
 & & & 2X & +7 & \qquad (=r).
\end{array}
$$