

---

## Ringe

Sei  $R$  eine Menge,  $+, \cdot : R \times R \rightarrow R$ . Es gebe  $0, 1 \in R$  mit

- $(R, +)$  ist eine abelsche Gruppe mit neutralem Element  $0$ .
- $(R \setminus \{0\}, \cdot)$  ist eine Halbgruppe mit neutralem Element  $1$ .
- Distributivgesetz:  $(a+b)c = ac+bc$  und  $c(a+b) = ca+cb$  für alle  $a, b, c \in R$ .

Dann heißt  $R$  ein Ring mit Nullelement  $0$  und Einselement  $1$ .

In einem Ring gilt:

1.  $0x = x0 = 0$ , denn wegen  $0+0=0$  folgt  $0x = (0+0)x = 0x+0x$  und damit  $0x = 0$  durch Kürzen. Analog geht man für  $x0$  vor.
2.  $(-x)y = x(-y) = -(xy)$ , denn  $xy + (-x)y = (x-x)y = 0y = 0$ , und analog mit  $x(-y)$ .
3.  $(-x)(-y) = xy$ , denn nach 2. gilt  $(-x)(-y) = -(-x)y = -(-(xy)) = xy$ .

---

## Ringe, Körper

Ist  $(R \setminus \{0\}, \cdot)$  abelsch, so heißt  $R$  kommutativ. Wir betrachten ab jetzt nur kommutative Ringe.

Die Elemente von  $R \setminus \{0\}$ , die in  $(R \setminus \{0\}, \cdot)$  invertierbar sind, heißen Einheiten von  $R$  und bilden eine Gruppe, die mit  $R^\times$  bezeichnet wird.

Sind  $a, b \in R \setminus \{0\}$  und  $c = ab$ , so nennen wir  $a, b$  Teiler von  $c$  und schreiben  $a \mid c$  und  $b \mid c$ . Gilt  $c = 0$ , so heißen  $a$  und  $b$  Nullteiler.

Ist  $R$  kommutativ und hat keine Nullteiler, so heißt  $R$  ein Integritätsring.

Ist  $R$  kommutativ und jedes Element ungleich Null invertierbar - also  $R^\times = R \setminus \{0\}$ , so heißt  $R$  ein Körper. Ein Körper ist auch ein Integritätsring (wegen  $a = (ab)b^{-1} = 0$  für  $ab = 0$ ).

---

## Ringe, Körper

Beispiel  $\mathbb{Z}$ :

- $\mathbb{Z}^\times = \{-1, 1\}$ .
- Keine Nullteiler.

Beispiel  $\mathbb{Z}/6\mathbb{Z}$ :

- Nullteiler  $(2+6\mathbb{Z}) \cdot (3+6\mathbb{Z}) = 0+6\mathbb{Z}$ .

Beispiel:  $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$  für  $p$  prim.

---

## Homomorphismen

Seien  $R, S$  Ringe und  $f : R \rightarrow S$ . Gilt  $f(a+b) = f(a)+f(b)$  und  $f(ab) = f(a)f(b)$  und  $f(1_R) = 1_S$  für alle  $a, b \in R$ , so heißt  $f$  ein Homomorphismus.

Epimorphismus = surjektiv.

Monomorphismus = injektiv.

Isomorphismus = bijektiv.

Endomorphismus =  $S = R$ .

Automorphismus =  $S = R$  und bijektiv.

Es gilt wie eben:

- $f(0_R) = 0_S, f(1_R) = 1_S$  (letzteres per Definition).
- $f(-a) = -f(a), f(a^{-1}) = f(a)^{-1}$ , wenn  $a^{-1}$  existiert.

---

## Unterringe, Ideale, Kern, Bild

Sei  $R$  ein Ring und  $U \subseteq R$  ein Ring. Stimmen Addition und Multiplikation von  $U$  mit der  $R$  überein und gilt  $1_U = 1_R$ , so heißt  $U$  ein Unterring von  $R$ .

Sei  $I \subseteq R$ . Wir schreiben  $RI = \sum_{a \in I} Ra = \{ \sum_{i=0}^n r_i a_i \mid r_i \in R, a_i \in I, n \in \mathbb{Z}^{\geq 0} \}$ . Gilt  $RI = I$ , so heißt  $I$  ein Ideal von  $R$ .

Für einen Homomorphismus  $f : R \rightarrow S$  definieren wir  $\ker(f) = f^{-1}(\{0_S\})$ . Dies ist ein Ideal von  $R$ .

- Sind  $a_i \in \ker(f)$  und  $r_i \in R$ , so gilt  $f(\sum_i r_i a_i) = \sum_i f(r_i) f(a_i) = 0$ , also  $\sum_i r_i a_i \in \ker(f)$  und  $R\ker(f) = \ker(f)$ .

Ähnlich ist  $\text{im}(f) = f(R)$  ein Unterring von  $S$ .

---

5

21. November 2006

---

## Faktoring

Sei  $R$  ein Ring und  $I$  ein Ideal von  $R$ .

Bezeichne  $R/I$  zunächst die Faktorgruppe der additiven Gruppen  $R$  und  $I$ .

Für  $a+I$  und  $b+I$  definieren wir  $(a+I) \cdot (b+I) = ab+I$ .

Dies ist wohldefiniert:

- Für  $a'+I = a+I$  und  $b'+I = b+I$  gibt es  $i_1, i_2 \in I$  mit  $a' = a + i_1$  und  $b' = b + i_2$ . Dann gilt  $a'b' = ab + ai_2 + bi_1 + i_1i_2 \in ab+I$  aufgrund der Idealeigenschaft, also  $a'b'+I = ab+I$ .

Einselement ist  $1_R + I$ .

Damit wird  $R/I$  zu einem Ring und  $f : R \rightarrow R/I, x \mapsto x+I$  zu einem Epimorphismus (Restklassenhomomorphismus).

Beispiel:  $R = \mathbb{Z}$  und  $I = 5\mathbb{Z}$ .  $I$  ist ein Ideal, und  $R/I = \mathbb{F}_5$  der Faktoring.

---

6

21. November 2006

---

## Isomorphiesatz

Thm: Ist  $f : R \rightarrow S$  ein Homomorphismus, so ist  $h : R/\ker(f) \cong \text{im}(f)$ ,  $x + \ker(f) \mapsto f(x)$  ein Isomorphismus.

Bew: Fassen wir  $R$  und  $S$  nur als additive abelsche Gruppen auf, ist der Satz bereits bewiesen. Wir müssen daher nur noch die Multiplikativität von  $h$  überprüfen. Es gilt  $h((x + \ker(f))(y + \ker(f))) = h(xy + \ker(f)) = f(xy) = f(x)f(y) = h(x + \ker(f))h(y + \ker(f))$ .  $\square$

---

7

21. November 2006

---

## Direktes Produkt

Sind  $R, S$  Ringe, so können wir  $R \times S$  durch

$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$  und  $(a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2)$  zu einem Ring machen.

Das Nullelement und Einselement sind hier  $(0, 0)$  bzw.  $(1, 1)$ .

Die Einheiten von  $R \times S$  sind genau die Paare, welche an der ersten und zweiten Koordinate eine Einheit zu stehen haben. Als Formel gilt also  $(R \times S)^\times = R^\times \times S^\times$ .

---

8

21. November 2006

---

## Euklidische Ringe

Sei  $R$  ein Integritätsring. Man nennt  $R$  einen euklidischen Ring, wenn es eine Gradfunktion  $d : R \setminus \{0\} \rightarrow \mathbb{Z}^{\geq 0}$  mit der folgenden Eigenschaft gibt: Zu  $a, b \in R$  und  $b \neq 0$  gibt es  $s, r \in R$  mit  $a = sb + r$  und  $r = 0$  oder  $d(r) < d(b)$  (Division mit Rest).

Beispiele:

- $\mathbb{Z}$  mit der Gradfunktion  $|\cdot|$ .
- $k[x]$  mit der Gradfunktion  $\deg$ .
- Jeder Körper mit der konstanten Gradfunktion 1.

Notation:  $s = a \operatorname{div} b$  und  $r = a \operatorname{mod} b$  (sofern  $s$  und  $r$  durch eine Zusatzregel eindeutig bestimmt sind).

---

9

21. November 2006

---

## Euklidische Ringe

Sei  $R$  ein euklidischer Ring mit Gradfunktion  $d$ .

Thm: Für jedes Ideal  $I$  von  $R$  gibt es ein  $b \in R$  mit  $I = Rb$  (das heißt  $I$  ist ein Hauptideal).

Bew: Ein Element  $b \in I \setminus \{0\}$  mit dem kleinsten  $d$ -Wert ist ein Erzeuger, da es jedes weitere Element  $a \in I$  teilt. Sonst hätte der Rest  $r = a - sb \in I \setminus \{0\}$  nämlich einen kleineren  $d$ -Wert.  $\square$

Sind  $a_1, a_2 \in R$ , so gibt es daher ein  $c \in R$  mit  $Rc = Ra_1 + Ra_2$ . Es gibt also  $\lambda_1, \lambda_2 \in R$  mit  $c = \lambda_1 a_1 + \lambda_2 a_2$  und  $c \mid a_1, c \mid a_2$ . Die Elemente  $\lambda_i$  können mit dem euklidischen Algorithmus ausgerechnet werden.

Die Verallgemeinerung auf  $n$  Elemente  $a_i$  ist induktiv möglich.

---

10

21. November 2006

---

## Euklidischer Algorithmus

Eingabe:  $a_1$  und  $a_2$  aus  $R$  mit  $a_1 a_2 \neq 0$ .

Ausgabe:  $c, \lambda_1, \lambda_2 \in R$  mit  $c = \lambda_1 a_1 + \lambda_2 a_2$  und  $c \mid a_1, c \mid a_2$ .

1.  $(u_1, u_2) \leftarrow (a_1, a_2)$ ,  $M \leftarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ . Im folgenden zusätzlich  $d(0) = -\infty$ .
2. Wenn  $d(u_1) > d(u_2)$ , dann vertausche  $u_1, u_2$  und die Spalten von  $M$ .
3. Wenn  $u_1 = 0$ , dann schreibe  $M = \begin{pmatrix} * & \lambda_1 \\ * & \lambda_2 \end{pmatrix}$ . Ausgabe von  $u_2, \lambda_1, \lambda_2$ .
4. Schreibe  $u_2 = su_1 + r$ . Setze  $u_2 \leftarrow r$  und subtrahiere das  $s$ -fache der ersten Spalte von  $M$  von der zweiten Spalte.
5. Gehe zu 2.

---

11

21. November 2006

---

## Euklidischer Algorithmus

Es gilt stets  $(u_1, u_2) = (a_1, a_2)M$  und  $M$  ist invertierbar in  $R^{2 \times 2}$ , da jede einzelne Transformation im Algorithmus invertierbar ist. Daher gilt stets  $(a_1, a_2) = (u_1, u_2)M^{-1}$  mit  $M^{-1} \in R^{2 \times 2}$  und  $Ru_1 + Ru_2 = Ra_1 + Ra_2$ .

Der Algorithmus terminiert, da in Schritt 4 der Wert  $d(u_1) + d(u_2)$  echt kleiner wird und somit irgendwann  $u_2 = 0$  wird.

Für  $u_1 = 0$  folgt  $Ru_2 = Ra_1 + Ra_2$ , und folglich ist  $u_2$  von der Form  $u_2 = \lambda_1 a_1 + \lambda_2 a_2$  mit  $u_2 \mid a_1$  und  $u_2 \mid a_2$ .

---

12

21. November 2006

---

## Primelemente und Faktorisierung

Sei  $c \in R \setminus (\{0\} \cup R^\times)$ . Folgt aus  $c \mid (ab)$  bereits  $c \mid a$  oder  $c \mid b$  für alle  $a, b \in R$ , so heißt  $c$  Primelement von  $R$ . Folgt aus  $c = ab$  bereits  $a \in R^\times$  oder  $b \in R^\times$ , so heißt  $c$  irreduzibel.

Thm: Sei  $R$  euklidisch.

i) Die Menge der Primelemente ist gleich der Menge der irreduziblen Elemente.

ii) Für jedes  $a \in R \setminus \{0\}$  gibt es  $u \in R^\times$ , Primelemente  $p_i$  und  $e_i \in \mathbb{Z}^{\geq 1}$  mit

$$a = u \prod_{i=1}^n p_i^{e_i}.$$

Die  $e_i$  und  $p_i$  (bis auf Elemente in  $R^\times$ ) sind eindeutig bestimmt.

Wir erhalten Funktionen  $v_{p_i} : R \setminus \{0\} \rightarrow \mathbb{Z}$  mit  $v_{p_i}(a) = e_i$ .

---

## Größter gemeinsamer Teiler

Sei  $c = \lambda_1 a_1 + \lambda_2 a_2$  die Ausgabe des euklidischen Algorithmus.

- Für  $d \mid a_1$  und  $d \mid a_2$  gilt wegen  $c = \lambda_1 a_1 + \lambda_2 a_2$  auch  $d \mid c$ . Daher ist  $c$  ein größter gemeinsamer Teiler von  $a_1$  und  $a_2$ , geschrieben  $c = \gcd\{a_1, a_2\}$ .
- Andererseits gilt  $\gcd\{a_1, a_2\} = \prod_i p_i^{\min\{v_{p_i}(a_1), v_{p_i}(a_2)\}}$ , wenn die  $p_i$  die in  $a_1 a_2$  vorkommenden Primelemente bezeichnen.
- Es gilt  $R \gcd\{a_1, a_2\} = Ra_1 + Ra_2$ .

Zwei Elemente  $a, b \in R$  heißen teilerfremd, wenn  $\gcd\{a, b\} = 1$  oder äquivalenterweise  $R = Ra + Rb$ .

$\gcd\{a_1, a_2\}$  ist (eigentlich) nur bis auf Einheiten eindeutig bestimmt.

---

## Kleinstes gemeinsames Vielfaches

Sei  $c = a_1 a_2 / \gcd\{a_1, a_2\} = \prod_i p_i^{\max\{v_{p_i}(a_1), v_{p_i}(a_2)\}}$ .

- Es gilt  $a_1 \mid c$  und  $a_2 \mid c$  und für jedes  $d \in R$  mit  $a_1 \mid d$  und  $a_2 \mid d$  folgt  $c \mid d$ . Damit ist  $c$  ein kleinstes gemeinsames Vielfaches von  $a_1$  und  $a_2$ , geschrieben  $c = \text{lcm}\{a_1, a_2\}$ .
- Es gilt entsprechend  $R \text{lcm}\{a_1, a_2\} = Ra_1 \cap Ra_2$ .
- Sind  $a_1$  und  $a_2$  teilerfremd, so folgt  $Ra_1 \cap Ra_2 = Ra_1 a_2$ .

---

## Beispiele

In  $\mathbb{Z}$  gilt  $\mathbb{Z}^\times = \{-1, 1\}$ . Die Primelemente sind  $\pm 2, \pm 3, \pm 5, \dots$

In  $k[x]$  gilt  $k[x]^\times = k^\times$ . Die Primelemente vom Grad eins sind  $u(x - x_0)$  für  $u \in k^\times$  und  $x_0 \in k$ .

In  $\mathbb{F}_2[x]$  ist  $x^2 + x + 1$  ein Primelement vom Grad zwei.

In  $\mathbb{Z}$  ist  $\pm 6$  ein ggT und  $\pm 210$  ein kgV von 42 und 30.

In  $k[x]$  gilt  $v_{x+1}(x^2 - 1) = 1$  und  $v_x(x^2 - 1) = 0$ .

Es gilt  $3\mathbb{Z} + 2\mathbb{Z} = \mathbb{Z}$  und  $2\mathbb{Z} \cap 3\mathbb{Z} = 2\mathbb{Z} \cdot 3\mathbb{Z} = 6\mathbb{Z}$ .