Wiederholung: Gruppe

Definition Gruppe

Eine *Gruppe* ist ein Tupel $(G, \circ)$ bestehend aus einer Menge G und einer Verknüpfung $\circ : G \times G \to G$ mit

1. **Neutrales Element:** $\exists! e \in G$ mit $e \circ g = g \circ e = g$ für alle $g \in G$.
2. **Inverses Element:** Für alle $g \in G$ existiert ein $g^{-1} \in G$ mit
$$g \circ g^{-1} = g^{-1} \circ g = e.$$
3. **Assoziativität:** Für alle $g, h, r \in G$ gilt $(g \circ h) \circ r = g \circ (h \circ r)$.

G heißt *abelsch* (kommutativ), falls $g \circ h = h \circ g$ für alle $g, h \in G$.

Beispiele für Gruppen

Bsp:

- $(\mathbb{Z}, +)$ ist eine abelsche Gruppe.
- $(\mathbb{Z}^n, +)$ ist eine abelsche Gruppe.
- $(\mathbb{N}, +)$ ist *keine* Gruppe.
- Die Bijektionen $\{1, \ldots, n\} \to \{1, \ldots, n\}$ bilden zusammen mit der Komposition von Funktionen die *symmetrische Gruppe S_n*.
  Für $n \geq 3$ ist S_n nicht abelsch:
  $$(123) \circ (13)(2) = (1)(23) \neq (12)(3) = (13)(2) \circ (123).$$
- Die invertierbaren $(n \times n)$-Matrizen über $\mathbb{Z}$ bilden eine Gruppe unter Matrixmultiplikation, bezeichnet als $GL(n, \mathbb{Z})$.
  Für $n \geq 2$ ist $GL(n, \mathbb{Z})$ nicht abelsch.

Wiederholung: Ringe und Ideale

Definition Ring

Ein *Ring* ist ein Tupel $(R, +, \cdot)$ bestehend aus einer Menge R und zwei assoziativen Verknüpfungen $+, \cdot : R \times R \to R$ mit

- $(R, +)$ ist eine abelsche Gruppe mit neutralem Element 0.
- $(R, \cdot)$ besitzt ein neutrales Element 1.
- **Distributivität:** Für alle $a, b, c \in R$ gilt

$$(a+b)c = ac + bc \text{ und } a(b+c) = ab + ac.$$

Statt $(R, +, \cdot)$ schreiben wir meist nur R.

Integritätsbereich

Definition

Ein Ring R heißt

- **kommutativer Ring** falls $a \cdot b = b \cdot a$ für alle $a, b \in R$.
- **Integritätsbereich** falls R kommutativ und Nullteiler-frei ist, d.h.
$$ab \neq 0 \text{ für } a, b \neq 0.$$
- **Schiefkörper** falls $(R \setminus \{0\}, \cdot)$ eine Gruppe ist.
- **Körper** falls R ein kommutativer Schiefkörper ist.

Bsp:

- $(\mathbb{Z}, +, \cdot)$ ist ein Integritätsbereich.
- $(\mathbb{Z}^{n \times n}, +, \cdot)$ ist ein Ring, der nicht kommutativ ist.
- Wir definieren den ganzzahligen Polynomring in einer Variablen
$$\mathbb{Z}[x] = \{\sum_{i=0}^{\infty} a_i x^i | a_i \in \mathbb{Z}, \text{ endlich viele } a_i \neq 0\}.$$
Dann ist $(\mathbb{Z}[X], +, \cdot)$ ein Integritätsbereich.
- $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sind Körper.

Ideale

Definition Ideal

Sei R ein Ring. $I \subseteq R$ heißt *Links-Ideal* (bzw. Rechts-Ideal), falls

- $(I, +)$ eine Gruppe ist,
- $R \cdot I \subseteq I$ (bzw. $I \cdot R \subseteq I$), d.h. $r \cdot f \in I$ für alle $r \in R, f \in I$.

I heißt *Ideal*, falls I sowohl Links- als Rechts-Ideal ist.

Notationen:

- Wird I von $f_1, \ldots, f_m$ erzeugt, so schreiben wir $I = \langle f_1, \ldots, f_m \rangle$.
- Für $m = 1$ heißt I ein Hauptideal.

Bsp:

- Im Ring $\mathbb{Z}$ sei $I_1 = \langle 6, 8 \rangle = \{a \cdot 6 + b \cdot 8 \mid a, b \in \mathbb{Z}\}$.
- I_1 ist ein Hauptideal, denn $I_1 = \langle 2 \rangle$.
- Im Ring $\mathbb{Q}[x]$ sei $I_2 = \langle 2x^2, x^4 \rangle = \{a \cdot 2x^2 + b \cdot x^4 \mid a, b \in \mathbb{Q}[x]\}$.
- I_2 ist ein Hauptideal, denn $I_2 = \langle x^2 \rangle$.

Teilbarkeit

Definition Teilbarkeit

Sei R ein Integritätsring und $a, b \in R$.

- Element a *teilt* b, falls $b = ac$ für ein $c \in R$. Wir schreiben $a \mid b$. Falls b nicht von a geteilt wird, schreiben wir $a \nmid b$.
- *Einheiten* R^* von R sind die Teiler der Eins, d.h.
$$R^* := \{u \in R \mid u \mid 1\}.$$
- Die Elemente a, b heißen *assoziert*, falls $a = bc$ für ein $c \in R^*$.

Bsp:

- In $\mathbb{Z}[X]$ gilt $-X - 1 \mid X^2 - 1$ und $\mathbb{Z}[X]^* = \{1, -1\}$.
- Ferner sind $X + 1$ und $-X - 1$ assoziiert.

Elementare Teilbarkeitsaussagen

Lemma Teilbarkeit

Sei R ein Integritätsring und $a, b \in R$. Dann gilt

1. $a \mid b \Rightarrow a \mid bd$
2. $a \mid b_1$ und $a \mid b_2 \Rightarrow a \mid d_1 b_1 + d_2 b_2$ für alle $d_1, d_2 \in R$
3. $a \mid b \Leftrightarrow da \mid db$
4. $a \mid b$ und $b \mid d \Rightarrow a \mid d$
5. $a \mid b$ und $b \mid a \Leftrightarrow a, b$ sind assoziiert.

Beweis: Übungsaufgabe.

Euklidische Ringe

Definition Euklidischer Ring

Sei R ein Integritätsring. R heißt *euklidisch*, falls eine Bewertungs-Funktion

$$N : R \setminus \{0\} \to \mathbb{N}_0$$

existiert, so dass für alle $a, b \in R$ mit $b \neq 0$ Elemente $q, r \in R$ existieren mit $a = qb + r$ und entweder $r = 0$ oder $N(r) < N(b)$.

Satz

Der Ring $\mathbb{Z}$ ist euklidisch.

Beweis:

- Wähle als Bewertungsfunktion den Betrag $N = |\cdot|$ und $q = \lfloor \frac{a}{b} \rfloor$.
- Damit gilt $r = a - qb = a - \lfloor \frac{a}{b} \rfloor b$ mit
$$0 \leq |r| < \max\{|a - (\tfrac{a}{b} - 1)b|, |a - (\tfrac{a}{b} + 1)b|\} = |b|.$$

Übung: Zeigen Sie, dass $\mathbb{Q}[X]$ euklidisch ist.

Die Gaußschen Zahlen besitzen euklidische Division.

Satz

Der Ring der Gaußschen Zahlen

$$\mathbb{Z}[i] := \mathbb{Z} \oplus i\mathbb{Z} = \{x + iy \mid x, y \in \mathbb{Z}\} \subset \mathbb{Q}[i] \subset \mathbb{C}$$

ist euklidisch.

Beweis:

- Sei $z = x + iy \in \mathbb{Z}[i]$ mit konjugiert Komplexem $\bar{z} = x - iy$.
- Wir definieren eine Berwertungsfunktion vermöge der Norm
$$N(z) := z\bar{z} = |z|^2.$$
- Offenbar gilt
$$N(z) = (x + iy)(x - iy) = x^2 + y^2 \geq 0 \text{ und } N(z) = 0 \Leftrightarrow z = 0.$$
- Die Normfunktion ist multiplikativ, denn
$$N(wz) = wz\overline{wz} = w\bar{w}z\bar{z} = N(w)N(z).$$

Die Gaußschen Zahlen besitzen euklidische Division.

Beweis: (Fortsetzung)

- Seien $a, b \in \mathbb{Z}[i]$. Wir berechnen $c = \frac{a}{b} = u + iv \in \mathbb{Q}[i]$.
- Wir definieren $q = \lfloor u \rceil + i \lfloor v \rceil \in \mathbb{Z}[i]$. Es folgt
$$N(c-q) = |c-q|^2 \leq (\tfrac{1}{2})^2 + (\tfrac{1}{2})^2 = \tfrac{1}{2}.$$
- Wir definieren $r = a - bq$. Damit folgt
$$N(r) = N(a-bq) = N(cb-bq) = N(c-q) \cdot N(b) < N(b).$$

Bsp:

- Sei $a = 3 - 2i$ und $b = 1 - 2i$. Dann folgt $b^{-1} = \frac{1}{5}(1+2i) \in \mathbb{Q}[i]$.
- Damit ist $c = \frac{1}{5}(7+4i) \in \mathbb{Q}[i]$ und wir runden zu $q = 1 + i \in \mathbb{Z}[i]$.
- Für $r = a - bq = (3-2i) - (1-2i)(1+i) = -i$ gilt
$$N(r) = 1 < 5 = N(b).$$

Übung: Zeigen Sie mittels Normfunktion $N(\cdot)$, dass $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.