2. Oktober 2019

ANHANG ZUR EINFÜHRUNG IN DIE ALGEBRA (WS 19/20, BONN)

JAN SCHRÖER

ZUSAMMENFASSUNG. In diesem Anhang zum Skript der Vorlesung *Einführung in die Algebra* finden Sie die benötigen Vorkenntnisse, einige kurze historische Notizen und ein Literaturverzeichnis.

INHALTSVERZEICHNIS

Anhang A. **Körper**

A.1. **Körperaxiome.** Ein **Körper** ist eine Menge K zusammen mit zwei Abbildungen

$$+\colon K \times K \to K$$

$$(a, b) \mapsto a + b$$

und

$$\cdot\colon K \times K \to K$$

$$(a, b) \mapsto a \cdot b$$

so dass folgende Regeln (Axiome) gelten:

(A1) $a+(b+c) = (a+b)+c$ für alle $a, b, c \in K$ (**Assoziativität der Addition**);

(A2) $a + b = b + a$ für alle $a, b \in K$ (**Kommutativität der Addition**);

(A3) Es existiert ein Element $0 = 0_K \in K$ mit $a + 0 = a$ für alle $a \in K$ (Existenz eines **Nullelements**);

(A4) Zu jedem $a \in K$ gibt es ein $-a \in K$ mit $a + (-a) = 0$ (Existenz eines **additiven Inversen**);

(M1) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ für alle $a, b, c \in K$ (**Assoziativität der Multiplikation**);

(M2) $a \cdot b = b \cdot a$ für alle $a, b \in K$ (**Kommutativität der Multiplikation**);

(M3) Es existiert ein Element $1 = 1_K \in K$ mit $1 \neq 0$ und $1 \cdot a = a$ für alle $a \in K$ (Existenz eines **Einselements**);

(M4) Zu jedem $a \in K$ mit $a \neq 0$ gibt es ein Element a^{-1} mit $a \cdot a^{-1} = 1$ (Existenz eines **multiplikativen Inversen**);

(D) $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ für alle $a, b, c \in K$ (**Distributivität**).

Die Abbildungen $+$ und $\cdot$ heißen **Addition** bzw. **Multiplikation**.

Beachte: Um Klammern zu sparen, legen wir fest: Punktrechnung geht vor Strichrechnung. Z.B. in (D) können wir dann schreiben $a \cdot c + b \cdot c$, ohne dass Verwirrung entsteht.

Sei K ein Körper. Für $a \neq 0$ sei

$$\frac{1}{a} := a^{-1}.$$

Für $a, b \in K$ mit $b \neq 0$ sei

$$\frac{a}{b} := a/b := a \cdot b^{-1}.$$

Für $a, b \in K$ sei $a - b := a + (-b)$ und $ab := a \cdot b$.

Wir definieren $K^\times := K \setminus \{0\}$.

A.2. **Beispiele von Körpern.**

(i) $\mathbb{Q}$ und $\mathbb{R}$ mit den üblichen Abbildungen $+$ und $\cdot$ sind Körper.

(ii) $\mathbb{Z}$ mit den üblichen Abbildungen $+$ und $\cdot$ ist kein Körper. (Nur (M4) ist nicht erfüllt.)

(iii) Sei $K := \mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subset \mathbb{R}$, und definiere

$$+\colon K \times K \to K \quad \text{und} \quad \cdot\colon K \times K \to K$$

durch

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) := (a + c) + (b + d)\sqrt{2}$$

und

$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) := (ac + 2bd) + (ad + bc)\sqrt{2}.$$

(Dies entspricht der üblichen Addition und Multiplikation aus $\mathbb{R}$.) Dann ist $(K, +, \cdot)$ ein Körper. Ein Element $a + b\sqrt{2}$ in $K^\times$ hat sicherlich ein Inverses in $\mathbb{R}$, man muss aber hier zeigen, dass dieses Inverse auch in K liegt. Behauptung:

$$(a + b\sqrt{2})^{-1} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}.$$

Dies folgt aus der Rechnung

$$\frac{1}{a + b\sqrt{2}} = \frac{1}{a + b\sqrt{2}} \cdot \frac{a - b\sqrt{2}}{a - b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}.$$

Wir haben stillschweigend verwendet, dass $\mathbb{R}$ nullteilerfrei ist (d.h. $a \cdot b = 0$ genau dann wenn $a = 0$ oder $b = 0$), und dass $a + b\sqrt{2} \neq 0$ genau dann wenn $a - b\sqrt{2} \neq 0$.

(iv) $\mathbb{C}$, der Körper der komplexen Zahlen (wird später definiert).

(v) Sei $K := \{a, b\}$ wobei $+$ und $\cdot$ definiert sind durch

$$\begin{aligned} a + a &= a, & a \cdot a &= a, \\ a + b &= b, & a \cdot b &= a, \\ b + a &= b, & b \cdot a &= a, \\ b + b &= a, & b \cdot b &= b. \end{aligned}$$

Dann ist K ein Körper. Das Element a ist die 0 von K, und b ist die 1 von K.

A.3. **Charakteristik eines Körpers.** Sei K ein Körper. Für $a \in K$ und $0 \neq m \in \mathbb{N}$ sei

$$m \cdot a := \underbrace{a + a + \cdots + a}_{m \text{ mal}}$$

Sei $\mathrm{char}(K) := 0$, falls $m \cdot 1_K \neq 0$ für alle $0 \neq m \in \mathbb{N}$, und andernfalls sei $\mathrm{char}(K) := \min\{0 \neq m \in \mathbb{N} \mid m \cdot 1_K = 0\}$. Wir nennen $\mathrm{char}(K)$ die **Charakteristik** von K.

Lemma A.1. *Sei K ein Körper mit $\mathrm{char}(K) = p > 0$, dann ist p eine Primzahl.*

Beweis. Angenommen es gibt $p_1, p_2 \in \mathbb{N}$ mit $p_1, p_2 \geq 2$ und $p = p_1 p_2$. Nach der Definition von $\mathrm{char}(K)$ folgt $p_1 \cdot 1_K \neq 0$ und $p_2 \cdot 1_K \neq 0$. Also gilt $(p_1 \cdot 1_K) \cdot (p_2 \cdot 1_K) = (p_1 p_2) \cdot 1_K = p \cdot 1_K = 0$. Wegen der Nullteilerfreiheit von K (Übungsaufgabe) gilt $p_1 \cdot 1_K = 0$ oder $p_2 \cdot 1_K = 0$. Widerspruch. □

A.4. **Die Ringe $\mathbb{Z}_m$.** Ein **Ring** ist eine Menge R zusammen mit zwei Abbildungen

$$+ \colon R \times R \to R$$

$$(a, b) \mapsto a + b$$

und

$$\cdot \colon R \times R \to R$$

$$(a, b) \mapsto a \cdot b$$

so dass folgende Regeln (Axiome) gelten:

(A1) $a + (b + c) = (a + b) + c$ für alle $a, b, c \in R$ (**Assoziativität der Addition**);

(A2) $a + b = b + a$ für alle $a, b \in R$ (**Kommutativität der Addition**);

(A3) Es existiert ein Element $0 = 0_R \in R$ mit $a + 0 = a$ für alle $a \in R$ (Existenz eines **Nullelements**);

(A4) Zu jedem $a \in R$ gibt es ein $-a \in R$ mit $a + (-a) = 0$ (Existenz eines **additiven Inversen**);

(R1) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ für alle $a, b, c \in R$ (**Assoziativität der Multiplikation**);

(R2) Es existiert ein Element $1 = 1_R \in R$ mit $1 \cdot a = a \cdot 1 = a$ für alle $a \in R$ (Existenz eines **Einselements**);

(D) $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ und $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ für alle $a, b, c \in R$ (**Distributivität**).

Ein Ring R heißt **kommutativ**, falls zusätzlich $a \cdot b = b \cdot a$ für alle $a, b \in R$ gilt.

Wir folgen wieder der klammersparenden Konvention *Punktrechnung vor Strichrechnung.*

Lemma A.2. *Seien $a, m \in \mathbb{N}$ mit $m \geq 1$. Dann existieren eindeutig bestimmte Elemente $r, q \in \mathbb{N}$ mit $0 \leq r < m$ und $a = q \cdot m + r$. Setze $r_m(a) := r$.*

Sei $m \in \mathbb{N}$ mit $m \geq 2$, und sei

$$\mathbb{Z}_m := \{0, 1, 2, \ldots, m - 1\}.$$

Für $a, b \in \mathbb{Z}_m$ sei $a + b := r_m(a + b)$ und $a \cdot b := r_m(a \cdot b)$

Lemma A.3. $(\mathbb{Z}_m, +, \cdot)$ *ist ein kommutativer Ring.*

Lemma A.4. $(\mathbb{Z}_m, +, \cdot)$ *ist ein Körper genau dann wenn* m *eine Primzahl ist.*

Beweis. Angenommen $\mathbb{Z}_m$ ist ein Körper. Dann gilt $\mathrm{char}(\mathbb{Z}_m) = m$. Nach Lemma A.1 ist m eine Primzahl.

Für die Umkehrung nehmen wir an, dass m eine Primzahl ist. Wir zeigen zuerst, dass dann $\mathbb{Z}_m$ nullteilerfrei ist:

Seien $a, b \in \mathbb{Z}_m$ mit $a \cdot b = 0$, also $r_m(a \cdot b) = 0$. Dann ist $a \cdot b$ durch m teilbar. Da m eine Primzahl ist, folgt: m teilt a oder m teilt b. Damit ist aber $a = 0$ oder $b = 0$, da $0 \leq a, b \leq m - 1$. Also haben wir gezeigt, dass $\mathbb{Z}_m$ nullteilerfrei ist.

Sei nun $a \in \mathbb{Z}_m$ mit $a \neq 0$. Definiere eine Abbildung

$$\begin{aligned} \rho_a \colon \mathbb{Z}_m &\to \mathbb{Z}_m \\ x &\mapsto x \cdot a. \end{aligned}$$

Dann ist ρ_a injektiv: Sei $\rho_a(x) = \rho_a(y)$. Also $xa = ya$. Es folgt, dass $(x - y)a = 0$. Wegen der Nullteilerfreiheit von $\mathbb{Z}_m$ gilt dann $x - y = 0$. Damit ist aber $x = y$.

Da $\mathbb{Z}_m$ eine endliche Menge ist, ist ρ_a auch surjektiv. Also sind die Elemente $0a, 1a, \ldots, (m-1)a$ paarweise verschieden. Insbesondere gilt: Es gibt ein $x \in \mathbb{Z}_m$ mit $xa = 1$. Daraus folgt aber Axiom (M4). Mit Lemma A.3 ist $\mathbb{Z}_m$ also ein Körper. □

Ist p eine Primzahl, so schreiben wir auch $\mathbb{F}_p$ statt $\mathbb{Z}_p$.

Anhang B. **Komplexe Zahlen**

B.1. **Komplexe Zahlen.**

B.1.1. *Definition.* Wir definieren nun den Körper $\mathbb{C}$ der **komplexen Zahlen**. Als zugrunde liegende Menge nehmen wir

$$\mathbb{C} := \mathbb{R} \times \mathbb{R}.$$

Für $(a, b), (c, d) \in \mathbb{C}$ sei

$$\begin{aligned} (a, b) + (c, d) &:= (a + c, b + d), \\ (a, b) \cdot (c, d) &:= (ac - bd, ad + bc). \end{aligned}$$

Man prüft nun leicht, dass $\mathbb{C}$ zusammen mit den oben definierten Operationen $+$ und $\cdot$ ein Körper ist.

Das Einselement 1 von $\mathbb{C}$ ist $(1, 0)$, und das Nullelement 0 von $\mathbb{C}$ ist $(0, 0)$.

Abkürzend schreibt man auch $\mathbf{i} := (0,1)$ und $a + b\mathbf{i}$ statt (a,b). Es gilt dann

$$\mathbf{i}^2 = -1 \quad \text{und} \quad a + b\mathbf{i} = (a,0) + (b,0)i.$$

Für $z = a + b\mathbf{i}$ seien $\mathrm{Re}(z) := a$ und $\mathrm{Im}(z) := b$ der **Realteil** bzw. der **Imaginärteil** von z.

Für $z = a + b\mathbf{i} \in \mathbb{C}$ sei

$$|z| := \sqrt{a^2 + b^2}$$

der **Betrag** von z. Stellt man sich z in der Ebene $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ vor, so ist $|z|$ einfach die *Länge* von z.

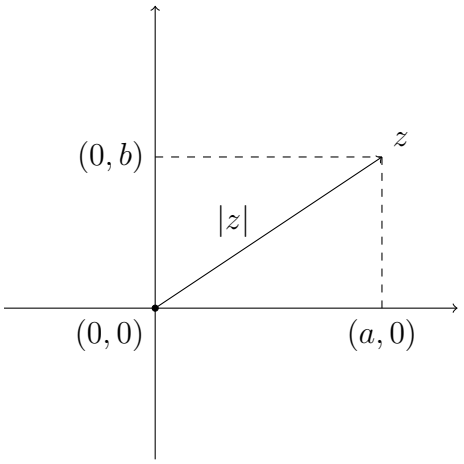

Abbildung 1. Betrag einer komplexen Zahl $z = a + b\mathbf{i}$.

B.1.2. *Komplexe Zahlen als reelle Matrizen.* Ordnet man nun $(a,b) \in \mathbb{C}$ die Matrix

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in M_2(\mathbb{R})$$

zu, so entspricht die Addition und Multiplikation in $\mathbb{C}$ genau der Addition und Multiplikation in $M_2(\mathbb{R})$. Nämlich für $(a,b),(c,d) \in \mathbb{C}$ erhalten wir

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} a+c & -b-d \\ b+d & a+c \end{pmatrix}$$

und

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} ac-bd & -ad-bc \\ ad+bc & ac-bd \end{pmatrix}.$$

B.1.3. *Komplexe Zahlen als reeller Vektorraum.*

Lemma B.1. $\mathbb{C}$ *ist ein* $\mathbb{R}$*-Vektorraum mit Basis* $\{1, \mathbf{i}\}$.

Beweis. Die Skalarmultiplikation auf $\mathbb{C}$ ist gegeben durch die Abbildung

$$\mathbb{R} \times \mathbb{C} \to \mathbb{C}$$
$$(a, z) \mapsto (a, 0) \cdot z.$$

Zusammen mit der Addition des Körpers $\mathbb{C}$ erhalten wir damit eine $\mathbb{R}$-Vektorraumstruktur auf $\mathbb{C}$. Man sieht nun leicht, dass $\{1, \mathbf{i}\}$ linear unabhängig ist und $\mathbb{C}$ erzeugt. □

Wir fassen zuweilen $\mathbb{R}$ als Teilmenge von $\mathbb{C}$ auf vermöge der Einbettung $a \mapsto (a, 0)$.

Der Betrag von $a \in \mathbb{R}$ ist dann

$$|a| = \begin{cases} a & : \text{ falls } a \geq 0, \\ -a & : \text{ falls } a < 0. \end{cases}$$

B.1.4. *Komplexe Konjugation.* Wir definieren die **komplexe Konjugation**

$$\overline{\cdot} \colon \mathbb{C} \to \mathbb{C}$$

durch $(a, b) \mapsto \overline{(a, b)} := (a, -b)$.

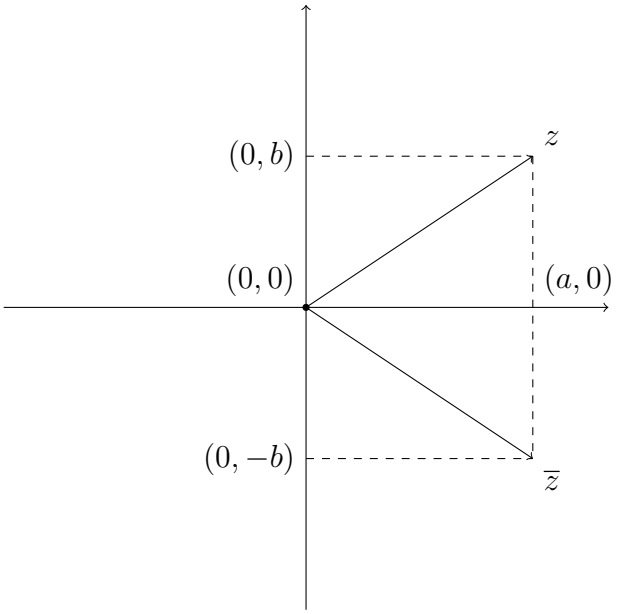

Abbildung 2. Komplexe Konjugation von $z = (a, b) = a + b\mathbf{i} \in \mathbb{C}$.

B.1.5. *Rechenregeln.*

(i) Für $z_1, z_2 \in \mathbb{C}$ gilt $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ und $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$.
(ii) Für $z = a + b\mathbf{i} \in \mathbb{C}$ gilt $z + \overline{z} = 2a$ und $z - \overline{z} = 2b\mathbf{i}$.
(iii) Für $z \in \mathbb{C}$ gilt $|z| = |\overline{z}|$.
(iv) Für $z_1, z_2 \in \mathbb{C}$ gilt $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$.

(v) Für $z = a + b\mathbf{i}$ gilt
$$z \cdot \overline{z} = a^2 + b^2 = |z|^2.$$

(vi) Für $z = (a, b) \in \mathbb{C}^\times$ gilt
$$z^{-1} = (\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}) = \frac{1}{a^2+b^2}(a, -b).$$
In Matrixschreibweise
$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}^{-1} = \frac{1}{a^2+b^2}\begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

B.2. **Trigonometrische Funktionen.** Für $x \in \mathbb{R}$ definieren wir
$$\sin(x) := \sum_{n=0}^{\infty}(-1)^n\frac{x^{2n+1}}{(2n+1)!}, \qquad \cos(x) := \sum_{n=0}^{\infty}(-1)^n\frac{x^{2n}}{(2n)!},$$

Sei
$$\arcsin\colon [-1,1] \to [-\frac{\pi}{2}, \frac{\pi}{2}]$$
die Umkehrfunktion der bijektiven Einschränkungsabbildung
$$\sin\colon [-\frac{\pi}{2}, \frac{\pi}{2}] \to [-1,1],$$
und sei
$$\arccos\colon [-1,1] \to [0,\pi]$$
die Umkehrfunktion der bijektiven Einschränkungsabbildung
$$\cos\colon [0,\pi] \to [-1,1].$$
Eigenschaften:
$$\begin{aligned} \sin(-x) &= -\sin(x), & \sin(x+y) &= \sin(x)\cos(y) + \cos(x)\sin(y), \\ \cos(-x) &= \cos(x), & \cos(x+y) &= \cos(x)\cos(y) - \sin(x)\sin(y), \\ & & 1 &= \sin^2(x) + \cos^2(x). \end{aligned}$$

Für $z \in \mathbb{C}$ setze
$$\exp(z) := \sum_{n=0}^{\infty}\frac{z^n}{n!}.$$
Für $x \in \mathbb{R}$ gilt dann
$$\exp(\mathbf{i}x) = \cos(x) + \sin(x)\mathbf{i}.$$
Die Menge
$$\mathbb{S}^1 := \{\exp(\mathbf{i}x) \mid x \in \mathbb{R}\} = \{\exp(\mathbf{i}x) \mid x \in [0, 2\pi)\}$$
ist der *Einheitskreis* in $\mathbb{R}^2$, d.h. alles Elemente in $\mathbb{R} \times \mathbb{R}$ mit *Abstand* 1 von $(0,0)$. (Zum Abstandsbegriff kommen wir später.)

Die Funktionen $\sin(-)$, $\cos(-)$ und $\exp(\mathbf{i}-)$ sind 2π-periodisch, d.h. für $f \in \{\sin(-), \cos(-), \exp(\mathbf{i}-)\}$ gilt
$$f(x + 2\pi) = f(x)$$
für alle $x \in \mathbb{R}$.

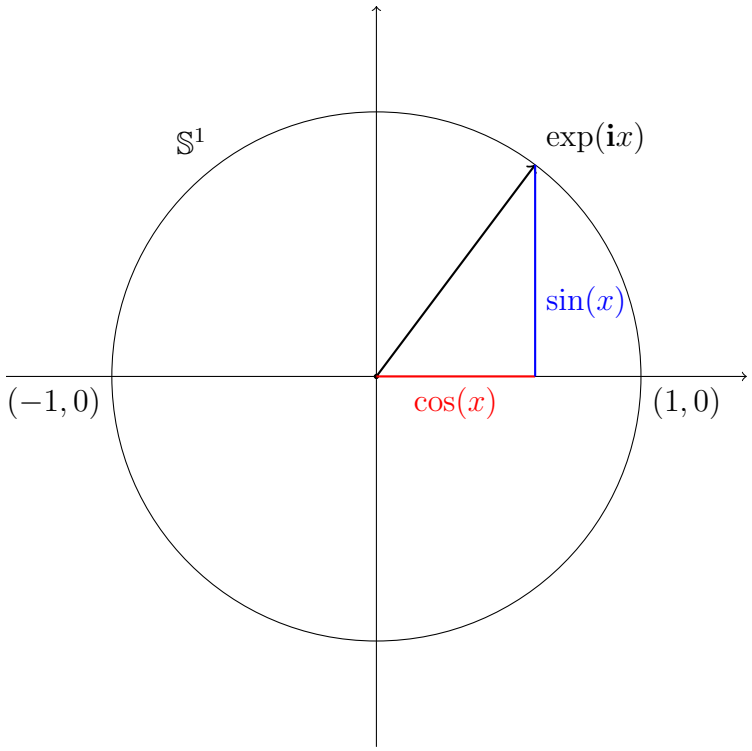

ABBILDUNG 3. Die komplexe Zahl $\exp(\mathbf{i}x) = \cos(x) + \sin(x)\mathbf{i}$.

B.3. **Polarkoordinaten.** Sei $z = a + b\mathbf{i} \in \mathbb{C}^\times$. Setze $r := |z| = \sqrt{a^2 + b^2}$. Es gibt dann ein eindeutig bestimmtes $\alpha \in [0, 2\pi)$ mit

$$z = r\exp(\mathbf{i}\alpha),$$

d.h. wir erhalten z indem wir den Vektor $(r, 0) \in \mathbb{C} = \mathbb{R}\times\mathbb{R}$ gegen den Uhrzeigersinn um den Winkel α drehen. Es gilt dann

$$a = r\cos(\alpha), \qquad b = r\sin(\alpha).$$

Die Zuordnung $(a, b) \mapsto (r, \alpha)$ definiert eine Bijektion

$$\mathbb{C}^\times \to \mathbb{R}_{>0} \times [0, 2\pi)$$

wobei $\mathbb{R}_{>0} := \{r \in \mathbb{R} \mid r > 0\}$. Das Paar (r, α) sind dann die **Polarkoordinate** von $z = a + b\mathbf{i}$. Als Konvention hat $0 \in \mathbb{C}$ die Polarkoordinate $(0, 0)$.

Für $r, s > 0$ und $\alpha, \beta \in [0, 2\pi)$ gelten die Regeln

$$r\exp(\mathbf{i}\alpha) \cdot s\exp(\mathbf{i}\beta) = rs \cdot \exp(\mathbf{i}(\alpha + \beta)),$$
$$(r\exp(\mathbf{i}\alpha))^{-1} = r^{-1}\exp(\mathbf{i}(-\alpha)).$$

B.4. **Warum komplexe Zahlen?** Sei $K[X]$ der Polynomring in einer Variablen X mit Koeffizienten in K. Die Elemente in $K[X]$ sind also Ausdrücke der Form

$$f = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$$

wobei $a_0, \ldots, a_n \in K$.

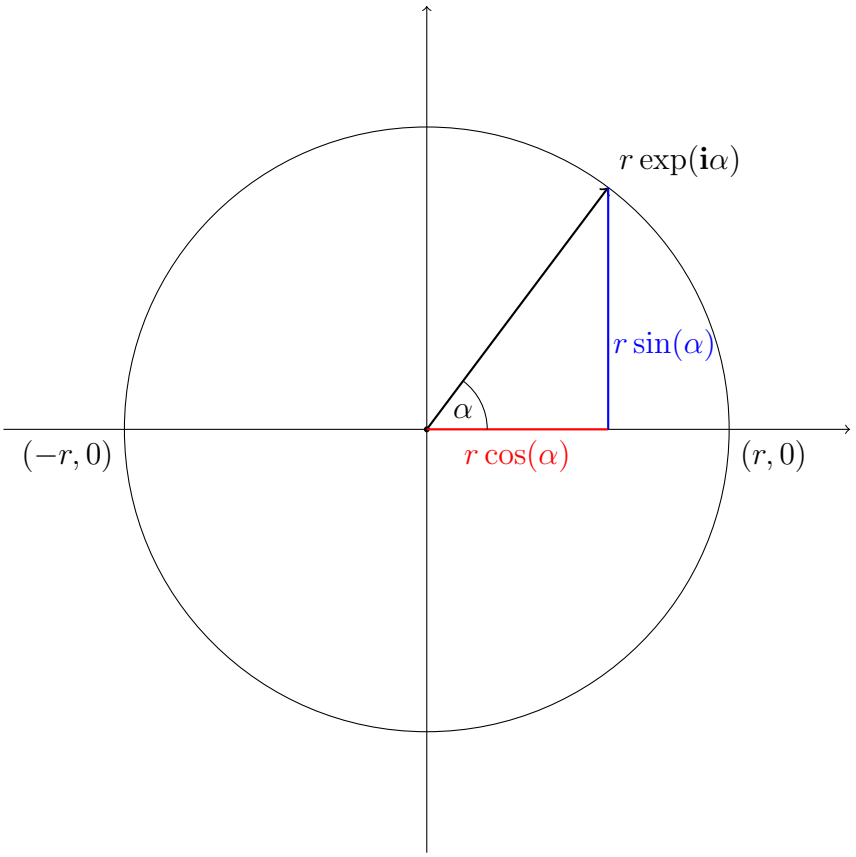

ABBILDUNG 4. Die komplexe Zahl $r\exp(\mathbf{i}\alpha)$.

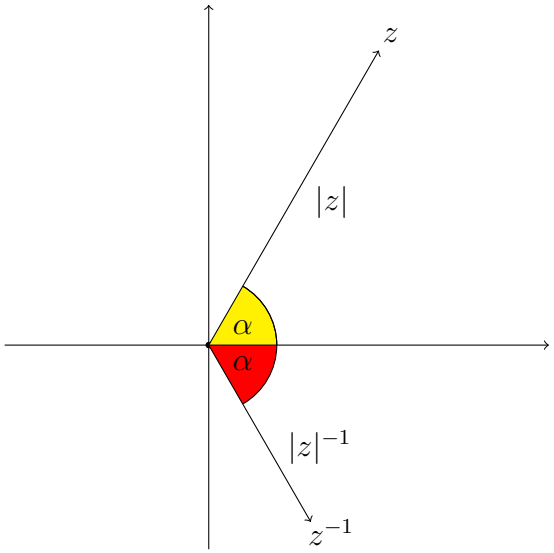

ABBILDUNG 5. Das Inverse einer komplexen Zahl.

Satz B.2 (Fundamentalsatz der Algebra (Gauß 1799 in seiner Doktorarbeit))**.** *Sei*

$$f = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$$

ein Polynom in $\mathbb{C}[X]$ *mit* $n \geq 1$ *und* $a_n \neq 0$. *Dann gibt es* $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ *mit*

$$f = a_n(X - \lambda_1)(X - \lambda_2) \cdots (X - \lambda_n).$$

Mit anderen Worten: Jedes Polynom vom Grad $n \geq 1$ in $\mathbb{C}[X]$ hat mindestens eine Nullstelle.

Anhang C. **Euklidische Vektorräume**

In der Algebra brauchen wir zunächst nur den euklidischen Vektorraum $(\mathbb{R}^n, s^n)$, wobei

$$s^n \colon \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$$
$$(v, w) \mapsto \langle v, w \rangle := \sum_{i=1}^{n} v_i w_i$$

das Standardskalarprodukt ist. Sei $v \in \mathbb{R}^n$. Die **Länge** von v ist definiert als

$$\|v\| := \sqrt{\langle v, v \rangle}.$$

Für $v, w \in \mathbb{R}^n$ ist der **Abstand** von v und w definiert durch

$$d(v, w) := \|v - w\| = \|w - v\|.$$

Lemma C.1 (Cauchy-Schwarzsche Ungleichung)**.** *Für alle* $v, w \in \mathbb{R}^n$ *gilt*

$$|\langle v, w \rangle| \leq \|v\| \cdot \|w\|.$$

Für $v, w \in \mathbb{R}^n$ folgt aus der Cauchy-Schwarzschen Ungleichung, dass

$$-1 \leq \frac{\langle v, w \rangle}{\|v\| \cdot \|w\|} \leq 1.$$

(Für $v = 0$ oder $w = 0$ behandeln wir den Ausdruck

$$\frac{\langle v, w \rangle}{\|v\| \cdot \|w\|}$$

als 0. Wir teilen hier nicht durch 0, sondern haben nur die Notation vereinfacht!)

Es gibt also genau ein $\alpha \in [0, \pi]$ mit

$$\cos(\alpha) = \frac{\langle v, w \rangle}{\|v\| \cdot \|w\|}.$$

Der **Winkel** zwischen v und w ist definiert als

$$\text{Winkel}(v, w) := \alpha = \arccos\left(\frac{\langle v, w \rangle}{\|v\| \cdot \|w\|}\right) \in [0, \pi].$$

Anhang D. **Polynomringe und Teilbarkeit**

D.1. **Polynomringe.** Sei $I := \mathbb{N}$. Wir wissen, dass $K^{(I)}$ ein K-Vektorraum ist. Sei $\{e_i \mid i \in I\}$ die Standardbasis von $K^{(I)}$, wobei e_i definiert ist durch

$$e_i \colon j \mapsto \begin{cases} 1 & : \text{ falls } i = j, \\ 0 & : \text{ sonst.} \end{cases}$$

Wir definieren zusätzlich eine Multiplikation

$$\begin{aligned} \cdot \colon K^{(I)} \times K^{(I)} &\to K^{(I)} \\ (f, g) &\mapsto fg, \end{aligned}$$

wobei fg definiert ist durch

$$fg \colon j \mapsto \sum_{\substack{(k,s) \in I \times I \\ k+s=j}} f(k) \cdot g(s).$$

Sei $f \in K^{(I)}$. Dann ist

$$f = \sum_{i \in I} f(i) \cdot e_i.$$

Es gibt ein $n \in I$ mit $f(m) = 0$ für alle $m > n$, da das Bild von f endlich ist. Wir schreiben X^i statt e_i und a_i statt $f(i)$.

Es gilt also

$$f = a_0 X^0 + a_1 X^1 + a_2 X^2 + \cdots + a_n X^n.$$

Weiter schreiben wir a_0 statt $a_0 X^0$ und 1 statt X^0. Wir nennen f ein **Polynom**. Die obige Multiplikation entspricht der üblichen Multiplikation von Polynomen. Nach der Definition der Multiplikation gilt

$$X^i \cdot X^j = X^{i+j}.$$

Beispiel. Sei $f = a_0 + a_1 X^1 + a_2 X^2$ und $g = b_0 + b_1 X^1$. Dann ist

$$fg = a_0 b_0 + (a_0 b_1 + a_1 b_0) X^1 + (a_1 b_1 + a_2 b_0) X^2 + (a_2 b_1) X^3.$$

Wir schreiben $K[X]$ statt $K^{(I)}$ und nennen $K[X]$ **Polynomring in** X.

Bemerkungen.

(i) Zusammen mit der oben definierten Multiplikation ist $K[X]$ eine K-Algebra.

(ii) $K[X]$ ist ein kommutativer Ring.

Sei

$$f = \sum_{i=0}^{n} a_i X^i \in K[X].$$

Der **Grad** von f ist definiert als

$$\operatorname{grad}(f) := \begin{cases} -\infty & : \text{ falls } 0 = a_0 = a_1 = \cdots = a_n, \\ \max\{0 \leq i \leq n \mid a_i \neq 0\} & : \text{ sonst.} \end{cases}$$

Ein $f \in K[X]$ heißt **normiert**, falls $\operatorname{grad}(f) = n \geq 0$ und $a_n = 1$.

Lemma D.1. *Es gilt*

(i) $\operatorname{grad}(fg) = \operatorname{grad}(f) + \operatorname{grad}(g)$.
(ii) $\operatorname{grad}(f+g) \leq \max\{\operatorname{grad}(f), \operatorname{grad}(g)\}$.

Beweis. Die erste Aussage folgt aus der Nullteilerfreiheit von K, die zweite folgt sofort aus der Definition von grad. □

Korollar D.2. *Der Ring $K[X]$ ist nullteilerfrei.*

Beweis. Wende Lemma D.1(i) an. □

D.2. **Teilbarkeit in Halbgruppen.** Eine **Halbgruppe** ist eine Menge zusammen mit einer Abbildung

$$\begin{aligned} H \times H &\to H \\ (h_1, h_2) &\mapsto h_1 h_2 \end{aligned}$$

so dass gilt:

(H1) Für alle $h_1, h_2, h_3 \in H$ gilt
$$(h_1 h_2) h_3 = h_1 (h_2 h_3);$$
(H2) Es gibt ein Element $1 \in H$ mit
$$1h = h1 = h$$
für alle $h \in H$.

Man kann leicht zeigen, dass das Einselement in Bedingung (H2) eindeutig bestimmt ist.

Eine Halbgruppe H ist **kommutativ** (oder **abelsch**), falls

$$gh = hg$$

für alle $g, h \in H$.

Beispiele.

(i) $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$ und $(\mathbb{N} \setminus \{0\}, \cdot)$ sind Halbgruppen;

(ii) Sei R ein Ring. Dann sind $(R, +)$, $(R, \cdot)$ und $(R \setminus \{0\}, \cdot)$ Halbgruppen;

Ein Element h einer Halbgruppe H ist **invertierbar**, falls es ein $h' \in H$ gibt mit $hh' = 1 = h'h$.

Sei $(H, \cdot)$ eine abelsche Halbgruppe, und seien $a, b \in H$. Wir sagen b **teilt** a, falls es ein $c \in H$ gibt mit $a = bc$. Wir schreiben dann $b \mid a$.

Ein Element $x \in H$ heißt **irreduzibel**, falls gilt:

- x ist nicht invertierbar;
- Falls $x = ab$ mit $a, b \in H$, so ist a oder b invertierbar.

Desweiteren ist $x \in H$ ein **Primelement**, falls gilt:

- x ist nicht invertierbar;
- Falls $x \mid (ab)$ mit $a, b \in H$, so gilt $x \mid a$ oder $x \mid b$.

Wir interessieren uns für Halbgruppen der Form $(R, \cdot)$ und $(R \setminus \{0\}, \cdot)$, wobei R ein kommutativer nullteilerfreier Ring ist. Die für uns wichtigsten Beispiele sind $(\mathbb{Z} \setminus \{0\}, \cdot)$ und $(K[X] \setminus \{0\}, \cdot)$.

Lemma D.3. *Sei R ein kommutativer nullteilerfreier Ring, und sei $(H, \cdot) := (R \setminus \{0\}, \cdot)$. Dann sind alle Primelemente in H irreduzibel.*

Beweis. Sei $x \in H$ ein Primelement, und sei $x = ab$ mit $a, b \in H$. Es ist zu zeigen, dass a oder b invertierbar ist. Wir wissen, dass $x \mid a$ oder $x \mid b$ gilt. Ohne Einschränkung nehmen wir $x \mid a$ an. Dann gibt es ein $c \in H$ mit $xc = a$, also $x = ab = xcb$. Es folgt $x(1 - cb) = 0$ und damit $1 = cb$. Also ist b invertierbar. □

D.3. **Beispiele.**

D.3.1. Erinnerung: Ein Element $a > 0$ in $\mathbb{Z}$ ist eine **Primzahl**, falls es genau zwei Elemente $b > 0$ in $\mathbb{Z}$ gibt mit $b \mid a$. (Dies sind dann notwendigerweise 1 und a.)

Lemma D.4. *Die invertierbaren Elemente in $(\mathbb{Z}, \cdot)$ sind 1 und -1. Für jedes nicht-invertierbare $0 \neq a \in \mathbb{Z}$ sind äquivalent:*

(i) *$|a|$ ist eine Primzahl;*

(ii) *a ist irreduzibel;*

(iii) *a ist ein Primelement.*

Beweis. Es ist klar, dass 1 und -1 die einzigen invertierbaren Elementen in $(\mathbb{Z}, \cdot)$ sind. (Man fasse $\mathbb{Z}$ als Unterring von $\mathbb{Q}$ auf usw.)

(i) $\iff$ (ii): Dies folgt aus der Definition einer Primzahl und dem Umstand, dass 1 und -1 die einzigen invertierbaren Elemente in $(\mathbb{Z}, \cdot)$ sind.

(iii) $\implies$ (ii): Dies folgt aus Lemma D.3, da $(\mathbb{Z}, \cdot)$ nullteilerfrei ist.

(ii) $\implies$ (iii): Später. □

D.3.2. Sei $(H, \cdot) := (\{1, 4, 8, 12, \dots\}, \cdot) = (\{1\} \cup 4\mathbb{N}_1, \cdot)$. Das einzige invertierbare Element in H ist 1. Beispiele irreduzibler Elemente in H sind

$$4, 8, 12, 20, 24, 28, 36, \dots$$

Beispiele für nicht irreduzible Elemente sind $16 = 4 \cdot 4$ und $32 = 4 \cdot 8$. Das Element 4 ist kein Primelement, da $4 \mid 64$, $64 = 8 \cdot 8$ aber $4 \nmid 8$ in H. Außerdem gilt $64 = 8 \cdot 8 = 4 \cdot 4 \cdot 4$. Es gibt also keine eindeutige Faktorisierung von 64 als Produkt irreduzibler Elemente.

D.4. **Teilen mit Rest.** Sind $a, b \in \mathbb{Z}$ mit $b \neq 0$, so gibt es $q, r \in \mathbb{Z}$ mit

$$a = qb + r$$

und $|r| < |b|$. Verlangt man zusätzlich, dass $r > 0$ ist, so sind q und r eindeutig bestimmt. Wir formulieren nun das entsprechende Ergebnis für Polynome.

Proposition D.5 (Division mit Rest)**.** *Sei K ein Körper, und seien $f, g \in K[X]$ mit $g \neq 0$. Dann gibt es eindeutig bestimmte Polynome $q, r \in K[X]$ mit*

$$f = qg + r$$

und $\operatorname{grad}(r) < \operatorname{grad}(g)$.

Beweis. Eindeutigkeit: Sei

$$f = q_1 g + r_1 = q_2 g + r_2$$

mit $\operatorname{grad}(r_i) < \operatorname{grad}(g)$ für $i = 1, 2$. Es folgt

$$(q_1 - q_2)g = r_2 - r_1$$

Wegen $\operatorname{grad}(r_2 - r_1) < \operatorname{grad}(g)$ gilt dann $q_1 - q_2 = 0$. Damit haben wir gezeigt, dass $q_1 = q_2$ und $r_1 = r_2$.

Existenz: Für $f = 0$ ist $q = 0$ und $r = 0$. Sei also $f \neq 0$. Sei weiter

$$f = \sum_{i=0}^{m} a_i X^i, \qquad g = \sum_{i=0}^{n} b_i X^i$$

mit $a_m \neq 0 \neq b_n$. Falls $m < n$ ist, dann wählen wir $q = 0$ und $r = f$. Sei also $m \geq n$.

Wir können ohne Einschränkung annehmen, dass g normiert ist. Sei

$$h := f - a_m X^{m-n} g.$$

Dann ist $\operatorname{grad}(h) \leq m - 1$. Mit Induktion folgt, dass es $q', r' \in K[X]$ gibt mit $h = q'g + r'$ und $\operatorname{grad}(r') < \operatorname{grad}(g)$.

Es gilt also

$$f = h + a_m X^{m-n} g = q'g + r' + a_m X^{m-n} g = (q' + a_m X^{m-n})g + r'.$$

Setze nun $q := q' + a_m X^{m-n}$ und $r := r'$. □

Für $a \in K$, sei

$$\eta_a \colon K[X] \to K$$

definiert durch

$$f = \sum_{i=0}^{m} a_i X^i \mapsto f(a) := \sum_{i=0}^{m} a_i a^i.$$

Man prüft leicht, dass η_a ein K-Algebrenhomomorphismus ist, d.h. $\eta_a(1) = 1$, $\eta_a(fg) = \eta_a(f)\eta_a(g)$, $\eta_a(f + g) = \eta_a(f) + \eta_a(g)$ und $\eta_a(bf) = b\eta_a(f)$ für alle $f, g \in K[X]$ und $b \in K$. Man nennt η_a **Einsetzungshomomorphismus**.

Sei $f \neq 0$ in $K[X]$. Dann ist $a \in K$ eine **Nullstelle** von f, falls $f(a) = 0$.

Lemma D.6. *Sei $a \in K$ eine Nullstelle von $0 \neq f \in K[X]$. Dann gibt es ein $q \in K[X]$ mit*

$$f = q \cdot (X - a).$$

Beweis. Sei $0 \neq f \in K[X]$, und sei a eine Nullstelle von f. Weiter sei $g := X - a$, also $g(a) = 0$. Dann existiert ein r mit $\operatorname{grad}(r) < \operatorname{grad}(g) = 1$ und $q \in K[X]$ mit $f = qg + r$. Also ist

$$0 = f(a) = (qg)(a) + r(a) = q(a)g(a) + r(a) = r(a)$$

und damit auch $r = 0$, da $\operatorname{grad}(r) \leq 0$. □

D.5. **Satz von Bézout.** Sei $R = \mathbb{Z}$, und seien $a_1, \ldots, a_n \in R \setminus \{0\}$. Dann ist $\operatorname{ggT}(a_1, \ldots, a_n) := d$, falls gilt:

- $d > 0$;
- $d \mid a_i$ für alle $1 \leq i \leq n$;
- Falls $e \in \mathbb{Z}$ mit $e \mid a_i$ für alle i, so gilt $e \mid d$.

Sei $R = K[X]$, und seien $a_1, \ldots, a_n \in R \setminus \{0\}$. Dann ist $\operatorname{ggT}(a_1, \ldots, a_n) := d$, falls gilt:

- d ist normiert;
- $d \mid a_i$ für alle $1 \leq i \leq n$;
- Falls $e \in K[X]$ mit $e \mid a_i$ für alle i, so gilt $e \mid d$.

Wir nennen dann d den **größten gemeinsamen Teiler** von $a_1, \ldots, a_n$.

Falls d existiert, so ist d offensichtlich eindeutig bestimmt.

Lemma D.7. *Sei $R = \mathbb{Z}$ oder $R = K[X]$. Sei $f = qg + r$ mit $f, g, q, r \in R$, und sei $d := \mathrm{ggT}(g, r)$. Dann gilt $d = \mathrm{ggT}(f, g)$.*

Beweis. Es gibt d', d'' mit $dd' = g$ und $dd'' = r$. Wir erhalten

$$f = qg + r = d(qd' + d'').$$

Also gilt $d \mid f$ und $d \mid g$.

Angenommen $e \mid f$ und $e \mid g$. Es gibt also e', e'' mit $ee' = f$ und $ee'' = g$, und damit

$$e(e' - qe'') = ee' - eqe'' = f - qg = r.$$

Also gilt $e \mid g$ und $e \mid r$, folglich gilt auch $e \mid d$. □

Satz D.8 (Bézout)**.** *Sei $R = \mathbb{Z}$ oder $R = K[X]$. Seien $a_1, \ldots, a_n \in R \setminus \{0\}$. Dann gibt es ein $b \in R$ mit $b = \mathrm{ggT}(a_1, \ldots, a_n)$, und es gibt $c_1, \ldots, c_n \in R$ mit*

$$b = \sum_{i=1}^{n} c_i a_i.$$

Beweis. Für $n = 1$ ist die Aussage klar. Sei $n = 2$.

Für $z \in R$ setze

$$\rho(z) := \begin{cases} |z| & : \text{ falls } R = \mathbb{Z}, \\ \mathrm{grad}(z) & : \text{ falls } R = K[X]. \end{cases}$$

Seien $f, g \in R \setminus \{0\}$. Wir nehmen ohne Einschränkung an, dass $\rho(f) \geq \rho(g)$. Sei $f_0 := f$ und $f_1 := g$. Teile f_0 durch f_1 mit Rest. Wir erhalten

$$f_0 = q_1 \cdot f_1 + f_2$$

mit $\rho(f_1) > \rho(f_2)$. Falls $f_2 \neq 0$, so teilen wir f_1 durch f_2 mit Rest und erhalten

$$f_1 = q_2 f_2 + f_3.$$

Wir fahren induktiv fort und bekommen so Gleichungen der Form

$$f_i = q_{i+1} f_{i+1} + f_{i+2}.$$

Es existiert ein minimales m mit $f_{m+1} = 0$. Es gilt dann

$$\rho(f_0) \geq \rho(f_1) > \rho(f_2) > \cdots > \rho(f_m).$$

Es gilt $f_{m-1} = q_m f_m$. Es gibt ein eindeutig bestimmtes invertierbares $\lambda \in R$, so dass

$$\tilde{f}_m := \lambda f_m$$

normiert bzw. > 0 ist. Es gilt dann $\tilde{f}_m = \mathrm{ggT}(f_{m-1}, f_m)$.

Weiter gilt $f_{m-2} = q_{m_1} f_{m-1} + f_m$. Mit Lemma D.7 und Induktion folgt nun

$$\tilde{f}_m = \mathrm{ggT}(f_{m-1}, f_m) = \mathrm{ggT}(f_{m-2}, f_{m-1}) = \cdots = \mathrm{ggT}(f_0, f_1).$$

Für $1 \leq i \leq m-1$ gilt $f_{i+1} = f_{i-1} - q_i f_i$. Dies liefert

$$\begin{aligned} f_m &= f_{m-2} - q_{m-1} f_{m-1} \\ &= (f_{m-4} - q_{m-3} f_{m-3}) - q_{m-1}(f_{m-3} - q_{m-2} f_{m-2}) \\ &= \cdots \\ &= a_0 f_0 + a_1 f_1 \end{aligned}$$

für geeignete $a_0, a_1 \in R$. Damit ist der Satz für $n = 2$ bewiesen.

Sei also $n > 2$. Nach Induktion stimmt der Satz für $n - 1$.

Sei $b' := \mathrm{ggT}(a_1, \ldots, a_{n-1})$ und $b := \mathrm{ggT}(b', a_n)$. Wir behaupten, dass $b = \mathrm{ggT}(a_1, \ldots, a_n)$. Wir zeigen dies in drei Schritten:

- b ist normiert, bzw. $b > 0$. Dies folgt unmittelbar aus der Definition.
- Es gilt $b \mid b'$ und daher $b \mid a_i$ mit $1 \leq i \leq n-1$, also $b \mid a_i$ für alle $1 \leq i \leq n$.
- Sei $e \in R$ mit $e \mid a_i$ für alle $1 \leq i \leq n$. Dann gilt $e \mid b$. (Wir wissen, dass $e \mid b'$ gilt, da $b' = \mathrm{ggT}(a_1, \ldots, a_{n-1})$ ist. Aus $b = \mathrm{ggT}(b', a_n)$ und $e \mid a_n$ folgt dann $e \mid b$.)

Nach Induktion gibt es ein $c_i \in R$ mit

$$b' = \sum_{i=1}^{n-1} c_i a_i,$$

und es gibt $c', c'' \in R$ mit $b = c' b' + c'' a_n$. Es folgt

$$b = \sum_{i=1}^{n-1} (c' c_i) a_i + c'' a_n.$$

□

Korollar D.9. *Sei $R = \mathbb{Z}$ oder $R = K[X]$, und sei $p \in R$ irreduzibel. Dann ist p ein Primelement.*

Beweis. Angenommen $p \mid (uv)$ mit $u, v \in R$. Dann gilt $pc = uv$ für ein geeignetes $c \in R$. Angenommen p ist kein Teiler von u. Da p irreduzibel ist, gilt dann $\mathrm{ggT}(p, u) = 1$.

Also gibt es nach Satz D.8 Elemente $a, b \in R$ mit $1 = ap + bu$. Es folgt

$$\begin{aligned} v &= 1 \cdot v = (ap + bu)v \\ &= apv + buv = apv + bpc \\ &= p(av + bc). \end{aligned}$$

Also gilt $p \mid v$. □

D.6. **Primfaktorzerlegung in $\mathbb{Z}$ und $K[X]$.** Zur Vereinfachung nennen wir $a \in \mathbb{Z}$ **normiert**, falls $a > 0$.

Satz D.10. *Sei $R = \mathbb{Z}$ oder $R = K[X]$. Jedes $0 \neq f \in R$ lässt sich schreiben als*

$$f = ap_1p_2 \cdots p_n$$

wobei $a \in R$ invertierbar ist, und die $p_i \in R$ sind irreduzibel und normiert, falls $R = K[X]$, und die p_i sind Primzahlen, falls $R = \mathbb{Z}$. Bis auf die Reihenfolge sind die p_i und auch a eindeutig bestimmt.

Beweis. Existenz: Die Existenz folgt durch Induktion über $\operatorname{grad}(f)$, falls $R = K[X]$ bzw. über $|f|$, falls $R = \mathbb{Z}$.

Eindeutigkeit: Sei im Folgenden $R = K[X]$ oder $R = \mathbb{Z}$, und sei $0 \neq f \in R$. Es gibt ein eindeutig bestimmtes invertierbares $b \in R$, so dass bf normiert ist. Wir setzen dann $a := b^{-1}$. Der Einfachheit halber nehmen wir an, dass $a = b = 1$ gilt. Sei also $f \in R$ normiert, und sei

$$f = p_1p_2 \cdots p_n = q_1q_2 \cdots q_m$$

mit p_i, q_i irreduzibel und normiert in R für alle i.

Offensichtlich ist p_1 ein Teiler von $q_1q_2 \cdots q_m$. Also gibt es nach Korollar D.9 und Induktion ein j mit $p_1 \mid q_j$. Ohne Einschränkung sei $j = 1$. Aus $p_1 \mid q_1$ folgt $p_1 = q_1$, da q_1 irreduzibel ist. Wir gehen mit Induktion nach n vor.

Für $n = 1$ folgt $p_1 = p_1(q_2 \cdots q_m)$. Da R nullteilerfrei ist, folgt $m = 1$.

Sei nun $n > 1$. Aus $p_1p_2 \cdots p_n = p_1q_2 \cdots q_m$ folgt (wieder aus der Nullteilerfreiheit von R), dass $p_2 \cdots p_n = q_2 \cdots q_m$. Es folgt mit Induktion, dass $n - 1 = m - 1$ und dass ein $\sigma \in S_n$ existiert mit $p_i = q_{\sigma(i)}$ für alle $1 \leq i \leq n$. □

Sei $f = ap_1p_2 \cdots p_n$ mit $0 \neq f \in R$ und p_i irreduzibel und normiert und $a \in R$ invertierbar. Sei p irreduzibel und normiert. Dann heißt

$$\mathrm{m}(f, p) := |\{1 \leq i \leq n \mid p_i = p\}|$$

die **Vielfachheit** oder auch **Multiplizität** von p in f.

Korollar D.11. *Jedes $f \neq 0$ in $K[X]$ hat höchstens* $\operatorname{grad}(f)$ *verschiedene Nullstellen.*

Beweis. Kombiniere Satz D.10 mit Lemma D.6. □

Korollar D.12. *Sei $0 \neq f \in K[X]$, und seien $\lambda_1, \ldots, \lambda_t$ die paarweise verschiedenen Nullstellen von f. Dann gibt es irreduzible normierte Polynome $p_1, \ldots p_r$ mit* $\operatorname{grad}(p_i) \geq 2$ *und $n_i \geq 1$ für alle i, und ein $a \in K^\times$ mit*

$$f = a p_1 \cdots p_r \cdot \prod_{i=1}^{t} (X - \lambda_i)^{n_i}.$$

Die p_i, n_i und a sind bis auf die Reihenfolge eindeutig bestimmt. Wir definieren

$$m(f, \lambda_i) := m(f, X - \lambda_i) = n_i$$

und nennen dies die **Vielfachheit** *oder auch* **Multiplizität** *von λ_i in f.*

Sei $0 \neq f \in K[X]$. Das Polynom f **zerfällt über K in Linearfaktoren**, falls $\operatorname{grad}(f) = 0$ oder falls es $a \in K^\times$ und paarweise verschiedene $\lambda_1, \ldots, \lambda_t \in K$ und $m_1, \ldots, m_t \geq 1$ gibt mit

$$f = a \cdot (X - \lambda_1)^{m_1} \cdots (X - \lambda_t)^{m_t}.$$

Dann sind $\lambda_1, \ldots, \lambda_t$ die Nullstellen von f.

Beispiel. Sei $K = \mathbb{R}$, und sei $f = X^2 + 1$ zerfällt nicht in Linearfaktoren über $\mathbb{R}$. Für $K = \mathbb{C}$ gilt aber

$$f = X^2 + 1 = (X + \mathbf{i})(X - \mathbf{i}).$$

Ein Körper ist **algebraisch abgeschlossen**, falls jedes $0 \neq f \in K[X]$ über K in Linearfaktoren zerfällt.

Bemerkungen.

(i) Ein Körper ist algebraisch abgeschlossen genau dann wenn alle irreduziblen normierten Polynome in $K[X]$ den Grad 1 haben, also von der Form $X - a$ sind.

(ii) Die Polynome $X - a$ mit $a \in K$, sind immer irreduzibel in $K[X]$.

(iii) Die irreduziblen normierten Polynome in $\mathbb{R}[X]$ sind

$$X - a$$

mit $a \in \mathbb{R}$ und

$$X^2 + a_1 X + a_0$$

mit $a_0, a_1 \in \mathbb{R}$, so dass $a_1^2 < 4a_0$. (Übungsaufgabe.)

Anhang E. **Historische Notizen**

In diesem Abschnitt werden einige Mathematiker erwähnt, die wesentlich zur Entwicklung der Algebra im weitesten Sinne beigetragen haben. Zumindest stichwortartig werden auch einige ihrer damit zusammenhängenden Leistungen genannt. Manchmal geben wir einfach nur ein Beispiel von nach ihnen benannten Objekten oder Aussagen.

E.1. **Mathematiker.**

- **(Einige) Babylonier** (1800 v. Chr.): Lösungsformeln für quadratische Gleichungen (d.h. Polynomgleichungen vom Grad 2).

- **Niels Henrik Abel** (∗1802 auf der Insel Finnøy, Ryfylke (Norwegen); †1829 in Froland, Aust-Agder (Norwegen)): Hat gezeigt, dass es für Polynome vom Grad mindestens 5 i.A. keine Lösungsformel gibt (1824). Ruffini hat dies 1799 mit einem lückenhaften Beweis ebenfalls veröffentlicht.

- **Emil Artin** (∗1898 Wien; †1962 Hamburg): van der Waerdens Bücher zur Algebra basieren auf Artins Vorlesungen. Artinsche Ringe. Löste das 17. Hilbertsche Problem.

- **Gerolamo Cardano** (∗1501 Pavia; †1576 Rom): Sein Buch *Ars magna sive de Regulis Algebraicis* (1545) enthält Lösungsformeln für Polynomgleichungen vom Grad 3 und 4 (die Lösung für den Grad 4 stammt von Ferrari). Verfasste auch das Buch *Liber de Ludo Aleae* über Glücksspiele, welches die Grundlagen der Wahrscheinlichkeitstheorie enthält.

- **Arthur Cayley** (∗1821 Richmond upon Thames; †1895 Cambridge): Satz von Cayley.

- **Jean Baptiste le Rond d'Alembert** (∗1717 Paris; †1783 Paris):

- **Julius Wilhelm Richard Dedekind** (∗1831 Braunschweig; †1916 Braunschweig):

- **Diophantos von Alexandria** (Lebte irgendwann zwischen 100 v. Chr. und 350 n. Chr. Die genauen Lebensdaten sind nicht bekannt.): Verfasser von *Arithmetica*, ein Werk, welches vermutlich aus 13 Bänden bestand.

- **Ferdinand Gotthold Max Eisenstein** (∗1823 Berlin; †1852 Berlin): Eisenstein-Kriterium für die Irreduzibilität von ganzzahligen Polynomen.

- **Euklid von Alexandria**: (Lebte im 3. Jhd. v. Chr. Die genauen Lebensdaten sind nicht bekannt.): Seine *Elemente* sind ein Klassiker der Mathematik.

- **Leonhard Euler** (∗1707 Basel; †1783 Sankt Petersburg): *Vollständige Anleitung zur Algebra* (1770) und 865 weitere Veröffentlichungen.

- **Pierre de Fermat** (∗1607 Beaumont-de-Lomagne; †1665 Castres): Fermat-Zahlen. Er vermutete, dass alle Fermat-Zahlen Primzahlen sind. Dies wurde erst von Gauß widerlegt.

- **Lodovico Ferrari** (∗1522 Bologna; †1565 Bologna): Lösungsformeln für Polynomgleichungen vom Grad 4. Schüler und Pflegesohn von Cardano. Wettstreit mit Tartaglia.

- **Ferdinand Georg Frobenius** (∗1849 Berlin; †1917 Charlottenburg): Frobenius-Automorphismus.

- **Carl Friedrich Gauß** (∗1777 Braunschweig; †1855 Göttingen): Konstruktion des regulären 17-Ecks. Fundamentalsatz der Algebra. Satz von Gauß (über faktorielle Polynomringe).

- **Évariste Galois** (∗1811 Bourg-la-Reine; †1832 Paris): Ohne ihn gäbe es diese Vorlesung nicht. Starb viel zu früh. Die Bedeutung seiner Arbeiten wurde erst nach seinem Tod erkannt.

- **William Rowan Hamilton** (∗1805 Dublin; †1865 Dunsink): Studium komplexer Zahlen und Quaternionen.

- **Charles Hermite** (∗1822 Dieuze, Lothringen; †1901 Paris): Transzendenz der Eulerschen Zahl e (1873).

- **David Hilbert** (∗1862 Königsberg; †1943 Göttingen):

- **Felix Christian Klein** (∗1849 Düsseldorf; †1925 Göttingen):

- **Leopold Kronecker** (∗1823 Liegnitz; †1891 Berlin): (Beinahe vollständige) Klassifikation von Paaren von Homomorphismen modulo Basiswechsel (1874). Satz von Kronecker-Weber.

- **Ernst Eduard Kummer** (∗1810 Sorau (Niederlausitz); †1893 Berlin):

- **Joseph-Louis de Lagrange** (∗1736 Turin; †1813 Paris): Beiträge zur Gruppentheorie (Satz von Lagrange). Himmelsmechanik (Dreikörperproblem).

- **Fortuné Landry** (∗1799 Paris; †1895 Paris): Primzahlfaktorisierung vieler Mersenne-Zahlen und einiger Fermat-Zahlen.

- **Pierre Alphonse Laurent** (∗1813 Paris; †1854 Paris): Ingenieur der französischen Armee. Posthum veröffentlichte Untersuchung der Konvergenz der später nach ihm benannten Laurent-Reihen.

- **Carl Louis Ferdinand von Lindemann** (∗1852 Hannover; †1939 München): Transzendenz der Kreiszahl π (1882).

- **Joseph Liouville** (∗1809 Saint-Omer; †1882 Paris): Erkannte als Erster die Bedeutung von Galois' Arbeiten und veröffentlichte diese im Jahr 1846 in seiner Fachzeitschrift *Journal de Mathématiques Pures et Appliquées*.

- **Amalie Emmy Noether** (∗1882 Erlangen; †1935 Bryn Mawr (Pennsylvania)): Noethersche Isomorphiesätze. Noether hat entscheidend zur Entwicklung der modernen Algebra beigetragen.

- **Paolo Ruffini** (∗1765 Valentano; †1822 Modena): Satz von Abel-Ruffini.

- **Theodor Schönemann** (∗1812 Driesen (heute: Drezdenko); †1868 Brandenburg an der Havel): Eisenstein-Kriterium.

- **Ernst Steinitz** (∗1871 Laurahütte (Oberschlesien); †1928 Kiel): Konstruktion des algebraischen Abschlusses eines Körpers.

- **Peter Ludwig Mejdell Sylow** (∗1832 Christiania, heute Oslo; †1918 Christiania): Grundlagen der Gruppentheorie. Sylow-Sätze.

- **Niccolò Tartaglia** (∗1499 oder 1500 Brescia; †1557 Venedig): Lösungsformeln für Polynomgleichungen vom Grad 3. Wettstreit mit Ferrari.

- **Ehrenfried Walther von Tschirnhaus** (∗1651 Kieslingswalde; †1708 Dresden): Universalgelehrter. Tschirnhaus-Transformation.

- **Bartel Leendert van der Waerden** (∗1903 Amsterdam; †1996 Zürich): Verfasst 1930 das Buch *Moderne Algebra*.

- **Pierre-Laurent Wantzel** (∗1814 Paris; †1848 Paris): Unmöglichkeit der Würfeldopplung und der Winkeldreiteilung durch Zirkel und Lineal (1837).

- **Heinrich Martin Weber** (∗1842 Heidelberg; †1913 Straßburg): Satz von Kronecker-Weber.

- **Joseph Wedderburn** (∗1882 Forfar (Schottland); †1948 Princeton): Matrizen über beliebigen Körpern.

- **Ernst Witt** (∗1911 auf Alsen, damals Deutsches Reich, heute Dänemark; †1991 Hamburg): Quadratische Formen über beliebigen Körpern. Wittscher Kürzungssatz.

E.2. **Zitate.**

- Sir Michael Francis Atiyah (∗1929): Algebra is the offer made by the devil to the mathematician. The devil says: 'I will give you this powerful machine, it will answer any question you like. All you need to do is give me your soul: give up geometry and you will have this marvellous machine.'

  An dieser Stelle könnte man einwenden, dass viele Algebraiker heutzutage auch Geometrie treiben, siehe hierzu Claus Michael Ringels Vortrag *Algebra ist Geometrie ist Algebra*.
- Neil deGrasse Tyson (∗1958 New York): The universe is under no obligation to make sense to you.
- John Maynard Smith (∗1920 London; †2004 Lewes (East Sussex)): If you can't stand algebra, keep out of evolutionary biology.
- Gottfried Wilhelm Leibniz (∗1646 Leipzig; †1716 Hannover): Menschen, die von der Algebra nichts wissen, können sich auch nicht die wunderbaren Dinge vorstellen, zu denen man mit Hilfe der genannten Wissenschaft gelangen kann.
- Johann Wolfgang von Goethe (∗1749 Frankfurt am Main; †1832 Weimar): Mit Mathematikern ist kein heiteres Verhältnis zu gewinnen.
- Aus einem Matheforum: Der Sonntag ist eigentlich zu spät, um einen Vortrag für Montag vorzubereiten.

Literatur

[Al] Heinz-Wilhelm Alten u.v.a., 4000 Jahre Algebra. Geschichte-Kulturen-Menschen. Second revised and extended edition. Vom Zählstein zum Computer. Springer, Berlin, 2014. xiv+745 pp.

[A] Emil Artin, Galois theory. Edited and with a supplemental chapter by Arthur N. Milgram. Reprint of the 1944 second edition. Dover Publications, Inc., Mineola, NY, 1998. iv+82 pp.

[Bo] Siegfried Bosch, Algebra. 8., korr. Aufl. Berlin [u.a.], Springer, 2013. viii+376 pp.

[C] David Cox, Galois theory. Second edition. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, 2012. xxviii+570 pp.

[D] Underwood Dudley, The trisectors. Revised edition. MAA Spectrum. Mathematical Association of America, Washington, DC, 1994. xviii+184 pp.

[E] Euklid von Alexandria. Die Elemente. Buch I-XIII. Based on Heiberg's text. Translated from the Greek and edited by Clemens Thaer. Bibliothek Klassischer Texte. Wissenschaftliche Buchgesellschaft, Darmstadt, 1991. vi+479 pp.

[FS] Gerd Fischer, Reinhard Sacher, Einführung in die Algebra. Zweite überarbeitete Auflage. Teubner Studienbücher: Mathematik. B. G. Teubner, Stuttgart, 1978. 240 pp.

[HW] Godfrey Harold Hardy, Sir Edward Maitland Wright, An introduction to the theory of numbers. Sixth edition. Revised by D. R. Heath-Brown and J. H. Silverman. With a foreword by Andrew Wiles. Oxford University Press, Oxford, 2008. xxii+621 pp.

[Hub] Andrew Hubery, Skript Galois Theory.

[H] Bertram Huppert, Endliche Gruppen. I. Die Grundlehren der Mathematischen Wissenschaften, Band 134 Springer-Verlag, Berlin-New York 1967. xii+793 pp.

[JS] Jens Carsten Jantzen, Joachim Schwermer, Algebra. Berlin [u.a.], Springer, 2006. 395 pp.

[Kr] Otto Krötenheerdt, Zur Theorie der Dreieckskonstruktionen. Eine vollständige Aufzählung aller unmöglichen Dreieckskonstruktionen aus Seiten, Winkeln, Höhen, Seitenhalbierenden und Winkelhalbierenden. Wiss. Z. Martin-Luther-Univ. Halle-Wittenberg Math.-Natur. Reihe 15 1966 677–700.

[K] Ernst Kunz, Algebra. Braunschweig [u.a.] : Vieweg, 1994 . x+254 pp.

[La] Serge Lang, Algebra. Revised third edition. Graduate Texts in Mathematics, 211. Springer-Verlag, New York, 2002. xvi+914 pp.

[L1] Falko Lorenz, Einführung in die Algebra. Teil I. Bibliographisches Institut, Mannheim, 1992. xii+338 pp.

[L2] Falko Lorenz, Einführung in die Algebra. Teil II. Bibliographisches Institut, Mannheim, 1990. x+386 pp

[M] Bernd Heinrich Matzat, Konstruktive Galoistheorie. Lecture Notes in Mathematics, 1284. Springer-Verlag, Berlin, 1987. x+286 pp.

[P] Oskar Perron, Algebra II. Theorie der algebraischen Gleichungen. Algebra. II. Theorie der algebraischen Gleichungen. (German) 3d ed. Walter de Gruyter & Co., Berlin, 1951. viii+261 pp.

[Sch] Olaf Schnürer, Skript Algebra.

[Soe] Wolfgang Soergel, Skript Algebra.

[Ste] Ian Steward, Galois theory. Fourth edition. CRC Press, Boca Raton, FL, 2015. xxii+321 pp.

[St] Catharina Stroppel, Skript Algebra.

[vdW1] Bartel Leendert van der Waerden, Algebra. Vol. I. Based in part on lectures by E. Artin and E. Noether. Translated from the seventh German edition by Fred Blum and John R. Schulenberger. Springer-Verlag, New York, 1991. xiv+265 pp.

[vdW2] Bartel Leendert van der Waerden, Algebra. Vol. II. Based in part on lectures by E. Artin and E. Noether. Translated from the fifth German edition by John R. Schulenberger. Springer-Verlag, New York, 1991. xii+284 pp.

[vdW3] Bartel Leendert van der Waerden, A history of algebra. From al-Khwārizmī to Emmy Noether. Springer-Verlag, Berlin, 1985. xi+271 pp.

Jan Schröer
Mathematisches Institut
Universität Bonn
Endenicher Allee 60
53115 Bonn
Germany

E-mail address: schroer@math.uni-bonn.de