

# Zusammenfassung Algebra 1

© Tim Baumann, <http://timbaumann.info/uni-spicker>

**Def.** Ein **Polynom** mit Unbestimmter  $X$  hat die Form

$$f(X) = a_0X^n + a_1X^{n-1} + \dots + a_{n-1}X + a_n.$$

**Def.** Falls oben  $a_0 \neq 0$  gilt, so ist  $\partial f = n$  der **Grad** des Polynoms.

**Def.** • Eine **Linearkombination** ist ein Polynom der Form

$$f(X_1, \dots, X_n) = a_1X_1 + \dots + a_nX_n.$$

• Ein **Monom** hat die Gestalt  $f(x) = bx^k$ .

**Algorithmus** (Euklid). Seien  $a, b \in \mathbb{R}$  mit  $a > b > 0$  gegeben. Schreibe

$$a = k \cdot b + r$$

mit  $k \in \mathbb{N}$  und  $r < b$ . Wiederhole diesen Schritt mit  $(a, b) := (b, r)$ , falls  $r \neq 0$ .

**Def.** Ein **gemeinsames Maß** zweier Zahlen  $a, b \in \mathbb{R}$  ist eine Zahl  $c \in \mathbb{R}$ , sodass es  $k, l \in \mathbb{Z}$  mit  $a = k \cdot c$  und  $b = l \cdot c$  gibt.

*Bemerkung.* Zwei Zahlen haben genau dann ein gemeinsames Maß, wenn der euklidische Algorithmus, angewandt auf diese Zahlen, abbricht.

**Def.** Zwei Zahlen  $a, b \in \mathbb{R}$ , die kein gemeinsames Maß besitzen, heißen **inkommensurabel**. Ihr Verhältnis ist dann **irrational**.

**Satz.** Die Längen der Seite und der Diagonalen eines regelmäßigen Fünfecks sind zueinander inkommensurabel.

**Def.** Der **goldene Schnitt** ist die Zahl

$$\Phi := \frac{1 + \sqrt{5}}{2} \approx 1.618.$$

*Bemerkung.* Der goldene Schnitt ist Lösung der Polynomgleichung

$$X^2 - X - 1 = 0.$$

**Def.** Ein **Binom** ist ein Ausdruck der Form  $(a + b)^n$  mit  $n \in \mathbb{N}$ .

**Def.** Für  $n \in \mathbb{N}$  und  $k \leq n$  schreibe  $\binom{n}{k} := \frac{n!}{k!(n-k)!}$ .

**Satz.** Es gilt  $(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$  für alle  $n \in \mathbb{N}$ .

**Verfahren** (Tschirnhaus-Transformation). Sei eine Polynomgleichung der Form

$$x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n = 0$$

gegeben. Substituiere  $x := \tilde{x} - \frac{a_1}{n}$ . Dann hat die neue Gleichung keinen  $x^{n-1}$ -Term. Lösungen der beiden Gleichungen können durch Addieren bzw. Subtrahieren von  $\frac{a_1}{n}$  ineinander überführt werden.

**Korollar.** Beim Lösen von Polynomgleichungen kann man also annehmen, dass kein  $x^{n-1}$ -Term vorhanden ist.

**Korollar** (Mitternachtsformel). Die Polynomgleichung zweiten Grades  $x^2 + ax + b = 0$  wird gelöst durch

$$x = -\frac{a}{2} \pm \frac{1}{2}\sqrt{a^2 - 4b}.$$

**Satz.** Eine Nullstelle der kubischen Gleichung  $x^3 + ax - b = 0$  ist gegeben durch

$$x = \sqrt[3]{\frac{b}{2} + \sqrt{D}} + \sqrt[3]{\frac{b}{2} - \sqrt{D}} \quad \text{mit } D := \left(\frac{a}{3}\right)^3 + \left(\frac{b}{2}\right)^2.$$

**Problem.** Was, wenn in der Quadratwurzel eine neg. Zahl steht?

**Def.** Für die **imaginäre Zahl**  $i$  gilt:  $i^2 = -1$ . Die **komplexen Zahlen**  $\mathbb{C}$  sind Zahlen der Form  $x + yi$  mit  $x, y \in \mathbb{R}$ . Es gelten die Rechenregeln

$$\begin{aligned}(x + yi) \pm (u + vi) &= (x + u) \pm (y + v)i \\ (x + yi) \cdot (u + vi) &= (xu - yv) + (xv + yu)i \\ \frac{1}{x + yi} &= \frac{x}{x^2 + y^2} + \frac{-y}{x^2 + y^2}i\end{aligned}$$

**Def.** Für eine komplexe Zahl  $z = x + yi$  mit  $x, y \in \mathbb{R}$  heißen

$$\Re(z) := x \text{ **Realteil** und } \Im(z) := y \text{ **Imaginärteil**}.$$

**Def.** Die Operation  $x + yi \mapsto x - yi$  heißt **komplexe Konjugation**. Man notiert sie mit einem Querstrich, also  $z \mapsto \bar{z}$  für  $z \in \mathbb{C}$ .

*Bemerkung.* Die komplexe Konjugation ist verträglich mit Addition und Multiplikation und sogar ein Körperautomorphismus.

**Def.** Der **Betrag** einer komplexen Zahl  $z = x + yi$  ist

$$|z| := \sqrt{x^2 + y^2} = \sqrt{z\bar{z}}.$$

**Satz.** Für komplexe Zahlen  $z, w \in \mathbb{C}$  gilt

$$\bullet |z + w| \leq |z| + |w| \quad (\Delta\text{-Ungl}) \quad \bullet |z| \cdot |w| = |z \cdot w|$$

**Def.** Die **Exponentialfunktion** ist die Abbildung

$$\exp : \mathbb{C} \rightarrow \mathbb{C}, \quad x \mapsto \sum_{k=0}^{\infty} \frac{x^k}{k!}.$$

**Satz.** Für alle  $x, y \in \mathbb{C}$  gilt  $\exp(x + y) = \exp(x) \cdot \exp(y)$ .

**Def.** Die **Eulersche Zahl** ist die Zahl

$$e := \exp(1) = \sum_{k=0}^{\infty} \frac{1}{k!} \approx 2,718.$$

**Notation.** Schreibe  $e^y := \exp(y)$  für alle  $y \in \mathbb{C}$ .

**Proposition.** Für alle  $t \in \mathbb{R}$  gilt  $|e^{ti}| = 1$ .

**Proposition.** Es gilt für alle  $t \in \mathbb{R}$ :

$$\bullet e^{2\pi i} = 1 \quad \bullet e^{\pi i} = -1 \quad \bullet e^{(2\pi + t)i} = e^{ti} \quad \bullet e^{ti} = \cos(t) + i \sin(t)$$

*Bemerkung.* Jede komplexe Zahl  $z \in \mathbb{C}$  lässt sich als  $z = |z| \cdot e^{si}$  mit  $s \in [0, 2\pi)$  darstellen. Mit  $w = |w| \cdot e^{ti}$  gilt  $z \cdot w = (|z| \cdot |w|) \cdot e^{i(s+t)}$ .

**Def.** Für  $z = |z| \cdot e^{ti} \in \mathbb{C}$  und  $n \in \mathbb{N}$  heißen die Zahlen

$$\sqrt[n]{|z|} e^{(t+k2\pi i)/n}$$

für  $k \in \{0, \dots, n-1\}$   **$n$ -te Wurzel** von  $z$ .

**Def.** Die  **$n$ -ten Einheitswurzeln** sind die Zahlen

$$\zeta_k := e^{2\pi i k/n} \quad \text{für } k = 0, \dots, n-1.$$

**Satz.** Jedes normierte Polynom vom Grad  $n \in \mathbb{N}$

$$f(x) = x^n + a_1x^{n-1} + \dots + a_n$$

mit Koeffizienten  $a_1, \dots, a_n \in \mathbb{C}$  hat eine Nullstelle in  $\mathbb{C}$ .

**Def.** Ein **Monoid** ist ein Tupel  $(M, \cdot, e)$  bestehend aus einer Menge  $M$  mit einer Verknüpfung  $\cdot : M \times M \rightarrow M$  und einem **neutralen Element**  $e \in M$ , sodass gilt:

- $\forall x, y, z \in G : (x \cdot y) \cdot z = x \cdot (y \cdot z)$  (Assoziativität)
- $\forall g \in G : e \cdot g = g = g \cdot e$  (Neutralität)

**Def.** Eine **Gruppe** ist ein Tupel  $(G, \cdot, e)$  bestehend aus einer Menge  $G$  mit einer Verknüpfung  $\cdot : G \times G \rightarrow G$  und einem **neutralen Element**  $e \in G$  zusammen mit einer Inversion  $^{-1} : G \rightarrow G$ , sodass:

- $\forall x, y, z \in G : (x \cdot y) \cdot z = x \cdot (y \cdot z)$  (Assoziativität)
- $\forall g \in G : e \cdot g = g = g \cdot e$  (Neutralität)
- $\forall g \in G : g \cdot g^{-1} = g^{-1} \cdot g = e$

**Def.** Ein **Ring** ist ein Tupel  $(R, +, \cdot, 0, 1)$  bestehend aus einer Menge  $R$ , zwei Verknüpfungen  $+, \cdot : R \times R \rightarrow R$  und zwei Elementen  $0, 1 \in R$ , sodass

- $(R, +, 0)$  eine Gruppe bildet,
- $(R, \cdot, 1)$  einen Monoid bildet und
- folgende Distributivgesetze für alle  $a, b, c \in R$  erfüllt sind:  
 $(a + b) \cdot c = a \cdot c + b \cdot c, \quad a \cdot (b + c) = a \cdot b + a \cdot c.$

**Def.** Ein **Körper** ist ein Tupel  $(\mathbb{K}, +, \cdot, 0, 1)$  bestehend aus einer Menge  $\mathbb{K}$ , zwei Verknüpfungen  $+, \cdot : \mathbb{K} \times \mathbb{K} \rightarrow \mathbb{K}$  und zwei Elementen  $0, 1 \in \mathbb{K}$ , sodass

- $(\mathbb{K}, +, 0)$  eine Gruppe bildet,
- $(\mathbb{K} \setminus \{0\}, \cdot, 1)$  eine Gruppe bildet und
- folgende Distributivgesetze für alle  $a, b, c \in R$  erfüllt sind:  
 $(a + b) \cdot c = a \cdot c + b \cdot c, \quad a \cdot (b + c) = a \cdot b + a \cdot c.$

*Bemerkung.* Jeder Körper ist auch ein Ring.

**Notation.**  $\mathbb{K}[x] := \{\text{Polynome mit Koeffizienten in } \mathbb{K}\}$

*Bemerkung.* Die Menge aller Polynome über  $\mathbb{K}$  bildet einen Ring.

**Def.** In einem Ring  $R$  teilt ein Element  $g \in R$  ein anderes Element  $f \in R$ , geschrieben  $g \mid f$ , falls es ein  $h \in R$  mit  $g \cdot h = f$  gibt.

*Bemerkung.* Ein Ring, in dem Division mit Rest möglich ist (z. B. der Polynomring oder  $\mathbb{Z}$ ), wird **euklidischer Ring** genannt. In solchen Ringen kann man den euklidischen Algorithmus ausführen.

**Satz.** Ist  $x_0 \in \mathbb{K}$  eine Nullstelle des Polynoms  $f \in \mathbb{K}[x]$ , dann gilt  $(X - x_0) \mid f$ , genauer  $f = (x - x_0) \cdot g$  für ein  $g \in \mathbb{K}[x]$  mit  $\partial g = \partial f - 1$ .

**Korollar.** Ein Polynom  $f \in \mathbb{K}[x]$  vom Grad  $n \geq 1$  hat höchstens  $n$  Nullstellen.

**Korollar.** Wenn  $\mathbb{K}$  unendlich viele Elemente hat, sind die Koeffizienten von jedem  $f \in \mathbb{K}[x]$  durch die Fkt.  $f$  eindeutig bestimmt.

**Satz** (Hauptsatz der Algebra). Jedes Polynom  $f \in \mathbb{C}[x]$  ist Produkt von Polynomen vom Grad 1, sogenannten Linearfaktoren, also

$$f = a \cdot (x - x_1) \cdot \dots \cdot (x - x_n) \quad \text{mit } a, x_1, \dots, x_n \in \mathbb{C}.$$

*Bemerkung.* Die Zahlen  $x_1, \dots, x_n$  müssen nicht alle verschieden sein.

**Def.** Die Anzahl der Vorkommen einer Nullstelle  $x_i$  in obiger Produktdarstellung heißt **Vielfachheit** der Nullstelle.

**Def.** Die **Ableitung** des Polynoms

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_0 \in \mathbb{K}[x]$$

ist das Polynom

$$f'(x) = na_0x^{n-1} + (n-1)a_1x^{n-2} + \dots + a_{n-1}.$$

*Bemerkung.* Sei  $x_i$  eine  $k$ -fache Nullstelle von  $f \in \mathbb{C}[x]$ . Dann ist  $x_i$  auch eine  $(k-1)$ -fache Nullstelle von  $f'$ .

**Def.** Ein Körper  $\mathbb{K}$  mit der Eigenschaft, dass jedes Polynom  $f \in \mathbb{K}[x]$  in Linearfaktoren zerfällt, heißt **algebraisch abgeschlossen**.

**Def.** Eine Zahl  $c \in \mathbb{C}$  heißt **algebraisch**, wenn es ein Polynom  $f \in \mathbb{Q}[x]$ ,  $f \neq 0$  mit  $f(c) = 0$  gibt.

*Bemerkung.* Man kann zeigen, dass die Menge der algebraischen Zahlen ein abzählbarer, algebraisch abgeschlossener Körper ist.

**Def.** Die **elementarsymmetrischen Funktionen** in  $x_1, \dots, x_n$  sind die Polynome

$$e_k(x_1, \dots, x_n) := \sum_{j_1 < \dots < j_k} x_{j_1} \cdot \dots \cdot x_{j_k} \quad \text{für } 1 \leq k \leq n.$$

*Bemerkung.* Bezeichne mit  $e_j$  für  $1 \leq j \leq n$  die elementarsymmetrischen Funktionen in den Variablen  $x_1, \dots, x_n$ , mit  $\tilde{e}_i$  für  $1 \leq i < n$  die elementarsymmetrischen Funktionen in den Variablen  $x_1, \dots, x_{n-1}$ . Dann gelten die Rekursionsgleichungen

$$e_1 = x^n + \tilde{e}_1, \quad e_i = \tilde{e}_i + x_n \cdot \tilde{e}_{i-1}, \quad e_n = x_n \cdot \tilde{e}_{n-1}.$$

**Satz** (Vieta). Sei  $f \in \mathbb{K}[X]$  ein normiertes Polynom, das über  $\mathbb{K}$  in Linearfaktoren zerfällt, also

$$f(x) = x^n + a_1x^{n-1} + \dots + a_n = (x - x_1) \cdot \dots \cdot (x - x_n),$$

dann gilt  $a_j = (-1)^j e_j(x_1, \dots, x_n)$  für alle  $1 \leq j \leq n$ .

**Def.** Eine **Permutation** der Zahlen  $\{1, \dots, n\}$  ist eine Bijektion

$$\sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\}.$$

Die Menge dieser Permutationen heißt **symmetrische Gruppe**  $S_n$ .

**Def.** Ein Polynom  $f \in \mathbb{K}[x_1, \dots, x_n]$  heißt **symmetrisch**, falls für alle  $x_1, \dots, x_n \in \mathbb{K}$  und Permutationen  $\sigma$  gilt:

$$f(x_1, \dots, x_n) = (\sigma f)(x_1, \dots, x_n) := f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$$

**Satz** (Hauptsatz über symmetrische Polynome). Jedes symmetrische Polynom  $f(\vec{x})$  mit  $\vec{x} = (x_1, \dots, x_n)$  lässt sich als Polynom in den elementarsymmetrischen Polynomen  $e_1(\vec{x}), \dots, e_n(\vec{x})$  darstellen.

**Korollar.** Sind  $x_1, \dots, x_n$  die Wurzeln eines normierten Polynoms  $f(x) = x^n + a_1x^{n-1} + \dots + a_n$ , dann gilt für jedes symmetrische Polynom  $s \in \mathbb{K}[y_1, \dots, y_n]$ :  $s(x_1, \dots, x_n)$  ist ein Polynomausdruck in den Koeffizienten  $a_1, \dots, a_n$  und damit aus diesen Zahlen berechenbar.

**Def.** Die **Diskriminante** eines Polynoms  $f = (x - x_1) \cdot \dots \cdot (x - x_n)$  ist der Ausdruck

$$\Delta(\vec{x}) := \pm \prod_{i \neq j} (x_i - x_j).$$

Da dieser Polynomausdruck symmetrisch ist, lässt er sich in den Koeffizienten des Polynoms  $f$  darstellen.

**Bsp.** Die Diskriminante des quadratischen Polynoms  $f(x) = x^2 - ax + b$  ist  $-\Delta = a^2 - 4b$ , die des kubischen Polynoms  $g(x) = x^3 - ax^2 + bx - c$  ist  $\Delta = a^2b^2 - 4a^3c - 4b^3 + 18abc - 27c^3$ .

**Def.** Seien  $\omega$  eine  $n$ -te Einheitswurzel, d. h.  $\omega^n = 1$  und  $x_1, \dots, x_n$  die Nullstellen von  $x^n + a_1x^{n-1} + \dots + a_n = 0$ , dann heißt

$$u_\omega := x_n + \omega x_{n-1} + \dots + \omega^{n-1} x_1 \quad \textbf{Lagrangesche Resolvente}.$$

*Bemerkung.* Es gilt  $\sigma u_\omega = \omega u_\omega$  für  $\sigma = (123 \dots n)$ .

**Def.** Ein **Gruppen-Homomorphismus** zwischen  $(G, *_G)$  und  $(H, *_H)$  ist eine Abbildung  $\phi : G \rightarrow H$ , sodass für alle  $g, h \in G$  gilt:

- $\phi(g *_G h) = \phi(g) *_H \phi(h)$
- $\phi(g)^{-1} = \phi(g^{-1})$

**Def.** Ein **Gruppen-Isomorphismus** ist ein bijektiver Gruppen-Homomorphismus. Die Umkehrabbildung ist automatisch ebenfalls ein Gruppen-Isomorphismus.

**Def.** Zwei Gruppen  $G$  und  $H$  heißen **isomorph** (notiert  $G \cong H$ ), wenn es einen Gruppenisomorphismus zwischen ihnen gibt. Dann ist die Umkehrabbildung ebenfalls ein Gruppenisomorphismus.

**Bspe.**

- $(\mathbb{Z}, +, 0)$  ist eine kommutative Gruppe.
- Die Menge der  $n$ -ten Einheitswurzeln bilden eine Gruppe  $(\Omega_n, \cdot, 1)$  mit  $\Omega_n := \{e^{2i\pi k/n} \mid 0 \leq k \leq n-1\}$

**Def.** Eine **Untergruppe** einer Gruppe  $(G, *, e)$  ist eine Teilmenge  $H \subset G$ , für die  $(H, *|_{H \times H}, e)$  selbst eine Gruppe ist, d. h. es gilt

$$\bullet e \in H \quad \bullet \forall h, h' \in H : h * h' \in H \quad \bullet \forall h \in H : h^{-1} \in H.$$

**Def.** Eine **Wirkung (Operation)** einer Gruppe  $(G, *, e)$  auf einer Menge  $X$  ist ein Gruppenhomomorphismus  $\phi : G \rightarrow \text{Aut}(X)$ , wobei  $\text{Aut}(X)$  die Menge der Bijektionen von  $X$  nach  $X$  bezeichnet bzw. äquiv. eine Abb.  $\phi : G \times X \rightarrow X, (g, x) \mapsto gx := \phi(g, x)$ , für die gilt:

$$\bullet \phi(e, -) = \text{id}_X, \quad \bullet \forall g, h \in G : \phi(g, -) \circ \phi(h, -) = \phi(g * h, -).$$

**Def.** Für jede Gruppenwirkung  $\phi$  von  $G$  auf  $X$  und jedes Element  $x \in X$  ist  $G_x := \{g \in G \mid gx = x\}$  eine Untergruppe von  $G$ , die **Standgruppe** oder **Stabilisator** von  $x$  unter  $\phi$ .

**Def.** Für  $x \in X$  heißt  $Gx := \{gx \mid g \in G\}$  **Orbit** oder **Bahn** von  $x$ .

*Bemerkung.* Für alle  $g \in G$  und  $x \in X$  gilt:  $Gx = G(gx)$ .

*Bemerkung.* Für alle  $x' = gx \in Gx$  für ein  $g \in G$  gilt  $Gx \cong G_{x'}$ , genauer  $G_{x'} = gG_xg^{-1}$ .

**Satz.** Für eine endliche Gruppe  $G$ , eine Menge  $X$  mit Gruppenwirkung  $\phi : G \times X \rightarrow X$  gilt:  $|Gx| = \frac{|G|}{|G_x|}$ .

**Def.** Für eine Untergruppe  $H \subset G$  und  $g \in G$  heißt

- $gH := \{gh \mid h \in H\}$  **Linksnebenklasse** von  $H$ ,
- $Hg := \{hg \mid h \in H\}$  **Rechtsnebenklasse** von  $H$ .

**Def.** Ein **Normalteiler** einer Gruppe  $(G, *, e)$  ist eine Untergruppe  $H$ , die die folgenden äquivalenten Bedingungen erfüllt:

- Links- und Rechtsnebenklassen sind gleich:  $\forall g \in G : gH = Hg$
- $\forall g \in G : gHg^{-1} = H$       •  $\forall g \in G, h \in H : ghg^{-1} \in H$

**Def.** Seien  $i, j \in \{1, \dots, n\}$  mit  $i \neq j$ . Dann ist die **Transposition** von  $i$  und  $j$  die Abbildung, die  $i$  und  $j$  vertauscht, also

$$(ij) : \{1, \dots, n\} \rightarrow \{1, \dots, n\}, \quad k \mapsto \begin{cases} j, & \text{falls } k = i, \\ i, & \text{falls } k = j, \\ k, & \text{sonst} \end{cases}$$

*Bemerkung.* Jede Permutation kann als Komposition von Transpositionen geschrieben werden.

**Def.** Ein **Fehlstand** einer Permutation  $\sigma$  auf  $\{1, \dots, n\}$  ist ein Zahlenpaar  $(i, j)$  mit  $i < j$  und  $\sigma(i) > \sigma(j)$ .

**Def.** Zwei Zahlen  $a, b \in \mathbb{Z}$  haben gleiche **Parität**, falls  $a \equiv b \pmod{2}$ , also  $a - b$  gerade ist.

**Proposition.** Die Anzahl der Fehlstände einer Permutation  $\sigma$  hat die gleiche Parität wie die Anzahl der Transpositionen in einer Darstellung von  $\sigma$  als Komposition von Transpositionen.

**Def.** Die Untergruppe  $A_n \subset S_n$  der symmetrischen Gruppe besteht aus allen Transpositionen mit gerader Anzahl an Fehlstellungen und heißt **Alternierende Gruppe**.

**Def.** Die **Galoisgruppe** eines Polynoms  $f$  ist die Untergruppe von  $G \subset S_n$ , die alle uns bekannten algebraischen Relationen zwischen den Wurzeln von  $f$  enthält.