Zusammenfassung Algebra 1

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

Def. Ein **Polynom** mit Unbestimmter X hat die Form
$$f(X) = a_0X^n + a_1X^{n-1} + ... + a_{n-1}X + a_n.$$

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

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

Bem. 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 $k \leqslant n$ schreibe $\binom{n}{k} := \frac{n!}{k!\cdot(n-k)!}$.

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

Verfahren (Tschirnhaus-Transformation)**.** Sei eine Polynomgleichung der Form
$$x^n + a_1x^{n-1} + ... + a_{n-1}x + a_n = 0$$
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.

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

Kor (Mitternachtsformel)**.** Die Polynomgleichung zweiten Grades $x^2 + ax + b = 0$ wird gelöst durch
$$x = -\tfrac{a}{2} \pm \tfrac{1}{2}\sqrt{a^2 - 4b}.$$

Satz. Eine Nullstelle der kubischen Gleichung $x^3 + ax - b = 0$ ist gegeben durch
$$x = \sqrt[3]{\tfrac{b}{2} + \sqrt{D}} + \sqrt[3]{\tfrac{b}{2} - \sqrt{D}} \quad \text{mit } D := (\tfrac{a}{3})^3 + (\tfrac{b}{2})^2.$$

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

Def. Für eine komplexe Zahl $z = x + yi$ mit $x, y \in \mathbb{R}$ heißen
$$\Re(z) := x \text{ **Realteil** } \quad \text{und} \quad \Im(z) := y \text{ **Imaginärteil**}.$$

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

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

Def. Der **Betrag** einer komplexen Zahl $z = x + yi$ ist
$$|z| := \sqrt{x^2 + y^2} = \sqrt{z\overline{z}}.$$

Satz. Für komplexe Zahlen $z, w \in \mathbb{C}$ gilt
- $|z + w| \leqslant |z| + |w|$ ($\triangle$-Ungl)
- $|z| \cdot |w| = |z \cdot w|$

Def. Die **Exponentialfunktion** ist die Abbildung
$$\exp : \mathbb{C} \to \mathbb{C}, \quad x \mapsto \sum_{k=0}^{\infty} \tfrac{x^k}{k!}.$$

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

Def. Die **Eulersche Zahl** ist die Zahl
$$e := \exp(1) = \sum_{k=0}^{\infty} \tfrac{1}{k!} \approx 2,718.$$

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

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

Prop. Es gilt für alle $t \in \mathbb{R}$:
- $e^{2\pi i} = 1$
- $e^{\pi i} = -1$
- $e^{(2\pi+t)i} = e^{ti}$
- $e^{ti} = \cos(t) + i\sin(t)$

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

Def. Die **n-ten Einheitswurzeln** sind die Zahlen
$$\zeta_k := e^{2\pi ik/n} \quad \text{für } k = 0, ..., n-1.$$

Satz. Jedes normierte Polynom vom Grad $n \in \mathbb{N}$
$$f(x) = x^n + a_1x^{n-1} + ... + a_n$$
mit Koeffizienten $a_1, ..., a_n \in \mathbb{C}$ hat eine Nullstelle in $\mathbb{C}$.

Def. Ein **Monoid** ist ein Tupel $(M, \cdot, e)$ bestehend aus einer Menge M mit einer Verknüpfung $\cdot : M \times M \to M$ 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 $\cdot : G \times G \to G$ und einem **neutralen Element** $e \in G$ zusammen mit einer Inversion $-^{-1} : G \to G$, 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. Eine Gruppe G heißt **abelsch**, wenn sie kommutativ ist, d. h. es gilt $ab = ba$ für alle $a, b \in G$.

Def. Ein **Ring** ist ein Tupel $(R, +, \cdot, 0, 1)$ bestehend aus einer Menge R, zwei Verknüpfungen $+, \cdot : R \times R \to R$ 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:
$$(a + b) \cdot c = a \cdot c + b \cdot c, \qquad a \cdot (b + c) = a \cdot b + a \cdot c.$$

Def. Ein **Körper** ist ein Tupel $(\mathbb{K}, +, \cdot, 0, 1)$ bestehend aus einer Menge $\mathbb{K}$, zwei Verknüpfungen $+, \cdot : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ und zwei Elementen $0, 1 \in \mathbb{K}$, sodass
- $(\mathbb{K}, +, 0)$ eine Gruppe bildet,
- $(\mathbb{K}\backslash\{0\}, \cdot, 1)$ eine Gruppe bildet und
- folgende Distributivgesetze für alle $a, b, c \in R$ erfüllt sind:
$$(a + b) \cdot c = a \cdot c + b \cdot c, \qquad a \cdot (b + c) = a \cdot b + a \cdot c.$$

Bem. Jeder Körper ist auch ein Ring.

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

Bem. 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.

Bem. 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 $\partial g = \partial f - 1$.

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

Kor. Wenn $\mathbb{K}$ unendlich viele Elemente hat, sind die Koeffi- zienten 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

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

Bem. Die Zahlen $x_1, \ldots, x_n$ 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

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_0 \in \mathbb{K}[x]$$

ist das Polynom

$$f'(x) = n a_0 x^{n-1} + (n-1) a 1 x^{n-2} + \ldots + a_{n-1}.$$

Bem. 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.

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

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

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

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

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

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

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_n = (x - x_1) \cdot \ldots \cdot (x - x_n),$$

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

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

$$\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}.$$

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

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

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

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

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

Def. Die **Diskriminante** eines Polynoms $f = (x - x_1) \cdot \ldots \cdot (x - x_n)$ 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 $\Delta = a^2 b^2 - 4a^3 c - 4b^3 + 18abc - 27c^3$.

Def. Seien ω eine n-te Einheitswurzel, d. h. $\omega^n = 1$ und $x_1, \ldots, x_n$ die Nullstellen von $x^n + a_1 x^{n-1} + \ldots + a_n = 0$, dann heißt

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

Bem. Es gilt $\sigma u_\omega = \omega u_\omega$ für $\sigma = (123 \cdots n)$.

Def. Ein **Gruppen-Homomorphismus** zwischen $(G, *_G)$ und $(H, *_H)$ ist eine Abbildung $\phi : G \to H$, 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 $\Omega_n := \{e^{2i\pi k/n} \mid 0 \leqslant k \leqslant n - 1\}$

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

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

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

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

Def. Für jede Gruppenwirkung ϕ 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 ϕ.

Def. Eine Gruppenwirkung ϕ von G auf X heißt **transitiv**, falls es für alle $x_1, x_2 \in X$ ein $g \in G$ mit $\phi(g, x_1) = x_2$ gibt.

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

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

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

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

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

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

Bem. Jede Permutation kann als Komposition von Transpositionen geschrieben werden.

Def. Ein **Fehlstand** einer Permutation σ auf $\{1, \ldots, n\}$ 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.

Prop. Die Anzahl der Fehlstände einer Permutation σ hat die gleiche Parität wie die Anzahl der Transpositionen in einer Darstellung von σ als Komposition von Transpositionen.

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

Def. Ein Polynom $f \in \mathbb{K}[x]$ heißt **separabel**, falls alle Nullstellen voneinander verschieden sind.

Bem. Ein Polynom vom Grad $\geqslant 1$ ist genau dann separabel, falls seine Diskriminante ungleich 0 ist.

Def. Sei $f \in \mathbb{K}[x]$ ein separables Polynom mit Nullstellen $x_1, \ldots, x_n$.

- Eine **algebraische Relation** zwischen den Nullstellen über $\mathbb{K}$ ist ein Polynom $f \in \mathbb{K}[x_1, \ldots, x_n]$ mit $f(\alpha_1, \ldots, \alpha_n) = 0$.

- Die **Galoisgruppe** G von f ist die Gruppe aller n-stelligen Permutationen, die alle algebraischen Relationen erhalten, d. h.

$$G := \{\sigma \in S_n \mid \forall\, f \in \mathbb{K}[x_1, ..., x_n] : f(\alpha_1, ..., \alpha_n) = 0 \implies (\sigma f)(\alpha_1, ..., \alpha_n) = 0\}.$$

Lem. Sei $f \in \mathbb{K}[x]$ reduzibel, d. h. $f = gh$ für zwei nicht-konstante Polynome $g, h \in \mathbb{K}[x]$. Dann wirkt die Galois nicht transitiv.

Bsp. Sei $f \in \mathbb{K}[x]$ separabel mit Diskriminante Δ. Angenommen,

$$D = \sqrt{\Delta} = \prod_{i<j} (x_i - x_j) \in \mathbb{K}.$$

Dann gilt $G \subset A_n$ für die Galoisgruppe G von f, da Transpositionen gerade das Vorzeichen von $\sqrt{\Delta}$ vertauschen.

Bsp. Die Galoisgruppe des Polynoms $f(x) = x^n - 1$, dessen Nullstellen **n-te Einheitswurzeln** genannt werden, ist

$$G = \{m \mapsto k \cdot m \pmod n \mid k \in \{1, ..., n-1\}, \mathrm{ggT}(k, n) = 1\}.$$

Bem. Der **Ikosaeder** ist der platonische Körper, der 20 gleichseitige Dreiecke als Seitenflächen, 12 Eckpunkte und 30 Kanten besitzt. Seine Drehgruppe ist die A_5.

Körpererweiterungen

Lem. Sei p eine Primzahl. Dann ist jedes Element $n \not\equiv 0 \pmod p$ invertierbar, d. h. es gibt $m \in \mathbb{Z}$ mit $n \cdot m \equiv 1 \pmod p$.

Def. Sei $p \in \mathbb{N}$ eine Primzahl. Dann bilden die Restklassen modulo p einen Körper $\mathbb{F}_p := \mathbb{Z}/(p\mathbb{Z})$.

Def. Ein Körper $\mathbb{K}$ hat **Charakteristik** $p \in \mathbb{N}\backslash\{0\}$, falls $1 + ... + 1 = 0$ (p-Mal die 1) in $\mathbb{K}$ gilt. Falls es kein solches p gibt, so hat der Körper Charakteristik 0.

Def. Sei R ein Ring. Ein **Ideal** in R ist eine Teilmenge $I \subset R$, für die gilt: $\forall\, r \in R, i \in I : ri \in I$ („Magneteigenschaft“).

Def. Ein Ideal $I \subset R$ heißt **maximal**, falls es kein Ideal $J \subsetneq R$ mit $I \subsetneq J$ gibt.

Bem. Für jede Primzahl p ist $p\mathbb{Z} := \{pz \mid z \in \mathbb{Z}\}$ ein maximales Ideal.

Def. Ein **Teilkörper** eines Körpers $\mathbb{L}$ ist eine Teilmenge $\mathbb{K} \subset \mathbb{L}$ mit $\{0, 1\} \subset \mathbb{K}$, die unter Multiplikation, Addition und multiplikativer und additiver Inversenbildung abgeschlossen ist.

Def. Sei $\mathbb{K} \subset \mathbb{C}$ ein Teilkörper und $\alpha_1, ..., \alpha_n \in \mathbb{C}$. Dann ist die Körpererweiterung $\mathbb{K}(\alpha_1, ..., \alpha_n)$ der Körper, der aus $\mathbb{K}$ durch Hinzufügen („Adjungieren“) von $\alpha_1, ..., \alpha_n$ und allen durch Multiplikation, Addition und Inversenbildung entstehenden Zahlen besteht.

Def. Eine Körpererweiterung $\mathbb{L} \supset \mathbb{K}$ heißt **endlich**, falls es Elemente $\alpha_1, ..., \alpha_k \in \mathbb{L}$ gibt, sodass jede Zahl $y \in \mathbb{K}$ eindeutig als Linearkombination $y = \lambda_1\alpha_1 + ... + \lambda_k\alpha_k$ mit $\lambda_1, ..., \lambda_k \in \mathbb{K}$ geschrieben werden kann. Die Zahl $[\mathbb{L} : \mathbb{K}] := k$ wird **Grad** der Körpererweiterung genannt.

Bem. Der Schnitt von beliebig vielen Teilkörpern ist ein Teilkörper. Man kann also $\mathbb{K}(\alpha_1, ..., \alpha_n)$ auch als kleinsten Teilkörper von $\mathbb{C}$, der die Menge $\mathbb{K} \cup \{\alpha_1, ..., \alpha_n\}$ enthält, beschreiben.

Def. Sei $f \in \mathbb{K}[x]$ und α eine Nullstelle von f. Das Polynom f heißt **Minimalpolynom** von α, falls für alle Polynome $g \in \mathbb{K}[x]$ gilt: $g(\alpha) = 0 \implies f \mid g$ (insbesondere).

Def. Ein Polynom $f \in \mathbb{K}[x]$ heißt **irreduzibel** über $\mathbb{K}$, falls es keine Zerlegung von f als $f = gh$ mit nicht konstanten $g, h \in \mathbb{K}[x]$ gibt.

Def. Sei $f \in \mathbb{K}[x]$ normiert, irreduzibel und α eine Nullstelle von f. Dann heißt f **Minimalpolynom** von α.

Bem. Sei α eine Nullstelle eines Polynoms $f \in \mathbb{Q}[x]$. Dann existiert ein eindeutiges, irreduzibles Polynom $g \in \mathbb{K}[x]$ mit $g(\alpha) = 0$.

Satz. Sei α eine Nullstelle eines irreduziblen Polynoms $f \in \mathbb{K}[x]$. Dann ist $\{1, \alpha, ..., \alpha^{n-1}\}$ eine Basis von $\mathbb{K}(\alpha)$.

Kor. $\mathbb{K}(\alpha) = \mathbb{K}[\alpha]$ und $[\mathbb{K}(\alpha) : \mathbb{K}] = n$.

Def. Wir betrachten die Zahlenebene $\mathbb{C}$. Eine Zahl $z \in \mathbb{C}$ heißt aus vorgegebenen Zahlen $\alpha_1, ...\alpha_k$ **konstruierbar**, wenn z der Schnitt zweier Kreise, zweier Geraden oder einer Geraden und eines Kreises ist, wobei wir nur solche Geraden betrachten, die durch zwei vorgegebenen Zahlen laufen und solche Kreise, die als Mittelpunkt eine vorgegebene Zahl haben und durch eine vorgegebene Zahl laufen.

Def. Eine Zahl $z \in \mathbb{C}$ heißt (in $k-2$ Schritten) **konstruierbar**, falls es eine Zahlenfolge $z_0 = 0, z_1 = 1, z_2, ..., z_k = k$ gibt, sodass z_m aus $z_0, ..., z_{m-1}$ für alle $m \geqslant 3$ konstruierbar ist.

Def. Sei x aus $0, 1, \alpha_1, ..., \alpha_k$ konstruierbar. Dann gilt

$$[\mathbb{Q}(\alpha_1, ..., \alpha_k, x) : \mathbb{Q}(\alpha_1, ..., \alpha_k)] \in \{1, 2\}.$$

Lem. Sind $\mathbb{K} \subset \mathbb{K}' \subset \mathbb{K}''$ endliche Körpererweiterungen, so gilt

$$[\mathbb{K}'' : \mathbb{K}] = [\mathbb{K}'' : \mathbb{K}'] \cdot [\mathbb{K}' : \mathbb{K}].$$

Satz. Sei $\alpha \in \mathbb{C}$ in n Schritten konstruierbar. Dann gilt

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^k \text{ für ein } k \leqslant n.$$

Satz. $\sqrt[3]{2}$ ist keine konstruierbare Zahl.

Satz. Die Zahl $e^{\pi/9i}$ ist nicht konstruierbar. Folglich kann der Winkel $\pi/3 = 60^\circ$ nicht gedrittelt werden.

Lem. Ist $p = qr$ ein Produkt teilerfremder Zahlen. Dann ist das regelmäßige p-Eck genau dann konstruierbar, wenn das regelmäßige q-Eck und das regelmäßige r-Eck konstruierbar ist.

Lem. Sei $p \in \mathbb{N}$ prim. Dann ist das p-te Kreisteilungspolynom

$$f(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + ... + x + 1$$

irreduzibel. Sei $\zeta \in \mathbb{C}$ mit $f(\zeta) = 0$. Dann gilt $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$.

Lem. Sei $2^s + 1$ eine Primzahl. Dann ist s eine Zweierpotenz.

Bem. Zahlen der Form $2^{2^r} + 1$ heißen **Fermatzahlen**. Die ersten 5 Fermatzahlen 3, 5, 17, 257, 65537 sind Primzahlen, die sechste nicht.

Satz. Sei p eine Primzahl. Wenn das p-Eck konstruierbar ist, dann ist p eine Fermatzahl.

Satz (Gauß)**.** Das 17-Eck ist konstruierbar.

Def. Ein Polynom $f \in \mathbb{Z}[x]$ heißt **reduzibel** über $\mathbb{Z}$, falls es nicht konstante Polynome $g, h \in \mathbb{Z}[x]$ mit $f = gh$ gibt.

Def. Sei p eine Primzahl. Ein Polynom $f \in \mathbb{F}_p[x]$ heißt **reduzibel** über $\mathbb{F}_p$, wenn es nichtkonstante $g, h \in \mathbb{F}_p[x]$ mit $f = gh$ gibt.

Def. Angenommen, ein normiertes Polynom $f \in \mathbb{Z}[x]$ ist reduzibel über $\mathbb{Z}$. Dann ist auch f aufgefasst als $f \in \mathbb{F}_p[x]$ reduzibel.

Satz (Eisenstein)**.** Sei p eine Primzahl und $f = a_0x^n + a_1x^{n-1} + ... + a_n \in \mathbb{Z}[x]$ mit $p \mid a_i$ für $i \in \{1, ..., n\}$, aber $p \nmid a_0$ und $p^2 \nmid a_n$. Dann ist f irreduzibel über $\mathbb{Z}$.

Bem. Oft kann man das Eisenstein-Kriterium für $f \in \mathbb{Z}[x]$ nicht direkt anwenden. Dann kann man $g(x) := f(x + k)$ für eine Zahl $k \in \mathbb{Z}$ betrachten. Dann ist f genau dann über $\mathbb{Z}$ irreduzibel, wenn g es auch ist. Man kann also versuchen, k so zu wählen, dass man das Eisenstein-Kriterium auf g anwenden kann.

Def. Ein Polynom $f = a_0x^n + ... + a_n \in \mathbb{Z}[x]$ heißt **primitiv**, falls $\mathrm{ggT}(a_0, ..., a_n) = 1$.

Lem. Sind $g, h \in \mathbb{Z}[x]$ primitiv, dann ist es auch gh.

Satz. Wenn $f \in \mathbb{Z}[x] \subset \mathbb{Q}[x]$ über $\mathbb{Q}$ reduzibel ist, also $f = gh$ mit $g, h \in \mathbb{Q}[x]$, dann auch über $\mathbb{Z}$, genauer $f = g_0h_0$ für $g_0, h_0 \in \mathbb{Z}[x]$, wobei g_0 und h_0 rationale Vielfache von g bzw. h sind.

Kor. Die Nullstellen von normierten ganzzahligen Polynomen sind ganzzahlig oder irrational.

Def. Ein Homomorphismus zwischen Körpern $\mathbb{K}$ und $\mathbb{K}'$ ist eine Abbildung $f : \mathbb{K} \to \mathbb{K}'$, sodass für alle $a, b \in \mathbb{K}$ gilt:

$$f(0) = 0, \quad f(1) = 1, \quad f(a + b) = f(a) + f(b), \quad f(a \cdot b) = f(a) \cdot f(b).$$

Bem. Die Verknüpfung von Körperhomomorphismen ist ein Körperhomomorphismus. Falls f bijektiv ist, dann ist auch f^{-1} ein Körperhomomorphismus und f heißt Körperisomorphismus. Wenn zusätzlich $\mathbb{K} = \mathbb{K}'$ ist, so heißt f Körperautomorphismus.

Notation. $\mathrm{Aut}(\mathbb{K}) := \{\sigma : \mathbb{K} \to \mathbb{K} \mid \sigma \text{ Körperautomorphismus}\}$

Def. Die **Galoisgruppe** einer Körpererweiterung $\mathbb{L} \supset \mathbb{K}$ ist

$$G = \mathrm{Gal}(\mathbb{L}, \mathbb{K}) := \{\sigma \in \mathrm{Aut}(\mathbb{L}) \mid \sigma|_{\mathbb{K}} = \mathrm{id}_{\mathbb{K}} .\}$$

Def. Sei $f \in \mathbb{K}[x]$ separabel mit Nullstellen $x_1, ..., x_n$. Dann heißt $\mathbb{L} = \mathbb{K}(x_1, ..., x_n)$ **Zerfällungskörper** von f über $\mathbb{K}$. Die Körpererweiterung $\mathbb{L}$ wird dann **normal** genannt.

Lem. Sei $f \in \mathbb{K}[x]$ und $N(f, \mathbb{L}) := \{x \in \mathbb{L} \mid f(x) = 0\}$. Dann gilt für alle $\sigma \in \mathrm{Gal}(\mathbb{L}, \mathbb{K})$:

- $f(\sigma x) = \sigma f(x)$ für jedes $x \in \mathbb{L}$
- $\sigma N(f, \mathbb{L}) = N(f, \mathbb{L})$

Bem. Sei $f \in \mathbb{K}[x]$ separabel mit Nullstellen $N(f) := x_1, ..., x_n$ und $\mathbb{L} = \mathbb{K}(x_1, ..., x_n)$. Wegen Punkt 2 wirkt die Galoisgruppe $\mathrm{Gal}(\mathbb{L}, \mathbb{K})$ auf der Nullstellenmenge $N(f) = N(f, \mathbb{L})$. Wenn man die Nullstellen durchnummeriert, erhält man eine Abbildung $\phi : \mathrm{Gal}(\mathbb{L}, \mathbb{K}) \to S_n$, sodass $\forall\, j \,:\, x_{\phi(\sigma)(j)} = \sigma(x_j)$.

Lem. Sei $\mathbb{L} = \mathbb{K}(x_1, ..., x_n)$ wie in der Bemerkung. Dann ist $\phi : G \to S_n$ injektiv und identifiziert G mit einer Untergruppe von S_n.

Satz. Sei $f \in \mathbb{K}[x]$ separabel mit Nullstellen $x_1, ..., x_n$ und $\mathbb{L} := \mathbb{K}(x_1, ..., x_n)$ der Zerfällungskörper von f. Sei

$$R := \{h \in \mathbb{K}[x_1, ..., x_n] \,|\, h(x_1, ..., x_n) = 0\}$$

die Menge der algebraischen Relationen zwischen $x_1, ..., x_n$. Dann ist

$$\phi(G) = \{\sigma \in S_n \,|\, \forall\, H \in R \,:\, \sigma H \in R\}.$$

Bem. Folglich entspricht die Galoisgruppe des Zerfällungskörpers von f über dem Grundkörper der vorher definierten Galoisgruppe von f.

Satz. Sei $\sigma : \mathbb{K} \to \tilde{\mathbb{K}}$ ein Körperisomorphismus, das Polynom $f \in \mathbb{K}[x]$ separabel mit Zerfällungskörper $\mathbb{L}$ sowie $\tilde{f} = \sigma f$ mit Zerfällungskörper $\tilde{\mathbb{L}}$. Dann gilt

$$|\{\hat{\sigma} \in \mathrm{Iso}(\mathbb{L}, \tilde{L}) \,|\, \hat{\sigma}|_{\mathbb{K}} = \sigma\}| = [\mathbb{L} : \mathbb{K}].$$

Kor. Ist $\mathbb{L} \supset \mathbb{K}$ der Zerfällungskörper eines separablen Polynoms $f \in \mathbb{K}[x]$, so gilt

$$|\mathrm{Gal}(\mathbb{L}, \mathbb{K})| = [\mathbb{L} : \mathbb{K}].$$

Bem. Angenommen, die Nullstellen eines separablen Polynoms $f \in \mathbb{K}[x]$ lassen sich durch einen Wurzelausdruck angeben. Dann muss es Reihen von Zahlen $\alpha_1, ..., \alpha_s \in \mathbb{L}$ und $n_1, ..., n_s \in \mathbb{N}$ und Körpererweiterungen $\mathbb{K}_0 \subset ... \subset \mathbb{K}_s$ geben mit

$$\mathbb{K}_0 = \mathbb{Q}, \quad \mathbb{K}_{j+1} = \mathbb{K}_j(\alpha_j) \text{ mit } \alpha_j^{n_j} \in \mathbb{K}_j, \quad \mathbb{K}_s = \mathbb{L}.$$

Wir sagen, $\mathbb{L}$ komme durch Adjunktion von Wurzeln zustande.

Lem. Sind $\mathbb{K} \subset \mathbb{K}' \subset \mathbb{L}$ endliche Körpererweiterungen, so ist $\mathrm{Gal}(\mathbb{L}, \mathbb{K}')$ eine Untergruppe von $\mathrm{Gal}(\mathbb{L}, \mathbb{K})$. Sei $\mathbb{K}'$ der Zerfällungskörper des separablen Polynoms $g \in \mathbb{K}[x]$. Dann lassen die Elemente von $\mathrm{Gal}(\mathbb{L}, \mathbb{K})$ den Körper $\mathbb{K}$ invariant (d. h. $\sigma(\mathbb{K}') \subset \mathbb{K}'$ für alle $\sigma \in \mathrm{Gal}(\mathbb{L}, \mathbb{K})$) und $\mathrm{Gal}(\mathbb{L}, \mathbb{K}')$ ist ein Normalteiler von $\mathrm{Gal}(\mathbb{L}, \mathbb{K})$.

Lem. Seien $\mathbb{K} \subset \mathbb{K}'$ und $\mathbb{K}' \subset \mathbb{L}$ endliche, normale Körpererweiterungen. Dann gilt

$$\mathrm{Gal}(\mathbb{K}', \mathbb{K}) = \mathrm{Gal}(\mathbb{L}, \mathbb{K}) / \mathrm{Gal}(\mathbb{L}, \mathbb{K}').$$

Lem. Sei $\rho : G \to H$ ein Gruppenhomomorphismus. Dann ist $K := \ker(\rho) \subset G$ ein Normalteiler von G. Wenn ρ surjektiv ist, dann definiert ρ einen Isomorphismus

$$\overline{\rho} : G/K \to H, \quad gK \mapsto \rho(g)$$

Def. Eine Gruppe G heißt **auflösbar**, wenn es eine absteigende Reihe von Untergruppen

$$G = G_0 \supset G_1 \supset\supset ... \supset G_r = \{\mathrm{id}\}$$

gibt, sodass G_{j+1} ein Normalteiler in G_j und G_j / G_{j+1} für alle $j = 1, ..., r$ abelsch ist.

Satz. Sei $f \in \mathbb{K}[x]$ separabel mit Zerfällungskörper $\mathbb{L}$. Dieser komme durch Adjunktion von r Wurzeln der Grade $n_1, ..., n_r$ zustande. Der Grundkörper $\mathbb{K}$ möge alle n_j-ten Einheitswurzeln für $j = 1, ..., n$ enthalten. Dann ist die Gruppe $\mathrm{Gal}(\mathbb{L}, \mathbb{K})$ auflösbar.

Bem. Man kann auf die Voraussetzung verzichten, dass die n_j-ten Einheitswurzeln in $\mathbb{K}$ enthalten sind.

Satz. Die Gruppe A_n ist einfach für alle $n \geqslant 5$.

Lem. Sei $\mathbb{L} \supset \mathbb{K}$ eine Galoiserweiterung, $G = \mathrm{Gal}(\mathbb{L}, \mathbb{K})$ und $G_1 \subseteq G$ eine Untergruppe. Dann ist $\mathbb{L}$ der Zerfällungskörper eines irreduziblen Polynoms $g \in \mathbb{L}^{G_1}[x]$ und $G_1 = \mathrm{Gal}(\mathbb{L}, \mathbb{L}^{G_1})$.

Satz (Hauptsatz der Galoistheorie)**.** Sei $f \in \mathbb{K}[x]$ ein separables Polynom mit Zerfällungskörper $\mathbb{L}_f$ und $G := \mathrm{Gal}(\mathbb{L}, \mathbb{K})$.
Dann gibt es eine 1–1-Beziehung

$$\begin{aligned} \{\text{ Untergruppen } G_1 \subseteq G \ \} &\longleftrightarrow \{\text{ Zwischenkörper } \mathbb{K} \subseteq \mathbb{K}_1 \subseteq \mathbb{L} \ \} \\ G_1 &\longmapsto L^{G_1} := \{\alpha \in \mathbb{L} \,|\, \forall\, \sigma \in G_1 \,:\, \sigma\alpha = \alpha\} \\ \mathrm{Gal}(\mathbb{L}, \mathbb{K}_1) &\longleftarrow \mathbb{K}_1 \end{aligned}$$

Satz. Ist $\mathbb{L} = \mathbb{K}(\alpha_1, ..., \alpha_k)$ eine endliche Körpererweiterung, so gibt es ein **primitives Element** $\alpha \in \mathbb{L}$ mit $\mathbb{L} = \mathbb{K}(\alpha)$.