Algebra WiSe 17/18 Kurzskript
(Ohne Beweise und Beispiele)

Prof. Scheithauer
Mitschrift von Daniel Kallendorf
Danke an Sandra Kühne für ihre Mitschriften

Version vom 21. März 2018

Inhaltsverzeichnis

1 Wiederholung

Satz 1.1. *Seien $\mathfrak{a} \subset A$, dann*

a) $\mathfrak{a}$ ist Primideal $\Leftrightarrow$ $A/\mathfrak{p}$ ist Integritätsbereich (nullteilerfrei)

b) $\mathfrak{a}$ ist maximales Ideal $\Leftrightarrow$ $A/\mathfrak{a}$ ist ein Körper.

Bemerkung. Insbesondere ist jedes maximale ideal prim.

Definition 1.2. Sei $A \neq \emptyset$. Eine **Relation** auf A ist eine Teilmenge $R \subset A \times A$. R heißt **partielle Ordnung** wenn

a) $\forall a \in A$ gilt $(a, a) \in R$ (Reflexivität)

b) $\forall a, b, c \in A$ gilt $(a, b) \in R$ und $(b, c) \in R$, so gilt auch $(a, c \in R)$ (Transitivität)

c) $\forall a, b \in A$ mit $(a, b \in R)$ und $(b, a) \in \mathbb{R}$, dann gilt $a = b$. (Antisymmetrie)

Ist R eine partielle Ordnungn auf A so schrieben wir für $(a, b) \in R$ auch $a \leq b$.
Zwei Elemente $a, b \in A$ heißen **vergleichbar**, wenn $a \leq b$ oder $b \leq a$ ist.
Eine Teilmenge $B \subset A$ heißt **Kette**, wenn für alle $a, b \in B$ gilt, dass $a \leq b$ oder $b \leq a$.

Lemma 1.3. *Sei $A \neq \emptyset$ partielle geordnet. Hat jede Kette $B \neq \emptyset$ in A eine obere Schranke in A, d.h. es gibt ein $a \in A$,sodass $b \leq a$ für alle $b \in B$., so besitzt A ein maximales Element.*

Theorem 1.4. *Sei $A \neq 0$ ein Ring, dann besitzt A ein maximales Ideal.*

Korollar 1.5. *Sei A ein Ring und $I \subsetneq A$ ein Ideal, dann ist I in einem maximalen Ideal enthalten.*

Korollar 1.6. *Sei A ein Ring und $a \in A \setminus A^*$. Dann ist a in einem maximalen Ideal enthalten.*

1.1 Lokale Ringe

Definition 1.7. Ein Ring A mit nur eine maximalen Ideal $\mathfrak{m}$ heißt **lokaler Ring** und $A/\mathfrak{m}$ heißt **Restklassenkörper** von A.

Satz 1.8. *Sei A ein Ring und $\mathfrak{m} \neq A$ eine Ideal in A.*
Ist jedes $x \in A \setminus +m$ eine Einheit, si ist A ein lokaler Ring mit maximalen Ideal $\mathfrak{m}$.

Satz 1.9. *Sei A ein Ring und $\mathfrak{m} \subset A$ eine maximales Ideal, sodass jedes Element m eine Einheit in A ist. Dann ist A ein lokaler Ring.*

1.2 Radikale

Satz 1.11. *Sei A eine Ring und $N = \{a \in A \mid a \text{ ist nilpotent}\}$. Dann ist N ein Ideal in A und A/N enthält keine nilpotenten Elemente $\neq 0$.*

Definition 1.12. Das Ideal $N = \{a \in A \mid a \text{ ist Nilpotent}\}$ heißt das **Nilikal** von A.

Definition 1.13. Sei A ein Ring dann nennt man $J = \{x \in A \mid \forall y \in A : 1 - xy \text{ ist Einheit}\}$ das **Jacobsonradikal**.

Satz 1.14. *Sei A eine Ring, dann ist*

a) das Nilradikal von A der Schnitt aller Primideal von A.

b) das Jacobsonradikal von A der Schnitt aller Maximalen Ideale von A.

Definition 1.15. Sei A ein Ring und $\mathfrak{a} \subset A$ ein Ideal in A. Dann wird

$$r(a) := \{x \in A \mid x^n \in \mathfrak{a} \text{ für ein } n > 0\}$$

als **Radikal** von $\mathfrak{a}$ bezeichnet. (auch $\mathrm{Rad}(\mathfrak{a})$, $\sqrt{\mathfrak{a}}$)

Satz 1.16. *Sei $\mathfrak{a}, \mathfrak{b}$ ein Ideal, dann gilt*

a) $\mathfrak{a} \subseteq r(\mathfrak{a})$

b) $r\big(r(\mathfrak{a})\big) = r(\mathfrak{a})$

c) $r(\mathfrak{a}\mathfrak{a}) = r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b})$

d) $r(\mathfrak{a}) = A \Leftrightarrow \mathfrak{a} = A$.

e) $r(\mathfrak{a} + \mathfrak{b}) = r\big(r(\mathfrak{a}) + r(\mathfrak{b})\big)$.

1.2.1 Operationen auf Radikalen

Definition 1.17. Sein A ein Ring.

a) Seien $\mathfrak{a}, \mathfrak{b} \subset A$ Ideale in A.
Dann ist
$$a + b =: \{x + y \mid x \in \mathfrak{a}, y \in \mathfrak{b}\}$$
ein Ideal in A.

b) Analog: Sei $(\mathfrak{a}_i)_{i \in I}$ eine Familie von Idealen in A, für eine Indexmenge I.
Dann ist
$$\sum_{i \in I} \mathfrak{a}_i =: \left\{ \sum_{i \in I} x_i \mid x_i \in \mathfrak{a}_i \text{ und fast alle } x_i = 0 \right\}$$
ein Ideal in A.

c) Sei $(\mathfrak{a}_i)_{i \in I}$ eine Familie von Idealen in A, für eine Indexmenge I. Dann ist der Schnitt
$$\bigcap_{i \in I} \mathfrak{a}_i$$
ein Ideal in A.

d) Seien $\mathfrak{a}, \mathfrak{b} \subset A$ Ideal in A. Dann ist
$$\mathfrak{a}\mathfrak{b} = \left\{ \sum_{i=1}^{n} a_i b_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b}, n \in \mathbb{N} \right\}$$
ein Ideal in A.

Satz 1.18. *Die Operationen Summe, Durchschnitt und Produkt auf Idealen sind kommutativ und Assoziativ und es gilt das Distributivgesetz.*

Definition 1.19. Sei A ein Ring. Zwei Ideale $\mathfrak{a}, \mathfrak{b} \subseteq A$ heißen **teilerfremd**, wenn $\mathfrak{a} + \mathfrak{b} = A = (1)$.

Satz 1.20. *Sei A ein Ring, $\mathfrak{a}, \mathfrak{b} \subset A$ Ideale in A. Dann sind äquivalent:*

a) $\mathfrak{a}, \mathfrak{b}$ *sind Teilerfremd*

b) Es gibt ein $x \in \mathfrak{a}, y \in \mathfrak{b}$, sodass $x + y = 1$.

Satz 1.21. *Sei A ein Ring und seinen $\mathfrak{a}_1, ..., \mathfrak{a}_n$ paarweise teilerfremde Ideal in A. Dann gilt*

a) Jedes $\mathfrak{a}_i$ ist teilerfremd zu $\prod_{\substack{j=1 \\ j \neq i}}^{n} \mathfrak{a}_j$.

b) Es gilt
$$\prod_{i=1}^{n} \mathfrak{a}_i = \bigcap_{i=1}^{n} \mathfrak{a}_i$$

Definition 1.22. Sei A ein Ring und seinen $\mathfrak{a}_i, ..., \mathfrak{a}_n$ Ideale in A.
Wir definieren die Abbildung

$$\begin{aligned} \phi : A &\to \prod_{i=1}^{n} (A/\mathfrak{a}_i) \\ a &\mapsto (a + \mathfrak{a}_1, ..., a + \mathfrak{a}_n) \end{aligned}$$

Proposition 1.23. a) ϕ ist ein Ringhomomorphismus und

$$\mathrm{Kern}(\phi) = \bigcap_{i=1}^{n} \mathfrak{a}_i$$

b) ϕ ist genau dann surjektiv, wenn die $\mathfrak{a}_i$ paarweise disjunkt sind.
Insbesondere ist

$$A/\prod_{i=1}^{n} \mathfrak{a}_i \simeq \prod_{i=1}^{n} A/\mathfrak{a}_i$$

1.3 Ringe von Brüchen

Definition 1.24. Sei A ein Ring. Eine Teilmenge $S \subset A$ heißt **multiplikativ abgeschlossen**, wenn

a) Für alle $s, t \in S$ gilt, dass $st \in S$

b) $1 \in S$.

Bemerkung 1.25. Auf $A \times S$ wird durch

$$(a, s) \sim (b, t) \Leftrightarrow (at - bs)u = 0 \text{ für ein } u \in S$$

eine Äquivalenzklasse definiert.
Für die Transitivität wird die multiplikative Abgeschlossenheit von S benötigt.
Die Äquivalenzklassen von (a, s) wird mit a/s bezeichnet.
Die Menge der Äquivalenzklasssen wir als $S^{-1}A$ geschrieben.

Definition 1.26. Seien $a/s, b/t \in S^{-1}A$. Man definiert

- $a/s + b/t := (at + bs)/st$
- $a/s \cdot b/t := ab/st$

Definition 1.27. Diese Verknüpfungen sind wohldefiniert und versehen $S^{-1}A$ mit einer Ringstruktur.
$S^{-1}A$ wird als der **Ring der Brüche** von A bezüglich S bezeichnet.

Korollar 1.29. *Die Abbildung*

$$\begin{aligned} \varphi_S : A &\to S^{-1}A \\ a &\mapsto a/1 \end{aligned}$$

hat folgende Eigenschaften:

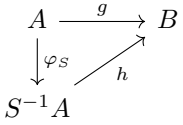
a) φ_S *ist ein Ringhomomorphismus. (i.A. nicht injektiv)*

b) Sei $s \in S$*, dann ist* $\varphi_S(s)$ *eine Einheit in* $S^{-1}A$*.*

c) $\mathrm{Kern}(\varphi_S) = \{a \in A \mid as = 0 \text{ für ein } s \in S\}$*.*

d) Jedes Element in $S^{-1}A$ *ist der Form* $\varphi_S(a)\varphi_S(s)^{-1}$ *für ein* $a \in A$*,* $s \in S$*.*

Satz 1.30. *Seien* A, B *Ringe und* $S \subset A$ *multiplikativ abgeschlossen. Sei* $g : A \to B$ *ein Ringhomomorphismus, der 1)-3) aus erfüllt, dann gibt es einen eindeutigen Isomorphismus* $h : S^{-1}A \to B$ *mit* $h \circ \varphi_S = g$*.*



Definition 1.31. Sei A ein Integritätsbereich und $S = A \setminus \{0\}$. Dann nennt man $S^{-1}A$ den **Quotientenkörper**

Lemma 1.32. *Der Quotientenkörper ist ein Körper,* φ_S *ist injektiv und wir können* A *mit seinem Bild in* $S^{-1}A$ *identifizieren.*

Definition 1.33. Sei A ein Ring. Sei $\mathfrak{p}$ ein Primideal in A. Man schreibt $A_\mathfrak{p}$ für $S^{-1}A$ und nennt $A_\mathfrak{p}$ die **Lokalisierung** von A bezüglich $\mathfrak{p}$.

Lemma 1.34. *Sei* A *ein Ring. Sei* $\mathfrak{p}$ *ein Primideal in* A*.*
Dann ist $S = A \setminus \mathfrak{p}$ *multiplikativ Abgeschlossen.*

Lemma 1.35. *Sei* $A = \mathbb{Z}$ *und* $p \in \mathbb{Z}$ *eine Primzahl. Dann ist* $\mathbb{Z}_{(p)} = \{m/n \mid m/n \in \mathbb{Q}, p \not| n\}$*.*

Satz 1.36. *Sei* A *ein Ring und* $S \subset A$ *multiplikativ abgeschlossen. Dann ist*

a) Ist I *ein Ideal in* A *so ist auch* $S^{-1}I = \{a/s \mid a \in I\}$ *ein Ideal in* $S^{-1}A$

b) Die Ideale in $S^{-1}A$ *sind der Form* $S^{-1}I$*, wobei* I *ein Ideal in* A *ist.*

c) Sind I, J *Ideal in* A*, dann gilt*

$$S^{-1}(I + J) = S^{-1}I + S^{-1}J$$
$$S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J$$
$$S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$$

1.4 Integritätsbereiche und Hauptidealringe

Definition 1.37. Sei A ein Ring. Ein Ideal der Form $(a) = Aa$ heißt **Hauptideal**.

Definition 1.38. Ein Ring A heißt **Hauptidealring**, wenn jede Ideal in A Hauptideal ist.

Definition 1.39. Ein Ring A heißt **euklidisch**, wenn es eine Abbildung

$$\lambda : A \setminus \{0\} \to \mathbb{N}_0$$

gibt, sodass zu je zwei Elementen $a, b \in A$ mit $b \neq 0$ Elemente $q, r \in A$ existieren mit $a = qb + r$ wobei $\lambda(r) < \lambda(b)$ oder $r = 0$.

Satz 1.41. *Sei A ein euklidischer Ring. Dann ist A ein Hauptidealring.*

Definition 1.42. Sei A ein Ring und seinen $a, b \in A$.
$d \in A$ heißt **Größter gemeinsamer Teiler** von a und b, wenn gilt

a) $d|a$ und $d|b$.

b) Wenn es $g \in A$ gibt mit $g|a$ und $g|b$, dann muss $g|d$.

Wir schreiben $d = \gcd(a, b) = (a, b)$

Definition 1.43. Sei A ein Ring und seinen $a, b \in A$.
$d \in A$ heißt **kleinstes gemeinsames Vielfaches** von a und b, wenn gilt

a) $a|v$ und $b|v$.

b) Wenn es $g \in A$ gibt mit $a|g$ und $b|g$, dann muss $v|v$.

Wir schreiben $v = \mathrm{lcm}(a, b) = (a, b)$

Satz 1.44. *Sei A ein Hauptidealring und seien $a, b \in A$.*
Dann existiert ein $d = \gcd(a, b)$ und $v = \mathrm{lcm}(a, b)$ von a, b und es gilt

a) $(a) + (b) = (d)$

b) $(a) \cap (b) = (v)$

Definition 1.45. Sei A in Integritätsbereich. Zwei Elemente $a, b \in A$ heißen **assoziiert**, wenn

- $a|b$ und $b|a$.
- (äquivalent) $a = bu$ für ein $u \in A^*$.
- (äquivalent) $(a) = (b)$.

Man schreibt dann $a \sim b$.

Definition 1.46. Sei A in Integritätsbereich. Ein Element $p \in A$ heißt **prim**, **Primelement**, wenn

- $p \notin A^*$, $p \neq 0$ und aus $p|ab$ folgt $p|a$ oder $p|b$.
- (äquivalent) $p \neq 0$ und (p) ist Primideal.

Definition 1.47. Sei A in Integritätsbereich. $c \in A$ heißt **irreduzibel** oder **unzerlegbar**, wenn

a) für $c \notin A^*$ und $c \neq 0$ aus $c = ab$ folgt, dass $a \in A^*$ oder $b \in A^*$.

b) (äquivalent) für $c \neq 0$ für alle $a \in A$ gilt, dass aus $(c) \subset (a)$ folgt, dass $(a) = A$ oder $(a) = (c)$.

Satz 1.48. *Sei A ein Integritätsbereich und $p \in A$ prim. Dann ist p irreduzibel.*

Satz 1.49. *Sei A ein Hauptidealring und Integritätsbereich. Dann gilt für $c \in A$*

$$c \text{ prim} \Leftrightarrow c \text{ irreduzibel}$$

Definition 1.50. Ein Integritätsbereich heißt **faktoriell**, wenn

a) Jedes $a \in A \setminus A^*$, $a \neq 0$ zerfällt in ein Produkt von irreduziblen Elementen.

b) Die Zerlegung ist bis auf Reihenfolge und Einheiten eindeutig. D.h.

D.h. wenn $a = c_1 \cdot ... \cdot c_m = d_1 \cdot ... \cdot d_n$ mit c_1, d_1 irreduzibel, so folgt $m = n$ und es gibt $\pi \in S_n$ mit $c_1 \sim d_{\pi(i)}$ für alle $i = 1, ..., n$.

Bemerkung 1.51. Die Eindeutigkeit der Faktorisierung impliziert, dass es irreduzibles Element in einem faktoriellen Integritätsbereich prim ist.

Lemma 1.52. *Sei A ein Hauptidealring und S eine nichtleere Menge von Idealen in A. Dann hat S ein maximales Element (bezüglich $\subset$)*

Theorem 1.53. *Sei A ein Integritätsbereich. Ist A ein Hauptidealring, so ist A faktoriell.*

1.5 Inverse und direkte Limiten

Definition 1.54. Man nennt I eine unter $\leq$ **partiell geordnete Menge**, wenn für alle $x, y, z \in I$ gilt

a) $x \leq x$.

b) Aus $x \leq y$ und $y \leq z$ folgt $x \leq z$.

c) Aus $x \leq y$ und $y \leq x$ folgt $x = y$.

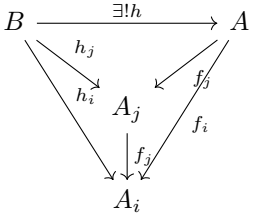
Definition 1.55. Für jedes $i \in I$sei A_i ein Ring und sei für jedes Paar $i, j \in I$ mit $i \leq j$ die Abbildung $f_{ij} : A_j \to A_i$ ein Ringhomomorphismus, sodass

a) $f_{ii} = \mathrm{id}_{A_i}$ für alle $i \in I$

b) $f_{ik} = f_{ij} \circ f_{jk}$ falls $i \leq j \leq k$.

Dann nennt man das System $(A_i, f_{ij})_{i,j \in I}$ **projektives System** von Ringen.

Definition 1.56. Ein Ring A zusammen mit dem Homomorphismus $f_i : A \to A_i$, sodass $f_i = f_{ij} \circ f_j$ für $i \leq j$ heißt **projektiver Limes** oder **inverser Limes** des Systems (A_i, f_{ij}), wenn folgende universelle Eingenschaft erfüllt ist:
Sind $h_u : B \to A_i$ für alle $i \in I$ Ringhomomorphismen mit $h_i = f_{ij} \circ h_j$ für $i \leq j$, so existiert genau ein Ringhomomorphismus $h : B \to A$ mit $h_i = f_i \circ h$ für alle $i \in I$.



Bemerkung 1.57. Falls ein projektiver Limes existiert, so ist er bis auf kanonische Isomorphie eindeutig:
Sind (A, f_i) und (B, h_i) projektive Limiten von (A_i, f_{ij}), so gibt es Homomorphismen $h : B \to A$ und $g : A \to B$, die die oben beschrieben Verträglichkeitsbedingungen erfüllen.
Durch Zusammensetzen dieser Homomorphismen erhalten wir Abbildungen Die Eindeutigkeitsbedingung Impliziert nun, dass $g \circ h = \mathrm{id}_B$ und $h \circ g = \mathrm{id}_A$.
Man schreibt auch $A = \varprojlim_{i \in I} A_i$ für den projektiven Limes des Systems (A_i, f_{ij}).

Satz 1.59. *Sei $x \in \mathbb{Z}_p$. Dann ist*

a) $x \in \mathbb{Z}_p^* \Leftrightarrow p \not| x$

b) Ist $x \neq 0$, so lässt sich x eindeutig schreiben als $x = p^n u$ mit $u \in \mathbb{Z}_p^*$ und $n \geq 0$.

Definition 1.60. Sei $x \in \mathbb{Z}_p$, $x \neq 0$. Schreibe $x = p^n u$ mit $u \in \mathbb{Z}_p^*$. Dann heißt

$$n = \nu_p(x)$$

die **p-adische Bewertung** von x.
Man setzt $\nu_p(0) = \infty$.
Man bezeichnet $|x|_p = p^{-\nu_p(x)}$ als den **p-adischen Betrag**.

Lemma 1.61. *Für die p-adische Bewertung gilt:*

a) $\nu_p(xy) = \nu_p(x) + \nu_p(y)$

b) $\nu_p(x + y) \geq \inf\{\nu_p(x), \nu_p(y)\}$

Satz 1.62. *$\mathbb{Z}_p$ ist ein Integritätsbereich.*
Der Quotientenkörper $\mathbb{Q}_p$ von $\mathbb{Z}_p$ wird als Körper der p-adischen Zahlen bezeichnet.
$\mathbb{Q}_p$ kann auch (analytisch) als Vervollständigung von $\mathbb{Q}$ bezüglich des p-adischen Betrage konstruiert werden.

Definition 1.63. Man nennt I eine unter $\leq$ **gerichtete Menge**, wenn für alle $x, yz \in I$ gilt

a) $x \leq x$

b) Aus $x \leq y$ und $y \leq z$ folgt $x \leq z$

c) Für alle x, y exitsiert ein $z \in I$mit $x \leq z$,$y \leq z$

Definition 1.64. Für jedes $i \in I$ sei ein Ring A_i und für jedes Paar $i, j \in I$ mit $i \leq j$ sei ein Ringhomomorphismus $f_{ij} : A_i \to A_j$ gegeben, mit

a) $f_{ii} = \mathrm{id}_{A_i}$ für alle $i \in I$

b) $f_{ik} = f_{jk} \circ f_{ij}$ für alle $i \leq j \leq k$

$$A_i \xrightarrow{f_{ij}} A_j \xrightarrow{f_{jk}} A_k$$
$$A_i \xrightarrow[f_{ik}]{} A_k$$

Ein solches System (A_j, f_{ij}) heißt **induktives System** von Ringen.

Definition 1.65. Ein Ring A zusammen mit dem einem Homomorphismus $f_i : A_i \to A$, sodass gilt $f_i = f_j \circ f_{ij}$ für $i \leq j$ heißt **induktiver Limes** oder **direkter Limes** des Systems (A_i, f_{ij}), wenn folgende Universelle Eigenschaft erfüllt ist:
Ist B ein Ring, und sind $h_i : A_i \to B$, $i \in I$ Ringhomomorphismen mit $h_i = h_j \circ f_{ij}$ für $i \leq j$, so existiert genau ein Ringhomomorphismus $h : A \to B$ mit $h_i = h \circ f_i$ für alle $i \in I$.

Lemma 1.66. *Falls ein indktiver Limes existiert, so ist er eindeutig.*

2 Polynomringe

2.1 Polynome mit einer Variable

Sei in diesem Abschnitt A ein Ring.

Definition 2.1. Sei $A[X]$ die Menge der Folgen $(a_0, a_1, ...,)$ mit $a_i \in A$ und $a_i = 0$ für fast alle $i \in \mathbb{N}$.
Die Elemente dieser Menge heißen **Polynome**.

Definition 2.2. $A[X]$ ist ein Ring mit

$$(a_0, a_1, ...,) + (b_0, b_1, ...) = (a_0 + b_0, a_1 + b_1, ...)$$
$$(a_0, a_1, ...,) \cdot (b_0, b_1, ...) = (c_0, c_1, ...)$$

mit $c_n = \sum_{k=0}^{n} a_{n-k} b_k$.
Das Nullelement ist $0 = (0, 0, ...)$ und $1 = (1, 0, 0, ...)$ ist das Neutrale Element der Multiplikation.

Definition 2.3. $A[X]$ wird als der **Polynomring** in der **Variablen** X bezeichnet.

Proposition 2.4. a) Die Abbildung $A \to A[X], a \mapsto (a, 0, 0, ...)$ ist ein Injektiver Ringhomomorphismus und A ist Unterring von $A[X]$.

b) Sei $X = (0, 1, 0, ...)$. Dann ist $X^n = (0, 0, ..., 0, 1, 0, ...)$ an n-ter Stelle und $aX^n = (0, ..., 0, a, 0, ...)$.

c) Polynome lassen sich schreiben als

$$(a_0, a_1, ...) = \sum_{i=0}^{n} a_i X^i$$

d) Dann gilt für Addition und Multiplkation:

$$\sum_k a_k X^k + \sum_k b_k X^k = \sum_k (a_k + b_k) X^k \left(\sum_k a_k X^k \right) \left(\sum_k b_k X^k \right) \quad = \sum_k c_k X^k$$

mit $c_k = \sum_{i+j=k} a_i b_j$.

Definition 2.5. a) Für ein Polynom $f = \sum_k a_k X^k$ heißt a_k der k-te **Koeffizient** von f.

b) Für $f \neq 0$ heißt

$$\deg(f) = \max\{i \mid a_i \neq 0\}$$

der **Grad** von f. (Falls $f = 0$, dann ist $\deg f := -\infty$)

c) Der Koeffizient a_n mit $n = \deg(f)$ heißt **Führender Koeffizient** von f.

d) Ist der führende Koeffizient $a_n = 1$, so heißt f **normiert**

Theorem 2.6. *Seien $f, g \in A[X]$.*

a) Dann ist $\deg(f+g) \leq \max(\deg(f), \deg(g))$ und $\deg(fg) \leq \deg(f)+\deg(g)$.

b) Sind die führenden Koeffizienten von f oder g keine Nullteiler, so idt $\deg(fg) = \deg(f) + \deg(g)$.

Korollar 2.7. *A ist genau dann Integritätsbereich wenn $A[X]$ Integritätsbereich ist.*
In diesem Fall gilt $A[X]^* = A^*$.

Satz 2.8. *Sei $f : A \to B$ ein Ringhomomorphismus und $b \in B$.*
Dann gibt es genau einen Homomorphismen $\varphi_A : A[X] \to B$ mit $\varphi_B \mid_A = \varphi$ und $\varphi_b(X) = b$.

Lemma 2.10. *Es gilt I ist Primideal in $A \Leftrightarrow I[X]$ ist Primideal in $A[X]$.*

Theorem 2.11. *Sei $g \in A[X]$, $g \neq 0$ mit führendem Koeffizient $b_n \in A^*$ und sei $f \in A[X]$.*
Dann existieren eindeutige Polynome $q, r \in A[X]$ mit $f = qg + r$ mit $\deg(r) < \deg(g)$.

Korollar 2.12. *Sei K ein Körper. Dann ist $K[X]$ ein euklidischer Ring unter der* deg*-Abbildung und somit ein Hauptidealring.*
Die Einheiten sind die konstruieren Polynome.

Satz 2.13. *Sei A ein Integritätsbereich. Dann ist*

$$A[X] \text{ ist Hauptidealring} \Leftrightarrow A \text{ ist Körper}$$

2.2 Nullstellen von Polynomen

Definition 2.14. Sei $f \in A[X]$, $f \neq 0$.
$a \in A$ heißt **Nullstelle** von f, wenn $f(a) = 0$.

Satz 2.15. *Sei $f \in A[X]$, $f \neq 0$ und $a \in A$. Dann gilt*

$$a \text{ ist Nullstelle von } f \Leftrightarrow (x-a)|f$$

Satz 2.16. *Sei $f \in A[X]$, $f \neq 0$ ein Polynom das eine Nullstelle in A hat. Dann gibt es paarweise verschiedene Elemente $a_1, ..., a_m \in A$ und $n_1, ..., n_m \in \mathbb{N}$ und ein Polynom $g \in A[X]$, welchen keine Nullstellen in A hat, sodass*

$$f = g \prod_{i=1}^{m} (x - a_i)^{n_i}$$

ist.
Es gilt

$$\sum_{i=1}^{m} n_i \leq \deg(f)$$

Definition 2.17. Lässt sich $f \in A[X]$, $f \neq 0$ schreiben als

$$f = c \prod_{i=1}^{m} (x - a_i)^{n_i}$$

mit $c, a_1, ..., a_m \in A$ und $n_1, ..., n_m \in \mathbb{N}$, dann sag man f **zerfällt in Linearfaktoren**.

Satz 2.18. *Sei A ein Integritätsbereich. Dann hat $f \in A[X]$ mit $f \neq 0$ höchsten $n = \deg(f)$ verschiedene Nullstellen in A.*

Korollar 2.19. *Sei A ein unendlicher Integritätsbereich und $f \in A[X]$, $f \neq 0$. Dann gibt es ein $a \in A$ mit $f(a) \neq 0$.*

Satz 2.21. *Sei G_1 zyklische Gruppe der Ordnung n_1, G_2 zyklische Gruppe der Ordnung n_2.*
Sein n_1, n_2 Teilerfremd, so ist $G_1 \times G_2$ zyklisch.

Theorem 2.22. *Sei K ein Körper und $G \subset K^*$ Untergruppe. Ist G endlich, so ist G zyklisch.*

Korollar 2.23. *Ist K endlicher Körper, so ist K^* zyklisch.*

Satz 2.24. *Sie A ein faktorieller Integritätsbereich mit Quotientenkörper K. Sei*

$$f = a_n X^n + a_{n-1} X^{n-1} + ... + a_i X^1 + a_0$$

ein Polynom in $K[X]$.
Ist $b = c/d$ eine Nullstelle von f in K mit teilerfremden c, d, so gilt

$$c | a_0 \text{ und } d | a_n$$

Definition 2.25. Sei $f \in A[X]$, $f \neq 0$. Ist $a \in A$ eine Nullstelle von f, so gibt es ein $n \in \mathbb{N}$ mit

$$(x-a)^n | f$$
$$(x-a)^{n-1} \nmid f$$

Dann heißt n die **Vielfachheit** oder **Multiplizität** von a und man nennt a eine **n-fache Nullstelle** von f.

Definition 2.26. Die Abbildung

$$D : A[X] \to A[X]$$
$$\sum_{j=0}^{n} a_j X^j \mapsto \sum_{j=1}^{n} j a_j X^{j-1}$$

Man schreibt $f' := D(f)$.

Lemma 2.27. *Seien $f, g \in A[X]$, $a, b \in A$ Für die Ableitung D gilt*

a) $D(af + bg) = aD(f) + bD(g)$ (Linearität)

b) $D(fg) = (Df)g + f(Dg)$ (Produktregel)

Satz 2.28. *Sei $f \in A[X]$, $f \neq 0$. Sei $a \in A$ eine Nullstelle von f. Dann gilt*

$$a \text{ hat Vielfachheit } 1 \Leftrightarrow f'(a) \neq 0$$

Definition 2.29. Die Abbildung

$$\chi : \mathbb{Z} \to A$$
$$n \mapsto n \cdot 1$$

Ist ein Ringhomomorphismus und

$$\text{Kern}(\chi) = (n) = n\mathbb{Z}$$

für ein $n \in \mathbb{Z}$, $n \geq 0$.
n heißt die **Charakteristik** von A und man schreibt $n = \text{char}(A)$.

Lemma 2.30. *Ist A ein Integritätsbereich, so ist $n = 0$ oder n ist prim.*

Satz 2.31. *Sei K ein Körper und $f \in K[X]$ $f \neq$const, dann gilt*

a) Ist $\mathrm{char}(K) = 0$, *so gilt*

$$\deg(f') = \deg(f) - 1$$

b) Ist $\mathrm{char}(K) = p > 0$, *so gilt*

$$\deg(f') \leq \deg(f) - 1$$

Weiterhin gilt

$$f' = 0 \Leftrightarrow f(X) = g(X^p) \text{ für ein } g \in K[X]$$

2.3 Polynome mehrerer Veränderlicher

Definition 2.32. Sei A ein Ring. Dann ist der Polynomring in mehreren Variablen $A[X_1, ..., X_n]$ induktiv definiert als

$$A[X_1, X_2] := A[X_1][X_2]$$
$$A[X_1, ..., X_n] := A[X_1, ..., X_{n-1}][X_n]$$

und ein Polynom $f \in A[X_1, ..., X_n]$ lässt sich schrieben als

$$f = \sum_{i_1,...,i_n} \underbrace{a_{i_1...i_n}}_{\in A} X_1^{i_1} ... X_n^{i_n}$$

Definition 2.33. Die Elemente $X_1^{i_1} ... X_n^{i_n} \in A[X_1, ..., X_n]$ heißen primitve Monome.

Definition 2.34. Der Grad des Polynoms $f \in A[X_1, ..., X_n]$ ist definiert als

$$\deg(f) = \max \left\{ \sum_{j=1}^{n} i_j \mid a_{i_1...i_n} \neq 0 \right\}$$

falls $f \neq 0$ und sonst $= -\infty$.

Definition 2.35. Ein Polynom $f \in A[X_1, ..., X_n]$ heißt homogen vom Grad m, falls alle Monome in f Grad m haben.

Satz 2.36. *Sei $\varphi : A \to B$ ein Ringhomomorphismus und $b_1, ..., b_n \in B$.*
Dann existiert genau ein Ringhomomorphismus $\psi : A[X_1, ..., X_n] \to B$ mit $\psi|_A = \varphi$ und $\psi(X_i) = b_i$ für alle i.

Satz 2.37. *Sei B ein Ring und $A \subset B$ ein Unterring. Seien $b_1, ..., b_n \in B$. Die Inklusion $\iota : A \hookrightarrow B$ lässt sich eindeutig fortsetzen zu einem Homomorphismus $\varphi : A[X_1, ..., X_n] \to B$ mit $\varphi|_A = \iota$ und $\varphi(X_j) = b_j$.*

Korollar 2.38. *Sei B ein Ring und $A \subset B$ ein Unterring. Seien $b_1, ..., b_n \in B$. Dann ist $A[b_1, ..., b_n]$ der Kleinste Unterring von B der A und $b_1, ..., b_n$ enthält.*

Korollar 2.39. *Ist $\varphi : A[X_1, ..., X_n] \to B$ mit $\varphi(X_j) = b_j$ injektiv, so ist $A[b_1, ..., b_n]$ isomorph zu $A[X_1, ..., X_n]$.*

Definition 2.40. Ist $\varphi : A[X_1, ..., X_n] \to B$ mit $\varphi(X_j) = b_j$ injektiv, so nennt man die b_j algebraisch unabhängig.
Ist φ nicht injektiv, so heißen die b_j algebraisch abhängig.

Satz 2.41 (**??** für mehrere Variablen)**.** *Sei A ein Ring*

$$A \text{ ist Integritätsbereich } \Leftrightarrow \ A[X_1, ..., X_n] \text{ ist Integritätsbereich}$$

Satz 2.42. *Sei A Integritätsbereich. Dann gilt*

$$A^* = A[X_1, ..., X_n]^*$$

Satz 2.43. *Es war einmal ein Integritätsbereich A. Der Integritätsbereich A hatte unendliche Teilmengen $T_1, ..., T_n \subset A$ als Freunde.*
Dann kam ein nettes $f \in A[X_1, ..., X_n]$ für welches $f(t_1, ..., t_n) = 0$ für alle $t_1 \in T_1, ..., t_n \in T_n$ war.
Der Held wusste sofort, dass $f = 0$ gellten musste.[1]

Definition 2.44. Sei $I \neq \emptyset$ ein Indexmenge. Dann bezeichnet $\mathbb{N}^(I)$ die Menge der Form $(a_i)_{i \in I}$ mit $a \in\in \mathbb{N}_0$ und $a_i = 0$ für fast alle $i \in I$.
Die Addition auf $\mathbb{N}^{(I)}$ ist definiert durch

$$(a_i)_{i \in I} + (b_i)_{i \in I} = (a_i + b_i)_{i \in I}$$

mit neutralem Element $0 = (0)_{i \in I}$.

Definition 2.45. Für Indexmengen I ist $A[(X_i)_{i \in I}]$ definiert als die Menge der Abbildungen $\varphi : \mathbb{N}^{(I)} \to A$ mit $\varphi(\alpha) = 0$ für fast alle $\alpha \in \mathbb{N}^{(I)}$, mit Addition und Multiplikation

$$\begin{aligned}(f + g)(\alpha) &= f(\alpha) + g(\alpha) \\ (fg)(\alpha) &= \sum_{\substack{\beta+\gamma=\alpha \\ \beta,\gamma \in N(I)}} f(\beta)g(\gamma)\end{aligned}$$

Dann ist $A[(X_i)_{i \in I}]$ ein Ring mit neutralem Element der Addition $0 = 0(\alpha)$ und der Multiplikation $e(\alpha) = 1$ falls $\alpha = 0$ und $e(\alpha) = 0$ sonst.

Bemerkung. Einem Element $a \in A$ ordnen wir die Abbildung ζ mit

$$\zeta(\alpha) \begin{cases} a & = \alpha = 0 \\ 0\alpha \neq 0 & \end{cases}$$

Dies liefert eine Einbettung von A in $A[(X_i)_{i \in I}]$ mit

$$X^\alpha(\beta) = \begin{cases} 0 & \beta \neq \alpha \\ 1 & \beta = \alpha \end{cases}$$

[1] by Sandra

Für ein beliebiges $f \in A[(X_i)_{i\in I}]$ ist dann

$$\zeta = \sum_{\alpha\in\mathbb{N}^{(I)}} f(\alpha)X^\alpha$$

und es gilt $X^\alpha X^\beta = X^{\alpha+\beta}$ und für $f = \sum f(\alpha)X^\alpha$ $g = \sum g(\alpha)X^\alpha$ ist

$$f + g = \sum \big(f(\alpha) + g(\alpha)\big)X^\alpha \tag{1}$$

$$f \cdot g = \sum h(\alpha)X^\alpha \text{mit } h(\alpha) \qquad = \sum_{\beta+\gamma=\alpha} f(\beta)g(\gamma) \tag{2}$$

Bemerkung 2.46. Für jedes $j \in I$ setzen wir $e_j = (b_i)_i$ mit $b_j = 1$, $b_i = 0$ f+r $j \neq i$.
Dann könne wir ein beliebiges $\alpha = (a_i)_i$ schreiben als $\alpha = \sum a_i e_i$.
Wir definieren $X^{e_i} := X_i$. Dann ist

$$X^\alpha = X^{\sum a_i e_i} = \prod X^{a_i e_i} = \prod X_i^{a_i}$$

Die X^α sind die primitiven Monome in den Variablen X_i und die Elemente aus $A[(X_i)_{i\in I}]$ lass sich eindeutig schreiben als

$$\sum_{\alpha\in\mathbb{N}^{(I)}} c_\alpha \prod X_i^{a_i}$$

mit eindeutig bestimmten Koeffizienten c_α die fast alle verschwinden.

2.4 Bewertungen

Definition 2.47. Sei K ein Körper. Ein **Betrag** auf K ist eine Abbildung

$$|\cdot| : K \to \mathbb{R}$$

mit

a) $|x| \geq 0$ und $|x| = 0 \Leftrightarrow x = 0$

b) $|xy| = |x|\,|y|$

c) $|x + y| \leq |x|\,|y|$

Definition 2.48. Ein Betrag $|\cdot|$ heißt **Archimedisch**, wenn es $x, y \in K$ gibt, sodass

$$|x + y| > \max\{|x|\,|y|\}$$

bzw **nicht-archimedisch**, wenn für alle x, y gilt, dass$|x + y| \leq \max\{|x|\,, |y|\}$.

Satz 2.49. *Sei $|\cdot|$ ein nicht-archimedischer Betrag auf K. Ist $|x| \neq |y|$, so gilt*

$$|x + y| = \max\{|x|\,, |y|\}$$

Definition 2.50. Sei A ein Integritätsbereich. Eine **Bewertung** auf A ist eine Abbildung

$$\nu : A \to \mathbb{R} \cup \{\infty\}$$

mit

a) $\nu(a) = \infty \Leftrightarrow a = 0$

b) $\nu(ab) = \nu(a) + \nu(b)$

c) $\nu(a+b) \geq \min\{\nu(a), \nu(b)\}$

Satz 2.51. *Sei A ein Integritätsbereich und $\nu : A \to \mathbb{R} \cup \{\infty\}$ eine Bewertung auf A.*

a) ν kann zu einer Bewertung auf dem Quotientenkörper K von A fortgesetzt werden, durch

$$\nu(a/b) = \nu(a) - \nu(b)$$

b) Sei $c \in \mathbb{R}$ und $c > 1$. Dann definiert

$$|x| = c^{-\nu(x)}$$

einen nciht-archimedischen Betrag auf K.

Theorem 2.53 (Lemma von Gauß)**.** *Sei A in Integritätsbereich mit Quotientenkörper K und sei $\nu : A \to \mathbb{R} \cup \infty$ eine Bewertung auf A.*
Setze ν fort zu einer Bewertung auf K durch

$$\nu(a/b) = \nu(a) - \nu(b)$$

Für $f = \sum a_j X^j \in K[X]$ definieren wir

$$\nu(f) = \min\{\nu(a_i)\}$$

für $f \neq 0$ und $\nu(0) = \infty$.
Dann ist ν eine Bewertung auf $K[X]$.

2.5 Der Satz von Gauß

Definition 2.54. Sei A ein faktorieller Integritätsbereich mit Quotientenkörper K.
Ein Polynom

$$f = a_n X^n + a_{n-1} X^{n-1} + ... + a_o \in A_[X]$$

heißt **primitiv**, wenn für seine Koeffizienten gilt: $\gcd(a_0, ..., a_n) = 1$.
Äquivalent dazu $\nu_p(f) = 1$ für alle Primelemente $p \in A$.
Ein Polynom $f \in K[X]$, $f \neq 0$ lässt sich schreiben als $f = c\tilde{f}$ mit $\tilde{f} \in A[X]$ primitiv und $c \in K$.

Satz 2.55. *Sei A ein faktorieller Integritätsbereich mit Quotientenkörper K und $f \in A[X]$ primitiv mit* $\deg(f) \geq 1$.
Dann gilt

$$f \text{ ist irreduzibel in } A[X] \Leftrightarrow f \text{ ist irreduzibel in } K[X]$$

Bemerkung. Sei A wie Oben, $f \in A[X]$, nicht zwingend Primitiv mit $\deg(f) \geq 1$ und f irreduzible in $K[X]$, dann ist $f$irreduzibel in $A[X]$.

Theorem 2.56 (Satz von Gauß)**.** *Sei A ein faktorieller Integritätsbereich. Dann ist auch $A[X]$ ein faktorieller Integritätsbereich.*

Korollar 2.57. *Sie K ein Körper, dann ist $K[X_1, ..., X_n]$ ein faktorieller Integritätsbereich.*

2.6 Der Hilbertsche Basissatz

Theorem 2.59 (Hilbertscher Basissatz)**.** *Sei A ein noetherscher Ring. Dann ist auch $A[X]$ noethersch.*

Für $f = \sum_{a_i X^i \in A[X]}$ sei $b_n(f) = a_n$.
Dann gilt

$$b_n(f+g) = n_b(f) + b_n(g)$$
$$b_n(af) = ab_n(f)$$

für alle $f, g \in A[X]$ und $a \in A$.
Die Menge $I(n) := b_n(I_n)$ ist ein Ideal in A und es gilt

$$I(0) \subset I(1) \subset ...$$

den $f \in I_n$ impliziert $Xf \in I_{n+1}$. Dann ist $b_n(f) = b_{n+1}(Xf) \in I(n+1)$.
Da A noethersch ist wird jede Folge stationär. Also gibt es $m \in \mathbb{N}$, mit

$$I(m) = I(m+1) = ...$$

Für jedes$n = 0, 1, ...$ wähle Polynome f_{n_j}, sodass $I(n)$ von den Koeffizienten $b_n(f_{n_j})$ erzeugt wird.
Dann wird I von den f_{n_j} über $A[X]$ erzeugt:
Sei $f \in I$ vom Grad t.

- Ist $t \leq m$, so hat
$$f - \sum_t a_{t_j} f_{t_j} \in I$$
Grad $\leq t-1$.
Nach endlich vielen Schritten hat man f als Linearkombination der f_{n_j} dargestellt.
- Ist $t > m$, so reduziert man den Grad von f durch
$$f - \sum a_{t_j} X^{t-m} f_{m_j} \in I$$

2.7 Eigenschaften von Polynomringen

Sei A ein Ring.

a) A Integritätsbereich $\Leftrightarrow$ $A[X_1, ..., X_n]$ Integritätsbereich.
Dann gilt $A[X-1, ..., X_n]^* = A^*$.

b) (Gauss) A faktorieller Integritätsbereich $\Leftrightarrow$ $A[X_1, ..., X_n]$ faktorieller Integritätsbereich.

c) (Hilbert) A noethersch $\Leftrightarrow$ $A[X_1, ..., X_n]$ noethersch.

d) Sei A zusätzlich Integritätsbereich, dann ist
A Körper $\Leftrightarrow$ $A[X]$ Hauptidealring.

2.8 Irreduziblitätskriterien

Theorem 2.60 (Eisenstein)**.** *Sei A ein faktoriell Integritätsbereich mit Quotientenkörper $K = Q(A)$.*
Sei

$$f = a_n X^n + ... + a_0 \in A[X]$$

mit $\deg(f) = n \geq 1$. *Sei $p \in A$ prim mit $p|a_i$ für $i = 0, ..., n-1$ und $a \not| a_n$ und $p^2 \not| a_0$.*
Dann ist f irreduzibel in $K[X]$.
Ist f zusätzlich primitiv, so ist f auch irreduzibel in $A[X]$.

Satz 2.62 (Reduktionskriterium)**.** *Sei A ein faktorieller Integritätsbereich mit Quotientenkörper K, $p \in A$ prim und $d = a_n X^n + ... + a_0$ ein Polynom in $A[X]$ mit* $\deg(f) \geq 1$ *und $\neq a_n$.*
Sei

$$\pi : A[X] \to \big(A/(p)\big)[X]$$

und $\pi(f)$ irreduzible in $\big(A/(p)\big)[X]$, dann ist f irreduzibel in $K[X]$.

2.9 Symmetrische Polynome

Definition 2.64. Für $f \in A[X_1, ..., X_n]$ und $\sigma \in S_n$ sei

$$\sigma(f) = \sigma(f(X_1, ..., X_n)) := f(X_{\sigma(1)}, ..., X_{\sigma(n)})$$

Dies liefert eine Operation von S_n auf $A[X_1, ..., X_n]$.

Bemerkung 2.65. Insbesondere gilt für $\sigma, \tau \in S_n$, dass $(\sigma\tau)(f) = \sigma(\tau(f))$.

Definition 2.66. Die Polynome in $A[X_1, ..., X_n]^{S_n}$ (invariant unter S_n) werden als **symmetrische Polynome** bezeichnet.

Proposition 2.67. Die Gruppenoperationen $\sigma \in S_n$ sind Automorphismen auf $A[X_1, ..., X_n][X]$.

Satz 2.68. *a) $A[X_1, ...X_n]^{S_n}$ enthält A und ist ein Unterring von $A[X_1, ..., X_n]$.*

b) S_n operiert auf $A[X_1, ..., X_n][X]$ durch

$$\sigma\left(\sum_{j=0}^{n} a_j X^j\right) = \sum_{j=0}^{n} \sigma(a_j) X^j$$

c) Sei $f = (X - X_1)(X - X_2)...(X - X_n)$. Dann ist

$$f = X^n + \sum_{j=1}^{n} (-1)^j s_j X^{n-j}$$

für eindeutig bestimmte Polynome $s_j \in A[X_1, ..., X_n]$

d) $\sigma(f) = f$

Definition 2.69. Sei $f \in [X-1, ..., X_n][X]$, $\sigma \in S_n$.
Dann bezeichnet man die s_j in

$$f = \sigma(f) = \sigma\left(X^n + \sum_{j=1}^{n}(-1)^j s_j X^{n-j}\right)$$

als **elementarsymmetrische Polynome**.

Lemma 2.70. *Die elementarsymmetrischen Polynom sind symmetrisch, d.h.* $\sigma(s_j) = s_j$. *Sie sind gegeben durch*

$$s_1 = X_1 + X_2 + ... + X_n s_2 \quad = X_1X_1 + X_1X_3 + ... + X_1X_n + X_2X_3 + ... + X_{n-1}X_n$$

$$= \sum_{i \le j} X_i X_j \vdots$$

$$s_n = X_1 ... X_n$$

Satz 2.71. *Die Polynome* s_j *sind homogen vom Grad* j.

Definition 2.72. Das Monom $X_1^{i_1} ... X_n^{i_n} \in A[X_1, ..., X_n]$ hat Grad $i_1 + ... + i_n$.
Für den **Grad** $\deg(f)$ für $f \in A[X_1, ..., X_n]$ ist das Maximum über den Grad der Monome.

Definition 2.73. Das Monom $X_1^{i_1} ... X_n^{i_n} \in A[X_1, ..., X_n]$ hat Gewicht $i_1 + 2i_2 + ... + ni_n$.
Das Gewicht $\text{gew}(f)$ für $f \in A[X_1, ..., X_n]$ ist das Maximum über das Gewicht der Monome.

Theorem 2.74. *a) Sei* $f \in A[X_1, .., X_n]^{S_n}$ *mit* $\deg(f) = d$.
Dann gibt es eine Polynom $g \in A[X_1, ..., X_n]$ *mit* $\text{gew}(g) \le d$, *sodass* $f = g(s_1, ..., s_n)$.

b) Ist f *zusätzlich homogen, so hat jedes Monom Gewicht* d.

Theorem 2.75. *Sie elementarsymmetrischen Polynome* $s_1, ..., s_n \in A[X - 1, ..., X_n]$ *sind algebraisch unabhängig über* A.

Definition 2.77. Sei $f \in A[X]$ ein normiertes Polynom vom Grad n.
Dann ist die **Diskriminante** von f definiert als

$$D(f) := d_n(-c_1, c_2, -c_3, ..., (-1)^n c_n) \in A$$

Dabei ist $d_n \in \mathbb{Z}[X-1, ..., X_n]$ mit

$$d_n(s_1, ..., s_n) := \prod_{i \le j}(X_i - X_j)^2$$

Satz 2.78. *Sei $f \in A[X]$ ein normiertes Polynom. Ist*

$$f = \prod_{i=1}^{n} (X - \alpha i)$$

eien Faktorisierung von f in einem Oberring $B \supset A$, dann ist

$$D(f) = \prod_{i \leq j} (\alpha_i - \alpha_j)^2$$

Satz 2.79. *Ist $B \supset A$ ein Integritätsbereich so gilt*

$$D(f) = 0 \Leftrightarrow \ f \text{ hat Mehrfache Nullstellen in } B$$

3 Körpererweiterungen

3.1 Grundbegriffe

Definition 3.1. Sei L ein Körper, $K \subset L$ heißt **Teilkörper** von L, wenn K abgeschlossen beglich Addition und Multiplikation ist und unter diesen Operationen selbst wieder Körper ist.

Definition 3.2. Sei K ein Körper. Sei $L \supset K$ selbst wieder Körper, dann bezeichnet man L als **Erweiterungskörper** von K und spricht von der **Körpererweiterung** L/K.

Definition 3.3. Sei L/K eine Körpererweiterung. Dann heißt der Körper M mit $K \subset M \subset L$ **Zwischenkörper** der Erweiterung L/K.

Definition 3.4. Sei L/K eine Körpererweiterung und $M \subset L$. Dann bezeichnet man mit $K(M)$ den **kleinsten Teilkörper** von L, der $K \cup M$ enthält.
Man sagt, dass $K(M)$ durch Adjunktion von M zu K entsteht.

Proposition 3.5. Sei L/K eine Körpererweiterung und $M \subset L$. Dann besteht $K(M)$ aus allen Elementen der Form

$$\frac{f(a_1, ..., a_n)}{g(a_1, ..., a_n)}$$

mit $f, g \in K[X_1, ..., X_n]$, $g(a_1, ..., a_n) \neq 0$ und $a_1, ..., a_n \in M$.

Proposition 3.6. Für jedes $a \in K(M)$ gibt es eine endliche Teilmenge $M' \subset M$, sodass $a \in K(M')$.

Definition 3.7. Sei K ein Körper. Sei

$$\begin{aligned} \mathbb{Z} &\xrightarrow{\phi} K \\ n &\mapsto n \cdot 1 \end{aligned}$$

Dann ist $\text{Kern}(\phi) = (n)$ für ein eindeutiges $n \in \mathbb{N}$. n wird als **Charakteristik** von K bezeichnet.

Korollar 3.8. *Sei K ein Körper, dann ist* $\mathrm{char}(K) = 0$ *oder prim.*

Proposition 3.10. Ist K ein Teilkörper von L, so gilt

$$\mathrm{char}(K) = \mathrm{char}(L)$$

Definition 3.11. Sei K ein Körper. Dann heißt

$$P := \bigcap_{L \text{ Teilkörper von } K} L$$

der **Primkörper** von K.

Satz 3.12. *Sei K ein Körper und P der Primkörper von K. Dann gilt*

a) $\mathrm{char}(K) = p$ *für* $p > 0$, *p prim* $\Leftrightarrow P \cong F_p$

b) $\mathrm{char}(K) = 0 \Leftrightarrow P \cong \mathbb{Q}$.

Definition 3.13. Ist K ein Teilkörper von L, sokönnen wir L als Vektorraum über K auffassen.
Die Dimension diese Vektorrausm heißt **Grad** von L über K.

$$[L : K] := \dim_K(L)$$

Definition 3.14. Die Erweiterung L/K heißt **endlich**, wenn $[L : K] < \infty$.

Proposition 3.15. Ist L endlich und K kein Teilkörper von L, so gilt

$$|L| = |K|^m$$

mit $m = [L : K]$.

Theorem 3.16 (Gradsatz)**.** *Seien $K \subset L \subset M$ Körpererweitungen. Dann gilt*

$$[M : K] = [M : L][L : K]$$

Ist $(x_i)_{i\in I}$ eine Basis von L/K und $(y_j)_{j\in J}$ eine Basi von M/L, so ist $(x_i y_j)_{(i,j)\in I\times J}$ eine Basis von M/K.

3.2 Algebraische Körpererweiterungen

Definition 3.17. Sei L/K eine Körpererweiterung. $\alpha \in L$ heißt **algebraische** über K, wenn es ein Polynom $g \in K[X] \setminus 0$ gibt, mit $g(\alpha) = 0$.
Äquivalent:Der Homomorphismus $K[X] \to L, f \mapsto f\alpha$ hat nicht trivialen Kern.

Definition 3.18. Ist $\alpha \in L$ nicht algebraisch, so nennt man es transzendent.

Definition 3.19. Der Körper L heißt algebraisch über K, wenn alle $\alpha \in A$ algebraisch sind.

Definition 3.21. Sei L/K eine Körpererweiterung und $\alpha \in L$ algebraisch über K. Sei $m_{\alpha,K} \in K[X]$ normiert und erzeuge den Kern von $\varphi : K[X] \to L, f \mapsto f(\alpha)$.
Man nennt es das Minimalpolynom in α über K.

Korollar 3.22. *$m_{\alpha,K}$ ist eindeutig und irreduzibel.*

Satz 3.23. *Sei L/K eine Körpererweiterung und $a \in L$ algebraisch über K. Sei $\varphi : K[X] \to L, g \mapsto g(\alpha)$ und $\mathrm{Im}(\varphi) = K[\alpha]$.*
Dann induziert φ eine Isomorphismus

$$K[X]/(m_{\alpha,K}) \cong K[\alpha]$$

Insbesondere ist $K[\alpha]$ Körper und es gilt

$$[K[\alpha] : K] = \deg(m_{\alpha,K})$$

Satz 3.25. *Eine endliche Körpererweiterung L/K ist algebraisch.*

Definition 3.26. Eine Körpererweiterung heißt einfach, wenn es $\alpha \in L$ gibt mit $L = K(\alpha)$.

Definition 3.27. Eine Körpererweiterung heißt endlich erzeugt, wenn es endlich viele Element $\alpha_1, ..., \alpha_n$ gibt sodass $L = K(\alpha_1, ..., \alpha_n)$.

Satz 3.28. *Sei $L = K(\alpha_1, ..., \alpha_n)$ eine endlich erzeugte Körpererweiterung und $\alpha_1, ..., \alpha_n$ algebraisch über K. Dann gilt*

a) $L = K(\alpha_1, ..., a_n))K[\alpha_1, ..., \alpha_n]$

b) L ist endlich und somit insbesondere algebraische Erweiterung von K.

Korollar 3.29. *Sei L/K eine Körpererweiterung. Dann sind äquivalent*

a) L/K ist endlich

b) L wird über K von endlich vielen Elementen erzeugt.

c) L ist eine endlich erzeugte algebraische Erweiterung.

Korollar 3.30. *Sei L/K eine Körpererweiterung. Dann sind äquivalent*

a) L/K ist algebraisch.

b) L wird über K von algebraisch Elementen erzeugt.

Satz 3.31. *Seien $K \subset L \subset M$ Körpererweiterungen, sei L/K algebraisch und $\alpha \in M$ algebraisch über L.*
Dann ist α algebraisch über K.
Insbesondere:

$$M/K \text{ ist algebraisch } \Leftrightarrow L/K \text{ ist algeraisch über } M/L$$

Definition 3.32. Sei L/K eine Körpererweiterung. Dann ist

$$L_{alg} := \{a \in L \mid a \text{ algebraisch über } K\}$$

der algebraische Abschluss von L in K.

Korollar 3.33. *Seien $a, b \in L$ algebraisch über K. Dann ist $K(a, b)$ algebraisch über K.*
Also ist auch $a - b \in K(a, b)$ algebraisch über K und falls $b \neq 0$ auch $ab^{-1} \in K(a, b)$.

3.3 Der algebraische Abschluss eines Körpers

Satz 3.35 (von Kronecker)**.** *Sei K ein Körper $f \in K[X] \setminus K$.*
Dann gibt es eine algebraische Erweiterung L/K sodass f eine Nullstelle in L hat.
Ist f irreduzibel, so kann man $L = K[X]/(f)$ setzen.

Definition 3.36. Ein Körper K heißt **algebraisch abgeschlossen** wenn jedes Polynom $f \in K[X] \setminus K$ eine Nullstelle in K hat.
(Äquivalent: f zerfällt in Linearfaktoren)

Satz 3.37. *Ein Körper K ist genau dann algebraisch abgeschlossen wenn es keine echte algebraische Erweiterung L/K zulässt.*

Theorem 3.38. *Sei K ein Körper. Dann gibt es einen algebraische abgeschlossen Körper L mit $K \subseteq L$.*

Satz 3.39. *Sei K ein Körper, dann gibt es einen algebraisch abgeschlossenen Körper $\overline{K}$, der K enthält und algebraisch über K ist. $\overline{K}$ wird als der algebraische Abschluss von K bezeichnet.*

Korollar 3.40. *Seien L, L' algebraische Abschlüsse des Körpers K, dann ist $L \cong L'$.*

Satz 3.41. *Sei K ein Körper und $K' = K(\alpha)$ eine einfache algebraische Körpererweiterung von K und $\sigma : K \to L$ ein Homomorphismus. Dann gilt*

a) Ist $\sigma' : K' \to L$ ein Homomorphismus der σ fortsetzt, so ist $\sigma'(\alpha)$ Nullstelle von

$$\sigma'(m_{\alpha,K}) = \sigma(m_{\alpha,K})$$

Satz 3.42. *Sei K ei Körper $K' = K(\alpha)$ eine einfache algebraische Erweiterung von K und $\sigma : K \to L$ ein Körperhomomorphismus.*

a) Ist $\sigma' : K' \to L'$ ein Homomorphismus, der σ Fortsetzt, so ist $\sigma'(\alpha)$ Nullstelle von $\sigma(m_{\alpha,K}) = \sigma'(m_{\alpha,K})$.

b) Es gibt zu jeder Nullstelle $\beta \in L$ von $\sigma(m_{\alpha,K})$ genau eine Fortsetzung $\sigma' : K' \to L'$ von σ mit $\sigma'(\alpha) = \beta$.

Theorem 3.43 (Fortsetzungssatz)**.** *Sei K ein Körper, L ein algebraisch abgeschlossener Körper und $\sigma : K \to L$ ein Körperhomomorphismus. Sei K'/K eine algebraische Körpererweiterung.*
Dann lässt sich σ fortsetzen zu einem Homomorphismus $\sigma' : K' \to L$.
Ist K' zusätzlich abgeschlossen und L algebraisch über $\sigma(K)$, so ist jedes Fortsetzung σ' von σ ein Isomorphismus.

Korollar 3.44. *Sei K ein Körper und seien $\overline{K}_1$ und $\overline{K}_2$ algebraische Abschlüsse von K. Dann gibt es einen Isomorphismus $\sigma : \overline{K}_1 \to \overline{K}_2$ der die Identität auf K fortsetzt.*

3.4 Zerfallskörper

Definition 3.46. Seien K/L und L'/K Körpererweiterungenund sien $\sigma : L \to L'$ ein Homomorphismus.
σ wird als **K-Homomorphismus** ($\sigma|_K = \mathrm{id}\,|_K$) bezeichnet, wenn σ eine Fortsetzung der Identität auf K ist.

Definition 3.47. Sei L/K eine Körpererweiterung und $F \subset K[X] \setminus K$eine Menge nicht-konstanter Polynome.
Eine Erweiterung L/K heißt **Zerfällungskörper** von F, über K, wenn

a) Jedes $f \in K$ zerfällt in Linearfaktoren über L

b) Die Körpererweiterung L/K wird con Nullstellen der $f \in F$ erzeugt.

Lemma 3.48. *Sei $\overline{K}$ ein algebraischer Abschluss von K und M die Menge der Nullstellen der Polynome von F in $\overline{K}$. Dann ist $L = K(M) \subset \overline{K}$ ein Zerfällungskörper von F.*

Satz 3.49. *Sei $F \subset K[X] \setminus K$ und seine L_1 und L_2 zwei Zerfällungskörper von F über K. Sei $\sigma : L_1 \to \overline{L}_2$ ein K-Homomorphismus in einen algebraischen Abschluss von L_2.*
Dann gilt $\sigma(L_1) = L_2$.

Korollar 3.50. *Sei $F \in K[X] \setminus K$ und seien L_1 und L_2 Zerfällungskörper von F über K.*
Dann gibt es einen K-Isomorphismus $L_1 \to L_2$

Theorem 3.51. *Sei L/K eine algebraische Körpererweiterung. Dann sind äquivalent:*

a) L ist der Zerfällungskörper einer Menge nicht-konstanter Polynome in $K[X]$.

b) Ist $\sigma : L \to \overline{L}$ ein K-Homomorphismus, so gilt $\sigma(L) = L$.

c) Jedes irreduzible Polynom $f \in K[X]$, das mindestens eine Nullstelle hat zerfällt in L vollständig in Linearfaktoren.

Definition 3.52. Eine algebraische Körpererweiterung L/K die eine der Bedingungen von **??** erfüllt heißt **normal**.

Satz 3.53. *Sei L/K eine normale Körpererweiterung und $K \subset M \subset L$ ein Zwischenkörper. Dann ist auch L/M normal.*

3.5 Separabel Körpererweiterungen

In diesem Abschnitt bezeichne K ein Körper.

Definition 3.55. Ein Polynom $f \in K[X]$ heißt **separabel**, wenn f nur einfache Nullstellen in einem algebraischen Abschluss $\overline{K}$ von K hat.
(Dies ist unabhängig von der Wahl von $\overline{K}$)

Satz 3.56. *Sei $f \in K[X]$ irreduzible, dann*

$$f \text{ separabel} \Leftrightarrow f' \neq 0$$

Definition 3.57. Sei L/K eine algebraische Körpererweiterung. $a \in L$ heißt **separabel** über K, wenn $m_{a,K}$ separabel ist.

Definition 3.58. Sei L/K eine algebraische Körpererweiterung. L heißt **separabel** über K, wenn jedes $a \in L$ separabel über K ist

Satz 3.59. *Sei $\mathrm{char}(K) = 0$ und L/K eine algebraische Körpererweiterung. Dann ist L/K separabel.*

Definition 3.60. Sei L/K eine algebraische Körpererweiterung und $\overline{K}$ der algebraische Abschluss von K.
Der **Separabilitätsgrad** $[L : K]_S$ von L über K ist definiert als

$$[L : K]_S := \left|\mathrm{Hom}_K(L, \overline{K})\right|$$

Diese Definition ist unabhängig von $\overline{K}$.

Satz 3.61. *Sei $K(a)/K$ eien einfach algebraische Körpererweiterung. Dann gilt*

a) Der Separabilitätsgrad $[K(a) : K]_S$ ist gleich der Anzahl der verschiedenen Nullstellen von $M_{a,K}$ in einem algebraischen Abschluss $\overline{K}$ von K.

b) aist genau dann separabel über K, wenn $[K(a) : K]_S = [K(a), K]$.

Theorem 3.62 (Gradsatz der Separabilität)**.** *Sei $K \subset L \subset M$ algebraische Körpererweiterungen. Dann gilt*

$$[M : K]_S = [M : L]_S [L : K]_S$$

Satz 3.63. *Sei L/K eine endliche Körpererweiterung. Dann gilt*

$$[L:K]_S \leq [L:K]$$

Theorem 3.64. *Sei L/K eine endliche Körpererweiterung. Dann sin äquivalent*

a) L/K ist separabel.

b) Es gibt über K separabele Elemente $a_1, ..., an \in L$, sodass $L = K(a_1, ...a_n)$.

c) $[L:K]_S = [L:K]$

Satz 3.65. *Sei $f \in K[X] \setminus K$ separabel. Dann ist auch der Zerfällungskörper von f über K separabel.*

Korollar 3.66. *Sei L/K eine algebraische Körpererweiterung und $M \subset L$, sodass $L = K(M)$. Dann sind äquivalent*

a) L/K ist separabel

b) Alle $a \in M$ sind separabel über K.

Ist ein dieser Bedingungen erfüllt, so gilt

$$[L:K]_S = [L:K]$$

Korollar 3.67. *Seien $K \subset L \subset M$ algebraische Körpererweiterungen. Dann gilt M/K ist genau dann separabel, wenn M/L und L/K separabel sind.*

Theorem 3.68 (Satz vo primitiven Element)**.** *Sei L/K einen endliche separable Körpererweiterung. Dann gibt es ein $a \in L$, sodass $L = K(a)$*

3.6 Endliche Körper

Definition 3.69. Sei p eine positiv Primzahl. Dann ist $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ein Körper mit p Elementen und $\text{char}(\mathbb{F}_p) = p$.

Satz 3.70. *Sei F ein endlicher Körper, dann ist* $\text{char}(F) = p > 0$ *und F enthält $q = p^n$ Elemente, wobei $n = [F:\mathbb{F}_p]$.*
F ist der Zerfällungskörper des Polynoms $X^q - X$ über $\mathbb{F}_p$. Die Erweiterung$F/\mathbb{F}_p$ ist normal.

Theorem 3.71. *Sei p eine positive Primzahl. Dann gibt es zu jedem positiven $n \in \mathbb{N}$ einen Erweiterungskörper $\mathbb{F}_q/\mathbb{F}_p$ mit $q = p^n$ Elementen. $\mathbb{F}_q$ ist bis auf Isomorphie eindeutig charakterisiert, als der Zerfällungskörper von $X^q - X$ über $\mathbb{F}_p$ und besteht aus den q Nullstellen. dieses Polynoms. Jeder endliche Körper ist isomorph zu genau einem Körper des Typs $\mathbb{F}_q$.*

Bemerkung 3.72. Wir können di Körper $\mathbb{F}_q$ auch Konstruieren, indem wir die Nullstellen eines irreduziblen Polynoms zu $\mathbb{F}_p$ adjungiert.

Satz 3.73. *Sei $n \in \mathbb{N}$. Dann gibt es ein irreduzibles Polynom f mit $\deg_{\mathbb{F}_p}(f) = n$.*

Satz 3.75. *Sei F eine endlicher Körper und K/F eine algebraische Erweiterung. Dann ist K/F normal und separabel.*

Definition 3.76. Sei F_q mit $q = p^n$ ein endlicher Körper.
Dann ist die Abbildung

$$\begin{aligned} \mathrm{Fr} : F_q &\to F_q \\ x &\mapsto x^p \end{aligned}$$

ein F_p-Automorphismus von F_q. Diese wir als **Frobenius-Automorphismus** bezeichnet.

Theorem 3.77. *Seiq $= p^n$, dann ist die Gruppe $\mathrm{Aut}_{F_p}(F_q)$ zyklisch mit Ordnung n. Und $\mathrm{Aut}_{F_p}(F_q) = \langle \mathrm{Fr} \rangle$ wird vom Frobenius-Automorphismus erzeugt.*

4 Galois-Erweiterungen

Definition 4.1. Eine algebraische, normale, separabele Körpererweiterung L/K heißt **Galoiserweiterung**.

Definition 4.2. Man bezeichnet $\mathrm{Aut}_K(L)$ als **Galoisgruppen** von L/K und schreibt $G(L/K)$ für $\mathrm{Aut}_K(L)$.

Satz 4.4. *Sei L/K eine normale Körpererweiterung und $f \in K[X]$ irreduzible. Dann permutiert $\mathrm{Aut}_K(L)$ die Nullstellen von f transitiv.*

Satz 4.5. *Sei L/K eine normale Körpererweiterung dann gilt*

$$|\mathrm{Aut}_K(L)| = [L : K]_S = \left|\mathrm{Hom}_K(L, \overline{K})\right|$$

Satz 4.6. *Sei L/K eine endliche Galois-Erweiterung. Dann ist*

$$[L : K] = |G(L/K)|$$

Definition 4.7. Sei L ein Körper und G eine Untergruppe von $\mathrm{Aut}_K(L)$. Dann ist

$$L^G := \{x \in L \mid g(x) = x \forall g \in G\}$$

ein Teilkörper von L. Dieser wird als **Fixkörper** von G bezeichnet.

Satz 4.8. *Sei L/K eine Galois-Erweiterung. Dann sit der Fixkörper von $G(L/K)$ genau K.*

Satz 4.9. *Sei L ein Körper und H eine endliche Untergruppe von $\mathrm{Aut}_K(L)$. Dann ist L/L^H eine endliche Galois-Erweiterung mit Galoisgruppe H und*

$$[L : L^H] = |H|$$

Bemerkung 4.10. Für $a \in L$ ist $m_{a,L^H} = f_a$ in der Notation des Beweises.

Theorem 4.11 (Hauptsatz der Galoistheorie)**.** *Sei L/K eine endliche Galois-Erweiterung. Sei U die Menge der Untergruppen von $G(L/K)$ und Z die Menge der Zwischenkörper von L/K. Dann sind die Abbildungen*

$$\begin{aligned} \Phi : Z &\to U & \qquad \Psi : U &\to Z \\ M &\mapsto G(L/M) & \qquad H &\mapsto L^H \end{aligned}$$

zueienander inverse Bijektionen. Für einen Zwischenkörper M von L/K ist die Erweiterung M/K normal genau dann wenn $G(L/M)$ normal in $G(L/K)$ ist. In diesem Fall ist

$$\begin{aligned} G(L/K) &\to G(M/K) \\ \sigma &\mapsto \sigma|_M \end{aligned}$$

eine surjektiver Gruppenhomomorphismus mit $\mathrm{Kern}() = G^0(L/M)$.
Dieser induziert einen Isomorphismus

$$G(M/K) \cong G(L/K)/G(L/M)$$

Satz 4.12. *Sei L/K eine endliche Galois-Erweiterung. Seien L_1, L_2 Zwischenkörper von L/K die zu Untergruppen H_1 und H_2 von $G(L/K)$ korrespondieren. Dann gilt für $\sigma \in G(L/K)$*

$$\sigma(L_1) = L_2 \Leftrightarrow \sigma H_1 \sigma^{-1} = H_2$$

Satz 4.13 (Translationssatz)**.** *Seien L/K und M/K Körpererweiterungen, sodass L und M in einem Gemeinsamen Erweiterungskörper von K enthalten sind.*
Ist L/K eine endliche Galois-Erweiterung, so ist auch L/K eine endliche Galois-Erweiterung und die Abbildung

$$\begin{aligned} G(L \cdot M/M) &\to G(L/K) \\ \sigma &\mapsto \sigma|_L \end{aligned}$$

definiert einen Isomorphismus

$$G(L \cdot M/M) \cong G(L/L \cap M)$$

(Dabei ist $L \cdot M$ das Kompositum $L \cdot M := L(M) = M(L)$)

Theorem 4.14 (Produktsatz)**.** *Seien L_1/K und L_2/K endliche Galois-Erweiterungen, sodass L_1 und L_2 in einem gemeinsamen Erweiterungskörper enthalten sind. Dann ist $L_1 \cdot L_2/K$ eine endliche Galois-Erweiterung und die Abbildung*

$$G(L_1 \cdot L_2/K) \to G(L_1/K) \times G(L_2/K)$$
$$\sigma \mapsto (\sigma|_{L_1}, \sigma|_{L_2})$$

definiert einen injektiven Gruppenhomomorphismus.
Ist $L_1 \cap L_2 = K$, so ist die Abbildung ein Isomorphismus.

Theorem 4.15. *Sei L/K eine endliche Galois-Erweiterung und sei a ein primitives Element, d.h. $L = K(a)$. Sei außerdem $H \subset G(L/K)$. Dann ist*

$$L^H = K(a_0, ..., q_1)$$

wobei die a_i die Koeffizienten von

$$f = \prod_{\sigma \in H} (X - \sigma(a)) = \sum_{i=0}^{n} a_i X^i$$

sind.

4.1 Die Galoisgruppe einer Gleichung

In diesem Abschnitt sei K ein Körper

Definition 4.16. Sei f ein separabeles Polynom und L ein Zerfällungskörper von f über K. Dann ist L/K einen endliche Galois-Erweiterung und $G(L/K)$ eird in diesem Falls als **Galoisgruppe von f über K** bezeichnet.

Satz 4.17. *Sei $f \in K[X] \setminus K$ separabel und vom Grad n mit Zerfällungskörper L über K.*
Seien $a_1, ..., a_n$ die Nullstellen von f in L. Dann definiert die Abbildung

$$G(L/K) \to S(\{a_1, ..., a_n\})$$
$$\sigma \mapsto \sigma|_{\{a_1,...,a_n\}}$$

einen injektiven Gruppenhomomorphismus. Insbesondere gilt $|G(L/K)|\,|n!$.
f ist genau dann irreduzible über K wenn $G(L/K)$ transitiv auf dem Nullstellen on f operiert.

Korollar 4.18. *Sei L/K eine endliche Galoiserweiterung vom Grad n. Dann ist $G(L/K)$ eine Untergruppe von S_n.*

Definition 4.22. Sei $L = K(X_1, ..., X_n)$ der Quotientenkörper von $K[X_1, ..., X_n]$. Die Element von L sin die rationalen Funktionen f/g mit $f, g \in K[X_1, ..., X_n]$ und $g \neq 0$.
S_n operiert durch Permutationen der X_i auf L.
$M = L^{S_n}$ wird als Körper der **symetrischen rationalen Funktionen** bezeichnet. Die Erweiterung L/M ist eine endliche Galois-Erweiterung mit Galoisgruppe S_n.

Satz 4.23. *Sei G eine endliche Gruppe, dann gibt es eine Galois-Erweiterung L/K mit $G(L/K) \cong G$.*

4.2 Kreisteilugspolynome

In diesem Abschnitt sei K ein Körper und $\overline{K}$ ein algebraischer Abschluss von K.

Definition 4.24. Die Nullstellen des Polynom $X^n - 1$ $n \geq 0$ werden als n-te **Einheitswurzeln** in $\overline{K}$ bezeichnet.

Proposition 4.25. Die n-ten Einheitswurzeln bilden einer Untergruppe U_n von $\overline{K}^*$.
Ist $\text{char}(K) = 0$ oder $\text{char}(K) \not| n$, so haben $X^n - 1$ und seine Ableitung nX^{n-1} keine gemeinsamen Nullstellen. Also ist $X^n - 1$ separabel.
In diesem Fall ist $|U_n| = n$.
Falls $\text{char}(K) = p > 0$ und $p|n$, so schreibt man $n ? mp^r$ mit $(m, p) = 1$.
Dann ist

$$(X^m - 1)^{p^r} = X^n - 1$$

Die Nullstellen von $X^m - 1$ stimmen mit den Nullstellen von $X^n - 1$ überein und $U_m = U_n$.

Satz 4.26. *Sei K ein Körper und $n \in \mathbb{Z}$, $n > 0$ mit $\text{char}(K) \not| n$, dann ist U_n eine zyklische Gruppe der Ordnung n.*

Definition 4.27. $\xi \in U_n$ heißt **primitive** n-te Einheitswurzel, wenn ξ die Gruppe U_n erzeugt.

Satz 4.28. *Seien $m, n \in \mathbb{Z}$, $m, n > 0$ mit $(m, n) = 1$ und K ein Körper mit $\text{char}(K) \neq |mn$.*
Dann ist die Abbildung

$$\begin{aligned} U_m \times U_n &\to U_{mn} \\ (\xi, \eta) &\mapsto \xi\eta \end{aligned}$$

ein Isomorphismus von Gruppen.

Definition 4.29. Für $n \in \mathbb{Z}$, $n > 0$ definiert

$$\varphi(n) = |(Z/n\mathbb{Z})^*|$$

die **Eulersche φ-Funktion**.

Lemma 4.30. *Ist p eine Primzahl, so gilt*

$$\varphi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$$

Satz 4.31. *Seien $m, n \in \mathbb{Z}$ mit $m, n > 0$ und $(m, n) = 1$. Dann ist*

$$\varphi(mn) = \varphi(m)\varphi(n)$$

Satz 4.32. *Sei $n \in \mathbb{Z}$, $n > 0$. Ein Element a erzeugt die additive zyklische Gruppe $\mathbb{Z}/n\mathbb{Z}$ genau dann wenn a eine Einheit in $\mathbb{Z}/n\mathbb{Z}$ ist.*

Satz 4.33. *Sei K ein Körper und $n \in \mathbb{Z}$, $n \geq 0$ mit $\mathrm{char}(K) \nmid n$. Dann enthält U_n genau $\varphi(n)$ primitive n-te Einheitswurzeln.*
Ist ξ primitive n-te Einheitswurzel, so ist ξ^r genau dann primitive n-te Einheitswurzel, wenn $(r, n) = 1$ ist.

Satz 4.34. *Sei $\mathrm{char}(K) \nmid n$ und ξ eine primitive Einheitswurzel.*
Dann ist $K(\xi)$ der Zerfällungskörper von $X^n - 1$.
Außerdem ist $K(\xi)/K$ eine endliche Galois-Erweiterung.

Definition 4.35. Falls $K = \mathbb{Q}$ ist so heißt $\mathbb{Q}(\xi)$ der **n-te Kreisteilungskörper**.

Theorem 4.36. *Sei $\xi \in \overline{\mathbb{Q}}$ eine primitive n-te Einheitswurzel. Dann ist $\mathbb{Q}(\xi)/\mathbb{Q}$ eine endliche Galois-Erweiterung mit*

$$[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(n)$$

Satz 4.37. *Seien $\xi_m, \xi_n \in \overline{\mathbb{Q}}$ primitive m-te bzw n-te Einheitswurzeln mit $(m, n) = 1$.*
Dann ist

$$\mathbb{Q}(\xi_m) \cap \mathbb{Q}(\xi_n) = \mathbb{Q}$$

Satz 4.38. *Sei $\xi \in \overline{K}$ eine primitive n-te Einheitswurzel mit $\mathrm{char}(K) \nmid n$.*
Dann gilt

a) $K(\xi)$ ist der Zerfällungskörper des separablen Polynom $X^n - 1$ über K. Und die Erweiterung $K(\xi)/K$ ist eine endliche Galois-Erweiterung mit Grad $\leq \varphi(n)$ und abelscher Galoisgruppe.

b) Zu jedem $\sigma \in G(K(\xi)/K)$ gibt es eine positive ganze Zahl, $r(\sigma)$ mit $\sigma(\xi) = \xi^{r(\sigma)}$, wobei die Restklasse $\overline{r(\sigma)} \in \mathbb{Z}/n\mathbb{Z}$ eine Einheit ist, die unabhängig von der Wahl von ξ eindeutig durch σ bestimmt ist.

Und die Abbildung

$$\begin{aligned} G(K(\xi)/K) &\to (\mathbb{Z}/n\mathbb{Z})^* \\ \sigma &\mapsto \overline{r(\sigma)} \end{aligned}$$

ist ein injektiver Gruppenhomomorphismus.

Korollar 4.39. *Sei $\xi \in \overline{\mathbb{Q}}$ eine primitive n-te Einheitswurzel. Dann ist $\mathbb{Q}(\xi)/\mathbb{Q}$ eine endliche Galois-Erweiterung mit Galoisgruppe $(\mathbb{Z}/n\mathbb{Z})^*$.*

Wir zeigen nun, dass sich jede endliche abelsche Gruppe als Galoisgruppe über $\mathbb{Q}$ realisieren lässt.

Theorem 4.40 (Dirichlet)**.** *Sei $a, b \in \mathbb{Z}$ mit $a, b > 0$ und $(a, b) = 1$. Dann enthält $\{a + nb \mid n \in \mathbb{Z}\}$ unendlich viele Primzahlen.*

Theorem 4.41. *Sei G eine endliche abelsche Gruppe.Dann gibt es eine endliche Galoiserweiterung $K/\mathbb{Q}$ mit $G(K/\mathbb{Q}) \tilde{=} G$.*

Theorem 4.42 (Kronecker-Weber)**.** *Sei $K/\mathbb{Q}$ eine endliche Galoiserweiterung mit abelscher Galoisgruppe. Dann ist K in einem Kreisteilungskörper enthalten.*

Definition 4.43. Sei $n \in \mathbb{Z}$, $n > 0$ und $\text{char}(K) \not| n$. Seien $\xi_1, ..., \xi_m$ mit $m = \varphi(n)$ die primitiven n-ten Einheitswurzeln in $\overline{K}$.
Dann heißt

$$\Phi_{n,K} = \prod_{i=1}^{m} (X - \xi_i)$$

das n-te **Kreisteilungspolynom** über K.
Im Fall $K = \mathbb{Q}$schreiben wir Φ_n für $\Phi_{n,K}$.

Satz 4.44. *a) $\Phi_{n,K}$ ist ein normiertes separables POlynom über K vom Grad $\phi(n)$*

b) Für $K = \mathbb{Q}$ gilt $\Phi_n \in \mathbb{Z}[X]$ und Φ_n ist irreduzibel in $\mathbb{Z}[X]$ und in $\mathbb{Q}[X]$.

c) $X^n - 1 = \prod_{d|n} \Phi_{d,K}$

Satz 4.45. *Sei $n \in \mathbb{Z}$, $n > 0$ und p prim mit $p \not| n$. Sei e die Ordnung von p in $(\mathbb{Z}/n\mathbb{Z})^*$. Dann zerfällt $\Phi_{n,\mathbb{F}_p}$ in $\varphi(n)/e$ verschiedene Faktoren vom Grad e über $\mathbb{F}_p$.*

Bemerkung 4.47. Sei p eine ungerade Primzahl. Dann ist $(\mathbb{Z}/p^n\mathbb{Z})^*$ zyklisch der Ordnung $p^n - p^{n-1}$.
Für $p = 2$ ist

$$\begin{aligned}(\mathbb{Z}/2\mathbb{Z})^* &= 1\\ (\mathbb{Z}/4\mathbb{Z})^* &= \mathbb{Z}/2\mathbb{Z}\\ (\mathbb{Z}/2^n\mathbb{Z})^* &= \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z} \text{ für } n \geq 3\end{aligned}$$

5 Moduln

5.1 Definitionen

Definition 5.1. Sei R ein Ring. Ein **Linksmodul** über R ist eine abelsche Gruppe M mit einer Abbildung

$$R \times M \to M$$

sodass

$$\begin{aligned}a(x + y) &= ax + ay\\ (a + b)x &= ax + bx\\ a(bx) &= (ab)x\\ 1x &= x\end{aligned}$$

für alle $a, b \in R$ und $x, y \in M$.

Definition 5.2. Seien M', M R-Moduln. Eine Abbildung

$$f : M \to M'$$

heißt $R-$**linear** oder **Modulhomomorphismus**, wenn

$$f(x+y) = f(x) + f(y)$$
$$f(ax) = af(x)$$

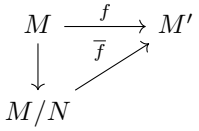
für alle $a \in R$ und $x, y \in M$.

Definition 5.4. Sei ; ein R-Modul. Ein Untermodul von M ist eine Untergruppe N von M, die Invariant unter Operstionen von R ist, d.h. $ax \in N$ für alle $a \in R$, $x \in N$.

5.2 Faktormoduln

Definition 5.6. Sei M ein R-Modul und $N \subset M$ ein Untermodul, so erhält man auf der **Faktorgruppe** M/N eine R-Modulstruktur. Mit $a(x+N) = ax + N$ für $x \in M$, $a \in R$ wird M/N als **Faktormodul** bezeichnet.
Die Abbildung $\pi : M \to M/N$, $x \mapsto x + N$ ist ein Modulhomomorphismus.

Theorem 5.7. *Seien M, M' R-Moduln, $f : M \to M'$ ein Modulhomomorphismus und $N \subset \mathrm{Kern}(f)$ ein Untermodul von M. Dann gibt es eine eindeutigen Homomorphismus $\overline{f} : M/N \to M'$, sodass*



Satz 5.8. *Sei M ein R-Modul und N ein Untermodul. Dann insuziert die Projektion $\pi : M \to M/N$ eine Bijektion zwischen den Untermoduln von M die N enthalten und den Untermoduln von M/N.*

5.3 Direkte Summen und Produkte

Definition 5.9. Sei $(M_i)_{i \in I}$ eine Familie von R-Moduln.
Dann ist das **Modul-Produkt**

$$\prod_{i \in I} M_i = \{(x_i)_{i \in I} \mid x_i \in M_i\}$$

ein R-Modul und

$$\bigoplus_{i \in I} M_i = \{(x_i)_{i \in I} \mid x_i \in M_i \text{ und fast alle } x_i = 0\}$$

ein Untermodul. Dieser wird als direkte Summe bezeichnet.

5.4 Erzeugendensysteme und Basen

Definition 5.10. Sei M ein R-Modul. Eine Familie $(x_i)_{i\in I}$ von Element in M heißt **Erzeugendensystem** von M über R, wenn

$$m = \sum_{i\in I} Rx_i$$

ist.
Besitzt M ein endliches Erzeugendensystem, so heißt M **endliche erzeugt** oder **endliche**r R-Modul.
Ein Familie $(x_i)_{i\in I}$ heißt **linear unabhängig**, wenn aus

$$\sum_{i\in I} a_i x_i = 0$$

(mit fast alle $a_i = 0$) folgt, dass alle $a_i = 0$ sind.

Definition 5.11. Ein linear unabhängiges Erzeugendensystem wird als **Basis** bezeichnet.
In diesem Falls lässt sich jedes $x \in M$ schreiben als

$$x = \sum_{i\in I} a_i x_i$$

mit eindeutig bestimmtem $a_i \in R$. In diesem Fall heißt M **frei**.

Satz 5.12. *Sei R ein Ring mit $1 \neq 0$ und M ein R-Modul.*
Sind $(v_,...,v_m)$ und $(w_1,...,w_n)$ zwei R-Basen von M, so ist $m = n$.

5.5 Exakte Sequenzen

Definition 5.13. Eine Folge von R-Moduln und R-linearen Abbildungen

$$... \to M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \to ...$$

heißt **exakt bei** M_i, wenn $\mathrm{Im}(f_i) = \mathrm{Kern}(f_{i+1})$.

Definition 5.14. Eine Sequenz heißt **exakte Sequenz**, wenn sie an jedem M_i exakt ist.

Definition 5.15. Ein **kurze exakte Sequenz** ist eine Sequenz der Form

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

Exakheit bedeuet hierbei, dass f injektiv, g surjektiv und $\mathrm{Im}(f) = \mathrm{Kern}(g)$.

Definition 5.17. Sei

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

eine kurze exakte Sequenz von R-Moduln.
Die Sequenz spaltet, wenn es einen Untermodul $N \subset M$ mit $M = N \oplus \mathrm{Kern}(g)$ gibt.

Satz 5.18. *Sei*

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

eine kurze exakte Sequenz von R-Moduln.
Dann sind äquivalent:

a) *Die Sequenz spaltet (Es gibt einen Untermodul $N \subset M$ mit $M = N \oplus \mathrm{Kern}(g)$)*

b) *Es gibt eine R-lineare Abbildung $s : M'' \to M$ mit $g \circ s = \mathrm{id}_{M'}$*

c) *Es gibt eine R-lineare Abbildung $t : M \to M'$ mit $t \circ f = \mathrm{id}_{M'}$*

Satz 5.19. *Sei $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ eine kurze exakte Sequenz von R-Moduln.*
Ist M'' frei, so spaltet die Sequenz $M \cong M' \oplus M''$.

Korollar 5.20. *Sei*

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

eine kurze exakte Sequenz von R-Moduln. Sind M' und M'' frei, so ist M frei.

5.6 Endlich erzeugbare Moduln

Definition 5.21. Ein R-Modul M heißt **endlich erzeugbar**, wenn M ein endliches Erzeugendensystem hat.
Äquivalent: Es gibt einen surjektiven Homomorphismus $R^n \to M$.

Satz 5.23. *Sei*

$$0 \to M'' \xrightarrow{f} M \xrightarrow{g} \to 0$$

eine kurze Exakte Sequenz von R-Moduln. Dann gilt

a) *Ist M endlich erzeugt, so auch M''.*

b) *Sind M' und M'' endlich erzeugt, so auch M.*

Satz 5.24. *Seien $M_1, ..., M_n$ R-Moduln und sei $M = \bigoplus_{i=1}^{n} M_i$.*
Dann ist M genau dann endlich erzeugt, wenn alle M_i endlich erzeugt sind.

Definition 5.25. Ein R-Modul heißt **noethersch**, wenn jeder Untermodul von M endlich erzeugbar ist.

Satz 5.26. *Sei M ein R-Modul. Dann sind äquivalent:*

a) *M ist noethersch.*

b) *Jede aufsteigende Kette von Untermoduln wird stationär.*

c) *Jede nichtleere Teilmenge von Untermoduln von M hat ein maximales Element*

Satz 5.27. *Sei*

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

eine kurze exakte Sequenz von R-Moduln. Dann ist M genau dann noethersch, wenn M' und M'' noethersch sind.

Satz 5.28. *Seien $M_1, ..., M_n$ R-Moduln und sei $M = \bigoplus_{i=1}^{n} M_i$.*
Dann ist M genau dann noethersch, wenn jedes M_i noethersch ist.

Satz 5.29. *Sei R ein noetherscher Ring und M ein endlich erzeugbarer R-Modul. Dann ist M noethersch.*

6 Ganze Ringerweiterungen

6.1 Definitionen und Eigenschaften

Definition 6.1. Sei B ein Ring und $A \subset B$ ein Unterring.
$x \in B$ heißt **ganz** über A, wenn es ein normiertes $f \in A[X]$ mit $f(x) = 0$ gibt.

Satz 6.2. *Sei B ein Ring, $A \subset B$ ein Unterring und $x \in B$.*
Dann sind äquivalent:

a) *x ist ganz über A.*

b) *Der Ring $A[x]$ ist ein endlich erzeugter A-Modul.*

c) *Der Ring $A[x]$ ist ein einem Unterring $C \subset B$ enthalten, sodass C ein endlich erzeugter A-Modul ist.*

Korollar 6.3. *Sei B ein Ring und A ein Unterring.*

a) *Sind $x_1, ..., x_n \in B$ ganz über A, so ist $A[x_1, ..., x_n]$ ein endlich erzeugter A-Modul.*

b) *Sei B ein Unterring eines Rings C. Ist B ein endlich erzeugter A-Modul und $y \in C$ ganz über B, so ist y ganz über A.*

Definition 6.4. Sei B ein Ring und $A \subset B$ ein Unterring. Dann nennt man

$$\overline{A} := \{x \in B \mid x \text{ ist ganz über } A\}$$

die **ganze Hülle** von A in B.

Satz 6.5. *Sei B ein Ring und $A \subset B$ ein Unterring. Dann ist die ganze Hülle $\overline{A}$ von A über B ein Unterring von B.*

Definition 6.6. Ist $\overline{A} = B$, so heißt B **ganz** über A.

Satz 6.7. *Seien $A \subset B \subset C$ Ringerweiterungen.*
Ist C ganz über B und B ganz über A, so ist auch B ganz über A.

Definition 6.8. Ein Integritätsbereich heißt **ganz abgeschlossen**, wenn er ganz abgeschlossen in seinem Quotientenkörper ist.

Satz 6.9. *Sei A ein faktorieller Integritätsbereich.*
Dann ist A ganz abgeschlossen.

Satz 6.10. *Sei A ein Integritätsbereich mit Quotientenkörper K und sei A ganz abgeschlossen in K. Sei L/K ein algebraisch Körpererweiterung.*
Dann ist $\alpha \in L$ genau dann ganz über A, wenn $m_{\alpha,K} \in A[X]$ liegt.

6.2 Dedekindringe

Definition 6.11. Ein Integritätsbereich A heißt **Dedekindring**, wenn

a) A noethersch

b) A ist ganz abgeschlossen

c) Jedes Primideal $\neq 0$ ist maximal.

Definition 6.12. Ein **algebraischer Zahlkörper** K ist eine endliche Erweiterung von $\mathbb{Q}$.

Definition 6.13. Die ganze Hülle von $\mathbb{Z}$ in K wird als **Ring der ganzen Zahlen** in K bezeichnet. Man schreibt diesen als

$$O_K := \{a \in K | \exists f \in \mathbb{Z}[X] \text{ normiert mit } f(a) = 0\}$$

Theorem 6.14. *Sei K ein algebraischer Zahlkörper. Dann ist O_K ein Dedekindring.*

Theorem 6.16. *Sei A ein Dedekindring, $I \neq 0$ und $I \neq A$ ein Ideal in A.*
Dann gilt

$$I = P_1 ... P_n$$

mit eindeutigen Primidealen P_i.

6.3 Der Noethersche Normalisierungssatz

Der Noethersche Normalisierungssatz impliziert den Hilbertschen Nullstellensatz und ist daher für die algebraische Geometrie von großer Bedeutung.

Theorem 6.17. *Sei K ein Körper und $B = [b_1, ..., b_n]$ endlich erzeugter Ring.*
Dann existieren Elemente $x_1, ..., x_r \in B$, die algebraisch unabhängig über K sind, sodass B als Modul endlich erzeugt über $K[x_1, ..., x_r]$ ist.

Satz 6.18. *Sei $A \subset B$ eine Ringerweiterungen, B ganz über A und seien A und B Integritätsbereiche.*
Dann ist A genau dann Körper, wenn B Körper ist.

Theorem 6.19. *Sei L/K eine Körpererweiterung und $L = K[x_1, ..., x_n]$ für geeignete $x_1, ..., x_n \in L$. Dann ist L/K endlich.*

Satz 6.20. *Sei K ein Körper und $\mathfrak{m} \subset K[X_1, ..., X_n]$ ein maximales Ideal. Dann ist L/K mit $L = K[X_1, ..., X_n]/\mathfrak{m}$ eine endliche Körpererweiterung.*

6.4 Anfänge der algebraischen Geometrie

Definition 6.21. Sei K ein beliebiger Körper.

$$A^n = A^n_K := \{(a_1, ..., a_n) \mid a_i \in K\}$$

A^n wird als **n-dimensionaler affiner Raum** bezeichnet.

Definition 6.22. Für $F \in K[x_1, ..., x_n]$ definiert man

$$V(F) := \{p \in A^n \mid F(p) = 0\}$$

die **V???-Menge**.
Für $S \subset K[X_1, ..., X_n]$ sei

$$V(S) := \{p \in A^n \mid F(p) = 0 \forall_{F \in S}\} = \bigcap_{F \in S} V(F)$$

Definition 6.24. Eine Teilmenge $Y \subset A_n$ heißt algebraisch, wenn $y = V(S)$ für ein $S \subset K[X_1, ..., X_n]$ ist.

Satz 6.25. *Sei $S \subset K[X_1, ..., X_n]$ und $I = (S)$ das erzeugte Ideal. Dann gilt*

$$V(S) = V(I)$$

Definition 6.26. Sei K ein Körper und $n \in \mathbb{N}$, dann ist $\mathbb{A}^n_K$ die Menge der Algebraischen Mengen in K^n.

Satz 6.28. *Die Abbildung*

$$V : \left\{ \begin{array}{c} \text{Ideale in} \\ K[X_1, ..., X_n] \end{array} \right\} \to \{\text{Algebraische Teilmengen von } \mathbb{A}^n_K\}$$

hat folgende Eigenschaften

a) $V(0) = \mathbb{A}^n_K$, $V\big(K[X_1, ..., X_n]\big) = \emptyset$

b) Wenn $I \subset J$, dann gilt $V(J) \subset V(I)$.

c) Für das Produkt gilt: $V(IJ) = V(I \cap J) = V(I) \cup V(J)$

d) Für die Summe gilt: $V(\sum_i J_i) = \bigcap_i V(J_i)$

Satz 6.29. *Die Abbildung I*

$$I : \{\textit{Algebraische Teilmengen von } \mathbb{A}_K^n\} \to \left\{ \begin{array}{c} \textit{Ideale in} \\ K[X_1, ..., X_n] \end{array} \right\}$$
$$M \mapsto \{f \in K[x_1, ..., x_n] \mid f(p) = 0 \forall p \in M\}$$

hat folgende Eigenschaften:

a) Sei $M \subset N$*, dann gilt* $I(M) \supset I(N)$

b) Für eine beliebige Teilmenge $M \subset \mathbb{A}_K^n$ *gilt*

$$M \subset V\big(I(M)\big)$$

Gleichheit gilt genau dann wenn M algebraisch ist.

c) Für ein Ideal $J \subset K[X_1, ..., X_n]$ *gilt*

$$J \subset I\big(V(J)\big)$$

Definition 6.30. Sei eine Menge $\mathbb{A}_K^n$ abgeschlossen wenn sie algebraisch ist und deren Komplemente offen.
Die erzeugte Topologie wird als **Zariski-Topologie** bezeichnet.

Satz 6.32. *Seien* $a_1, ..., a_n \in K$*. Dann ist*

$$J = (X_1, a_1, x_2 - a_2, ..., X_n - a_n)$$

maximal in $K[X_1, ..., X_n]$ *und K ist isomorph zu* $K[X_1, ..., X_N]/J$

Theorem 6.33 (Schwacher Nullteilersatz)**.** *Sei K algebraisch abgeschlossen und*

$$J \subsetneqq K[X_1, ..., X_n]$$

Dann ist $V(J) \neq \emptyset$*.*

Theorem 6.34 (Hilbertscher Nullstellensatz)**.** *Sei K algebraisch abgeschlossen und J ein Ideal in* $K[X_1, ..., X_n]$*. Dann gilt*

$$I\big(V(J)\big) = \mathrm{rad}(J) = \{f \in K[X_1, ..., X_n] \exists n > 0 : \mathrm{id}\, f^n \in J\}$$