Algebra WiSe 17/18 Definitionen

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

Version vom 21. März 2018

Inhaltsverzeichnis

1 Wiederholung

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 $b \leq a$.

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.

1.2 Radikale

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**.

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 $\mathrm{Rad}(\mathfrak{a})$, $\sqrt{\mathfrak{a}}$)

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.

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

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

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

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) $1 \in S$.

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.

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

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 $\mathfrak{p}$.

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 $r = 0$.

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 $v = \text{lcm}(a, b) = (a, b)$

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 $(a) = (c)$.

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 $i = 1, ..., n$.

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 $x = y$.

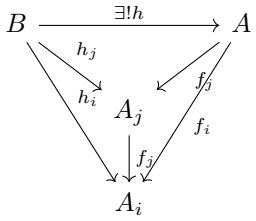
Definition 1.55. Für jedes $i \in I$sei A_i ein Ring und sei für jedes Paar $i, j \in I$ mit $i \leq j$ die Abbildung $f_{ij} : A_j \to A_i$ ein Ringhomomorphismus, sodass

a) $f_{ii} = \text{id}_{A_i}$ 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 $i \in I$.



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**.

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

a) $x \leq x$

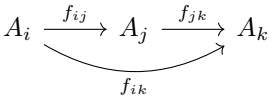
b) Aus $x \leq y$ und $y \leq z$ folgt $x \leq z$

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 $i \leq j \leq k$



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 $i \in I$.

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.

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**

2.2 Nullstellen von Polynomen

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

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**.

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 $f' := D(f)$.

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 $n = \text{char}(A)$.

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

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

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.

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.

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

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

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

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

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

$$f + g = \sum \big(f(\alpha) + g(\alpha)\big) X^\alpha \tag{1}$$
$$f \cdot g = \sum h(\alpha) X^\alpha \text{mit } h(\alpha) = \sum_{\beta+\gamma=\alpha} f(\beta)g(\gamma) \tag{2}$$

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$|x + y| \leq \max\{|x|\,, |y|\}$.

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

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 $c \in K$.

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 $A[X]$.

2.6 Der Hilbertsche Basissatz

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

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

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

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 $A[X_1, ..., X_n]$.

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

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**.

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.

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

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

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.

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.

Definition 3.11. Sei K ein Körper. Dann heißt

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

der **Primkörper** von K.

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 $[L : K] < \infty$.

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.

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 $L = K(\alpha_1, ..., \alpha_n)$.

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.

3.3 Der algebraische Abschluss eines Körpers

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)

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.

Definition 3.52. Eine algebraische Körpererweiterung L/K die eine der Bedingungen von **??** erfüllt heißt **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 $\overline{K}$)

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

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 $\overline{K}$.

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 $\mathrm{char}(\mathbb{F}_p) = p$.

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.

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 $\mathrm{Aut}_K(L)$.

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.

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.

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.

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.

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

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

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

die **Eulersche φ-Funktion**.

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

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

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 $\Phi_{n,K}$.

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

$$\begin{aligned} f(x+y) &= f(x) + f(y) \\ f(ax) &= af(x) \end{aligned}$$

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.

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**.

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.

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 $R^n \to M$.

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

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.

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.

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

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

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

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

6.3 Der Noethersche Normalisierungssatz

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

6.4 Anfänge der algebraischen Geometrie

Definition 6.21. Sei K ein beliebiger Körper.

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

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.

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

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.