

Algebra WiSe 17/18

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

Version vom 15. März 2018

Inhaltsverzeichnis

1	Wiederholung	2
1.1	Lokale Ringe	3
1.2	Radikale	4
1.2.1	Operationen auf Radikalen	5
1.3	Ringe von Brüchen	7
1.4	Integritätsbereiche und Hauptidealringe	9
1.5	Inverse und direkte Limiten	12
2	Polynomringe	15
2.1	Polynome mit einer Variable	15
2.2	Nullstellen von Polynomen	18
2.3	Polynome mehrerer Veränderlicher	21
2.4	Bewertungen	24
2.5	Der Satz von Gauß	27
2.6	Der Hilbertsche Basissatz	29
2.7	Eigenschaften von Polynomringen	30
2.8	Irreduzibilitätskriterien	30
2.9	Symmetrische Polynome	31
3	Körpererweiterungen	35
3.1	Grundbegriffe	35
3.2	Algebraische Körpererweiterungen	37
3.3	Der algebraische Abschluss eines Körpers	40
3.4	Zerfallskörper	44
3.5	Separabel Körpererweiterungen	46
3.6	Endliche Körper	50
4	Galois-Erweiterungen	52
4.1	Die Galoisgruppe einer Gleichung	58
4.2	Kreisteilungspolynome	62

5	Moduln	69
5.1	Definitionen	69
5.2	Faktormoduln	71
5.3	Direkte Summen und Produkte	71
5.4	Erzeugendensysteme und Basen	71
5.5	Exakte Sequenzen	72
5.6	Endlich erzeugbare Moduln	73
6	Ganze Ringerweiterungen	76
6.1	Definitionen und Eigenschaften	76
6.2	Dedekindringe	79
6.3	Der Noethersche Normalisierungssatz	80
6.4	Anfänge der algebraischen Geometrie	82

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.

Beweis. a) \Rightarrow Sei $a + \mathfrak{a} \in A/\mathfrak{p}$ ein Nullteiler, dann existiert $x \in A \setminus \mathfrak{p}$, sodass

$$(a + \mathfrak{a})(x + \mathfrak{a}) = ax + \mathfrak{a} = \mathfrak{p}$$

Also ist $ax \in \mathfrak{a}$ und da \mathfrak{a} Primideal folgt $a \in \mathfrak{a}$.

\Leftarrow Sei A/\mathfrak{a} Integritätsbereich und sei $ab \in \mathfrak{a}$, dann ist

$$(a + \mathfrak{a})(b + \mathfrak{a}) = ab + \mathfrak{a} = \mathfrak{a}$$

Da A/\mathfrak{a} Integritätsbereich ist gilt $a + \mathfrak{a} = \mathfrak{a}$ oder $b + \mathfrak{a} = \mathfrak{a}$, also $a \in \mathfrak{a}$ oder $b \in \mathfrak{a}$.

b) \Rightarrow Sei I/\mathfrak{a} ein Ideal in A/\mathfrak{a} .

Hierbei ist I eine Ideal in A welches \mathfrak{a} enthält, also $\mathfrak{a} \subseteq I \subseteq A$.

Da \mathfrak{a} maximal ist, muss $\mathfrak{a} = I$ oder $\mathfrak{a} = A$. Also ist A/\mathfrak{a} ein Körper.

\Leftarrow Sei I ein Ideal in A mit $\mathfrak{a} \subseteq I \subseteq A$.

Dann ist I/\mathfrak{a} eine Ideal in A/\mathfrak{a} , d.h.

$$I/\mathfrak{a} = \mathfrak{a}/\mathfrak{a} \quad \text{oder} \quad I/\mathfrak{a} = A/\mathfrak{a}$$

Damit folgt $I = \mathfrak{a}$ oder $I = A$.

□

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 $(b, a) \in R$, dann gilt $a = b$. (Antisymmetrie)

Ist R eine partielle Ordnungen auf A so schreiben 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.

Beweis. Sei $\Sigma = \{I \subset A \mid I \text{ ist Ideal}\}$. Dann ist $0 \in \Sigma$ und Σ ist partielle geordnet durch die mengentheoretische Inklusion.

Sei $(C_i)_{i \in I}$ eine Kette in Σ . Dann ist

$$C = \bigcup_{i \in I} C_i$$

ein Ideal in A . Aus $I \not\subseteq C_i$ für alle $i \in I$ folgt, dass $I \not\subseteq C$, d.h. $C \in \Sigma$. Somit hat Σ ein maximales Element. \square

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.

Beweis. Betrachte $(a) = Aa \neq A$. \square

1.1 Lokale Ringe

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

Satz 1.8. Sei A ein Ring und $\mathfrak{m} \neq A$ ein Ideal in A .

Ist jedes $x \in A \setminus \mathfrak{m}$ eine Einheit, so ist A ein lokaler Ring mit maximalem Ideal \mathfrak{m} .

Beweis. Für jedes Ideal $I \subsetneq A$ gilt $I \cap A^* = \emptyset$, enthält also keine Einheiten und ist somit in \mathfrak{m} enthalten. Somit ist \mathfrak{m} das einzige maximale Ideal. \square

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

Beispiel 1.10.1. Jedes Ideal in \mathbb{Z} ist der Form $(m) = \mathbb{Z}m$ mit $m \in \mathbb{Z}_{\geq 0}$.

Es gilt, dass (m) genau dann Primideal ist, wenn $m = 0$ oder m Primzahl.

Ist \mathfrak{p} Primzahl, so ist (\mathfrak{p}) maximal.

Sei K ein Körper und $A = K[X_1, \dots, X_n]$. Dann ist der Kern des Homomorphismus $\phi: A \rightarrow K, f \mapsto f(0)$ ein maximales Ideal in A .

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 $\neq 0$.

Beweis. • Zz: N ist eine additive Untergruppe von A
Seien $x, y \in N$ mit $x^n = y^m = 0$. Dann ist

$$(x + y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k y^{n+m-k} = 0$$

denn kann nicht sowohl $k < n$, als auch $n + m - k < m$ sein.

- Zz. $AN \subset N$.

Sei $x \in N$ mit $x^n = 0$ und $a \in A$. Dann ist $(ax)^n = a^n x^n = 0$, also $ax \in N$.

Also ist N Ideal in A .

Sei nun $a + N \in A/N$ nilpotent. Dann ist $(a + N)^n = 0$ für ein $n > 0$.

Also ist $a^n + N = 0$, also $a^n \in N$.

Dann ist $(a^n)^m = 0$ und somit $a^{nm} = 0$, also nilpotent. Es folgt, dass $a \in N$.

□

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

- das Nilradikal von A der Schnitt aller Primideale von A .
- 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

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

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

Beweis. Sei $\pi : A \rightarrow A/\mathfrak{a}$ die Kanonische Projektion. Dann ist $r(\mathfrak{a}) = \pi^{-1}(N_{A/\mathfrak{a}})$. Also ist $r(\mathfrak{a})$ ein Ideal. □

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

- $\mathfrak{a} \subseteq r(\mathfrak{a})$
- $r(r(\mathfrak{a})) = r(\mathfrak{a})$
- $r(\mathfrak{a}\mathfrak{b}) = r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b})$
- $r(\mathfrak{a}) = A \Leftrightarrow \mathfrak{a} = A$.
- $r(\mathfrak{a} + \mathfrak{b}) = r(r(\mathfrak{a}) + r(\mathfrak{b}))$.

1.2.1 Operationen auf Radikalen

Definition 1.17. Seien A ein Ring.

- a) Seien $\mathfrak{a}, \mathfrak{b} \subset A$ Ideale in A .
Dann ist

$$\mathfrak{a} + \mathfrak{b} =: \{x + y \mid x \in \mathfrak{a}, y \in \mathfrak{b}\}$$

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 $x + y = 1$.

Beweis. **2) \Rightarrow 1)** Sei $z \in A$ und $x \in \mathfrak{a}, y \in \mathfrak{b}$, mit $x + y = 1$.

Dann ist $z = zx + zy$, wobei $zx \in \mathfrak{a}, zy \in \mathfrak{b}$, also $z \in \mathfrak{a} + \mathfrak{b}$.

1) \Rightarrow 2)

□

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

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

b) Es gilt

$$\prod_{i=1}^n \mathfrak{a}_i = \bigcap_{i=1}^n \mathfrak{a}_i$$

Beweis. a) Sei i fest. Es gibt Elemente $x_j \in \mathfrak{a}_i, y_j \in \mathfrak{a}_j$ mit $1 = x_j + y_j$ für $i \neq j$. Dann ist

$$1 = \prod_{\substack{j=1 \\ j \neq i}}^n (x_j + y_j) = \underbrace{x}_{\in \mathfrak{a}_i} + \underbrace{\prod_{\substack{j=1 \\ j \neq i}}^n y_j}_{\in \prod_{\substack{j=1 \\ j \neq i}}^n \mathfrak{a}_j} \in \mathfrak{a}_i + \prod_{\substack{j=1 \\ j \neq i}}^n \mathfrak{a}_j$$

b) Durch Induktion über n .

$n = 2$ Sei $z \in \mathfrak{a} \cap \mathfrak{b}$. Schreibe $1 = x + y$ mit $x \in \mathfrak{a}, y \in \mathfrak{b}$. Dann ist $z = zx + zy \in \mathfrak{a}\mathfrak{b}$.

$n > 2$ Sei

$$\mathfrak{b} = \prod_{i=1}^{n-1} \mathfrak{a}_i$$

Wir nehmen an es gelte

$$\prod_{i=1}^{n-1} \mathfrak{a}_i = \prod_{i=1}^{n-1} \mathfrak{a}_i$$

Dann ist aber

$$\prod_{i=1}^n \mathfrak{a}_i = \mathfrak{a}_i \mathfrak{b}_i = \mathfrak{a}_i \cap \mathfrak{b} = \bigcap_{i=1}^n \mathfrak{a}_i$$

□

Definition 1.22. Sei A ein Ring und seien $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ Ideale in A . Wir definieren die Abbildung

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

Proposition 1.23. a) ϕ ist ein Ringhomomorphismus und

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

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

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

Beweis. b) \Rightarrow Sei ϕ surjektiv. Wir zeigen, dass \mathfrak{a}_1 und \mathfrak{a}_2 teilerfremd sind.

Es gibt ein $x \in A$ mit $\phi(x) = (1_{A/\mathfrak{a}_1}, 0, \dots, 0)$.

Also ist $x = 1 \pmod{\mathfrak{a}_1}$ und $x = 0 \pmod{\mathfrak{a}_2}$.

Dann ist

$$1 = \underbrace{(1-x)}_{\in \mathfrak{a}_1} + \underbrace{x}_{\in \mathfrak{a}_2} \in \mathfrak{a}_1 + \mathfrak{a}_2$$

\Leftarrow Seien nun die \mathfrak{a}_i paarweise teilerfremd.

Es reicht zu zeigen, dass es Elemente $x_i \in A$ mit

$$\phi(x_i) = (0, \dots, 0, 1, 0, \dots, 0)$$

(1 an der i -ten Position) gibt.

Wir zeigen für $i = 1$:

Da $\mathfrak{a}_1 + \mathfrak{a}_j = A$ für alle $j > 1$, gibt es $x_j \in \mathfrak{a}_1, y_j \in \mathfrak{a}_j$ mit $x_j + y_j = 1$

Sei nun

$$x := \prod_{i=2}^n y_i = \prod_{i=2}^n (1 - x_i) = 1 \pmod{\mathfrak{a}_1}$$

und $x = 0 \pmod{\mathfrak{a}_j}$ für $j > 1$.

□

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 Äquivalenzklassen wird 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.

Beispiel 1.28. Sei $A = \mathbb{Z}$ und $S = \mathbb{Z} \setminus \{0\}$. Dann ist $S^{-1}A$ isomorph zu \mathbb{Q} .

Korollar 1.29. Die Abbildung

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

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

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

Beweis. b) Sei $s \in S$, dann ist $s/1 \cdot 1/s = s/s = 1/1 = 1_{S^{-1}A}$

c) Sei $a \in \text{Kern}(\varphi_S)$, dann ist $a/1 = 0/1$, also $(a1 - 01)s = 0$ für ein $s \in S$.
Also ist $as = 0$ für ein $s \in S$.

d) Sei $a/s \in S^{-1}A$. Dann ist

$$\varphi_S(a) = a/1 \quad \varphi_S(s) = s/1 \quad \varphi_S(s)^{-1} = 1/s$$

Es folgt

$$\varphi_S(a)\varphi_S(s)^{-1} = a/1 \cdot 1/s = a/s$$

□

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

$$\begin{array}{ccc} A & \xrightarrow{g} & B \\ \downarrow \varphi_S & \nearrow h & \\ S^{-1}A & & \end{array}$$

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 $\mathbb{Z}_{(p)} = \{m/n \mid m/n \in \mathbb{Q}, p \nmid n\}$.

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

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

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

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

Beweis. Wir beweisen nur 2).

Sei J ein Ideal in $S^{-1}A$. Dann ist $I = \varphi_S^{-1}(J)$ ein Ideal in A und $J = S^{-1}I$:

Sei $a/s \in S^{-1}I$. Aus $I = \varphi_S^{-1}(J)$ folgt, dass $\varphi_S(a) \in J$. Also ist

$$a/s = \underbrace{a/1}_{\varphi_S(a)} \cdot \underbrace{1/s}_{\in S^{-1}A} \in J$$

d.h. $s \in \varphi_S^{-1}(J) = I$ und $a/s \in S^{-1}I$. □

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

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

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 $r = 0$.

Beispiel 1.40. a) \mathbb{Z} ist euklidisch unter $\lambda(x) = |x|$.

b) Sei K ein Körper. Dann ist $K[X]$ euklidisch mit $\lambda(f) = \deg(f)$.

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

Beweis. Sei $\mathfrak{a} \neq 0$ ein Ideal in A . Dann hat

$$\lambda(x) \mid x \in \mathfrak{a}, x \neq 0$$

ein kleinstes Element, d.h. es gibt ein $x \in \mathfrak{a} \setminus \{0\}$ mit $\lambda(x) \leq \lambda(y)$ für alle $y \in \mathfrak{a} \setminus \{0\}$.

Es gilt $\mathfrak{a} = (x)$.

Sei $y \in \mathfrak{a} \setminus \{0\}$. Schreibe $y = qx + r$ mit $r = 0$ oder $\lambda(r) < \lambda(x)$.

Dann ist $r \in \mathfrak{a}$ und aus der Minimalität von $\lambda(x)$ folgt $r = 0$ und damit $\mathfrak{a} \subset (x)$. □

Definition 1.42. Sei A ein Ring und seien $a, b \in A$.

$d \in A$ 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 seien $a, b \in A$.

$d \in A$ 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 $v|g$.

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

Satz 1.44. Sei A ein Hauptidealring und seien $a, b \in A$.

Dann existiert ein $d = \text{gcd}(a, b)$ und $v = \text{lcm}(a, b)$ von a, b und es gilt

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

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

Beweis. • Da A ein Hauptidealring ist, gilt $(a) + (b) = (d)$ für ein $d \in A$.

Es gilt $a, b \in (d)$, also $d|a$ und $d|b$.

Sei $g \in A$ mit $g|a$ und $g|b$. Dann ist $(a) \subset (g)$ und $(b) \subset (g)$.

Daraus folgt, dass $(a) + (b) \subseteq (g)$, also $(d) \subset (g)$. Damit folgt $g|d$.

- Analog für lcm .

□

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

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

Beweis. Sei $p = ab$, dann gilt $p|ab$. Es folgt $p|a$ oder $p|b$.

Angenommen $p|a$, dann ist $a = px$ für ein $x \in A$ und $p = pxb$. Es folgt, dass $p(1 - bx) = 0$ und da A Integritätsbereich ist $1 - bx = 0$.

Also muss $bx = 1$ also ist $b \in A^*$.

□

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

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

Beweis. Sei c irreduzibel, also ist (c) maximal. Daraus folgt, dass (c) Primideal ist und somit c prim.

□

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

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)

Beweis. Angenommen S hat kein maximales Element. Dann gibt es zu jedem $\mathfrak{a}_1 \in S$ ein $\mathfrak{a}_2 \in S$ mit $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2$. Es gibt also eine unendliche Kette

$$\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \dots$$

von Idealen in S . Sei nun $\mathfrak{a} := \bigcup_{j=1}^{\infty} \mathfrak{a}_j$.

Dann ist \mathfrak{a} ein Ideal in A , also ist \mathfrak{a} ein Hauptideal und $\mathfrak{a} = (x)$ für ein $x \in A$. Dann folgt insbesondere, dass $x \in \mathfrak{a}$. Damit folgt, dass es $j_0 \in \mathbb{N}$ gibt, mit $x \in \mathfrak{a}_{j_0}$.

Somit ist $(x) \subset \mathfrak{a}_{j_0}$ und somit $\mathfrak{a} = \mathfrak{a}_{j_0}$.

Dies bedeutet aber, dass die Kette stationär wird, was ein Widerspruch zur Annahme ist. \square

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

Beweis. Zerlegbarkeit der Elemente Sei $S = \{(a) \mid a \in A, a \notin A^*, a \neq 0\}$.

Angenommen $S \neq \emptyset$. Dann hat S ein maximales Element (a) und a ist nicht irreduzibel.

Dann gibt es $b, c \in A \setminus A^*$, mit $a = bc$.

Also ist $(a) \subsetneq (b)$ und $(a) \subsetneq (c)$. Da (a) maximal in S ist folgt daraus, dass $(b), (c) \notin S$.

Somit zerfallen b, c in irreduzible Faktoren und damit gilt $a \in S$. Widerspruch!.

Eindeutigkeit der Zerlegung Sei $a \in A$. Angenommen es gäbe zwei irreduzible Zerlegungen $a = c_1 \dots c_m = d_1 \dots d_n$ mit $m \leq n$.

Dann ist c_1 irreduzibel und somit prim. Also muss $c_1 \mid d_i$ für ein i gelte.

Nach Umnummerierung gilt $c_1 \mid d_1$, also $d_1 = u_1 c_1$ für $u_1 \in A^*$.

Also ist

$$\begin{aligned} c_1 \dots c_m &= u_1 c_1 d_2 \dots d_n \\ \Rightarrow c_2 \dots c_m &= d_2 \dots d_n \end{aligned}$$

Fortsetzen des Argumentes liefert

$$1 = u_1 \dots u_m d_{m+1} \dots d_n$$

für geeignete $u_i \in A^*$.

Dann sind aber d_{m+1}, \dots, d_n Einheiten und damit Eindeutig bis auf Einheiten und Reihenfolge.

□

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

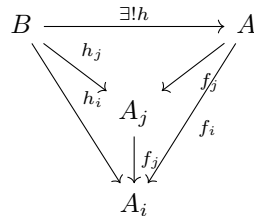
- a) $x \leq x$.
- b) Aus $x \leq y$ und $y \leq z$ folgt $x \leq z$.
- c) Aus $x \leq y$ und $y \leq x$ folgt $x = y$.

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 $f_{ij} : A_j \rightarrow A_i$ 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 $f_i : A \rightarrow A_i$, 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 Eigenschaft erfüllt ist: Sind $h_i : B \rightarrow A_i$ für alle $i \in I$ Ringhomomorphismen mit $h_i = f_{ij} \circ h_j$ für $i \leq j$, so existiert genau ein Ringhomomorphismus $h : B \rightarrow A$ 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 $h : B \rightarrow A$ und $g : A \rightarrow B$, die die oben beschriebenen Verträglichkeitsbedingungen erfüllen.

Durch Zusammensetzen dieser Homomorphismen erhalten wir Abbildungen. Die Eindeigkeitsbedingung impliziert nun, dass $g \circ h = \text{id}_B$ und $h \circ g = \text{id}_A$.

Man schreibt auch $A = \varprojlim_{i \in I} A_i$ für den projektiven Limes des Systems (A_i, f_{ij}) .

Existenz des Projektiven Limes. Sei $(A_i, f_{ij})_{i,j \in I}$ ein projektives System von Ringen.

Setze

$$A = \{(x_i)_{i \in I} \mid f_{ij}(x_j) = x_i \text{ für } i \leq j\} \subset \prod_{i \in I} A_i$$

und $h_j : A \rightarrow A_j, (x_i)_{i \in I} \mapsto x_j$.

Dann ist $(A, h_i)_{i \in I}$ ein projektiver Limes von (A_i, f_{ij}) .

Insebesondere definiert jede Familie $(x_i)_{i \in I}$ mit $f_{ij}(x_j) = x_i$ ein eindeutiges Element $x \in \varprojlim_{i \in I} A_i$. \square

Beispiel 1.58. Ein Beispiel für einen projektiven Limes sind die p -adischen ganzen Zahlen.

Sei $p \in \mathbb{Z}$ eine Primzahl, $I = \mathbb{N}$, mit der Ordnung \leq .

Für $n \geq 1$ sei $A_n = \mathbb{Z}/p^n\mathbb{Z}$. Sei

$$\begin{aligned} f_{mn} : A_n = \mathbb{Z}/p^n\mathbb{Z} &\rightarrow A_m = \mathbb{Z}/p^m\mathbb{Z} \\ x &\mapsto x \pmod{p^m} \end{aligned}$$

Dann ist $(A_m, f_{mn})_{m,n \geq 1}$ ein projektives System. Der projektive Limes wird als Ring der p -adischen ganzen Zahlen

$$\mathbb{Z}_p = \varprojlim_{n \geq 1} A_n$$

bezeichnet. Also ist

$$\begin{aligned} \mathbb{Z}_p &= \{(x_n)_{n \geq 1} \mid x_n \in \mathbb{Z}/p^n\mathbb{Z}, f_{mn}(x_n) = x_m \text{ für } m \leq n\} \\ &= \{(x_n)_{n \geq 1} \mid x_n \in \mathbb{Z}/p^n\mathbb{Z}, x_n \pmod{p^{n-1}} = x_{n-1}\} \end{aligned}$$

Wir schreiben die Elemente aus \mathbb{Z}_p auch als Folgen

$$x = (x_n)_{n \geq 1} = (\dots, x_{n+1}, x_n, \dots, x_1)$$

mit $x_n \pmod{p^{n-1}} = x_{n-1}$.

Addition und Multiplikation erfolgen komponentenweise.

Sie Abbildung

$$\begin{aligned} \mathbb{Z} &\rightarrow \mathbb{Z}_p \\ m &\mapsto (\dots, m + p^n, \dots, m + p) \end{aligned}$$

ist ein injektiver Ringhomomorphismus.

Sei $x = (\dots, x_n, x_{n-1}, \dots, x_1)$. Ist $x \neq 0$, so ist x der Form $(\dots, x_{n+1}, x_n, 0, \dots, 0)$ und für $j \leq n$ sind alle Einträge $x_j \neq 0$.

Weiterhin gilt

$$p|x \Leftrightarrow x|_n \text{ für alle } n \geq 1$$

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

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

Beweis. a) \Rightarrow Sei $x = (\dots, x_n, \dots, x_1) \in \mathbb{Z}_p^*$. Dann existiert ein $y = (\dots, y_n, \dots, y_1) \in \mathbb{Z}_p$ mit

$$\begin{aligned} xy &= (\dots, x_n, \dots, x_1)(\dots, y_n, \dots, y_1) \\ &= (\dots, x_n y_n, \dots, x_1 y_1) \\ &= (\dots, 1, \dots, 1) = 1 \end{aligned}$$

d.h. jeder Eintrag von x ist invertierbar, d.h. $p \nmid x_n$ für alle $n \geq 1$.

\Leftarrow Angenommen $p \nmid x$, dann muss $p \nmid x_n$ für ein $n \geq 1$.
Dann muss aber $p \nmid x_n$ für alle $n \geq 1$.
d.h. jedes x_n ist invertierbar. Sei

$$y = (\dots, x_n^{-1}, \dots, x_1^{-1}) \in \prod_{n \geq 1} \mathbb{Z}/p\mathbb{Z}$$

dann erfüllt y die Kompatibilitätsbedingungen, d.h. $y \in \mathbb{Z}_p$ und $xy = 1$.

b) Ist klar. □

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 Betrags konstruiert werden.

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

- a) $x \leq x$
- b) Aus $x \leq y$ und $y \leq z$ folgt $x \leq z$
- c) Für alle x, y existiert 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 $f_{ij} : A_i \rightarrow A_j$ gegeben, mit

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

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

$$\begin{array}{ccccc} A_i & \xrightarrow{f_{ij}} & A_j & \xrightarrow{f_{jk}} & A_k \\ & \searrow & \nearrow & & \\ & & f_{ik} & & \end{array}$$

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

Definition 1.65. Ein Ring A zusammen mit dem einem Homomorphismus $f_i : A_i \rightarrow A$, 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 $h_i : A_i \rightarrow B$, $i \in I$ Ringhomomorphismen mit $h_i = h_j \circ f_{ij}$ für $i \leq j$, so existiert genau ein Ringhomomorphismus $h : A \rightarrow B$ mit $h_i = h \circ f_i$ für alle $i \in I$.

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

Beweis. Sei

$$\hat{A} = \bigcup_{i \in I} A_i = \bigcup_{i \in I} \{(i, x) \mid x \in A_i\}$$

Wir definieren die Äquivalenzrelation \sim auf \hat{A} :

Seien $x, y \in \hat{A}$, d.h. $x \in A_i, y \in A_j$.

$$x \sim y \Leftrightarrow \text{es gibt ein } k \in I \text{ mit } i \leq k \text{ und } j \leq k \text{ und } f_{ik}(x) = f_{jk}(y)$$

□

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, \dots) 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

$$\begin{aligned} (a_0, a_1, \dots) + (b_0, b_1, \dots) &= (a_0 + b_0, a_1 + b_1, \dots) \\ (a_0, a_1, \dots) \cdot (b_0, b_1, \dots) &= (c_0, c_1, \dots) \end{aligned}$$

mit $c_n = \sum_{k=0}^n a_{n-k} b_k$.

Das Nullelement ist $0 = (0, 0, \dots)$ und $1 = (1, 0, 0, \dots)$ 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 $A \rightarrow A[X], a \mapsto (a, 0, 0, \dots)$ ist ein injektiver Ringhomomorphismus und A ist Unterring von $A[X]$.

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

c) Polynome lassen sich schreiben als

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

d) Dann gilt für Addition und Multiplikation:

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

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 ist $\deg(fg) = \deg(f) + \deg(g)$.

Korollar 2.7. A ist genau dann Integritätsbereich wenn $A[X]$ Integritätsbereich ist.

In diesem Fall gilt $A[X]^* = A^*$.

Beweis. \Leftarrow Ist $A[X]$ ein Integritätsbereich, dann ist insbesondere $A \subset A[X]$.

\Rightarrow Sei A ein Integritätsbereich. Dann gilt $\deg(fg) = \deg(f) + \deg(g)$. Sei zusätzlich $f, g \in A[X]$ mit $fg = 0$, dann ist $\deg(fg) = -\infty$.

Also muss $\deg(f) = -\infty$ oder $\deg(g) = -\infty$. Damit $f = 0$ oder $g = 0$.

Also ist $A[X]$ Integritätsbereich.

Sei nun $fg = 1$, dann ist $\deg(fg) = 0$, also muss $\deg(f) = \deg(g) = 0$. Dann sind $f, g \in A^*$. \square

Satz 2.8. Sei $f : A \rightarrow B$ ein Ringhomomorphismus und $b \in B$.

Dann gibt es genau einen Homomorphismen $\varphi_A : A[X] \rightarrow B$ mit $\varphi_B|_A = \varphi$ und $\varphi_b(X) = b$.

Beweis. Existenz Für $\varphi = \sum_j a_j X^j$ setze $\varphi_s(f) = \varphi_b(a) = \varphi(a)$ für alle $a \in A$ und $\varphi_b(X) = b$.

Dann ist φ_s ein Homomorphismus.

Eindeutigkeit Sei $\psi : A[X] \rightarrow B$ ein zweiter Homomorphismus mit $\psi|_A = \varphi$ und $\psi(X) = b$. Dann ist

$$\begin{aligned}\psi(f) &= \psi\left(\sum_j a_j X^j\right) = \sum_j \psi(a_j) \psi(X)^j \\ &= \sum_j \varphi(a_j) b^j = \varphi_b(f)\end{aligned}$$

□

Beispiel 2.9. Sei I ein Ideal in A . Die Komposition $A \rightarrow A/I \rightarrow (A/I)[X]$ ist ein Ringhomomorphismus. Dieser induziert einen Ringhomomorphismus $\pi : A[X] \rightarrow (A/I)[X]$ mit $\pi(x) = x$.

Diese Abbildung ist die Reduktion der Koeffizienten modulo I .

$$\text{Kern}(\pi) = \left\{ \sum_i a_i X^i \mid a_i \in I \right\} = I[X]$$

und somit

$$(A/I)[X] \cong A[X/I[X]]$$

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 $\deg(r) < \deg(g)$.

Beweis. Existenz Falls $f = 0$ dann gilt $q, r = 0$. Falls $\deg(f) < \deg(g)$ dann ist $q = 0, r = f$.

Sei als $f \neq 0$, $m = \deg(f)$ $h = \deg(g)$ und $m \geq h$.

f, g lassen sich schreiben als

$$f = \sum_{k=1}^m a_k X^k \qquad g = \sum_{j=0}^n b_j X^j$$

Dabei ist $b_n \in A^*$.

Durch Induktion:

$m = 0$ Dann gilt $f = a_0$, $g = b_0$. Dann $q = a_0 b_0^{-1}$ und $r = 0$.

$m \geq 1$ Definiere $h := f - X^{m-n} a_m b_n^{-1} g$.

Dann ist $\deg(h) \leq m - 1$. Nach der Induktionshypothese gibt es $q, r \in A[X]$ mit $h = qg + r$ und $\deg(r) < \deg(g)$.

Es folgt

$$f = X^{m-n} a_m b_n^{-1} qg + r = (X^{m-n} a_m b_n^{-1} + q)g + r$$

Eindeutigkeit Angenommen es gibt $q_1, q_2, r_1, r_2 \in A[X]$, sodass $f = gq_1 + r_1 = gq_2 + r_2$ und $\deg(r_1), \deg(r_2) < \deg(g)$.
Dann folgt aber

$$\begin{aligned} &\Rightarrow (q_1 - q_2)g = r_2 - r_1 \\ &\Rightarrow \deg(q_1 - q_2) + \deg(g) = \underbrace{\deg(r_2 - r_1)}_{< \deg(g)} \\ &\Rightarrow \deg(q_1 - q_2) \leq 0 \end{aligned}$$

daraus folgt $q_1 - q_2 = 0$ und damit $r_1 = r_2$. □

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 konstanten Polynome.

Satz 2.13. Sei A ein Integritätsbereich. Dann ist

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

Beweis. \Rightarrow bereits gezeigt.

\Leftarrow Die Abbildung $\varphi_0 : A[X] \rightarrow A, f \mapsto f(0)$ ist ein Ring-Homomorphismus.
Dann ist

$$\text{Kern}(\varphi_0) = \left\{ f = \sum_{k=0}^n a_k X^k \in A[X] \mid a_0 = 0 \right\}$$

Dann gilt $\text{Kern}(\varphi_0)$ ist ein Primideal in $A[X]$ und somit ein maximales Ideal.

Also ist $A[X]/\text{Kern}(\varphi_0)$ ist Körper und $A[X]/\text{Kern}(\varphi_0) \cong A$.

Also ist A 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

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

Beweis. \Rightarrow Sei $f(a) = 0$. Division mit Rest liefert

$$f = q(x - a) + r$$

mit $\deg(r) < 1$. Aus $f(a) = r$ folgt $(x - a) \mid f$ □

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 $a_1, \dots, a_m \in A$ und $n_1, \dots, n_m \in \mathbb{N}$
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

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

Beweis. Teilen mit Rest. □

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

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

Beweis. Durch Induktion über n :

Induktionsanfang: Sei $n = 0$. (Konstantes Polynom \Rightarrow keine Nullstelle)

Induktionsschritt: Sei $n > 0$. Ist $a \in A$ eine Nullstelle von f , so ist $f = g(x - a)$ mit $\deg(g) = n - 1$.

Sei $b \neq a$ eine weitere Nullstelle von f , dass ist $0 = f(b) = g(b)(b - a)$.

Da aber $(b \neq a)$ ist, muss b Nullstelle von g sein.

Nach Induktionsannahme hat g höchstens $n - 1$ verschiedene Nullstellen. □

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

Beispiel 2.20. Sei K ein endlicher Körper und sei

$$f = \prod_{a \in K} (x - a)$$

Dann ist $f(a) = 0$ für alle $a \in K$.

Satz 2.21. Sei G_1 zyklische Gruppe der Ordnung n_1 , G_2 zyklische Gruppe der Ordnung n_2 .

Seien n_1, n_2 teilerfremd, so ist $G_1 \times G_2$ zyklisch.

Beweis. Sei $G_1 = \langle x_1 \rangle$ und $G_2 = \langle x_2 \rangle$. Die Abbildung

$$\begin{aligned} \mathbb{Z} &\rightarrow G_1 \times G_2 \\ m &\mapsto (mx_1, mx_2) \end{aligned}$$

hat den Kern $n_1, n_2 \in \mathbb{Z}$ und ist surjektiv nach ??.

Dann ist

$$\mathbb{Z}/n_1n_2\mathbb{Z} \cong G_1 \times G_2$$

□

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

Beweis. Da G eine endliche abelsche Gruppe ist zerfällt G in

$$g = \bigotimes_{p \text{ prim}} G_p$$

Dabei ist $G_p = \{g \in G \mid g^q = 1 \text{ für ein } q = p^n\}$.

Angenommen G_p ist nicht zyklisch. Dann ist $\text{ord}(g) \leq |G_p|$ für alle $g \in G_p$ und es gibt ein $q = p^n < |G_p|$ mit $g^q = 1$ für alle $g \in G_p$. Dann hat aber das Polynom $X^q - 1$ mehr als q Nullstellen in K . Widerspruch!

Also sind alle G_p zyklisch. Dann folgt nach ??, dass G zyklisch ist. \square

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

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

$$f = a_n X^n + a_{n-1} X^{n-1} + \dots + a_i X^i + a_0$$

ein Polynom in $K[X]$.

Ist $b = c/d$ eine Nullstelle von f in K mit teilerfremden c, d , so gilt

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

Beweis. Aus $f(b) = 0$ folgt

$$a_n (c/d)^n + a_{n-1} (c/d)^{n-1} + \dots + a_0 = 0$$

Dann ist (nach Multiplikation mit d^n)

$$a_n c^n + a_{n-1} c^{n-1} d + \dots + a_n d^n = 0$$

Dann ist

$$\begin{aligned} a_n d^n &= c(\dots) \\ a_n c^n &= d(\dots) \end{aligned}$$

Also gilt $c|a_0$ und $d|a_n$ \square

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

$$\begin{aligned} (x-a)^n &| f \\ (x-a)^{n-1} &\nmid f \end{aligned}$$

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

Definition 2.26. Die Abbildung

$$\begin{aligned} D : A[X] &\rightarrow A[X] \\ \sum_{j=0}^n a_j X^j &\mapsto \sum_{j=1}^n j a_j X^{j-1} \end{aligned}$$

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

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

$$a) \ D(af + bg) = aD(f) + bD(g) \text{ (Linearität)}$$

$$b) \ D(fg) = (Df)g + f(Dg) \text{ (Produktregel)}$$

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

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

Beweis. Da a eine Nullstelle von f ist gilt

$$f = q(x - a)$$

für ein $q \in A[X]$. Es folgt

$$f' = q + q'(X - a)$$

und a hat genau dann Vielfachheit 1, wenn $(x - a) \nmid q$, also $(x - a) \nmid f'$, bzw. $f'(a) \neq 0$. \square

Definition 2.29. Die Abbildung

$$\begin{aligned} \chi : \mathbb{Z} &\rightarrow A \\ n &\mapsto n \cdot 1 \end{aligned}$$

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 $f \in K[X]$ $f \neq \text{const}$, dann gilt

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

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

b) Ist $\text{char}(K) = p > 0$, 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 $A[X_1, \dots, X_n]$ induktiv definiert als

$$A[X_1, X_2] := A[X_1][X_2]$$

$$A[X_1, \dots, X_n] := A[X_1, \dots, X_{n-1}][X_n]$$

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

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

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

Definition 2.34. Der Grad des Polynoms $f \in A[X_1, \dots, X_n]$ 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 $f \in A[X_1, \dots, X_n]$ heißt homogen vom Grad m , falls alle Monome in f Grad m haben.

Satz 2.36. Sei $\varphi : A \rightarrow B$ ein Ringhomomorphismus und $b_1, \dots, b_n \in B$. Dann existiert genau ein Ringhomomorphismus $\psi : A[X_1, \dots, X_n] \rightarrow B$ 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 $b_1, \dots, b_n \in B$. Die Inklusion $\iota : A \hookrightarrow B$ lässt sich eindeutig fortsetzen zu einem Homomorphismus $\varphi : A[X_1, \dots, X_n] \rightarrow B$ mit $\varphi|_A = \iota$ und $\varphi(X_j) = b_j$.

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

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

Definition 2.40. Ist $\varphi : A[X_1, \dots, X_n] \rightarrow B$ 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 (2.7 für mehrere Variablen). Sei A ein Ring

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

Beweis. Korollar 2.7 iterativ anwenden. □

Satz 2.42. Sei A Integritätsbereich. Dann gilt

$$A^* = A[X_1, \dots, X_n]^*$$

Satz 2.43. Es war einmal ein Integritätsbereich A . Der Integritätsbereich A hatte unendliche Teilmengen $T_1, \dots, T_n \subset A$ als Freunde.

Dann kam ein nettes $f \in A[X_1, \dots, X_n]$ für welches $f(t_1, \dots, t_n) = 0$ für alle $t_1 \in T_1, \dots, t_n \in T_n$ war.

Der Held wusste sofort, dass $f = 0$ gelten musste.¹

Beweis. Induktion über n :

$n = 1$ durch Negation von 2.18.

¹by Sandra

$n > 1$ Schreibe $f \in A[X_1, \dots, X_n]$ als

$$f = \sum_{j=0}^n \underbrace{\varphi_j(X_1, \dots, X_{n-1})}_{\in A[X_1, \dots, X_n]} X_n^j$$

Angenommen es existieren t_1, \dots, t_{n-1} , sodass $\varphi_j(t_1, \dots, t_{n-1}) \neq 0$ für ein j .

Dann ist f ein Polynom welches unendlich viele verschiedenen Nullstellen hat aber $\neq 0$ ist. Widerspruch!

Also muss $f = 0$.

□

Definition 2.44. Sei $I \neq \emptyset$ ein Indexmenge. Dann bezeichnet $\mathbb{N}^{(I)}$ die Menge der Form $(a_i)_{i \in I}$ mit $a \in \mathbb{N}_0$ 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 $\varphi : \mathbb{N}^{(I)} \rightarrow A$ mit $\varphi(\alpha) = 0$ für fast alle $\alpha \in \mathbb{N}^{(I)}$, mit Addition und Multiplikation

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

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

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

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

$$f + g = \sum (f(\alpha) + g(\alpha)) X^\alpha \quad (1)$$

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

Bemerkung 2.46. Für jedes $j \in I$ setzen wir $e_j = (b_i)_i$ mit $b_j = 1$, $b_i = 0$ für $j \neq i$.

Dann können 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 $A[(X_i)_{i \in I}]$ lassen 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

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

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-archimedisches Betrag auf K . Ist $|x| \neq |y|$, so gilt

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

Beweis. Sei $|x| \leq |y|$. Dann ist

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

Andererseits ist $x = (x + y) + (-y)$, sodass

$$|x| = |(x + y) + (-y)| \leq \max\{|x + y|, |y|\} = |x + y|$$

also $|x| \leq |x + y|$. □

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

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

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 $\nu : A \rightarrow \mathbb{R} \cup \{\infty\}$ 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 nicht-archimedischen Betrag auf K .

Beispiel 2.52.1. Sei A ein faktorieller Integritätsbereich und $p \in A$ prim. Dann lässt sich ein beliebiges $a \in A \setminus \{0\}$ schreiben als

$$a = a' p^{\nu_p(a)}$$

mit $\gcd(a', p) = 1$ und $\nu_p(a) \in \mathbb{N}_0$.

Mit der Bedingung, dass $\nu_p(0) = \infty$, ist die Abbildung

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

eine Bewertung auf A .

Diese setzt sich zu einer Bewertung auf dem Quotientenkörper fort.

Beispiel 2.52.2. Sei $p \in \mathbb{Z}$ eine positive Primzahl. Dann definiert

$$\nu_p : \mathbb{Z} \rightarrow \mathbb{R} \cup \{\infty\}$$

wie Oben eine Bewertung auf \mathbb{Z} . Diese setzt sich zu einer Bewertung auf \mathbb{Q} fort. Man definiert für $x \in \mathbb{Q}$

$$|x|_p := p^{-\nu_p(x)}$$

Dies liefert einen Betrag auf \mathbb{Q} .

Sei $x \in \mathbb{Q}$. Schreibe $x = a/bp^n$ mit $p \nmid ab$. Dann ist $|x|_p = p^{-n}$ und die Folge $1, p, p^2, \dots$ ist eine Nullfolge, bzgl. $|\cdot|_p$.

Die Vervollständigung von \mathbb{Q} bezüglich $|\cdot|_p$ ist isomorph zu \mathbb{Q}_p .

Theorem 2.53 (Lemma von Gauß). Sei A ein Integritätsbereich mit Quotientenkörper K und sei $\nu : A \rightarrow \mathbb{R} \cup \infty$ 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 $K[X]$.

Beweis. Wir zeigen

$$\nu(fg) = \nu(f) + \nu(g).$$

- Seien f, g Konstant, dann ist die Aussage klar.
- Sei nun $g = c \in K$. Dann ist

$$\begin{aligned}\nu(gf) &= \nu(cf) \\ &= \min\{\nu(ca_i)\} = \min\{\nu(c) + \nu(a_i)\} \\ &= \nu(c) + \min\{\nu(a_i)\} \\ &= \nu(g) + \nu(f)\end{aligned}$$

- Seien nun f, g nicht Konstant.
Durch multiplikation mit geeigneter Konstante können wir erreichen, dass

$$\nu(f) = \nu(g) = 0$$

Es ist zu zeigen, dass $\nu(fg) = 0$.

Sei dazu $f = \sum_{i=0}^n a_i X^i$, $g = \sum_{j=0}^m b_j x^j$. Dann ist

$$fg = \sum_{k=0}^{m+n} c_k X^k$$

mit

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

Es gilt

$$\nu(c_k) \geq \min\left\{ \underbrace{\nu(a_i b_j)}_{=\nu(a_i) + \nu(b_j) \geq 0} \right\} \geq 0$$

sodass $\nu(fg) \geq 0$.

Aus $c_{s+t} = a_0 b_{s+t} + a_1 b_{s+t-1} + \dots + a_s b_t + \dots + a_{s+t} b_0$ folgt

$$a_s b_t = c_{s+t} - a_0 b_{s+t} - a_1 b_{s+t-1} - \dots - a_{s+t} b_0$$

Dann ist also

$$\nu(a_s b_t) \geq \min\left\{ \nu(c_{s+t}), \underbrace{\nu(a_0 b_{s+t})}_{=\nu(a_0) + \nu(b_{s+t}) > 0}, \dots, \nu(a_{s+t} b_0) \right\} > 0$$

damit $\nu(a_s) + \nu(b_t) > 0$. Widerspruch!

□

2.5 Der Satz von Gauß

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

Ein Polynom

$$f = a_n X^n + a_{n-1} X^{n-1} + \dots + a_0 \in A[X]$$

heißt **primitiv**, wenn für seine Koeffizienten gilt: $\gcd(a_0, \dots, a_n) = 1$.

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

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

Beweis. \Rightarrow Sei f irreduzibel in $A[X]$. Sei $f = gh$ eine Zerlegung von f in $K[X]$.
Schreibe

$$g = c\tilde{g} \qquad h = d\tilde{h}$$

mit $\tilde{g}, \tilde{h} \in A[X]$ primitiv. Dann ist

$$f = cd\tilde{g}\tilde{h}$$

und insbesondere

$$\underbrace{\nu_p(f)}_{\geq 0} = \nu_p(cd) + \underbrace{\nu_p(\tilde{g})}_{=0} + \underbrace{\nu_p(\tilde{h})}_{=0}$$

Also $\nu_p(cd) \geq 0$ für alle $p \in A$ prim.

Dann muss aber die Potenz von jedem Primfaktor des Nenners $= 0$ sein.

Also ist $a = cd \in A$. Da $A[X]^* = A^*$ und $f = a\tilde{g}\tilde{h}$ und da f irreduzibel ist muss $a\tilde{g}$ oder \tilde{h} eine Einheit in $A[X]$ sein.

Dann ist $a\tilde{g}$ oder \tilde{h} in A^* , also g oder h konstant und somit in $K^* = K[X]^*$.

\Leftarrow Sei f irreduzibel in $K[X]$. Sei $f = gh$ in $A[X]$. Dann ist g oder h in $K[X]^*$, also konstant.

Sei $g = c$ für ein $c \in A$, dann ist

$$\nu_p(f) = \nu_p(c) + \nu_p(h)$$

Da f primitiv ist, ist $\nu_p(f) = 0$.

Dann gilt $\nu_p(c) = \nu_p(h) = 0$ für alle $p \in A$ prim.

Also muss $c \in A^* = A[X]^*$.

□

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

Beweis. Sei K der Quotientenkörper von A . Sei $f \in A[X] \setminus (A[X^*] \cup \{0\})$.

Wir zeigen, dass f über $A[X]$ in irreduzible Faktoren zerfällt.

Wir schreiben $f = c\tilde{f}$ mit $\tilde{f} \in A[X]$ primitiv und $c \in A$.

c zerfällt in A in irreduzible Faktoren.

Diese sind auch irreduzibel in $A[X]$.

Da $K[X]$ auch faktoriell ist, zerfällt \tilde{f} in $K[X]$ in irreduzible Faktoren $\tilde{f} = \tilde{f}_1 \cdot \dots \cdot \tilde{f}_n$ mit $\deg(\tilde{f}_i) \geq 1$.

Es gibt insbesondere eine Zerlegung

$$\tilde{f} = d\tilde{f}_1 \cdot \dots \cdot \tilde{f}_n$$

mit $d \in K$ und $\tilde{f}_i \in A[X]$ primitiv und $\deg(\tilde{f}_i) \geq 1$.

Mit 2.55 sind die \tilde{f}_i auch irreduzible in $A[X]$.

Aus

$$\underbrace{\nu_p(\tilde{f})}_{=0} = \nu_p(d) + \underbrace{\nu_p(\tilde{f}_1)}_{=0} + \dots + \underbrace{\nu_p(\tilde{f}_n)}_{=0}$$

folgt $\nu_p(d) = 0$ für alle $p \in A$ prim.

Jetzt ist noch zu zeigen, dass die gefundenen Zerlegung eindeutig ist. Se

$$\begin{aligned} f &= c_1 \cdot \dots \cdot c_m g_1 \cdot \dots \cdot g_r \\ &= d_1 \cdot \dots \cdot d_n h_1 \cdot \dots \cdot h_s \end{aligned}$$

mit $c_i, d_j \in A$ irreduzibel und $g_i, h_j \in A[X]$ irreduzibel mit $\deg \geq 1$.

Dann ist

$$c/d \cdot g_1 \cdot \dots \cdot g_r = h_1 \cdot \dots \cdot h_s$$

mit $c = c_1 \cdot \dots \cdot c_m$, $d = d_1 \cdot \dots \cdot d_n$ sind die g_i, h_j irreduzible in $A[X]$ und somit auch in $K[X]$.

Da $K[X]$ faktoriell ist, ist $r = s$ und nach Umsortierung ist

$$\begin{aligned} c/d \cdot g_1 &= x_1 h_1 \\ g_j &= x_j h_j \end{aligned}$$

für alle $j > 1$.

Dann ist

$$\begin{aligned} \nu_p(c/d) + \underbrace{\nu_p(g_1)}_{=0} &= \nu_p(x_1) + \underbrace{\nu_p(h_1)}_{=0} \\ \nu_p(x_i) - \nu_p(c/d) &= 0 \\ \nu_p(x_i \cdot d/c) &= 0 \end{aligned}$$

Wir definieren $\epsilon_1 := x_1 \cdot d/c$. Dann ist $\epsilon_1 \in A^*$.

Zusätzlich ist

$$\underbrace{\nu_p(g)}_{\geq 0} = \nu_p(x_j) + \underbrace{\nu_p(h_j)}_{=0}$$

Sei $\epsilon_j = x_j$ für $j \geq 1$. Dann ist $\epsilon_j = x_j \in A^*$.

Also ist

$$g_i = \underbrace{\epsilon_i}_{\in A^*} h_i$$

Weiterhin folgt $c = \epsilon d$ für ein $\epsilon \in A^*$.

Da A faktoriell ist, gilt $m = n$ und nach Umnummerieren $c_i \eta_i d_i$ mit $\eta_i d_i \in A^*$. \square

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

Beispiel 2.58.1. $\mathbb{Z}[X]$ ist ein faktorieller Integritätsbereich aber kein Hauptidealring.

Beispiel 2.58.2. Sei K ein Körper. $K[X]$ ist ein Hauptidealring und somit faktorieller. $K[X, Y]$ ist kein Hauptidealring aber faktoriell.

2.6 Der Hilbertsche Basissatz

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

Beweis. Sei $I \subset A[X]$ ein Ideal. Wir zeigen, dass I endlich erzeugt ist. Für $n \in \mathbb{N}_0$ sei

$$I_n := \{f \in I \mid \deg(f) \leq n\}$$

\square

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

$$\begin{aligned} b_n(f + g) &= b_n(f) + b_n(g) \\ b_n(af) &= ab_n(f) \end{aligned}$$

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

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

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

$$I(m) = I(m+1) = \dots$$

Für jedes $n = 0, 1, \dots$ 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 $\Leftrightarrow A[X_1, \dots, X_n]$ Integritätsbereich.
Dann gilt $A[X_1, \dots, X_n]^* = A^*$.
- b) (Gauss) A faktorieller Integritätsbereich $\Leftrightarrow A[X_1, \dots, X_n]$ faktorieller Integritätsbereich.
- c) (Hilbert) A noethersch $\Leftrightarrow A[X_1, \dots, X_n]$ noethersch.
- d) Sei A zusätzlich Integritätsbereich, dann ist
 A Körper $\Leftrightarrow A[X]$ Hauptidealring.

2.8 Irreduzibilitätskriterien

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

Sei

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

mit $\deg(f) = n \geq 1$. Sei $p \in A$ prim mit $p|a_i$ für $i = 0, \dots, n-1$ und $p \nmid a_n$ und $p^2 \nmid a_0$.

Dann ist f irreduzibel in $K[X]$.

Ist f zusätzlich primitiv, so ist f auch irreduzibel in $A[X]$.

Beweis. Sei $f = c\tilde{f}$ mit $\tilde{f} \in A[X]$ primitiv und $c \in A$.

Es reicht zu zeigen, dass \tilde{f} irreduzibel in $A[X]$ ist.

Angenommen $f = gh$ mit $g, h \in A[X] \setminus A$. Sei

$$\begin{aligned}\tilde{f} &= \sum_{k=0}^n \tilde{a}_k X^k \\ g &= \sum_{k=0}^s b_k X^k \\ h &= \sum_{k=0}^t a_k X^k\end{aligned}$$

Dann folgt aus $p \nmid a_n$, dass $p \nmid c$ und aus $p|a_0$, dass $p|\tilde{a}_0 = b_0 d_0$.

Wir können annehmen, dass $p|b_0$.

Aus $p^2 \nmid a_0$ folgt, dass $p \nmid d_0$. Es gibt aber j , sodass $p \nmid b_j$ (da sonst $p|g$).

Wähle nun j , sodass $p|b_i$ für alle $i < j$ und $p \nmid b_j$.

Dann muss $1 \leq j \leq s \leq n$. Aus

$$\tilde{a}_j = b_0 d_j + b_1 d_{j-1} + \dots + b_j d_0$$

folgt, (da $p|\tilde{a}_j$), dass $p|b_j d_0$ und $p|d_0$. Widerspruch! □

Beispiel 2.61. Sei $p \in \mathbb{Z}$ eine positive Primzahl, dann ist das p -te Kreisteilungspolynom

$$f = X^{p-1} + X^{p-2} + \dots + 1$$

irreduzibel in $\mathbb{Z}[X]$.

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

Sei

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

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

Beweis. Wir nehmen an, dass f primitiv ist.

Ist f reduzibel über $K[X]$ so auch über $A[X]$.

Sei $f = gh$ mit $g, h \in A[X] \setminus A$. Da p den höchsten Koeffizienten von f nicht teilt, gilt dies auch für g und h und es gilt

$$\pi(f) = \pi(gh) = \pi(g)\pi(h)$$

d.h. $\pi(f)$ zerfällt in $(A/(p))[X]$.

Sei f nun beliebig. Schreibe $f = c\tilde{f}$ mit $c \in A$ und $\tilde{f} \in A[X]$ primitiv.

Angenommen f ist nicht irreduzibel in $K[X]$, dann gilt f reduzibel in $K[X] \Rightarrow \tilde{f}$ ist reduzibel in $K[X] \Rightarrow \tilde{f}$ ist reduzibel in $A[X] \Rightarrow \tilde{f} = gh$ mit $g, h \in A[X] \setminus A \Rightarrow f = cgh$.

Somit ist

$$\pi(f) = \pi(cg)\pi(h)$$

eine Zerlegung von $\pi(f)$. □

Beispiel 2.63.1. Wir zeigen, dass $F = X^2 + 3X^2$ irreduzibel in $\mathbb{Q}[X]$ ist. Wir fassen f als Polynom über \mathbb{Z} auf und reduzieren die Koeffizienten mod 3.

$$\pi(f) = X^3 - X - 1$$

Da $\pi(f)(t) \neq 0$ für alle $t \in \Pi_3$ ist, ist $\pi(f)$ irreduzibel über Π_3 und somit auch über \mathbb{Q} .

Beispiel 2.63.2. Das Polynom $f = X^4 + 1$ ist irreduzibel in $\mathbb{Q}[X]$ und in $\mathbb{Z}[X]$. Allerdings ist $\pi(f) \in \Pi_p[X]$ reduzibel für alle positiven Primzahlen p .

2.9 Symmetrische Polynome

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

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

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

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

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

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

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

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

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

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

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

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

d) $\sigma(f) = f$

Definition 2.69. Sei $f \in A[X_1, \dots, X_n][X]$, $\sigma \in S_n$.
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 Polynome sind symmetrisch, d.h. $\sigma(s_j) = s_j$. Sie sind gegeben durch

$$\begin{aligned} s_1 &= X_1 + X_2 + \dots + X_n \\ s_2 &= X_1 X_2 + X_1 X_3 + \dots + X_1 X_n + X_2 X_3 + \dots + X_{n-1} X_n \\ &= \sum_{i \leq j} X_i X_j \\ s_n &= X_1 \dots X_n \end{aligned}$$

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

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

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

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

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

Beweis. a) Wir beweisen durch vollständige Induktion über n . Für $n = 1$ gilt die Behauptung, da $s_1 = x_1$.

Angenommen die Behauptung gilt für Polynome in $A[X_1, \dots, X_{n-1}]^{S_{n-1}}$.

Sei $f \in A[X_1, \dots, X_n]$. Es ist zu zeigen, dass f ein Polynom in s_1, \dots, s_n ist.

Setzt man $X_n = 0$ in

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

für $s_j = s_j(X_1, \dots, X_n)$, so erhält man

$$(X - X_1)(X - X_2) \dots (X - X_{n-1})(X) = X^n \sum_{j=1}^n (-1)^j (s_j)_0 X^{n-j}$$

mit $(s_j)_0 := s_j(X_1, \dots, X_{n-1}, 0)$.

Andererseits ist

$$(X - X_1)(X - X_2) \dots (X - X_{n-1})(X) = X \left(X^{n-1} \sum_{j=1}^{n-1} (-1)^j \tilde{s}_j X^{n-1-j} \right)$$

Dann muss aber $(s_1)_0 = \tilde{s}_1, \dots, (s_{n-1})_0 = \tilde{s}_{n-1}$ und $(s_n)_0 = 0$.

Wir beweisen die Aussage durch Induktion über $d = \deg(f)$.

Hat f Grad 0, so ist die Behauptung trivial.

Sei also $\deg(f) = d > 0$. Dann gibt es ein Polynom $g_1 \in A[X_1, \dots, X_{n-1}]$ mit $\text{gew}(g) \leq d$, sodass

$$f(X_1, \dots, X_{n-1}, 0) = g_1((s_1)_0, \dots, (s_{n-1})_0)$$

Grad $\leq d$ in X_1, \dots, X_{n-1} hat, da $f(X_1, \dots, X_{n-1}, 0)$ symmetrisch unter S_{n-1} ist.

Das Polynom $g_1(s_1, \dots, s_{n-1})$ hat Grad $\leq d$ in X_1, \dots, X_n weil die s_j homogen sind.

Das Polynom

$$f_1(X_1, \dots, X_n) = \underbrace{f(X_1, \dots, X_n)}_{\text{Grad} \leq d \text{ in } X_1, \dots, X_n} - \underbrace{g(s_1, \dots, s_{n-1})}_{\text{Grad} \leq d \text{ in } X_1, \dots, X_n}$$

hat Grad $\leq d$ in X_1, \dots, X_n und ist symmetrisch.

Aus $f_1(X_1, \dots, X_{n-1}, 0) \geq 0$ folgt $X_n | f_1$. Damit auch $X_i | f_1$ und somit $s_n | f_1$.

Dann gibt es f_2 , sodass $f_1 = s_n f_2$.

Dabei ist f_2 symmetrisch unter S_n und hat Grad $\leq d - n$.

Nach Induktionshypothese gibt es ein Polynom $g_2 \in A[X_1, \dots, X_n]$ mit Gewicht $\leq d - n$, sodass

$$f_2 = g_2(s_1, \dots, s_n)$$

Es folgt $f = f_1 + g_1 = s_n g_2 + g_1$.

Dann ist

$$f(X_1, \dots, X_n) = g_1(s_1, \dots, s_{n-1}) + s_n g_2(s_1, \dots, s_n) = g(s_1, \dots, s_n)$$

mit

$$g(X_1, \dots, X_n) = \underbrace{g_1(X_1, \dots, X_n)}_{\text{Gewicht} \leq d} + \underbrace{\underbrace{X_n}_{\text{Gew } n} \underbrace{g_2(X_1, \dots, X_n)}_{\text{Gew} \leq d-n}}_{\text{Gew} \leq d}$$

b) Siehe Lang

□

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

Beweis. Durch Induktion über n .

Für $n = 1$ ist die Behauptung klar.

Sei $n > 1$ und die s_1, \dots, s_n seien nicht algebraisch unabhängig.

Wähle $f \in A[X_1, \dots, X_n]$ mit kleinstem Grad und $f \neq 0$, sodass

$$f(s_1, \dots, s_n) = 0$$

Schreibe f als Polynom in X_n mit Koeffizienten in $A[X_1, \dots, X_{n-1}]$.

$$f(X_1, \dots, X_n) = f_0(X_1, \dots, X_{n-1}) + f_1(X_1, \dots, X_{n-1})X_n + \dots + f_d(X_1, \dots, X_{n-1})X_n^d$$

Angenommen $f = X_n \psi$ für ein $\psi \in A[X - 1, \dots, X_n]$ und $x_n \psi(s_1, \dots, s_n) = 0$, dann muss $\psi(s_1, \dots, s_n) = 0$ sein.

Dies ist ein Widerspruch zu der Annahme, dass f minimalen Grad hat.

Also muss $f_0 \neq 0$ sein.

Wir setzen nun $x_i = s_i$ und erhalten

$$\begin{aligned} 0 &= f(s_1, \dots, s_n) \\ &= f_0(s_1, \dots, s_n) + \dots + f_d(s_1, \dots, s_{n-1})s_n^d \end{aligned}$$

Nun setzen wir $X_n = 0$. Dann ist

$$0 = f((s_1)_0, \dots, (s_{n-1})_0) = f_0(\tilde{s}_1, \dots, \tilde{s}_{n-1})$$

Nach Induktionshypothese sind die $\tilde{s}_1, \dots, \tilde{s}_n$ algebraisch unabhängig. Widerspruch! □

Beispiel 2.76. Sei $n = 3$ Dann ist $X_1^3 + X - 2^3 + X_3^3$ ein symmetrisches Polynom. Es gilt

$$X_1^3 + X_2^3 + X_3^3 = s_1^3 - 3s_1s_2 + 3s_3$$

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

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

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

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

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

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

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

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

Beweis. Es ist

$$\prod_{i=1}^n = X^n + \sum_{i=1}^n (-1)^i s_i X^{n-i}$$

so dass

$$f = \prod_{i=1}^n (X - \alpha_i) = X^n + \sum_{i=1}^n (-1)^i s_i(\alpha_1, \dots, \alpha_n) X^{n-i} = X^n + \sum_{i=1}^n x_i X^{n-i}$$

d.h.

$$c_i = (-1)^i s_i(\alpha_1, \dots, \alpha_n)$$

und

$$\begin{aligned} D(f) &= d_n(-c_1, c_2, \dots, (-1)^n c_n) \\ &= d_n(s_1(\alpha_1, \dots, \alpha_n), \dots, s_n(\alpha_1, \dots, \alpha_n)) \\ &= \prod_{i \leq j} (\alpha_i - \alpha_j)^2 \end{aligned}$$

□

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

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

Beispiel 2.80.1. Für $f = X^2 + aX + b$ ist $D(f) = a^2 - 4b$ (Wurzel der pq-Formel)

Beispiel 2.80.2. Für $f = X^3 + aX + b$ ist $D(f) = -4a^3 - 27b^2$.

3 Körpererweiterungen

3.1 Grundbegriffe

Definition 3.1. Sei L ein Körper, $K \subset L$ heißt **Teilkörper** von L , wenn K abgeschlossen bezüglich 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

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

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

Beweisskizze. Die angegebenen Elemente bilden einen Teilkörper von L , der $K \cup M$ enthält und jeder Teilkörper von L der $K \cup M$ enthält, enthält auch die angegebenen Elemente. \square

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 $\text{char}(K) = 0$ oder *prim*.

Beweis. Da $\mathbb{Z}/(n) = \mathbb{Z}/\text{Kern}(\phi) \cong \text{Im}(f) \subset K$ keine Nullteiler hat. \square

Beispiel 3.9. a) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ haben Charakteristik 0.

b) Sei $p \in \mathbb{Z}$ eine positive Primzahl. Dann hat $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ Charakteristik p .

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

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

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) $\text{char}(K) = p$ für $p > 0$, p prim $\Leftrightarrow P \cong \mathbb{F}_p$

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

Definition 3.13. Ist K ein Teilkörper von L , so können wir L als Vektorraum über K auffassen.

Die Dimension dieses Vektorraums 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 $K \subset L \subset M$ Körpererweiterungen. 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 Basis von M/L , so ist $(x_i y_j)_{(i,j) \in I \times J}$ eine Basis von M/K .

Beweis. Es reicht die zweite Behauptung zu zeigen.

Sei $z \in M$. Dann ist

$$z = \sum_{j \in J} a_j y_j$$

mit $a_j \in L$ und $a_j = 0$ für fast alle $j \in J$.

Wir können a_j schreiben als

$$a_j = \sum_{i \in I} b_{ij} x_i$$

mit $b_{ij} \in K$ und $b_{ij} = 0$ für fast alle $i \in I$.

Also ist

$$z = \sum_{i \in I, j \in J} b_{ij} x_i y_j$$

d.h. $(x_i y_j)_{(i,j) \in I \times J}$ ist ein Erzeugendensystem von M/K .

Wir zeigen, dass die Vektoren x_i, y_i linear unabhängig über K sind.

Sei

$$\sum_{i,j} \underbrace{c_{ij}}_{\in K} \underbrace{x_i}_{\in K} \underbrace{y_j}_{\in M} = 0$$

Dann gilt für jedes j , dass

$$\sum_{i \in I} c_{ij} x_i = 0$$

weil die y_i linear unabhängig über L sind.

Aus der linearen Unabhängigkeit der x_i über K folgt $c_{ij} = 0$. □

3.2 Algebraische Körpererweiterungen

Definition 3.17. Sei L/K eine Körpererweiterung. $\alpha \in L$ heißt **algebraisch** über K , wenn es ein Polynom $g \in K[X] \setminus 0$ gibt, mit $g(\alpha) = 0$.

Äquivalent: Der Homomorphismus $K[X] \rightarrow L, f \mapsto f\alpha$ 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.

Beispiel 3.20. π und e sind transzendent über \mathbb{Q} .

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 $\varphi : K[X] \rightarrow L, f \mapsto f(\alpha)$.

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 $\varphi : K[X] \rightarrow L, g \mapsto g(a)$ und $\text{Im}(\varphi) = K[a]$. Dann induziert φ eine Isomorphismus

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

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

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

Beweis. Da $m_{\alpha,K}$ irreduzibel ist ist $(m_{\alpha,K})$ ein Maximales Ideal in $K[X]$ und damit $K[X]/(m_{\alpha,K})$ Körper.

Aus der Isomorphie folgt dass $K[\alpha]$ Körper ist.

Sei nun $g \in K[X]$. Dann ist $g = qm_{\alpha,K} + r$ mit $q, r \in K[X]$ und $\deg(r) < \deg(m_{\alpha,K})$.

Somit bilden die Restklassen $(m_{\alpha,K}), X + (m_{\alpha,K}), \dots, X^{n-1} + (m_{\alpha,K})$ mit $n = \deg(m_{\alpha,K})$ eine Basis von $K[X]/(m_{\alpha,K})$ über K .

Dann bildet auch $1, \alpha, \dots, \alpha^{n-1}$ eine Basis von $K[\alpha]$ über K . \square

Beispiel 3.24. Sei $n \in \mathbb{Z}, n > 0$ und p eine positive Primzahl. Dann ist $\sqrt[n]{p}$ eine Nullstelle von $f = X^n - p$.

D.h. $\sqrt[n]{p}$ ist algebraisch über \mathbb{Q} .

Das Eisenstein-Kriterium zeigt, dass f irreduzibel über \mathbb{Q} und $[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = n$ ist.

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

Beweis. Sei $[L : K] = n, n < \infty$ und $\alpha \in L$.

Dann sind die Elemente $\alpha^0, \alpha^1, \dots, \alpha^n$ linear abhängig über K .

(d.h. es existieren nicht trivial $c_0, \dots, c_n \in K$ sodass $c_0\alpha^0 + \dots + c_n\alpha^n = 0$.)

Also ist α Nullstelle des Polynoms und damit algebraisch. \square

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 $\alpha_1, \dots, \alpha_n$ gibt sodass $L = K(\alpha_1, \dots, \alpha_n)$.

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

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

$$b) \ L \text{ ist endlich und somit insbesondere algebraische Erweiterung von } K.$$

Beweis. jeweils durch Induktion über n

a) Angenommen die Aussage gelte für n :

$$\begin{aligned} K[\alpha_1, \dots, \alpha_{n+1}] &= K[\alpha_1, \dots, \alpha_n][\alpha_{n+1}] \\ &\stackrel{=}{=} \overline{IHK}(\alpha_1, \dots, \alpha_n)[\alpha_{n+1}] \end{aligned}$$

Da α_{n+1} algebraisch über $K \subseteq K(\alpha_1, \dots, \alpha_n)$

$$\begin{aligned} &= K(\alpha_1, \dots, \alpha_n)(\alpha_{n+1}) \\ &= K(\alpha_1, \dots, \alpha_{n+1}) \end{aligned}$$

b) Es gilt

$$[K(\alpha_1, \dots, \alpha_{n+1}) : K] = \underbrace{[K(\alpha_1, \dots, \alpha_n) : K(\alpha_1, \dots, \alpha_n)]}_{< \infty} [K(\alpha_1, \dots, \alpha_n) : K] < \infty$$

da α_{n+1} algebraisch über 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.

Beweis. 1) \Rightarrow 2) $K(L) = L$ ist algebraisch

2) \Rightarrow 1) Sei $K = L(m)$ für $m \subset L$ algebraisch über K .

Sei $\alpha \in L$. Dann gibt es $\alpha_1, \dots, \alpha_n \in M$ mit $\alpha \in K(\alpha_1, \dots, \alpha_n)$. Also ist α algebraisch über K .

□

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:

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

Beweis. Sei α algebraisch. Dann existiert ein Polynom $G = \sum_{i=0}^n a_i X^i \in L[X]$ mit $G(\alpha) = 0$.

Also ist $\alpha \in K(a_0, \dots, a_n, \alpha) = K(a_0, \dots, a_n)(\alpha)$.

Durch n -faches anwenden des Gradsatzes folgt $[K(a_0, \dots, a_n) : K] < \infty$.

Da α algebraisch über a_1, \dots, a_n gilt

$$[K(a_0, \dots, a_n, \alpha) : K(a_0, \dots, a_n)] < \infty$$

Also ist auch $[K(a_0, \dots, a_n, \alpha) : K] < \infty$ und daher folgt, dass α algebraisch über K ist.

□

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 $ab^{-1} \in K(a, b)$.

Beispiel 3.34. Der algebraische Abschluss von \mathbb{Q} in \mathbb{C} ist algebraisch über \mathbb{Q} aber nicht endlich über \mathbb{Q} da er u.a. die Teilkörper $\mathbb{Q}(\sqrt[p]{p})$ (p prim) enthält.

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.

Beweis. Sei $f \in K[X] \setminus K$ und sei f irreduzibel.

Dann ist (f) ein maximales Ideal in $K[X]$ und daher $K[X]/(f)$ Körper.

Die Komposition $K \hookrightarrow K[X] \xrightarrow{\Pi} K[X]/(f)$ ist ein Homomorphismus von Körpern und daher injektiv.

Fasse nun K als Teilkörper von L auf und definiere

$$a := \Pi(X) = X + (f)$$

Dann gilt mit $f = \sum_{i=0}^n a_i X^i$, dass

$$\begin{aligned} f(a) &= \sum_{i=0}^n a_i a^i = \sum_{i=0}^n a_i \Pi(X^i) = \Pi\left(\sum_{i=0}^n a_i X^i\right) \\ &= \Pi(f) \equiv 0 \end{aligned}$$

D.h. a ist Nullstelle von f .

Sei nun f nicht irreduzibel ist a Nullstelle eines irreduziblen Faktors.

Aus der Polynomdivision folgt, dass $[L : K] = \deg(f) < \infty$ und somit ist L/K algebraisch. \square

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 abgeschlossenen Körper L mit $K \subseteq L$.

Artin. Sei $K \hookrightarrow L_i$ eine Einbettung, sodass jedes nicht Konstante Polynome in $K[X]$ eine Nullstelle in L_i hat. Sei $I = K[X] \setminus K$.
Wir betrachten den Polynomring

$$K[(X_i)_{i \in I}]$$

Sei

$$A = \{f(X_f) \mid f \in I\}$$

Dann ist $A \neq K[(X_i)_{i \in I}]$, denn:
Angenommen $A = K[(X_i)_{i \in I}]$, dann ist $1 \in A$, d.h.

$$1 = \sum_{j=1}^n g_j f_j(X_{f_j})$$

für geeignete $g_j \in K[(X_i)_{i \in I}]$ und $f_i \in I$.
Es gibt aber einen Erweiterungskörper K' von K , sodass jedes f_j eine Nullstelle $a_j \in K'$ hat.
Definiere

$$K[(X_i)_{i \in I}] \rightarrow K[(X_i)_{i \in I}]$$

mit $\varphi|_K = \text{id}$.
Dann ist $\varphi(X_i) = X_i$ für $i \in I \setminus \{f_1, \dots, f_n\}$ und $\varphi(X_{f_i}) = a_i$ für $i \in \{1, \dots, n\}$
und

$$1 = \varphi(1) = \sum_{j=1}^m f(g_j) \underbrace{f(f(x_{f_j}))}_{=0} = 0$$

Widerspruch, da in Körpern $1 \neq 0$ sein muss.
Also ist $A \subsetneq K[(X_i)_{i \in I}]$.

Dann ist A in einem maximalen Ideal M enthalten und es gibt π

$$K \hookrightarrow K[(X_i)_{i \in I}] \xrightarrow{\pi} \underbrace{K[(X_i)_{i \in I}]/M}_{=L_i}$$

Setze $K = L_0$. Dann ist

$$L_0 \xrightarrow{\varphi_{01}} L_1$$

Sei $f \in I$. Dann ist

$$\underbrace{\varphi_{01}}_{\in L_1[X]}(\pi(X_f)) = \pi(f(X_f)) = 0$$

d.h. $\varphi_{01}(f)$ hat eine Nullstelle in L_1 . Durch Fortführung dieser Konstruktion erhalten wir eine Sequenz

$$L_0 \xrightarrow{\varphi_{01}} L_1 \xrightarrow{\varphi_{12}} \dots$$

und die Abbildungen

$$L_i \xrightarrow{\varphi_{ij}}$$

Sei nun

$$L = \varprojlim L_i = \bigcup_{i=1}^{\infty} L_i / \sim$$

der Direkten L_i und sein die Abbildungen

$$\varphi_i : L_i \rightarrow L$$

die entsprechenden Einbettungen.

Dann ist L ein Ring und die φ_i Ringhomomorphismen.

Seien $a, b \in L$. Dann existieren $a_i, b_i \in L_i$, mit $a = \varphi_i(a_i)$, $b = \varphi_i(b_i)$ und

$$\begin{aligned} a + b &= \varphi_i(a_i + b_i) \\ ab &= \varphi_i(a_i b_i) \end{aligned}$$

Somit ist L Körper.

Sei $g \in L[X] \setminus L$. Dann gibt es ein i und ein $g_i \in L_i[X] \setminus L_i$, sodass

$$g = \varphi_i(g_i)$$

Die Abbildung $\varphi_{ii+1}(g_i)$ zerfällt über L_{i+1} in Linearfaktoren. Somit zerfällt auch

$$g = \varphi_i(g_i) = \varphi_j(f_{ij}(g_i))$$

□

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.*

Beweis. Es gibt einen algebraisch abgeschlossenen Körper L der K enthält. Setze

$$\overline{K} = \{a \in L \mid a \text{ algebraisch über } K\}$$

Dann ist \overline{K} ein Teilkörper von L der K enthält.

Zz: \overline{K} ist algebraisch abgeschlossen:

Sei $f \in \overline{K}[X] \setminus \overline{K}$. Dann hat f eine Nullstelle α in L . α ist algebraisch über \overline{K} . Da \overline{K} algebraisch über K ist ist α auch algebraisch über K . Damit ist $\alpha \in \overline{K}$.

□

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

Beweis. Ist $\sigma : K \rightarrow L$ ein Homomorphismus von Körpern, so induziert σ einen Homomorphismus $K[X] \rightarrow L[X]$.

Ist α eine Nullstelle von $f \in K[X]$ in K , so ist $\sigma(\alpha)$ eine Nullstelle von $\sigma(f)$ in L . □

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

$$\begin{array}{ccccc}
& & K[X] & & \\
& \swarrow \varphi & \downarrow \pi & \searrow \psi & \\
K[\alpha] & \xleftarrow{\overline{\varphi}} & K[X]/(m_{\alpha,K}) & \xrightarrow{\overline{\psi}} & L
\end{array}$$

Abbildung 1: Kommutierendes Diagramm der Algebraischen Körpererweiterungen

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

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

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

- a) Ist $\sigma' : K' \rightarrow L'$ 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 $\sigma' : K' \rightarrow L'$ von σ mit $\sigma'(\alpha) = \beta$.

Beweis. Wir zeige nur b)

- b) Sei $\beta \in L$ Nullstelle von $\sigma(m_{\alpha,K})$ und sei

$$\begin{array}{ll}
\phi : K[X] \rightarrow K[\alpha] & \psi : K[X] \rightarrow L \\
g \mapsto g(\alpha) & g \mapsto \sigma(g)(\beta)
\end{array}$$

Dann ist $(m_{\alpha,K}) = \text{Kern}(\phi)$ und $(m_{\alpha,K}) \subset \text{Kern}(\psi)$.

Wir erhalten das kommutierende Diagramm 1 invertierbar. Definiere $\sigma' := \overline{\psi} \circ \overline{\phi}^{-1}$.

Dann ist $\sigma : K[\alpha] \rightarrow L$ und

$$\sigma'(\alpha) = \overline{\psi}(X + (m_{\alpha,K})) = \psi(X) = \beta$$

Das beweist die Existenz von σ' . Die Eindeutigkeit folgt draus, dass jedes Fortsetzung σ' durch ihren Wert auf α festgelegt ist.

□

Theorem 3.43 (Fortsetzungssatz). Sei K ein Körper, L ein algebraisch abgeschlossener Körper und $\sigma : K \rightarrow L$ ein Körperhomomorphismus. Sei K'/K eine algebraische Körpererweiterung.

Dann lässt sich σ fortsetzen zu einem Homomorphismus $\sigma' : K' \rightarrow L$.

Ist K' zusätzlich abgeschlossen und L algebraisch über $\sigma(K)$, so ist jedes Fortsetzung σ' von σ ein Isomorphismus.

Beweis. Sei M die Menge der Paare (F, τ) , wobei $K \subset F \subset K'$ ein Zwischenkörper und $\tau : F \rightarrow L$ eine Fortsetzung von σ ist. Dann ist M partiell geordnet durch

$$(F_1, \tau_1) \leq (F_2, \tau_2) \Leftrightarrow F_1 \subset F_2 \text{ und } \tau_2|_{F_1} = \tau_1$$

Es gilt $M \neq \emptyset$, weil $(K, \sigma) \in M$.

Jede Kette in M hat eine obere Schranke. somit hat M ein maximales Element

(F, τ) .

Es gilt $F = K'$, denn:

Angenommen $F \neq K'$. Sei $\alpha \in K' \setminus F$. Dann lässt sich τ fortsetzen zu einem Homomorphismus $\tau : F(\alpha) \rightarrow L$. Widerspruch!

Sei nun K' algebraisch abgeschlossen, L algebraisch über $\sigma(K)$ und $\sigma' : K' \rightarrow L$ eine Fortsetzung von σ .

L ist algebraisch über $\sigma(K)$ und damit über $\sigma'(K')$.

$\sigma'(K')$ ist aber bereits algebraisch abgeschlossen.

Es folgt $\sigma'(K') = L$. \square

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 $\sigma : \overline{K}_1 \rightarrow \overline{K}_2$ der die Identität auf K fortsetzt.

Beweis. Die Einbettung $\sigma : K \hookrightarrow \overline{K}_2$ lässt sich fortsetzen zu einem Homomorphismus $\sigma : \overline{K}_1 \rightarrow \overline{K}_2$. Diese ist ein Isomorphismus.

(Dieser ist i.a. nicht Kanonisch) \square

Beispiel 3.45. Der algebraische Abschluss $\overline{\mathbb{Q}} = \{a \in \mathbb{C} \mid a \text{ ist algebraisch über } \mathbb{Q}\}$ von \mathbb{Q} in \mathbb{C} ist ein algebraischer Abschluss von \mathbb{Q} .

3.4 Zerfallskörper

Definition 3.46. Seien K/L und L'/K Körpererweiterungen und sei $\sigma : L \rightarrow L'$ ein Homomorphismus.

σ wird als **K -Homomorphismus** ($\sigma|_K = \text{id}|_K$) 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 $f \in F$ zerfällt in Linearfaktoren über L
- b) Die Körpererweiterung L/K wird von 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 seien L_1 und L_2 zwei Zerfällungskörper von F über K . Sei $\sigma : L_1 \rightarrow L_2$ ein K -Homomorphismus in einen algebraischen Abschluss von L_2 .

Dann gilt $\sigma(L_1) = L_2$.

Beweis. Wir beweisen schrittweise:

- Wir nehmen zuerst an, dass F nur ein Polynom f enthält.
Seien a_1, \dots, a_n die Nullstellen von f in L_1 und b_1, \dots, b_n die Nullstellen von f in L_2 . Dann ist

$$f = \prod_{i=1}^n (x - a_i)$$

mit $c \in K$ und

$$\sigma(f) = c \prod_{i=1}^n (X - \sigma(a_i)) = c \prod_{i=1}^n (X - b_i)$$

d.h. nach Umm Nummerierung also $\sigma(a_i) = b_i$.

Es folgt

$$L_2 = K(b_1, \dots, b_n) = K(\sigma(a_1), \dots, \sigma(a_n)) = \sigma(K(a_1, \dots, a_n)) = \sigma(L_1)$$

- Falls f endlich viele Polynome enthält, so argumentiert man analog mit dem Produkt der Polynome.
- Sei F nun unendlich, M_1 die Menge der Nullstelle von F in L_1 , M_2 die Menge der Nullstellen von F in L_2 und sei $a \in L_1$.
Dann gibt es eine endliche Teilmenge $M'_1 \subset M_1$, sodass $a \in K(M'_1)$, d.h. es gibt eine endliche Teilmenge $F' \subset F$, sodass a im Zerfällungskörper L'_1 von F' über K in L_1 liegt.
Dann gilt $\sigma(L'_1) = L'_2$, d.h. $\sigma(a) \in L_2$ und $\sigma(L_1) \subset L_2$.
Analog gilt $L_2 \subset \sigma(L_1)$.

□

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 $L_1 \rightarrow L_2$

Beweis. Die Inklusion $K \hookrightarrow \overline{L}_2$ lässt sich zu einer K -Homomorphismus $L_1 \xrightarrow{\sigma} \overline{L}_2$ fortsetzen. Für diesen gilt $\sigma(L_1) = L_2$ □

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

- L ist der Zerfällungskörper einer Menge nicht-konstanter Polynome in $K[X]$.
- Ist $\sigma : L \rightarrow \overline{L}$ ein K -Homomorphismus, so gilt $\sigma(L) = L$.
- Jedes irreduzible Polynom $f \in K[X]$, das mindestens eine Nullstelle hat zerfällt in L vollständig in Linearfaktoren.

Beweis. 1) \Rightarrow 2) Folgt aus 3.49 mit $L_1 = L_2 = L$

2) \Rightarrow 3) Sei $f \in K[X]$ irreduzibel und $a \in L$ eine Nullstelle von f in L . Dann ist f bis auf eine Konstante das Minimalpolynom $m_{a,K}$. Ist b eine weitere Nullstelle von f in \overline{L} , so hat die Einbettung $K \hookrightarrow \overline{L}$ eine Fortsetzung $\sigma : K(\alpha) \rightarrow \overline{L}$ mit $\sigma(a) = b$ (3.42). Diese lässt sich Fortsetzen (3.43) zu einem K -Homomorphismus $\sigma : L \rightarrow \overline{L}$.
Aus $\sigma(L) = L$ folgt $b \in L$.

3) \Rightarrow 1) Es ist $L = K(M)$ für eine Teilmenge $M \subset L$ bestehend aus algebraischen Elementen (über K).

Für $a \in M$ ist $m_{a,K}$ irreduzibel über K und hat a als Nullstelle in L . Somit zerfällt $m_{a,K}$ in Linearfaktoren über L .

Also ist L der Zerfällungskörper der $m_{a,K}$.

□

Definition 3.52. Eine algebraische Körpererweiterung L/K die eine der Bedingungen von 3.51 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.

Beweis. Sei $\sigma \in \text{Hom}_M(L, \bar{L})$, dann ist $\sigma \in \text{Hom}_K(L, \bar{L})$. Dann ist $\sigma(L) = L$. \square

Beispiel 3.54. a) Sei L/K eine Körpererweiterung von Grad 2, dann ist L/K normal.

b) Die Erweiterungen $\mathbb{Q}(\sqrt[4]{2})/(\mathbb{Q}(\sqrt{2}))$ und $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ sind normal.
Die Erweiterung $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ hingegen nicht.

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 \bar{K} von K hat.
(Dies ist unabhängig von der Wahl von \bar{K})

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

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

Beweis. Sei $\alpha \in K$ eine Nullstelle von f . Dann ist $f = cm_{\alpha, K}$ für ein $c \in K^*$ und es gilt

$$\alpha \text{ ist mehrfache Nullstelle} \Leftrightarrow f(\alpha) = f'(\alpha) = 0 \Leftrightarrow f' = 0 \text{ weil } \deg(f') < \deg(f)$$

\square

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 $\text{char}(K) = 0$ und L/K eine algebraische Körpererweiterung. Dann ist L/K separabel.

Definition 3.60. Sei L/K eine algebraische Körpererweiterung und \bar{K} der algebraische Abschluss von K .

Der **Separabilitätsgrad** $[L : K]_S$ von L über K ist definiert als

$$[L : K]_S := |\text{Hom}_K(L, \bar{K})|$$

Diese Definition ist unabhängig von \bar{K} .

Satz 3.61. Sei $K(a)/K$ eine 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 \bar{K} von K .

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

Beweis. a) 3.43 gibt, dass die Anzahl der verschiedene K -Homomorphismen $\varphi : K(a) \rightarrow \bar{K}$ gleich der Anzahl der verschiedenen Nullstellen von $m_{a,K}$ in \bar{K} ist.

b) Es gilt

$$\begin{aligned} a \text{ ist separabel über } K & \\ \Leftrightarrow m_{a,K} \text{ ist separabel} & \\ \Leftrightarrow m_{a,K} \text{ hat nur einfache Nullstellen in } \bar{K} & \\ \Leftrightarrow \text{die Anzahl der Nullstellen von } m_{a,K} \text{ ist } \deg(m_{a,K}) & \\ \Leftrightarrow [K(a) : K]_S = [K(a) : K] & \end{aligned}$$

□

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

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

Beweis. Sei \bar{K} ein algebraischer Abschluss von M . Dann ist \bar{K} auch ein algebraischer Abschluss von K und $K \subset L \subset M \subset \bar{K}$. Sei

$$\begin{aligned} \text{Hom}_K(L, \bar{K}) &= \{\sigma_i \mid i \in I\} \\ \text{Hom}_L(M, \bar{K}) &= \{\tau_j \mid j \in J\} \end{aligned}$$

mit paarweise verschiedenen σ_i und τ_j .

Wir können $\sigma_i : L \rightarrow \bar{K}$ zu einem K -Automorphismus $\bar{\sigma}_i : \bar{K} \rightarrow \bar{K}$ fortsetzen. Es gilt

- a) Die Abbildung $\bar{\sigma}_i \circ \bar{\tau}_j$ sind paarweise verschiedene, denn:
Sei $\bar{\sigma}_i \circ \bar{\tau}_j = \bar{\sigma}_{i'} \circ \bar{\tau}_{j'}$. Die Restriktionen beider Seiten auf L liefert $\sigma_i = \sigma_{i'}$, d.h. $i = i'$. Es folgt $\tau_j = \tau_{j'}$ und $j = j'$.
- b) $\text{Hom}_K(M, \bar{K}) = \{\bar{\sigma} \circ \tau_j \mid i \in I, j \in J\}$, denn:
Die Abbildungen $\bar{\sigma}_i \circ \tau_i$ sind K -Homomorphismen. Es bleibt zu zeigen, dass jedes Element in $\text{Hom}_K(M, \bar{K})$ dieser Form ist.
Sei $\tau \in \text{Hom}_K(M, \bar{K})$. Dann ist $\tau|_L = \sigma_i$ für ein i . Die Abbildung $\bar{\sigma}_i^{-1} \circ \tau$ ist in $\text{Hom}_L(M, \bar{K})$. d.h. $\bar{\sigma}_i^{-1} \circ \tau = \tau_j$ für ein $j \in J$. Also ist $\tau = \bar{\sigma}_i \circ \tau_j$.

Es folgt die Behauptung. □

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

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

Beweis. L/K ist algebraisch, d.h. $L = K(a_1, \dots, a_n)$ für geeignete $a_1, \dots, a_n \in L$. Sei $L_0 = K$, $L_1 = K(a_1), \dots, L_n = K(a_1, \dots, a_n)$.

Äquivalent dazu ist $L_i = L_{i-1}(a_i)$ für $1 \leq i \leq n$.
Dann gilt

$$\begin{aligned} [L_i : L_{i-1}] &= [L_{i-1}(a_i) : L_{i-1}] = \deg(m_{a_i, L_{i-1}}) \\ &\geq \text{Anzahl der verschiedenen Nullstellen von } m_{a_i, L_{i-1}} \text{ in } \overline{K} = [L_i : L_{i-1}]_S \end{aligned}$$

Da aber zusätzlich

$$\begin{aligned} [L : K] &= \prod_{i=1}^n [L_i : L_{i-1}] \\ [L : K]_S &= \prod_{i=1}^n [L_i : L_{i-1}]_S \end{aligned}$$

folgt $[L : K]_S \leq [L : K]$ □

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

- a) L/K ist separabel.
- b) Es gibt über K separable Elemente $a_1, \dots, a_n \in L$, sodass $L = K(a_1, \dots, a_n)$.
- c) $[L : K]_S = [L : K]$

Beweis. 1) \Rightarrow 2) ist klar.

2) \Rightarrow 3) Setze $L_0 = K$, $L_i = L_{i-1}(a_i)$.

Dann ist a_i separabel über K , d.h. $m_{a_i, K}$ hat nur einfache Nullstellen in \overline{K} . Es gilt $m_{a_i, L_{i-1}} \mid m_{a_i, K}$.

Also hat auch $m_{a_i, L_{i-1}}$ nur einfache Nullstellen in \overline{K} .

Somit ist a_i separabel über L_{i-1} und daher gilt $[L_i : L_{i-1}]_S = [L_i : L_{i-1}]$.

Es folgt

$$[L : K]_S = \prod_{i=1}^n [L_i : L_{i-1}]_S = \prod_{i=1}^n [L_i : L_{i-1}] = [L : K]$$

3) \Rightarrow 1) Sei $a \in L$. Dann ist a algebraisch über K und $K \subset K(a) \subset L$.
Dann gilt mit dem Gradsatz

$$\begin{aligned} [L : K]_S &= [L : K(a)]_S [K(a) : K]_S \\ [L : K] &= [L : K(a)] [K(a) : K] \end{aligned}$$

Mit der Annahme dass $[L : K] = [L : K]_S$ und 3.63

$$\begin{aligned} [L : K(a)]_S &\leq [L : K(a)] \\ [K(a) : K]_S &\leq [K(a) : K] \end{aligned}$$

folgt, dass

$$[K(a) : K]_S \leq [K(a) : K]$$

d.h. a ist separabel über K . □

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

Beweis. Seien a_1, \dots, a_n die Nullstellen von f in \overline{K} . Dann ist $K(a_1, \dots, a_n)$ ein Zerfällungskörper von f über K . Aus $f(a_i) = 0$ folgt, dass $m_{a_i, K} | f$. Somit hat $m_{a_i, K}$ nur einfache Nullstellen in \overline{K} d.h. a_i ist separabel über K . \square

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 eine dieser Bedingungen erfüllt, so gilt

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

Beweis. 1) \Rightarrow 2) klar.

2) \Rightarrow 1) Sei $c \in L$. Dann gibt es immer endlich viele $a_1, \dots, a_n \in M$, sodass $c \in K(a_1, \dots, a_n)$. Nach ?? ist $K(a_1, \dots, a_n)$ separabel über K und somit auch c .

Für L/K endlich gilt ??.

Sei also $[L : K] = \infty$. Da L/K separabel ist, gilt dies auch für jeden Zwischenkörper $K \subset E \subset L$. Falls $[E : K] < \infty$, so gilt

$$[L : K]_S = [L : E]_S [E : K]_S \geq [E : K]_S = [E : K]$$

Es folgt $[L : K]_S = \infty$, weil L/K Zwischenkörper beliebig hohen aber endlichen Grad hat. \square

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.

Beweis. \Rightarrow Sei M/K separabel. Dann ist auch L/K separabel. Sei $a \in M$. Dann gilt $m_{a, L} | m_{a, K}$, d.h. a ist separabel über L .

\Leftarrow Seien M/L und L/K separabel. Sei $a \in M$. Der Erweiterungskörper L' von K der von den Koeffizienten von $m_{a, L}$ erzeugt wird ist endlich über K .

Aus $L' \subset L$ folgt $m_{a, L} | m_{a, L'}$. Da $m_{a, L} \in L'[X]$ gilt aber auch $m_{a, L'} | m_{a, L}$. Also ist $m_{a, L} = m_{a, L'}$ und $L'(a)/L'$ ist separabel. \square

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

Beweis. **K endlich** Sei K endlich, so auch L . Sei a ein Erzeuger von L^* , Dann ist $L = K(a)$.

K unendlich Sei K unendlich. Da L/K eine endliche Erweiterung ist gibt es Elemente $a_1, \dots, a_n \in L$, sodass $L = K(a_1, \dots, a_n)$. Durch zusammenfassen $a_i a_j$ zu c reicht es für $n = 2$ zu zeigen:

Sei $L = K(a, b)$ für geeignete $a, b \in L$ gegeben. Sei $m = [L : K]_S$ und seien $\sigma_1, \dots, \sigma_m$ die verschiedenen Elemente in $\text{Hom}_K(L, \bar{K})$. Definiere

$$g = \prod_{i \neq j} ((\sigma_i(a) - \sigma_j(a)) + (\sigma_i(b) - \sigma_j(b))) \in \bar{K}[X]$$

Dann ist g nicht das Nullpolynom, denn für $i \neq j$ ist $\sigma_i(a) \neq \sigma_j(a)$ oder $\sigma_i(b) \neq \sigma_j(b)$. Da K unendlich gibt es ein $c \in K$, sodass mit $g(c) \neq 0$. Es folgt

$$((\sigma_i(a) - \sigma_j(a)) + (\sigma_i(b) - \sigma_j(b))) c \neq 0$$

bzw. $\sigma_i(a + bc) \neq \sigma_j(a + bc)$ für alle $i \neq j$.

Die Elemente $\sigma(a + bc)$ sind also paarweise verschieden. Sei f das Minimalpolynom von $a + bc$ über K . Es folgt

$$[L : K]_S = m \leq \deg(f) = [K(a + bc) : K] \leq [L : K]$$

Da L/K separabel ist folgt Gleichheit. □

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.

Beweis. Da F endlich ist hat F einen endlichen Primkörper \mathbb{F}_p und $\text{char}(F) = p$. F ist ein endlich-dimensionaler Vektorraum über \mathbb{F}_p , d.h. $F = \mathbb{F}_p^n$ mit $n = [F : \mathbb{F}_p]$ und $|F| = p^n = q$.

Die multiplikative Gruppe F^* hat $q - 1$ Elemente, d.h. $a^{q-1} = 1$ für alle $a \in F^*$. Jedes $a \in F$ ist also Nullstelle von $f = X(X^{q-1} - 1) = X^q - X$.

F ist also der Zerfällungskörper von $f = X^q - X$ über \mathbb{F}_p . □

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 .

Beweis. Sei $f = X^q - X \in \mathbb{F}_p[X]$ und $L \subset \bar{\mathbb{F}_p}$ der Zerfällungskörper von f über \mathbb{F}_p .

Da $f' = -1$ hat f nur einfache Nullstellen in $\bar{\mathbb{F}_p}$.

Seien $a, b \in \overline{\mathbb{F}_p}$ zwei Nullfolge von f . Dann gilt

$$\begin{aligned}(a+b)^q &= \sum_{j=0}^q \binom{q}{j} a^{q-j} b^j \\ &= a^q + \underbrace{\binom{q}{1}}_{=0} a^{q-1} b + \dots + b^q \\ &= a^q + b^q \\ &= a + b\end{aligned}$$

Da heißt $a - b$ ist Nullstelle von f in $\overline{\mathbb{F}_p}$. Für $b \neq 0$ ist

$$\begin{aligned}(ab^{-1})^q &= a^q (b^{-1})^q \\ &= a^q (b^q)^{-1} \\ &= ab^{-1}\end{aligned}$$

D.h. ab^{-1} ist Nullstelle von f .

Die Nullstellen von f in $\overline{\mathbb{F}_p}$ bilden als einen Teilkörper von $\overline{\mathbb{F}_p}$.

Folglich besteht L aus den q Nullstellen von f in $\overline{\mathbb{F}_p}$.

Sei F ein zweiter Körper mit q Elementen, dann ist na3.70 F ein Zerfällungskörper von $X^q - X$ über seinem Primkörper \mathbb{F}_p . F ist somit isomorph. \square

Bemerkung 3.72. Wir können die 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 $\deg_{\mathbb{F}_p}(f) = n$.

Beweis. Sei $q = p^n$. Dann ist $\mathbb{F}_q/\mathbb{F}_p$ eine separable Erweiterung vom Grad n .

Nach dem Satz vom primitiven Element 3.68 ist $\mathbb{F}_q = \mathbb{F}_p(a)$ für ein $a \in \mathbb{F}_q$.

Dann ist m_{a, \mathbb{F}_p} irreduzibel und vom Grad n . \square

Beispiel 3.74. Das Polynom $X^2 + 1$ ist irreduzibel über \mathbb{F}_3 .

Also

$$\mathbb{F}_9 = \mathbb{F}_3(\theta) = \{a + \theta b \mid a, b \in \mathbb{F}_3\} \cong \mathbb{F}_3[X]/(X^2 + 1)$$

mit $\theta^2 = -1$.

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

Beweis. Sei \mathbb{F}_p der Primkörper von F und \overline{K} ein algebraischer Abschluss von \mathbb{F}_p . Dann ist \overline{K} auch ein algebraischer Abschluss von F_p . Schreibe $\overline{K} = \overline{F_p}$. Dann

$$F_p \subset F \subset K \subset \overline{F_p}$$

Falls $|K| \leq \infty$, so ist K isomorph zu \mathbb{F}_q mit $q = p^n$ und K ist als Zerfällungskörper des separablen Polynom $X^q - X$ normal und separabel über F_p und somit über F .

Sei $|K| = \infty$. Wähle $M \subset K$ mit $K = F(M)$.

Dann ist K die Vereinigung von Körper $F(M')$ wobei M' eine endliche Teilmenge von M ist.

$F(M')$ ist eine endliche Erweiterung von F und somit von F_p , d.h. $F(M')$ ist isomorph zu \mathbb{F}_q . Somit ist K normal und separabel über F . \square

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

$$\begin{aligned}\text{Fr} : F_q &\rightarrow F_q \\ x &\mapsto x^p\end{aligned}$$

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

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

Beweis. Sei s die Ordnung von Fr , d.h. $s = |\langle \text{Fr} \rangle|$.

Für $a \in F_q$ gilt

$$\text{Fr}^n(a) = a^{p^n} = a^q = a$$

s.h. $s|n$. Andererseits ist $\text{Fr}^s(a) = a^{p^s} = a$ für alle $a \in F_q$.

Das Polynom $X^{p^s} - X$ hat höchstens p^s verschiedene Nullstellen, d.h. $p^s \geq q = p^n$. Also gilt $s = n$.

Die Erweiterungen F_q/F_p ist normal und separabel, sodass

$$|\text{Aut}_{F_p}(F_q)| = |\text{Hom}_{F_p}(F_q, \overline{F_p})|$$

da F_q/F_p normal ist.

$$\begin{aligned}&= [F_q : F_p]_S \\ &= [F_q : F_p]\end{aligned}$$

Da F_q/F_p separabel ist

$$= n$$

d.h. Fr erzeugt $\text{Aut}_{F_p}(F_q)$. □

4 Galois-Erweiterungen

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

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

Beispiel 4.3.

Sei F ein endlicher Körper und K/F eine algebraische Körpererweiterung. Dann ist K/F eine Galois-Erweiterung.

Sei p eine positive Primzahl und $q = p^n$. $\mathbb{F}_q/\mathbb{F}_p$ ist eine Galois-Erweiterung. Die Galoisgruppe ist zyklisch der Ordnung n und wird vom Frobenius-Automorphismus erzeugt.

\mathbb{C}/\mathbb{R} ist eine Galois-Erweiterung. Die Galoisgruppe wird von der komplexen Konjugation erzeugt.

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

Beweis. Falls f keine Nullstellen in L hat so ist nichts zu zeigen. Sei $a \in L$ eine Nullstelle von f und $\varphi \in \text{Aut}_K(L)$. Dann gilt

$$f(\varphi(a)) = \varphi(\underbrace{f(a)}_{=0}) = 0$$

d.h. $\varphi(a)$ ist Nullstelle von f .

Weiterhin ist $f = cm_{a,K}$ für ein $c \in K$.

Sei nun b eine weitere Nullstelle von f in L . Dann ist b auch Nullstelle von $m_{a,K}$ und die Einbettung

$$K \hookrightarrow \bar{L}$$

lässt sich fortsetzen als

$$K(a) \xrightarrow{a} \bar{L}$$

mit $\sigma(a) = b$ bzw. einem K -Homomorphismus

$$L \xrightarrow{\sigma} \bar{L}$$

Da L/K normal ist gilt $\sigma(L) = L$.

Somit ist $\sigma \in \text{Aut}_K(L)$ mit $\sigma(a) = b$. □

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

$$|\text{Aut}_K(L)| = [L : K]_S = |\text{Hom}_K(L, \bar{K})|$$

Beweis. Sei \bar{L} ein algebraischer Abschluss von L . Dann ist \bar{L} auch ein algebraischer Abschluss von K .

Ist $\varphi : L \rightarrow \bar{L}$ ein K -Homomorphismus, so gilt $\varphi(L) = L$. Als ist die Abbildung

$$\text{Hom}_K(L, \bar{K}) \rightarrow \text{Aut}_K(L)$$

eine Bijektion. □

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

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

Beweis. Nach 4.5 gilt mit Separabilität

$$|\text{Aut}_K(L)| = [L : K]_S = [L : K]$$

□

Definition 4.7. Sei L ein Körper und G eine Untergruppe von $\text{Aut}_K(L)$. 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 ist der Fixkörper von $G(L/K)$ genau K .

Beweis. Sei $G = G(L/K)$. Dann ist $\subset L^G$.

Sei $a \in L/K$. Dann ist $\deg(m_{a,K}) \geq 2$. Da L/K normal ist, zerfällt $m_{a,K}$ über L in Linearfaktoren. Weil L/K separabel ist, ist a eine einfache Nullstelle von $m_{a,K}$. Es gibt also ein $b \in L$ mit $b \neq a$ mit $m_{a,K}(b) = 0$. Da $G(L/K)$ die Nullstellen von $m_{a,K}$ transitiv permutiert gibt es ein $\varphi \in G(L/K)$ mit $\varphi(a) = b$. \square

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

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

Beweis. Sei $a \in L$ und $Y_a = \{\varphi(a) \mid \varphi \in H\} \subset L$.

Seien a_1, \dots, a_n die verschiedenen Elemente von Y_a . Sei

$$f_a = \prod_{i=1}^n (X - a_i)$$

Dann ist für $\varphi \in H$

$$\varphi(f_a) = \prod_{i=1}^n (X - \varphi(a_i)) = f_a$$

Also ist $f_a \in L^H[X]$. Da a Nullstelle des Polynoms f_a ist ist a separabel.

Die Erweiterung L/L^H ist also separabel.

Dann ist L der Zerfällungskörper der Polynome $F = \{f_a \mid a \in L\}$. Somit ist L/L^H eine Galoiserweiterung.

Aus $m_{a,L^H} \mid f_a$ folgt

$$\deg(m_{a,L^H}) \leq \deg(f) \leq |H| \quad (\star)$$

Ist $|H| < [L : L^H] \leq \infty$, so gibt es eine endliche Teilmenge $S \subset L$, sodass für $M = L^H(S)$ gilt

$$\infty > [M : L^H] > |H|$$

Zusätzlich ist M/L^H separabel, da L/L^H separabel ist.

Nach Satz 3.68 gibt es ein $c \in L$, sodass $M = L^H(c)$ ist. Dann gilt

$$\deg(m_{c,L^H}) = [M : L^H] > |H|$$

Widerspruch zu (\star) .

Also ist $[L : L^H] \leq |H|$.

D.h. L/L^H ist eine endliche Galoiserweiterung.

Aus $H \subset \text{Aut}_{L^H}(L)$ folgt

$$|H| \leq |\text{Aut}_{L^H}(L)| = [L : L^H] \leq |H|$$

Somit gilt $H = \text{Aut}_{L^H}(L)$ \square

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*

$$\begin{array}{ll} \Phi : Z \rightarrow U & \Psi : U \rightarrow Z \\ M \mapsto G(L/M) & H \mapsto L^H \end{array}$$

zueinander 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

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

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

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

Beweis. Sei M ein Zwischenkörper von L/K . Dann ist L/M eine Galois-Erweiterung und $G(L/M) = \text{Aut}_M(L)$, sowie $c\text{Aut}_K(L) = G(L/K)$, weil $L \subset M$. Somit ist Φ wohldefiniert. Sei $M \in Z$, dann ist

$$\begin{aligned} M &= L^{G(L/M)} = L^{\Phi(M)} \\ &= \Psi(\Phi(M)) \end{aligned}$$

Somit ist $\Psi \circ \Phi = \text{id}_Z$.

Sei $H \in U$. Dann ist L/L^H eine Galois-Erweiterung mit Galoisgruppe H . Also ist

$$\begin{aligned} H &= G(L/L^H) = \Phi(L^H) \\ &= \Phi(\Psi(H)) \end{aligned}$$

d.h. $\Phi \circ \Psi = \text{id}_U$.

Somit sind Φ und Ψ zueinander inverse Bijektionen.

Sei M ein Zwischenkörper von L/K . Dann ist $M = L^H$ für ein $H \in U$. Ist die Erweiterung M/K normal, so ist die Abbildung

$$\begin{aligned} \varphi : G(L/K) &\rightarrow G(M/K) \\ \sigma &\mapsto \sigma_M \end{aligned}$$

ein surjektiver Gruppenhomomorphismus.

Sei \bar{L} ein algebraischer Abschluss von L . Dann ist \bar{L} auch ein algebraischer Abschluss von K und von M . Sei $\sigma \in G(L/K)$. Dann ist

$$M \xrightarrow{\sigma} \bar{L}$$

Da M normal ist gilt $\sigma(M) = M$ d.h. $\sigma|_M \in G(M/K)$.

Also ist φ wohldefiniert. Weiterhin gilt

$$(\sigma_1\sigma_2)|_M = \sigma_1|_M\sigma_2|_M$$

Sei $\sigma \in G(M/K)$. Dann lässt sich die Abbildung

$$M \xrightarrow{\sigma} \bar{L}$$

fortsetzen zu einem K -Homomorphismus

$$L \xrightarrow{\sigma} \bar{L}$$

weil L/M algebraisch ist. Da L/K normal ist folgt $\sigma(L) = L$. φ ist also surjektiv.

Es gilt $\text{Kern}(\varphi) = G(L/M)$, d.h. $G(L/M)$ ist eine normaler Untergruppe von $G(L/K)$.

Sei nun H eine normale Untergruppe von $G(L/K)$. Wir zeigen, dass die Erweiterung L/L^H normal ist:

Sei \bar{L} ein algebraischer Abschluss von L und $\sigma : L^H \rightarrow \bar{L}$ ein K -Homomorphismus. Dann gilt $\sigma(L^H) = L^H$. Da $K \subset L^H \subset L \subset \bar{L}$ können wir σ zu einem K -Homomorphismus $\sigma : L \rightarrow \bar{L}$ fortsetzen weil L/L^H algebraisch ist. Da L/K normal ist gilt $\sigma(L) = L$. Wir können σ also auffassen als K -Homomorphismus $\sigma : L^H \rightarrow L$.

Sei $b \in \sigma(L^H)$. Dann ist $b = \sigma(a)$ für ein $a \in L^H$.

Sei $\tau \in H$. Da $H\sigma = \sigma H$ ist gibt es $\tau' \in H$, sodass

$$\tau(b) = \tau(\sigma(a)) = \sigma(\underbrace{\tau'(a)}_{=a}) = \sigma(a) = b$$

d.h. $b \in L^H$ und $\sigma(L^H) \subset L^H$.

Zum Beweis der Gleichheit setzen wir den K -Homomorphismus

$$\underbrace{\sigma(L^H)}_{\subset L^H} \xrightarrow{\sigma^{-1}} L^H \rightarrow \bar{L}$$

zu einem K -Homomorphismus $\rho : L^H \rightarrow \bar{L}$ fort.

Diesen können wir wie oben als K -Homomorphismus $L^H \rightarrow L$ auffassen.

Dann ist $\rho(L^H) \subset L^H$ und

$$L^H \xrightarrow{\sigma} L^H \xrightarrow{\rho} L^H$$

ist die Identität auf L^H , d.h. $\rho\sigma = \text{id}_{L^H}$.

Analog konstruieren wir einen K -Homomorphismus $\eta : L^H \rightarrow L$ mit $\eta(L^H) \subset L^H$ und $\eta\rho = \text{id}_{L^H}$.

Es folgt

$$\sigma\rho = \text{id}_{L^H} \sigma\rho = \eta\rho\sigma\rho = \eta\rho = \text{id}_{L^H}$$

□

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, so dass 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

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

definiert einen Isomorphismus

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

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

Beweis. Sei a ein Primelement der Erweiterung L/K und seien a_1, \dots, a_n die Nullstelle von $m_{a,K}$ in L . Dann ist

$$L = K(a_1, \dots, a_n)$$

und damit

$$L \cdot M = M(L) = M(a_1, \dots, a_n)$$

d.h. $L \cdot M/M$ ist eine endliche Galois-Erweiterung.

Wohldefiniertheit Sei $\sigma \in G(L \cdot M/M)$ und $b \in L$. Dann zerfällt $m_{b,K}$ in L , also

$$m_{b,K} = \prod_{j=1}^n (X - \underbrace{b_j}_{\in L})$$

und

$$m_{b,K} = \sigma(m_{b,K}) = \prod_{j=1}^n (X - \underbrace{\sigma(b_j)}_{\in L})$$

Es folgt $\sigma(b) \in L$.

Injektivität Sei $\sigma \in G(L \cdot M/M)$ mit $\sigma|_L = \text{id}_L$. Aus $L \cdot M = M(L) = M(a_1, \dots, a_n)$ und $\sigma(a_i) = a_i$ folgt $\sigma = \text{id}$.

Sei H das Bild der Abbildung. Dann ist

$$L^H = L \cap (L \cdot M)^{G(L \cdot M/M)} = L \cap M$$

Die Erweiterung L/L^H ist eine endliche Galois-Erweiterung mit Galoisgruppe H . Aus der Injektivität der Abbildung folgt

$$G(L \cdot M/M) \cong H = H(L/L^H) = G(L/L \cap M)$$

□

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*

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

definiert einen injektiven Gruppenhomomorphismus.

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

Beweis. Sei $L_1 = K(a)$ und $L_2 = K(b)$. Seien a_1, \dots, a_n die Nullstellen von $m_{a,K}$ und b_1, \dots, b_n die Nullstellen von $m_{b,K}$. Dann ist

$$\begin{aligned} L_1 &= K(a_1, \dots, a_n) \\ L_2 &= K(b_1, \dots, b_n) \\ L_1 \cdot L_2 &= L_1(L_2) = L_2(L_1) \\ &= K(a_1, \dots, a_n, b_1, \dots, b_n) \end{aligned}$$

$L_1 \cdot L_2/K$ ist als eine endliche Galois-Erweiterung.

Wohldefiniertheit wie oben.

Injektivität Sei $\sigma \in G(L_1 \cdot L_2/K)$ mit $\sigma|_{L_1} = \text{id}_1$ und $\sigma|_{L_2} = \text{id}_2$.

Dann folgt, aus $L_1 \cdot L_2 = L_1(L_2)$, dass $\sigma = \text{id}_{L_1 \cdot L_2}$ ist.

Die Gruppen $G(L_1 \cdot L_2/L_1)$ und $G(L_1 \cdot L_2/L_2)$ sind Untergruppen von $G(L_1 \cdot L_2/K)$.

Sei nun $L_1 \cap L_2 = K$. Dann

$$G(L_1 \cdot L_2/L_1) \cap G(L_1 \cdot L_2/L_2) = \{1\}$$

Aus dem Transpositionssatz folgt dann

$$\begin{aligned} G(L_1 \cdot L_2/L_1) &\cong G(L_2/L_1 \cap L_2) = G(L_2/K) \\ G(L_1 \cdot L_2/L_2) &\cong G(L_1/L_1 \cap L_2) = G(L_1/K) \end{aligned}$$

Die Abbildung ist in diesem Fall also 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

$$L^H = K(a_0, \dots, a_1)$$

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 separables Polynom und L ein Zerfällungskörper von f über K . Dann ist L/K eine endliche Galois-Erweiterung und $G(L/K)$ wird in diesem Fall 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, \dots, a_n die Nullstellen von f in L . Dann definiert die Abbildung

$$\begin{aligned} G(L/K) &\rightarrow S(\{a_1, \dots, a_n\}) \\ \sigma &\mapsto \sigma|_{\{a_1, \dots, a_n\}} \end{aligned}$$

einen injektiven Gruppenhomomorphismus. Insbesondere gilt $|G(L/K)| \mid n!$.
 f ist genau dann irreduzibel über K wenn $G(L/K)$ transitiv auf den Nullstellen von f operiert.

Beweis. Sei $\sigma \in G(L/K)$. Da $\sigma(f) = f$ bildet σ Nullstellen von f in Nullstellen von f ab.

Da σ injektiv ist, ist die Einschränkung auf $\{a_1, \dots, a_n\}$ eine Bijektion.

Wegen $L = K(a_1, \dots, a_n)$ ist $\sigma \in G(L/K)$ eindeutig durch seine Operation auf $\{a_1, \dots, a_n\}$ festgelegt.

Somit ist f injektiv.

Wir haben bereits gesehen, dass $G(L/K)$ transitiv auf den Nullstellen von f operiert, wenn f irreduzibel ist.

Angenommen $G(L/K)$ permutiert die Nullstellen von f transitiv.

Sei a eine Nullstellen von f . Dann sind die Nullstellen von f gegeben durch $\sigma_1(a), \dots, \sigma_n(a)$ für geeignete $\sigma_i \in G(L/K)$ und

$$f = c \prod_{i=1}^n (X - \sigma_i(a))$$

Es ist $f = cm_{a,K}$, denn $\sigma_1(a), \dots, \sigma_n(a)$ sind auch Nullstellen von $m_{a,K}$. Somit ist f irreduzibel. \square

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

Beispiel 4.19. Sei K ein Körper mit $\text{char}(K) \neq 2$, $f \in K[X]$ ein irreduzibles, separables, normiertes Polynom vom Grad 3 und L ein Zerfällungskörper von f . Dann gilt

$$G(L/K) = \begin{cases} \mathbb{Z}/3\mathbb{Z} & , \text{ falls } \Delta f \text{ ein Quadrat in } K \text{ ist} \\ S_3 & , \text{ sonst} \end{cases}$$

Beweis. Sei a eine Nullstelle von f in L . Dann ist

$$[L : K] = [L : K(a)] \underbrace{[K(a) : K]}_{=3}$$

weil f irreduzibel und nach 4.18 muss $[L : K]$ teilt 6.

D.h. $[L : K] = 3$ oder $= 6$. Im ersten Fall ist $G(L/K)$ eine Untergruppe von S_3 mit Index 2. Also muss $G(L/K) \cong A_3 \cong \mathbb{Z}/3\mathbb{Z}$.

Seien a_1, a_2, a_3 die Nullstellen von f in L . Dann ist

$$\delta := (a_1 - a_2)(a_1 - a_3)(a_2 - a_3) \neq 0$$

Dann ist $\Delta(f) = \delta^2$.

Falls $G(L/K) = S_3$ ist, so gilt

$$\tau(\delta) = \text{sgn}(\tau)\delta$$

für alle $\tau \in G(L/K)$.

Ist $G(L/K) = A_3$, so gilt $\tau(\delta) = \delta$ für alle $\tau \in G(L/K)$.

Da $\text{char}(K) \neq 2$ folgt

$$G(L/K) = A_3 \Leftrightarrow \tau(\delta) = \delta \forall \tau \in G(L/K) \Leftrightarrow \delta \in K$$

□

Beispiel 4.20. Für $f = X^3 + aX + b$ ist

$$\Delta(f) = -4a^3 - 27b^2$$

Das Polynom $f = X^3 - x + 1 \in \mathbb{Q}[X]$ ist irreduzibel und hat Diskriminante

$$\Delta(f) = 4 - 27 = -23$$

somit gilt für den Zerfällungskörper L von \mathbb{Q} , dass $G(L/\mathbb{Q}) = S_3$.

Beispiel 4.21. Sei $f = X^4 - 2 \in \mathbb{Q}[X]$. Dann gilt

$$f = (X - a)(X + a)(X - ia)(X + ia)$$

mit $a = \sqrt[4]{2}$. Der Zerfällungskörper von f über \mathbb{Q} ist $L = \mathbb{Q}(a, i)$.

Das Eisenstein Kriterium zeigt, dass f irreduzibel über \mathbb{Q} ist. Somit ist $f = m_{a, \mathbb{Q}}$ und $[\mathbb{Q}(a), \mathbb{Q}] = 4$.

Weiterhin ist $[L : \mathbb{Q}(a)] = 2$, da $\mathbb{Q}(a)$ keine negativen Quadrate hat und damit nicht i enthält. Es folgt

$$[L : \mathbb{Q}] = 8$$

Wir bestimmen die Galoisgruppe von f . Da f 4 Nullstellen hat und die Galoisgruppe die Nullstellen permutiert muss $G(L/\mathbb{Q}) \subset S_4$ sein.

Jedoch muss zusätzlich für $\sigma \in G(L/K)$ gelte, dass

$$\sigma(-a) = -\sigma(a)$$

$$\sigma(-ia) = -\sigma(ia)$$

Es gibt 8 Permutationen in $S(\{a, -a, ia, -ia\})$ die die Bedingungen erfüllen.

Diese sind somit die Elemente in $G(L/\mathbb{Q})$.

Seien $\sigma, \tau \in G(L/\mathbb{Q})$ durch

$$\sigma(a) = ia$$

$$\sigma(ia) = -a$$

(d.h. $\sigma(i) = i$)

$$\tau(a) = -a$$

$$\tau(ia) = ia$$

(d.h. $\tau(i) = -i$)

Die von σ erzeugte Untergruppe $\langle \sigma \rangle$ hat Ordnung 4 und ist somit normal in $G(L/\mathbb{Q})$.

Weil $\tau \notin \langle \sigma \rangle$ gilt

$$\begin{aligned} G(L/\mathbb{Q}) &= \langle \sigma \rangle \cup \langle \sigma \rangle \tau \\ &= \langle \sigma \rangle \cup \tau \langle \sigma \rangle \\ &= \{1, \sigma, \sigma^2 \sigma^3, \tau, \tau \sigma, \tau \sigma^2, \tau \sigma^3\} \end{aligned}$$

τ und σ genügen der Relation $\tau \sigma = \sigma^3 \tau$.

Für Untergruppen von $G(L/\mathbb{Q})$ erhält man folgendes Schema 2

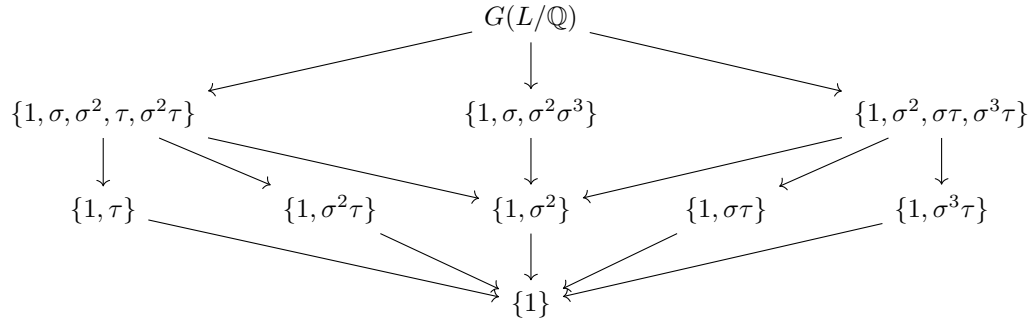


Abbildung 2: Untergruppen

Definition 4.22. Sei $L = K(X_1, \dots, X_n)$ der Quotientenkörper von $K[X_1, \dots, X_n]$. Die Element von L sind die rationalen Funktionen f/g mit $f, g \in K[X_1, \dots, X_n]$ und $g \neq 0$.

S_n operiert durch Permutationen der X_i auf L .

$M = L^{S_n}$ wird als Körper der **symmetrischen rationalen Funktionen** bezeichnet. Die Erweiterung L/M ist eine endliche Galois-Erweiterung mit Galoisgruppe S_n .

Beweis. Es gilt $M = K(s_1, \dots, s_n)$:

Die Inklusionen $K(s_1, \dots, s_n) \subset M \subset L$ impliziert

$$L : K(s_1, \dots, s_n) = \underbrace{[L : M][M : K(s_1, \dots, s_n)]}_{=n!}$$

Das Polynom

$$f = \prod_{i=1}^n (X - X_i) \in K(s_1, \dots, s_n)[X] \subset L[X]$$

ist separabel und hat L als Zerfällungskörper. Also ist

$$[L : K(s_1, \dots, s_n)] \leq n!$$

Es folgt die Behauptung. □

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

Beweis. Sei $n = |G|$. Für $a \in G$ definiere

$$\begin{aligned}\tau_a : G &\rightarrow G \\ g &\mapsto ag\end{aligned}$$

Dann ist τ_a eine Permutation von G . Weiterhin ist

$$\tau_a \tau_b = \tau_{ab}$$

Wir haben also eine Injektion

$$G \rightarrow S_n$$

Wir können G also mit einer Untergruppe von S_n identifizieren.

Dann operiert G auf $L = K(X_1, \dots, X_n)$ durch Permutation der X_i .

Sei $M = L^G$ dann ist L/M eine Galoiserweiterung mit Galoisgruppe G . \square

4.2 Kreisteilungspolynome

In diesem Abschnitt sei K ein Körper und \bar{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 \bar{K} bezeichnet.

Proposition 4.25. Die n -ten Einheitswurzeln bilden eine Untergruppe U_n von \bar{K}^* .

Ist $\text{char}(K) = 0$ oder $\text{char}(K) \nmid n$, 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 $p \mid n$, 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 $\text{char}(K) \nmid n$, 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 $\text{char}(K) \nmid mn$.

Dann ist die Abbildung

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

ein Isomorphismus von Gruppen.

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

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

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

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

Beweis. Die Aussage folgt aus dem Chinesischen Restsatz:
Der Ring-Isomorphismus

$$\begin{aligned} \mathbb{Z}/mn\mathbb{Z} &\rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ (x \bmod mn) &\mapsto (x \bmod m, x \bmod n) \end{aligned}$$

liefert einen Isomorphismus

$$(\mathbb{Z}/mn\mathbb{Z})^* \rightarrow (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^* = (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$$

Daraus folgt die Multiplikativ der φ Funktion. \square

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 $\text{char}(K) \nmid n$. 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 $\text{char}(K) \nmid n$ 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

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

Beweis. Jedes $\sigma \in G(\mathbb{Q}(\xi)/\mathbb{Q})$ bildet U_n nach U_n (Menge der n -ten Einheitswurzeln).

Insbesondere ist $\sigma(\xi)$ wieder eine primitive n -te Einheitswurzel.

Sei $f = m_{\xi, \mathbb{Q}}$. Da f irreduzibel über \mathbb{Q} ist operiert $G(\mathbb{Q}(\xi)/\mathbb{Q})$ transitiv auf den Nullstellen von f , d.h. jede Nullstelle von f ist eine primitive n -te Einheitswurzel.

Also gilt

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

Wir zeigen jetzt, dass jede primitive n -te Einheitswurzel Nullstelle von f ist.
Da ξ Nullstelle von $X^n - 1$ ist gilt

$$X^n - 1 = fg$$

für ein normiertes $g \in \mathbb{Q}[X]$.

Sei p Primzahl. Wir betrachten die p -adische Bewertung. Da $X^n - 1$ nicht von p geteilt wird ist

$$\begin{aligned} 0 &= \nu_p(fg) \\ 0 &= \underbrace{\nu_p(f)}_{\geq 0} + \underbrace{\nu_p(g)}_{\geq 0} \end{aligned}$$

Dann muss aber $\nu_p(f) = \nu_p(g) = 0$ für alle Primzahlen p gelten.
Somit ist $f, g \in \mathbb{Z}[X]$.

Sei nun p eine Primzahl mit $p \nmid n$. Dann ist ξ^p eine primitive n -te Einheitswurzel.

Angenommen $f(\xi^p) \neq 0$, dann muss $g(\xi^p) = 0$ (da ξ Nullstelle von fg).

D.h. ξ ist Nullstelle von X^p , dann $f|g(X^p)$. Sei $g(X^p) = fh$, dann ist h ein normiertes Polynom in $\mathbb{Z}[X]$.

Reduzieren der Koeffizienten mod p

$$\mathbb{Z}[X] \rightarrow (\mathbb{Z}/p\mathbb{Z})[X]$$

Dann geht

$$g = \sum_{j=0}^m a_j X^j$$

über in

$$\bar{g} = \sum_{j=0}^m \bar{a}_j X^j$$

In \mathbb{F}_p gilt $a^p = a$, sodass

$$\begin{aligned} \bar{g}^p &= \left(\sum_{j=0}^m \bar{a}_j X^j \right)^p \\ &= \sum_{j=0}^m \bar{a}_j^p X^{jp} \\ &= \sum_{j=0}^m \bar{a}_j X^{jp} \\ &= \bar{g}(X^p) \\ &= \overline{fh} \end{aligned}$$

Aus $\bar{g}^p = \overline{fh}$ folgt, dass \bar{f} und \bar{g} nicht teilerfremd sind in \mathbb{F}_p . Somit hat $X^n - 1 = \bar{f}\bar{g}$ mehrfache Nullstellen in \mathbb{F}_p . Dies widerspricht $p \nmid n$!

Also muss ξ^p eine Nullstelle von f .

Sei nun η eine beliebige primitive n -te Einheitswurzel. Dann ist $\eta = \xi^m$ mit $(m, n) = 1$. Sei $m = p_1 \cdot \dots \cdot p_k$ die Zerlegung von m in Primfaktoren, sodass

$$\eta = \xi^m = (\dots(\xi^{p_1})^{p_2} \dots)^{p_k}$$

Also ist ξ^{p_1} eine Nullstelle in f . f ist auch das Minimalpolynom von ξ^{p_1} . Analog zeigt man, dass $(\xi^{p_1})^{p_2}$ eine Nullstelle von f ist. Es folgt schließlich, dass η eine Nullstelle von f ist.

Dann folgt

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

□

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

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

Beweis. Es ist $\xi_{mn} = \xi_n \xi_m$ auch primitive Einheitswurzel. Es folgt

$$\mathbb{Q}(\xi_{mn}) = \mathbb{Q}(\xi_m, \xi_n)$$

und

$$\underbrace{[\mathbb{Q}(\xi_{mn}) : \mathbb{Q}]}_{=\varphi(mn)} = [\mathbb{Q}(\xi_{mn} : \mathbb{Q}(\xi_m))] \underbrace{[\mathbb{Q}(\xi_m) : \mathbb{Q}]}_{=m}$$

sodass

$$[\mathbb{Q}(\xi_{mn}) : \mathbb{Q}(\xi_m)] = \varphi(m)$$

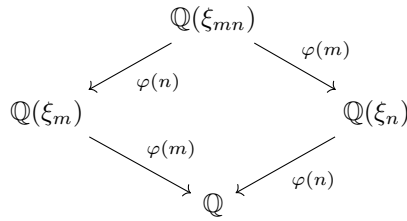


Abbildung 3: Körperdiagramm mit Erweiterungsgrad

Sei $L = \mathbb{Q}(\xi_m) \cap \mathbb{Q}(\xi_n)$. Es ist

$$\begin{aligned} \deg(m_{\xi_m, \mathbb{Q}(\xi_n)}) &= \varphi(m) \\ \deg(m_{\xi_m, L}) &\geq \varphi(m) \end{aligned}$$

und

$$\begin{aligned} \mathbb{Q} &\subset L \subset \mathbb{Q}(\xi_m) \\ \mathbb{Q}(\xi_m) &\subset L(\xi_m) \subset \mathbb{Q}(\xi_m) \end{aligned}$$

d.h.

$$L(\xi_m) = \mathbb{Q}(\xi_m)$$

Damit folgt

$$\underbrace{[L(\xi_m) : \mathbb{Q}]}_{=\varphi(n)} = \underbrace{[L(\xi_m) : L]}_{\geq \varphi(m)} [L : \mathbb{Q}]$$

Also muss $[L : \mathbb{Q}] = 1$, also $L = \mathbb{Q}$. □

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

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

ist ein injektiver Gruppenhomomorphismus.

Beweis.

Sei $\sigma \in G(K(\xi)/K)$. Dann ist $\sigma(U_n) = U_n$. Also $\sigma(\xi) = \xi^{r(\sigma)}$ für eine positive ganze Zahl $r(\sigma)$.

Da ξ primitive n -te Einheitswurzel ist, ist $r(\sigma)$ eindeutig modulo n und $(n, r(\sigma)) = 1$.

Es gilt

$$\sigma(\xi^s) = \sigma(\xi)^s = (\xi^{r(\sigma)})^s = (\xi^s)^{r(\sigma)}$$

sodass $r(\sigma)$ nicht von der Wahl von ξ abhängt. Die Abbildung

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

ist ein Gruppenhomomorphismus, denn für $\sigma, \tau \in G(K(\xi)/K)$

$$\begin{aligned} (\sigma\tau)(\xi) &= \sigma(\tau(\xi)) \\ &= \sigma(\xi^{r(\tau)}) \\ &= (\xi^{r(\tau)})^{r(\sigma)} \\ &= \xi^{r(\tau)r(\sigma)} \end{aligned}$$

sodass

$$\begin{aligned} \Psi(\sigma\tau) &= \overline{r(\sigma\tau)} \\ &= \overline{r(\sigma)r(\tau)} \\ &= \overline{r(\sigma)}\overline{r(\tau)} \\ &= \Psi(\sigma)\Psi(\tau) \end{aligned}$$

Aus $\overline{r(\sigma)} = 1$ folgt, dass $\sigma(\xi) = \xi$, also ist σ die Identität auf $K(\xi)$. \square

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 $G(K/\mathbb{Q}) \cong G$.

Beweis. G zerfällt in zyklische Gruppen, d.h.

$$G = \bigoplus_{i=1}^n \mathbb{Z}/p_i^{l_i}$$

mit p_i prim.

Nach 4.40 gilt $\{1 + m_i p_i^{l_i}\}$ enthält unendlich viele Primzahlen, d.h. wir können teilerfremde Primzahlen q_i wählen, mit

$$q_i \equiv 1 \pmod{p_i^{l_i}}$$

Schreibe $q_i = 1 - m_i p_i^{l_i}$. Sei $q = \prod_{i=1}^n q_i$, $\xi \in \overline{\mathbb{Q}}$ eine primitive q -te Einheitswurzel und wähle $K = \mathbb{Q}(\xi)$. Dann ist

$$\begin{aligned} G(K/\mathbb{Q}) &\cong (\mathbb{Z}/q\mathbb{Z})^* \\ &= \bigoplus_{i=1}^n (\mathbb{Z}/q_i\mathbb{Z})^* \\ &= \bigoplus_{i=1}^n \mathbb{Z}/m_i p_i^{l_i} \mathbb{Z} \end{aligned}$$

Wähle nun

$$H_i = p_i^{l_i} \mathbb{Z}/m_i p_i^{l_i} \mathbb{Z}$$

dann ist H_i eine Untergruppe von $\mathbb{Z}/m_i p_i^{l_i} \mathbb{Z}$ mit

$$\frac{\mathbb{Z}/m_i p_i^{l_i} \mathbb{Z}}{H_i} = \mathbb{Z}/p_i^{l_i} \mathbb{Z}$$

Definiere nun $H = \bigoplus_{i=1}^n H_i$. Dann ist

$$G(K/\mathbb{Q})/H \cong G$$

d.h. K^H/\mathbb{Q} ist eine Galoiserweiterung mit Galoisgruppe

$$G(K^H/\mathbb{Q}) = \frac{G(K/\mathbb{Q})}{G(K/K^H)} = \frac{G(K/\mathbb{Q})}{H} = G$$

\square

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 $\text{char}(K) \nmid n$. Seien ξ_1, \dots, ξ_m mit $m = \varphi(n)$ die primitiven n -ten Einheitswurzeln in \overline{K} . Dann heit

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

das n -te **Kreisteilungspolynom** ber K .

Im Fall $K = \mathbb{Q}$ schreiben wir Φ_n fr $\Phi_{n,K}$.

Satz 4.44. a) $\Phi_{n,K}$ ist ein normiertes separables Polynom ber K vom Grad $\phi(n)$

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

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

Beweis. a) Sei $L = K(\xi_i)$. Dann ist L/K eine Galoiserweiterung un $L^{G(L/K)} = K$. Sei $\sigma \in G(L/K)$.

Dann permutiert σ die Primitiven Einheitswurzeln, d.h. $\Phi_{n,K} = \Phi_{n,K}$. Somit liegen die Koeffizienten von $\Phi_{n,K}$ in K .

b) Sei $\xi \in \overline{\mathbb{Q}}$ primitive n -te Einheitswurzel. Dann hat $m_{\xi,\mathbb{Q}}$ Grad $\varphi(n)$. Da $\Phi_n(\xi) = 0$ ist und Φ_n Grad $\varphi(n)$ hat ist $\Phi_n = m_{\xi,\mathbb{Q}}$.

Somit ist Φ_n irreduzibel ber \mathbb{Q} . Aus $\Phi_n | (X^n - 1)$ und der Normiertheit von Φ_n folgt $\Phi_n \in \mathbb{Z}[X]$.

c) Es ist

$$\begin{aligned} X^n - 1 &= \prod_{\xi \in U_n} (X - \xi) = \prod_{d|n} \prod_{\xi \in P_d} (X - \xi) \\ &= \prod_{d|n} \Phi_{d,K} \end{aligned}$$

wobei P_d die Menge der d -ten Einheitswurzeln in U_n ist. □

Satz 4.45. *Sei $n \in \mathbb{Z}$, $n > 0$ und p prim mit $p \nmid n$. Sei e die Ordnung von p in $(\mathbb{Z}/n\mathbb{Z})^*$. Dann zerfllt Φ_{n,\mathbb{F}_p} in $\varphi(n)/e$ verschiedene Faktoren vom Grad e ber \mathbb{F}_p .*

Beweis. Sei f ein irreduzibler normierter Faktor von Φ_{n,\mathbb{F}_p} . Dann ist f das Minimalpolynom einer primitiven n -te Einheitswurzel $\xi \in \overline{\mathbb{F}_p}$ ber \mathbb{F}_p . Sei $K = \mathbb{F}_p(\xi)$ und $m = [K : \mathbb{F}_p]$. Dann ist $m = \deg(f)$.

Wir zeigen $m = e$:

ξ hat Ordnung n in U_n , K^* ist zyklisch der Ordnung P^{m-1} . Es folgt

$$\begin{aligned} n | P^m - 1 \\ P^m &\equiv 1 \pmod{n} \\ e | m \\ e &\leq m \end{aligned}$$

Andererseits folgt aus $p^e \equiv 1 \pmod n$, dass

$$\xi^{p^e} = \xi^1 = \xi$$

so dass die Abbildung

$$\begin{aligned} k &\rightarrow K \\ x &\mapsto x^{p^e} \end{aligned}$$

trivial auf K ist, da das Polynom $X^{p^e} - X$ höchstens p^e Nullstellen hat, ist

$$\begin{aligned} |K| &\leq p^e \\ p^m &\leq p^e \\ m &\leq e \end{aligned}$$

Es folgt $m = e$. □

Beispiel 4.46. Sei p eine ungerade Primzahl und $\xi \in \overline{\mathbb{F}_p}$ eine primitive 8-te Einheitswurzel. Dann ist

$$G(\mathbb{F}_p(\xi)/\mathbb{F}_p) \hookrightarrow (\mathbb{Z}/8\mathbb{Z})^*$$

$$= \{1, 3, 5, 7\} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Somit ist

$$G(\mathbb{F}_p(\xi)/\mathbb{F}_p) = \begin{cases} 1 & , \text{ falls } p \equiv 1 \pmod 8 \\ \mathbb{Z}/2\mathbb{Z}, & \text{ sonst} \end{cases}$$

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

$$R \times M \rightarrow M$$

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

$$f : M \rightarrow M'$$

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 $x, y \in M$.

Beispiel 5.3. a) Sei G eine abelsche Gruppe. Dann ist G ein \mathbb{Z} -Modul unter

$$ng = \begin{cases} \underbrace{g + \dots + g}_{n \text{ Summanden}} & n > 0 \\ 0 & n = 0 \\ \underbrace{(-g) + \dots + (-g)}_{n \text{ Summanden}} & n < 0 \end{cases}$$

- b) Jeder \mathbb{Z} -Modul ist eine abelsche Gruppe (indem man die Modul-Struktur vergisst)
- c) Zwei \mathbb{Z} -Moduln sind genau dann isomorph, wenn sie als abelsche Gruppen isomorph sind.
- d) Sei R ein Ring und M ein R -Modul und $f : M \rightarrow M$ ein Modulhomomorphismus. Dann ist M ein $R[X]$ -Modul unter

$$\begin{aligned} R[X] \times M &\rightarrow M \\ (a_i X^i, v) &\mapsto \sum a_i f^i(v) \end{aligned}$$

- e) Für zwei R -Moduln M und M' ist die Menge der R -linearen Abbildungen unter

$$(af)(v) = af(v)$$

ein R -Modul

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

Beispiel 5.5. Sei M ein R -Modul und $(M_i)_{i \in I}$ eine Familie von Untermoduln. Dann sind

$$\bigcap_{i \in I} M_i \quad \text{und} \quad \sum_{i \in I} M_i = \left\{ \sum_{i \in I} x_i \mid x_i \in M_i, \text{ fast alle } x_i = 0 \right\}$$

Untermoduln von M .

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 $\pi : M \rightarrow M/N$, $x \mapsto x + N$ ist ein Modulhomomorphismus.

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

$$\begin{array}{ccc} M & \xrightarrow{f} & M' \\ \downarrow & \nearrow \bar{f} & \\ M/N & & \end{array}$$

Satz 5.8. Sei M ein R -Modul und N ein Untermodul. Dann induziert die Projektion $\pi : M \rightarrow M/N$ 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

$$m = \sum_{i \in I} R x_i$$

ist.

Besitzt M ein endliches Erzeugendensystem, so heißt M **endliche erzeugt** oder **endlicher 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, \dots, v_m) und (w_1, \dots, 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

$$\dots \rightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \rightarrow \dots$$

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

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

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

Exaktheit bedeutet hierbei, dass f injektiv, g surjektiv und $\text{Im}(f) = \text{Kern}(g)$.

Beispiel 5.16. Sei M ein R -Modul und $N \subset M$ ein Untermodul. Dann ist

$$0 \rightarrow N \hookrightarrow M \rightarrow M/N \rightarrow 0$$

eine kurze exakte Sequenz.

Definition 5.17. Sei

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

eine kurze exakte Sequenz von R -Moduln.

Die Sequenz spaltet, wenn es einen Untermodul $N \subset M$ mit $M = N \oplus \text{Kern}(g)$ gibt.

Satz 5.18. Sei

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

eine kurze exakte Sequenz von R -Moduln.

Dann sind äquivalent:

- a) Die Sequenz spaltet (Es gibt einen Untermodul $N \subset M$ mit $M = N \oplus \text{Kern}(g)$)
- b) Es gibt eine R -lineare Abbildung $s : M'' \rightarrow M$ mit $g \circ s = \text{id}_{M''}$
- c) Es gibt eine R -lineare Abbildung $t : M \rightarrow M'$ mit $t \circ f = \text{id}_{M'}$

Beweis. 1) \Rightarrow 2) $g|_N$ ist injektiv und $g(N') = g(M) + g(\text{Kern } g) = M''$ sodass $g : N \rightarrow M''$ einen Isomorphismus liefert.

Wir erhalte die Abbildung $M'' \xrightarrow{g^{-1}} N \hookrightarrow M$.

Sei s die Komposition dieser Abbildungen, dann ist $g \circ s = \text{id}_{M''}$.

1) \Rightarrow 3) Es ist $M = \text{Kern}(g) \oplus N' = f(M') \oplus N'$ und $f : M' \rightarrow M$ ist injektiv, also ist $M' \cong f(M')$, sodass wir die Abbildung $M \rightarrow f(M') \xrightarrow{f^{-1}} M'$ erhalten.

Die Komposition erfüllt $f \circ f = \text{id}_{M'}$.

2) \Rightarrow 1) Setze $N' = s(M'')$ und sei $x \in M$. Dann ist

$$x = \underbrace{x - s(g(x))}_{\in \text{Kern}(g)} + \underbrace{s(g(x))}_{\in N'}$$

denn

$$g(x - s(g(x))) = g(x) - gs(g(x)) = g(x) - \text{id } g(x) = 0$$

Sei nun $y \in M''$ und $s(y) \in \text{Kern}(g)$, dann ist $y = g(s(y)) = 0$.

3) \Rightarrow 1)

□

Satz 5.19. Sei $0 \rightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow 0$ eine kurze exakte Sequenz von R -Moduln.

Ist M'' frei, so spaltet die Sequenz $M \cong M' \oplus M''$.

Beweis. Sei (v_i) eine R -Basis von M'' , $x_i \in M$ mit $g(x_i) = v_i$ für alle $i \in I$ und $s : M'' \rightarrow M$ definiert durch $s(v_i) = x_i$.

Dann gilt $g \circ s = \text{id}_M$, d.h. die Folge spaltet.

Außerdem gilt

$$\begin{aligned} N &\cong \text{Kern}(g) \oplus s(M'') \\ &\cong \text{Im}(f) \oplus M'' \\ &\cong M' \oplus M'' \end{aligned}$$

□

Korollar 5.20. Sei

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

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

Beweis. Da M'' frei ist gilt $M \cong M' \oplus M''$.

□

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 $R^n \rightarrow M$.

Beispiel 5.22. Sei K ein Körper und $R = K[X_1, X_2, \dots]$ der Polynomring über K in abzählbar vielen Variablen und sei

$$I = \{f \in R \mid \text{Konstanter Term } a_0 = 0\}$$

Dann ist I ein Ideal in R , d.h. I ist ein R -Untermodul von R .

Dann ist zwar R endlich erzeugbar ($R^1 \rightarrow R$) aber I ist nicht endlich erzeugt als R -Modul.

Satz 5.23. *Sei*

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

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 .*

Beweis. a) Ist (v_1, \dots, v_n) ein Erzeugendensystem von M , so ist $(g(v_1), \dots, g(v_n))$ ein Erzeugendensystem von M'' .

- b) Sei (v_1, \dots, v_N) ein Erzeugendensystem von M' und (x_1, \dots, x_m) ein Erzeugendensystem von M'' . Setze

$$s_i = f(v_i) \quad w_i = g(t_i)$$

Dann ist $(s_1, \dots, s_n, t_1, \dots, t_m)$ ein Erzeugendensystem von M , denn:

Sei $x \in M$. Dann gilt

$$g(x) = \sum_{i=1}^n a_i w_i = \sum_{i=1}^n a_i g(t_i)$$

Dann folgt, dass insbesondere

$$g\left(x - \sum_{i=1}^n a_i t_i\right) = 0$$

also ist

$$x - \sum_{i=1}^n a_i t_i \in \text{Kern}(g) = \text{Im}(f)$$

$$x - \sum_{i=1}^n a_i t_i = \sum_{j=1}^m b_j s_j$$

Sodass abschließend gilt

$$x = \sum_{j=1}^m b_j s_j + \sum_{i=1}^n a_i t_i$$

□

Satz 5.24. *Seien M_1, \dots, 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.

Beweis. „ \Leftarrow “ Klar: Endliche Menge von endlichen Erzeugendensystemen.

„ \Rightarrow “ Setze $M' = \bigoplus_{i \neq j} M_i$. Dann ist für jedes j

$$0 \rightarrow M' \rightarrow M \rightarrow M_j \rightarrow 0$$

eine exakte Sequenz.

Dann ist M_j endlich nach ??.

□

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

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

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

Beweis. „ \Rightarrow “ Sei M noethersch. Dann ist M' noethersch weil Untermoduln von M' isomorph unter f zu einem Untermodul von M ist.

Jeder Untermodul von M'' ist das homomorphe Bild eines Untermoduls von M unter g und somit endlich erzeugbar.

„ \Leftarrow “ Sei nun M' und M'' noethersch. Sei N ein Untermodul von M . Dann ist

$$0 \rightarrow f^{-1}N \xrightarrow{f} N \xrightarrow{g} g(N) \rightarrow 0$$

exakte Sequenz. Da $f^{-1}(N)$ und $g(N)$ endlich erzeugt sind ist auch N endlich erzeugt.

□

Satz 5.28. Seien M_1, \dots, 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.

Beweis. „ \Leftarrow “ Durch Induktion über n .

Für $n = 1$ ist $M = M_1$.

Sei $n > 1$. Definiere $M' = \bigoplus_{i=1}^{n-1} M_i$. Dann definiert

$$0 \rightarrow M' \rightarrow M \rightarrow M_n \rightarrow 0$$

eine kurze exakte Sequenz bei der M' und M_n noethersch sind.

Somit ist M noethersch.

„ \Rightarrow “ Sei $M' = \bigoplus_{i \neq j}$. Dann ist für jedes j

$$0 \rightarrow M' \rightarrow M \rightarrow M_j \rightarrow 0$$

eine kurze exakte Sequenz. Da M noethersch ist auch M_j noethersch. \square

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

Beweis. Es gibt einen subjektiven Homomorphismus $g : R^n \rightarrow M$ und eine exakte Sequenz

$$0 \rightarrow \text{Kern}(g) \rightarrow R^n \xrightarrow{g} M \rightarrow 0$$

Somit ist M noethersch. \square

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 in einem Unterring $C \subset B$ enthalten, sodass C ein endlich erzeugter A -Modul ist.

Beweis. „1) \Rightarrow 2)“ Ist $x \in B$ ganz, so gibt es ein normiertes $f \in A[X]$ mit $f(x) = 0$, d.h.

$$x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$$

für geeignete $a_i \in A$.

Es folgt, dass

$$x^n = -a_{n-1}x^{n-1} - \dots - a_0$$

D.h. $A[x]$ wird von $1, x, x^2, \dots, x^{n-1}$ als A -Modul erzeugt.

„2) \Rightarrow 3)“ Wähle $C = A[x]$.

„3) \Rightarrow 1)“ Sei $C = \sum_{i=1}^n A c_i$.

Weil $A[x] \subset C$ gilt $x c_i \in C$.

Es gibt also $\gamma_{ij} \in A$ mit

$$x c_i = \sum_{j=1}^n \gamma_{ij} c_j$$

Wir können diese Gleichung schreiben als

$$\begin{aligned}\sum_{j=1}^n (xc_j\delta_{ij} - \gamma_{ij}c_j) &= 0 \\ \sum_{j=1}^n \underbrace{(x\delta_{ij} - \gamma_{ij})}_{:=m_{ij}} c_j &= 0 \\ Mu &= 0\end{aligned}$$

Definiere nun $M = (m_{ij})$ und $u = (c_1, \dots, c_n)^T$. Sei M^{ad} die zu M adjungierte Matrix. Dann ist

$$M^{ad}Mu = \det(M)u$$

Es folgt

$$\det(M)c_i = 0$$

und damit

$$\det(M)c = 0$$

für alle $c \in C$. Da $1 \in C$ ist $\det(M) = 0$.

Da $\det(M)$ ein normiertes Polynom in X mit Koeffizienten in A ist, ist X ganz.

□

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

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

Beweis. a) Durch Induktion über n . Im Fall $n = 1$ gilt ??.

Sei $n > 1$. Nach Induktionsvoraussetzung ist $A[x_1, \dots, x_{n-1}]$ ein endlich erzeugter A -Modul.

x_n ist ganz über A , somit ist x_n auch ganz über $A[x_1, \dots, x_{n-1}]$. Somit ist $A[x_1, \dots, x_{n-1}][x_n]$ ein endlich erzeugter $A[x_1, \dots, x_{n-1}]$ -Modul.

$$A[x_1, \dots, x_{n-1}] = \sum_{i=1}^k Af_i$$

mit $f_i \in A[x_1, \dots, x_{n-1}]$

$$A[x_1, \dots, x_n] = \sum_{j=1}^l A[x_1, \dots, x_{n-1}]g_j$$

mit $g_j \in A[x_1, \dots, x_n]$

$$= \sum_{j=1}^l \sum_{i=1}^k Af_i g_j$$

Dann ist auch $A[x_1, \dots, x_n]$ ein endlich erzeugter A -Modul.

- b) $B[y]$ ist ein endlich erzeugter B -Modul. Da B ein endlich erzeugter A -Modul ist gilt $A[y] \subset B[y]$ und dann mit ??, dass y ganz über A ist. \square

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 .

Beweis. Sind $x, y \in B$ ganz über A , so ist $A[x, y]$ ein endlich erzeugter A -Modul. Dieser enthält $x - y$, $x + y$ und xy . Somit sind diese Elemente ganz über $A[x, y]$ und somit auch über A . \square

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 C ganz über A .

Beweis. Sei $c \in C$. Dann ist

$$x^n + b_{n-1}c^{n-1} + \dots + b_0 = 0$$

für geeignete $b_i \in B$.

Sei $R = A[b_0, \dots, b_{n-1}]$. Dann ist $R[c]$ ein endlich erzeugter R -Modul

Da die b_i ganz sind ist R ein endlich erzeugter A -Modul. Somit ist R ein endlich erzeugter A -Modul.

Es folgt, dass \overline{A} ganz abgeschlossen ist (also $x \in B$ ist ganz über \overline{A} und \overline{A} ist ganz über A . Also ist x ganz über A). \square

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.

Beweis. Sei K der Quotientenkörper von A .

Sei $\frac{a}{b} \in K$ mit $a, b \in A, (a, b) = 1$ und ganz über A . Dann ist

$$\left(\frac{a}{b}\right)^n + c_{n-1}\left(\frac{a}{b}\right)^{n-1} + \dots + c_0 = 0$$

für geeignete $c_i \in A$. Multiplikation mit b^n liefert

$$a^n + c_{n-1}a^{n-1}b + \dots + c_0b^n = 0$$

d.h. $b|a^n$.

Somit muss b eine Einheit sein, also $\frac{a}{b} \in A$. \square

Satz 6.10. Sei A ein Integritätsbereich mit Quotientenkörper K und sei A ganz abgeschlossen in K . Sei L/K eine algebraische Körpererweiterung.

Dann ist $\alpha \in L$ genau dann ganz über A , wenn $m_{\alpha, K} \in A[X]$ liegt.

Beweis. „ \Leftarrow “ Klar weil $m_{\alpha,K}$ normiert ist.

„ \Rightarrow “ Sei $\alpha \in L$ ganz über A . Es gibt als eine normiertes Polynom $f \in A[X]$ mit $f(\alpha) = 0$.

In $K[X]$ gilt $m_{\alpha,K} | f$

Über einem geeigneten algebraisch Abschluss \bar{L} von L zerfällt $m_{\alpha,K}$ d.h.

$$m_{\alpha,K} = \prod_{i=1}^n (X - \alpha_i)$$

Aus $m_{\alpha,K} | f$ folgt, dass $f(\alpha_i) = 0$ für alle α_i .

Somit ist jedes α_i ganz über A .

Dann sind auch die Koeffizienten von $m_{\alpha,K}$ ganz über A .

Da A ganz abgeschlossen in K ist gilt $m_{\alpha,K} \in A[X]$.

□

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.

Beispiel 6.15. Sei $d \in \mathbb{Z}$, $n \neq 1$ und quadratfrei.

Wähle $K = \mathbb{Q}(\sqrt{d})$ und

$$\omega_d = \begin{cases} \sqrt{d} & , \text{ falls } d \equiv 2, 3 \pmod{4} \\ \frac{1}{2}(1 + \sqrt{d}) & , \text{ falls } d \equiv 1 \pmod{4} \end{cases}$$

Dann ist

$$O_K = \mathbb{Z} + \mathbb{Z}\omega_d$$

Betrachte nun $\mathbb{Q}(\sqrt{-5})$. Dann ist in O_K

$$21 = 3 \cdot 7 = (1 - 2\sqrt{-5})(1 + 2\sqrt{-5})$$

D.h. man erhält Faktorisierungen in Primfaktoren von 21, die nicht zueinander assoziiert sind.

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

$$I = P_1 \dots P_n$$

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

Beweis. Sind b_1, \dots, b_n algebraisch unabhängig über K so kann man $x_1, \dots, x_r \in B$ finden, die algebraisch unabhängig sind.

Angenommen b_1, \dots, b_n sind algebraisch abhängig über K . Dann existiert eine Relation

$$\sum_{(\nu_1, \dots, \nu_n) \in I} a_{\nu_1, \dots, \nu_n} b_1^{\nu_1} \dots b_n^{\nu_n} = 0 \quad (\text{Gl. 6.1})$$

mit $a_{\nu_1, \dots, \nu_n} \in K \setminus \{0\}$ und endlichem I .

Sei

$$\begin{aligned} x_1 &= b_1 - b_n^{s_1} \\ &\vdots \\ x_{n-1} &= b_{n-1} - b_n^{s_{n-1}} \end{aligned}$$

mit $s_1, \dots, s_{n-1} \in \mathbb{N} \setminus \{0\}$. Dann ist

$$\begin{aligned} B &= K[b_1, \dots, b_n] \\ &= K[x_1, \dots, x_{n-1}, b_n] \\ &= K[x_1, \dots, x_{n-1}][b_n] \end{aligned}$$

Setzt man $b_i = x_i + b_n^{s_i}$ in Gl. 6.1 und spaltet

$$b_i^{\nu_i} = (x_i + b_n^{s_i})^{\nu_i} = b_n^{s_i \nu_i} + \dots$$

so erhält man

$$\sum_{(\nu_1, \dots, \nu_n) \in I} a_{\nu_1, \dots, \nu_n} b_n^{s_1 \nu_1 + s_2 \nu_2 + \dots + s_{n-1} \nu_{n-1} + \nu_n} + \underbrace{f(x_1, \dots, x_{n-1}, b_n)}_{\in K[x_1, \dots, x_{n-1}, b_n]} = 0 \quad (\text{Gl. 6.2})$$

Dabei ist $f(x_1, \dots, x_{n-1}, b_n)$ ein Polynom in b_n mit Koeffizient in $K[x_1, \dots, x_{n-1}]$ wobei der Grad in b_n echt kleiner ist als das Maximum der Summe $s_1 \nu_1 + \dots + s_{n-1} \nu_{n-1} + \nu_n$ mit $(\nu_1, \dots, \nu_n) \in I$.

Wir können nun die Exponenten s_1, \dots, s_{n-1} so wählen, dass die Summen $s_1 \nu_1 + \dots + s_{n-1} \nu_{n-1} + \nu_n$ für alle $(\nu_1, \dots, \nu_n) \in I$ paarweise verschieden sind.

(\mathbb{Q}^n wird nicht durch endlich viele Hyperebenen ausgeschöpft)

Dann ist Gl. 6.2 eine Gleichung der Form

$$\underbrace{ab_n^N}_{\in K \setminus \{0\}} + \underbrace{g(x_1, \dots, x_{n-1}, b_n)}_{\in K[x_1, \dots, x_{n-1}][b_n]} = 0$$

wobei b_n^N die höchste Auftretenden Potenz von b_n ist. Multiplikation mit $a^{-1} \in K$ zeigt, dass b_n ganz über $K[x_1, \dots, x_{n-1}]$ ist.

Somit ist

$$B = K[x_1, \dots, x_{n-1}][b_n]$$

ein endlich erzeugter $K[x_1, \dots, x_{n-1}]$ -Modul.

Sind x_1, \dots, x_{n-1} algebraisch unabhängig über K gilt die Behauptung. Ansonsten wenden wir das Verfahren auf den Ring $K[x_1, \dots, x_{n-1}]$ an und finden y_1, \dots, y_{n-1} , sodass $K[x_1, \dots, x_{n-1}]$ ein endlich erzeugter $K[y_1, \dots, y_{n-2}]$ -Modul ist.

Auf diese Weise fährt man fort, bis man ein über K algebraisch unabhängiges System gelangt ist. \square

Satz 6.18. *Sei $A \subset B$ eine Ringerweiterung, B ganz über A und seien A und B Integritätsbereiche.*

Dann ist A genau dann Körper, wenn B Körper ist.

Beweis. Sei A ein Körper und $b \in B \setminus \{0\}$. Wähle $f \in A[X]$ normiert und minimalen Grades, sodass $f(b) = 0$. Dann ist

$$f = X^n + a_1 X^{n-1} + \dots + a_n$$

mit $a_n \neq 0$ und

$$b(b^{n-1} + a_{n-1}b^{n-2} + \dots + a_1) = 0$$

$$b \underbrace{\left(-\frac{1}{a_n}\right)}_{\in A} \underbrace{(b^{n-1} + a_{n-1}b^{n-2} + \dots + a_1)}_{\in B} = 1$$

Also ist $b \in B^*$.

Sei B ein Körper und $a \in A \setminus \{0\}$. Dann ist $a^{-1} \in B$ und a^{-1} ist ganz über A , d.h.

$$(a^{-1})^n + a_i(a^{-1})^{n-1} + \dots + a_n = 0$$

für geeignete $a_i \in A$.

Es folgt

$$a^{-n} = -a_1 a^{-n+1} - \dots - a_n$$

$$a^{-1} = \underbrace{-a_1 - \dots - a_n a^{n-1}}_{\in A}$$

Also ist A ein Körper. \square

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

Beweis. Nach dem Noetherschen Normalisierungssatz 6.17 gibt es über K algebraisch unabhängige Elemente $y_1, \dots, y_r \in L$, sodass L ein endlich erzeugter $K[y_1, \dots, y_r]$ -Modul ist. Aus

$$K[y_1, \dots, y_r] \subset L$$

folgt, dass $K[y_1, \dots, y_r]$ ein Körper ist. Also ist $r = 0$. \square

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

Beweis. Es gilt $L = K[x_1, \dots, x_n]$ mit $x_i = X_i + m$. \square

6.4 Anfänge der algebraischen Geometrie

Definition 6.21. Sei K ein beliebiger Körper.

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

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

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

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

die **V???-Menge**.

Für $S \subset K[X_1, \dots, X_n]$ sei

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

Beispiel 6.23. Sei $n = 2$, $K = \mathbb{R}$, $F = X_1^2 - X_2$.

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

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

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

Beweis. \supset Ist klar.

\subset Sei $p \in V(S)$ und $F \in I$. Dann ist $F = \sum c_i F_i$ mit $c_i \in K[X_1, \dots, X_n]$, $F_i \in S$ und

$$F(p) = \sum c_i(p) \underbrace{F_i(p)}_{=0} = 0$$

Da $K[X_1, \dots, X_n]$ noethersch ist (Hilbertscher Basissatz ??) ist

$$I = (F_1, \dots, F_m) = \sum_i K[X_1, \dots, X_n] F_i$$

für geeignete $F_i \in I$.

Wie eben sieht man

$$V(I) = V((F_1, \dots, F_m)) = V(F_1, \dots, F_m)$$

□

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 .

Beispiel 6.27. Betrachte $V(Y^2 - X(X^2 - 1)) \subset \mathbb{A}_{\mathbb{R}}^2$.

Satz 6.28. Die Abbildung

$$V : \left\{ \begin{array}{c} \text{Ideale in} \\ K[X_1, \dots, X_n] \end{array} \right\} \rightarrow \{ \text{Algebraische Teilmengen von } \mathbb{A}_K^n \}$$

hat folgende Eigenschaften

- a) $V(0) = \mathbb{A}_K^n$, $V(K[X_1, \dots, X_n]) = \emptyset$
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: $V(\sum_i J_i) = \bigcap_i V(J_i)$

Beweis. Wir zeigen nur

Es gilt

$$\begin{aligned} IJ &\subset I \cap J \subset I \\ IJ &\subset I \cap J \subset J \end{aligned}$$

dann mit 2):

$$\begin{aligned} V(IJ) &\supset V(I \cap J) \supset V(I) \\ V(IJ) &\supset V(I \cap J) \supset V(J) \end{aligned}$$

es folgt, dass

$$V(IJ) \supset V(I \cap J) \supset V(I) \cup V(J)$$

Sei nun $p \in \mathbb{A}_K^n \setminus (V(I) \cup V(J))$.

Dann gibt es ein $f \in I$ mit $f(p) \neq 0$ und ein $g \in J$ mit $g(p) \neq 0$. Also ist

$$0 \neq \underbrace{(fg)}_{\in IJ}(p)$$

d.h. $p \notin V(IJ)$. Also ist $V(IJ) \subset V(I) \cup V(J)$ und es gilt Gleichheit.

□

Satz 6.29. Die Abbildung I

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

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

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

Gleichheit gilt genau dann wenn M algebraisch ist.

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

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

Beweis. Wir zeigen:

- b) „ \Rightarrow “ Sei $M = V(I(M))$, so ist M algebraisch.

„ \Leftarrow “ Sei M algebraisch, dann ist $M = V(J)$ für ein Ideal J . Dann ist

$$J \subset I(M) \quad (3)$$

$$V(J) \supset V(I(M)) \quad (4)$$

Es folgt Gleichheit.

□

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.

Beispiel 6.31. Sei K algebraisch abgeschlossen. Dann sind in \mathbb{A}_K^1 die Menge \mathbb{A}_K^1 und $\{\}$ offen und abgeschlossen.

Sei $M \subsetneq \mathbb{A}_K^1$ abgeschlossen. Dann ist

$$\begin{aligned} M &\stackrel{M \text{ alg.}}{=} V(I) \stackrel{K[X] \text{ HIR}}{=} V(f) \\ &= V((X - a_1) \dots (X - a_n)) \\ &\stackrel{K \text{ alg. abg.}}{=} \{a_1, \dots, a_n\} \end{aligned}$$

d.h. M ist endlich. Die nicht-leeren offenen Teilmengen von \mathbb{A}_K^1 sind dicht in \mathbb{A}_K^1 .

Die nicht-leere offenen Teilmenge von \mathbb{A}_K^1 sind dicht in \mathbb{A}_K^1 .

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

$$J = (X_1 - a_1, X_2 - a_2, \dots, X_n - a_n)$$

maximal in $K[X_1, \dots, X_n]$ und K ist isomorph zu $K[X_1, \dots, X_n]/J$

Beweis. Sei $f \in K[X_1, \dots, X_n] = K[X_1, \dots, X_{n-1}][X_n]$. Dann ist

$$f = (X_n - a_n)g_n + c_n$$

wobei $(X_n - a_n)$ Grad 1 in X_n hat, $g_n \in K[X_1, \dots, X_{n-1}][X_n]$ ist und c_n Grad 0 in X_n hat, d.h. $c_n \in K[X_1, \dots, X_{n-1}]$. Dann folgt

$$\begin{aligned} f &= (X_n - a_n)g_n + (X_{n-1} - a_{n-1})g_{n-1} + c_{n-1} \\ &\vdots \\ &= (X_n - a_n)g_n + \dots + (X_1 - a_1)g_1 + \underbrace{c_1}_{\in K} \end{aligned}$$

Also ist $K[X_1, \dots, X_n]/J = K$ und J ist maximal. □

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

$$J \subsetneq K[X_1, \dots, X_n]$$

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

Beweis. J ist in einem maximalen Ideal \mathfrak{m} enthalten und $V(\mathfrak{m}) \subset V(J)$.
Die Abbildung

$$K \hookrightarrow K[X_1, \dots, X_n] \xrightarrow{\pi} L := K[X_1, \dots, X_n]/\mathfrak{m}$$

Liefert eine Einbettung $K \hookrightarrow L$.

Sei $a_i = \pi(X_i) \in L$. Dann folgt aus dem Noethersche Normalisierungssatz 6.17, dass $L = K[a_1, \dots, a_n]$ und dass L/K algebraisch ist.

Da K algebraisch abgeschlossen ist folgt $K = L$.

Weiterhin ist $X_i - a_i \in \mathfrak{m}$ und $(X_1 - a_1, \dots, X_n - a_n) \subset \mathfrak{m}$. Da $(X_1 - a_1, \dots, X_n - a_n)$ maximal ist folgt

$$(X_1 - a_1, \dots, X_n - a_n) = \mathfrak{m}$$

Es folgt, dass

$$V(\mathfrak{m}) = \{(a_1, \dots, a_n)\}$$

□

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

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

Rabinowitsch. $\text{rad}(J) \subset I(V(J))$: Sei $f \in \text{rad}(J)$, dann ist f^n in J . Dann $f^n \in I(V(J))$, dann $f^n(p) = 0 \forall p \in V(J)$, dann $f(p) = 0 \forall p \in V(J)$ und damit $f \in I(V(J))$.

$\text{rad}(J) \supset I(V(J))$ Sei $g \in I(V(J))$. Schreibe $J = (f_1, \dots, f_t)$ und definiere

$$I = (f_1, \dots, f_t X_{n+1} g - 1) \subset K[X_1, \dots, X_n, X_{n+1}]$$

Dann ist

$$\begin{aligned} f_1(x_1, \dots, x_n) &= 0 \\ &\vdots \\ f_t(x_1, \dots, x_n) &= 0 \\ x_{n+1} f(x_1, \dots, x_n) - 1 &= 0 \end{aligned}$$

Dann ist $V(I) \subset A_K^{n+1}$ leer.

(Denn: Sei $f_1(x_1, \dots, x_n) = 0, \dots, f_t(x_1, \dots, x_n) = 0$, dann ist $(x_1, \dots, x_n) \in V(J)$.

Außerdem ist $x_{n+1} g(x_1, \dots, x_n) - 1 = 0$ mit $g(x_1, \dots, x_n) = 0$ auf $V(J)$. Widerspruch!)

Aus dem Schwartzschen Nullstellensatz folgt $I = K[X_1, \dots, X_n]$.

Schreibe nun

$$\sum_{i=1}^t A_i(x_1, \dots, x_{n+1}) f_i + B(x_1, \dots, x_{n+1})(x_{n+1} g - 1) = 1$$

Sei $x_{n+1} = \frac{1}{y}$.

Multipliziert man mit einer genügend hohen Potenz von Y , so erhält man

$$\sum_{i=1}^t C_i(X_1, \dots, X_n, Y) f_i + D(X_1, \dots, X_n, Y)(g - Y) = Y$$

dabei sind $C_i(X_1, \dots, X_n, Y), D(X_1, \dots, X_n, Y) \in K[X_1, \dots, X_n, Y]$.
 Setze $Y = g$, dann ist

$$g^n = \sum_{i=1}^t \underbrace{C_i(X_1, \dots, X_n, g)}_{\in K[X_1, \dots, X_n]} f_i \in J$$

Also ist $g \in \text{rad}(J)$.

□