

Satz 0.1. 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 0.2. 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 0.3. 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 0.4. 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 $O \in \Sigma$ 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 $I \notin C_i$ für alle $i \in I$ folgt, dass $I \notin C$, d.h. $C \in \Sigma$. Somit hat Σ ein maximales Element. \square

Korollar 0.5. Sei A ein Ring und $I \subsetneq A$ ein Ideal, dann ist I in einem maximalen Ideal enthalten.

Korollar 0.6. 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

0.1 Lokale Ringe

Definition 0.7. Ein Ring A mit nur einem maximalen Ideal \mathfrak{m} heißt **lokaler Ring** und A/\mathfrak{m} heißt **Restklassenkörper** von A .

Satz 0.8. 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 0.9. 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 0.10.1. 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 (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 .

0.2 Radikale

Satz 0.11. Sei A ein 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.

- Z.z. $AN \subset N$.
 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 0.12. Das Ideal $N = \{a \in A \mid a \text{ ist Nilpotent}\}$ heißt das **Nilradikal** von A .

Definition 0.13. Sei A ein Ring dann nennt man $J = \{x \in A \mid \forall y \in A : 1 - xy \text{ ist Einheit}\}$ das **Jacobsonradikal**.

Satz 0.14. 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 0.15. 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 0.16. Sei $\mathfrak{a}, \mathfrak{b}$ ein Ideal, dann gilt

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

0.2.1 Operationen auf Radikalen

Definition 0.17. Seien A ein Ring.

- 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 0.18. Die Operationen Summe, Durchschnitt und Produkt auf Idealen sind kommutativ und Assoziativ und es gilt das Distributivgesetz.

Definition 0.19. Sei A ein Ring. Zwei Ideale $\mathfrak{a}, \mathfrak{b} \subseteq A$ heißen **teilerfremd**, wenn $\mathfrak{a} + \mathfrak{b} = A = (1)$.

Satz 0.20. 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 0.21. 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 $\prod_{\substack{j=1 \\ j \neq i}}^n \mathfrak{a}_j$.

- b) Es gilt

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

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

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

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

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

Wir nehmen an es gelte

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

Dann ist aber

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

□

Definition 0.22. Sei A ein Ring und seinen $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ 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 0.23. 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 $j > 1$.

□

0.3 Ringe von Brüchen

Definition 0.24. 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 0.25. 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 0.26. 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 0.27. 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 0.28. Sei $A = \mathbb{Z}$ und $S = \mathbb{Z} \setminus \{0\}$. Dann ist $S^{-1}A$ isomorph zu \mathbb{Q} .

Korollar 0.29. 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 0.30. 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 0.31. Sei A ein Integritätsbereich und $S = A \setminus \{0\}$. Dann nennt man $S^{-1}A$ den **Quotientenkörper**

Lemma 0.32. Der Quotientenkörper ist ein Körper, φ_S ist injektiv und wir können A mit seinem Bild in $S^{-1}A$ identifizieren.

Definition 0.33. 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 0.34. Sei A ein Ring. Sei \mathfrak{p} ein Primideal in A . Dann ist $S = A \setminus \mathfrak{p}$ multiplikativ Abgeschlossen.

Lemma 0.35. 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 0.36. 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

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

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 $a/s \in S^{-1}I$.

□

0.4 Integritätsbereiche und Hauptidealringe

Definition 0.37. Sei A ein Ring. Ein Ideal der Form $(a) = Aa$ heißt **Hauptideal**.

Definition 0.38. Ein Ring A heißt **Hauptidealring**, wenn jede Ideal in A Hauptideal ist.

Definition 0.39. 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 0.40. 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 0.41. Sei A ein euklidischer Ring. Dann ist A ein Hauptidealring.

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

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

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 $\mathfrak{a} \subset (x)$. \square

Definition 0.42. Sei A ein Ring und seien $a, b \in A$.

$d \in A$ heißt **Größter gemeinsamer Teiler** von a und b , wenn gilt

a) $d \mid a$ und $d \mid b$.

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

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

Definition 0.43. Sei A ein Ring und seien $a, b \in A$.

$d \in A$ heißt **kleinstes gemeinsames Vielfaches** von a und b , wenn gilt

a) $a \mid v$ und $b \mid v$.

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

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

Satz 0.44. Sei A ein Hauptidealring und seien $a, b \in A$.

Dann existiert ein $d = \gcd(a, b)$ 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 0.45. 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 0.46. 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 0.47. 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 0.48. 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 0.49. 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 0.50. Ein Integritätsbereich heißt **faktoriell**, wenn

- Jedes $a \in A \setminus A^*$, $a \neq 0$ zerfällt in ein Produkt von irreduziblen Elementen.
- 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 0.51. Die Eindeutigkeit der Faktorisierung impliziert, dass es irreduzibles Element in einem faktoriellen Integritätsbereich prim ist.

Lemma 0.52. *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 0.53. *Sei A ein Integritätsbereich. Ist A ein Hauptidealring, so ist A faktoriell.*

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

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. \square

0.5 Inverse und direkte Limiten

Definition 0.54. Man nennt I eine unter \leq **partiell geordnete Menge**, wenn für alle $x, y, z \in I$ gilt

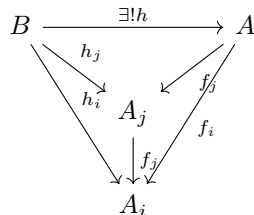
- a) $x \leq x$.
- b) Aus $x \leq y$ und $y \leq z$ folgt $x \leq z$.
- c) Aus $x \leq y$ und $y \leq x$ folgt $x = y$.

Definition 0.55. 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 0.56. 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 0.57. 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}) .

Inbesondere 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 0.58. 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 in 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

$$p \mid x \Leftrightarrow x \mid x_n \text{ für alle } n \geq 1$$

Satz 0.59. 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_j 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 0.60. 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 0.61. 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 0.62. \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 0.63. 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 0.64. 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 0.65. 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 0.66. 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. $x \in A_i, y \in A_j$.

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

□

0.6 Nullstellen von Polynomen

Definition 0.67. Sei $f \in A[X]$, $f \neq 0$.

$a \in A$ heißt **Nullstelle** von f , wenn $f(a) = 0$.

Satz 0.68. 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 0.69. 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 0.70. 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 0.71. 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 0.72. 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 0.73. 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 0.74. 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 $n_1 n_2 \mathbb{Z}$ und ist surjektiv nach ??.

Dann ist

$$\mathbb{Z}/n_1 n_2 \mathbb{Z} \cong G_1 \times G_2$$

□

Theorem 0.75. 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. □

Korollar 0.76. Ist K endlicher Körper, so ist K^* zyklisch.

Satz 0.77. 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 $d|a_n$ □

Definition 0.78. 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 0.79. 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 0.80. Seien $f, g \in A[X]$, $a, b \in A$. Für die Ableitung D gilt

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

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

Satz 0.81. 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 0.82. 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 0.83. Ist A ein Integritätsbereich, so ist $n = 0$ oder n ist prim.

Satz 0.84. 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

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

0.7 Bewertungen

Definition 0.85. 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 0.86. 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 0.87. 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 0.88. 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 0.89. 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 0.90.1. 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 0.90.2. 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 0.91 (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

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

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

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

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

□

0.8 Der Satz von Gauß

Definition 0.92. 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 0.93. 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 0.94 (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 0.93 sind die \tilde{f}_i auch irreduzibel 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 $\epsilon_1 := x_i \cdot d/c$. 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 $\eta_i d_i \in A^*$. □

Korollar 0.95. *Sie K ein Körper, dann ist $K[X_1, \dots, X_n]$ ein faktorieller Integritätsbereich.*

Beispiel 0.96.1. $\mathbb{Z}[X]$ ist ein faktorieller Integritätsbereich aber kein Hauptidealring.

Beispiel 0.96.2. Sei K ein Körper. $K[X]$ ist ein Hauptidealring und somit faktorieller. $K[X, Y]$ ist kein Hauptidealring aber faktoriell.

0.9 Der Hilbertsche Basissatz

Theorem 0.97 (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

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

□

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

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

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

$$f - \sum a_{t_j} X^{t-m} f_{m_j} \in I$$

0.10 Eigenschaften von Polynomringen

Sei A ein Ring.

- A Integritätsbereich $\Leftrightarrow A[X_1, \dots, X_n]$ Integritätsbereich.
Dann gilt $A[X_1, \dots, X_n]^* = A^*$.
- (Gauss) A faktorieller Integritätsbereich $\Leftrightarrow A[X_1, \dots, X_n]$ faktorieller Integritätsbereich.
- (Hilbert) A noethersch $\Leftrightarrow A[X_1, \dots, X_n]$ noethersch.
- Sei A zusätzlich Integritätsbereich, dann ist
 A Körper $\Leftrightarrow A[X]$ Hauptidealring.

0.11 Irreduzibilitätskriterien

Theorem 0.98 (Eisenstein). Sei A ein faktoriell 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 $a_n \not\equiv 0 \pmod{p}$ 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 $\tilde{f} = gh$ 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 $p \mid a_0$, dass $p \mid \tilde{a}_0 = b_0 d_0$.
 Wir können annehmen, dass $p \nmid b_0$.
 Aus $p^2 \nmid a_0$ folgt, dass $p \nmid d_0$. Es gibt aber j , sodass $p \nmid b_j$ (da sonst $p \mid g$).
 Wähle nun j , sodass $p \mid b_i$ 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 $p \mid \tilde{a}_j$), dass $p \mid b_j d_0$ und $p \mid d_0$. Widerspruch! \square

Beispiel 0.99. 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 0.100 (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 $\nmid a_n$.*

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 $\pi(f)$. \square

Beispiel 0.101.1. 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 $\pmod{3}$.

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

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 0.101.2. 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 .

0.12 Symmetrische Polynome

Definition 0.102. 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 0.103. Insbesondere gilt für $\sigma, \tau \in S_n$, dass $(\sigma\tau)(f) = \sigma(\tau(f))$.

Definition 0.104. Die Polynome in $A[X_1, \dots, X_n]^{S_n}$ (invariant unter S_n) werden als **symmetrische Polynome** bezeichnet.

Proposition 0.105. Die Gruppenoperationen $\sigma \in S_n$ sind Automorphismen auf $A[X_1, \dots, X_n][X]$.

Satz 0.106. 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 0.107. Sei $f \in [X - 1, \dots, X_n][X]$, $\sigma \in S_n$. 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 0.108. Die elementarsymmetrischen Polynome sind symmetrisch, d.h. $\sigma(s_j) = s_j$. Sie sind gegeben durch

$$\begin{aligned} s_1 &= X_1 + X_2 + \dots + X_n \\ s_2 &= X_1X_2 + X_1X_3 + \dots + X_1X_n + X_2X_3 + \dots + X_{n-1}X_n \\ &= \sum_{i \leq j} X_iX_j \\ s_n &= X_1 \dots X_n \end{aligned}$$

Satz 0.109. Die Polynome s_j sind homogen vom Grad j .

Definition 0.110. 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 0.111. 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 0.112. 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 $f \in A[X_1, \dots, X_n]^{S_n}$. 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

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

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

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

b) Siehe Lang

□

Theorem 0.113. *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! \square

Beispiel 0.114. 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 0.115. 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 0.116. 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 0.117. Ist $B \supset A$ ein Integritätsbereich so gilt

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

Beispiel 0.118.1. Für $f = X^2 + aX + b$ ist $D(f) = a^2 - 4b$ (Wurzel der pq-Formel)

Beispiel 0.118.2. Für $f = X^3 + aX + b$ ist $D(f) = -4a^3 - 27b^2$.

1 Körpererweiterungen

1.1 Grundbegriffe

Definition 1.1. 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 1.2. 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 1.3. Sei L/K eine Körpererweiterung. Dann heißt der Körper M mit $K \subset M \subset L$ **Zwischenkörper** der Erweiterung L/K .

Definition 1.4. 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 1.5. 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. □

Proposition 1.6. Für jedes $a \in K(M)$ gibt es eine endliche Teilmenge $M' \subset M$, sodass $a \in K(M')$.

Definition 1.7. 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 1.8. 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 1.9. 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 1.10. Ist K ein Teilkörper von L , so gilt

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

Definition 1.11. Sei K ein Körper. Dann heißt

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

der **Primkörper** von K .

Satz 1.12. Sei K ein Körper und P der Primkörper von K . Dann gilt

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

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

Definition 1.13. 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 1.14. Die Erweiterung L/K heißt **endlich**, wenn $[L : K] < \infty$.

Proposition 1.15. Ist L endlich und K kein Teilkörper von L , so gilt

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

mit $m = [L : K]$.

Theorem 1.16 (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

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

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

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

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 $c_{ij} = 0$. □

1.2 Algebraische Körpererweiterungen

Definition 1.17. Sei L/K eine Körpererweiterung. $\alpha \in L$ heißt **algebraisch** über K , wenn es eine

Definition 1.18. 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 1.19. Ein Körper K ist genau dann algebraisch abgeschlossen wenn es keine echte algebraische Erweiterung L/K zulässt.

Theorem 1.20. Sei K ein Körper. Dann gibt es eine algebraisch abgeschlossene Körper L mit $K \subseteq L$.

Artin. Sei $K \hookrightarrow L_i$ eine Einbettung, sodass jedes nicht konstante Polynom 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

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

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

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

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

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

Zz: \bar{K} ist algebraisch abgeschlossen:

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

Korollar 1.22. *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 1.23. *Sei K ein Körper und $K' = K(\alpha)$ eine einfache algebraische Körpererweiterung von K und $\sigma : K \rightarrow L$ ein Homomorphismus. Dann gilt*

- 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 1.24. *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 $\sigma(m_{\alpha, K}) = \sigma'(m_{\alpha, K})$.*

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

Abbildung 1: Kommutierendes Digramm der Algebraischen Körpererweiterungen

- 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. • 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 $\sigma' := \overline{\psi} \circ \overline{\varphi}^{-1}$.

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. \square

Theorem 1.25 (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 1.26. 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 $\sigma : \overline{K}_1 \rightarrow \overline{K}_2$. Dieser ist ein Isomorphismus.
(Dieser ist i.a. nicht Kanonisch) \square

Beispiel 1.27. 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} .

1.3 Zerfallskörper

Definition 1.28. 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 1.29. 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 1.30. 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 1.31. 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 Nullstelle von f in L_1 und b_1, \dots, b_n die Nullstelle 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 1.32. 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 1.33. 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 1.31 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 $\sigma(a) = b$ (1.24). Diese lässt sich Fortsetzen (1.25) 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 1.34. Eine algebraische Körpererweiterung L/K die eine der Bedingungen von 1.33 erfüllt heißt **normal**.

Satz 1.35. Sei L/K eine normale Körpererweiterung und $K \subset M \subset L$ ein Zwischenkörper. Dann ist auch L/M normal.

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

Beispiel 1.36. 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.

1.4 Separabel Körpererweiterungen

In diesem Abschnitt bezeichne K ein Körper.

Definition 1.37. Ein Polynom $f \in K[X]$ heißt **separabel**, wenn f nur einfache Nullstellen in einem algebraischen Abschluss \overline{K} von K hat.
(Dies ist unabhängig von der Wahl von \overline{K})

Satz 1.38. 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

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

□

Definition 1.39. Sei L/K eine algebraische Körpererweiterung. $a \in L$ heißt **separabel** über K , wenn $m_{a,K}$ separabel ist.

Definition 1.40. Sei L/K eine algebraische Körpererweiterung. L heißt **separabel** über K , wenn jedes $a \in L$ separabel über K ist