Erinnerung:

2.11.1 Definition: Ein *Primideal von* R ist ein echtes Ideal $\mathfrak{p} \subsetneq R$ mit der Eigenschaft:

$$\forall x, y \in R\colon xy \in \mathfrak{p} \longrightarrow (x \in \mathfrak{p} \text{ oder } y \in \mathfrak{p}).$$

2.11.2 Proposition: Ein Ideal $\mathfrak{p}$ von R ist ein Primideal genau dann, wenn der Faktorring $R/\mathfrak{p}$ ein Integritätsbereich ist.

2.11.3 Definition: Ein *maximales Ideal von* R ist ein echtes Ideal $\mathfrak{m} \subsetneq R$, welches unter allen echten Idealen maximal ist, das heisst, so dass jedes Ideal $\mathfrak{a}$ mit $\mathfrak{m} \subset \mathfrak{a}$ entweder gleich $\mathfrak{m}$ oder gleich R ist.

2.11.4 Proposition: Ein Ideal $\mathfrak{m}$ von R ist maximal genau dann, wenn der Faktorring $R/\mathfrak{m}$ ein Körper ist.

2.11.5 Folge: Jedes maximale Ideal ist ein Primideal.

Beweis: $\mathfrak{m}$ maximal $\Rightarrow$ $R/\mathfrak{m}$ Körper $\Rightarrow$ $R/\mathfrak{m}$ Integritätsbereich $\Rightarrow$ $\mathfrak{m}$ prim. ged.

$R/(0) \xrightarrow{\sim} R$.

2.11.6 Beispiele: (a) Das Nullideal ist prim genau dann, wenn R ein Integritätsbereich ist.

(b) Das Nullideal ist maximal genau dann, wenn R ein Körper ist.

(c) Betrachte eine Menge X, einen Körper K, und einen Unterring R des Rings aller Funktionen $\mathrm{Abb}(X, K)$, welcher alle konstanten Funktionen $X \to K$ enthält. Für jedes $x \in X$ ist dann $\mathfrak{m}_x := \mathrm{Kern}(R \to K,\ f \mapsto f(x))$ ein maximales Ideal.

Homomorphiesatz: $R/\mathfrak{m}_x \xrightarrow{\sim} \mathrm{Bild} = K = \text{Körper} \Rightarrow \mathfrak{m}_x$ maximal.

$[f] \longmapsto f(x)$

2.11.7 Folge: Seien K ein Körper und $0 \neq f \in K[X]$. Dann ist (f) ein maximales Ideal genau dann, wenn f irreduzibel ist.

$\Leftarrow$ d.h. f keine Einheit und $\forall g, h \in K[X]: f = gh \Rightarrow g$ oder h Einheit.

Bew.: $(f) \neq (1) \Leftrightarrow f$ keine Einheit. | $f = gh \Rightarrow [f] = [g]\cdot[h]$. g, h keine Einheiten $\Leftrightarrow [g], [h] \neq 0$

$\Rightarrow$ " 0 " $\Rightarrow K[X]/(f)$ Integritätsbereich $\Leftrightarrow f$ irreduzibel.

Rechne in $K[X]/(f)$

2.11.8 Beispiele: (a) Das Ideal $(X^2+1) \subset \mathbb{R}[X]$ ist ein maximales Ideal, und der Faktorring ist isomorph zu $\mathbb{C}$.

$f \neq 0 \Rightarrow \dim_K K[X]/(f) = \deg(f) < \infty$. Beweise 3.2.8. qed

(b) Für jede ganze Zahl d, die kein Quadrat ist, ist das Ideal $(X^2 - d) \subset \mathbb{Z}[X]$ ein Primideal, aber kein maximales Ideal. Für den Faktorring gilt

$$\mathbb{Z}[X]/(X^2 - d) \ \cong\ \mathbb{Z}[\sqrt{d}].$$

in $\mathbb{C}$ gerechnet.

$\varphi: \mathbb{Z}[X] \twoheadrightarrow \mathbb{Z}[\sqrt{d}]$, $f \mapsto f(\sqrt{d})$ $\Rightarrow X^2 - d \in \mathrm{Kern}(\varphi)$.

$\mathbb{Z}[X]/(X^2-d) \ni [a+bX]$ $\quad \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$

Polynomdivision mit Rest:
$\forall f \in \mathbb{Z}[X]\ \exists g \in \mathbb{Z}[X], a, b \in \mathbb{Z}$ eindeutig:
$f(X) = g(X)\cdot(X^2 - d) + a + bX$.

2.11.9 Satz: *(Krull)* Für jedes echte Ideal $\mathfrak{a} \subsetneq R$ existiert ein maximales Ideal $\mathfrak{m} \subset R$ mit $\mathfrak{a} \subset \mathfrak{m}$.

Bew.: $\mathcal{S} := \{ \text{Ideale } \mathfrak{b} \subsetneq R \mid \mathfrak{a} \subset \mathfrak{b} \}$.

Partialordnung "$\subset$".

$\mathcal{S} \ni \mathfrak{a} \Rightarrow \mathcal{S} \neq \emptyset$.

Für jede Kette $\mathcal{K} \subset \mathcal{S}$, $\mathcal{K} \neq \emptyset$, setze $\mathfrak{t} := \bigcup_{\mathfrak{b} \in \mathcal{K}} \mathfrak{b}$.

$\exists \mathfrak{b} \in \mathcal{K}: 0 \in \mathfrak{b} \Rightarrow 0 \in \mathfrak{t}$.

(*) $\forall a, b \in \mathfrak{t}: \exists \mathfrak{b} \in \mathcal{K}: a, b \in \mathfrak{b} \Rightarrow a+b \in \mathfrak{b} \Rightarrow a+b \in \mathfrak{t}$.

$\forall a \in \mathfrak{t}\ \forall x \in R: ax \in \mathfrak{t}$. analog.

$\Rightarrow \mathfrak{t}$ ist Ideal.

$\forall \mathfrak{b} \in \mathcal{K}: 1 \notin \mathfrak{b} \Rightarrow 1 \notin \mathfrak{t} \Rightarrow \mathfrak{t} \subsetneq R$.

$\forall \mathfrak{b} \in \mathcal{K}: \mathfrak{a} \subset \mathfrak{b} \subset \mathfrak{t} \Rightarrow \mathfrak{a} \subset \mathfrak{t}$

$\Rightarrow \mathfrak{t} \in \mathcal{S}$.

$\forall \mathfrak{b} \in \mathcal{K}: \mathfrak{b} \subset \mathfrak{t}$

$\Rightarrow \mathfrak{t}$ obere Schranke von $\mathcal{K}$

Zornsches Lemma $\Rightarrow \mathcal{S}$ besitzt ein max. Element $\mathfrak{m}$.

$\Rightarrow \mathfrak{m}$ ist max. Ideal mit $\mathfrak{a} \subset \mathfrak{m}$. qed.

(*) $\exists \mathfrak{a}, \mathfrak{b} \in \mathcal{K}: a \in \mathfrak{a} \wedge b \in \mathfrak{b}$

$a, b \in \mathfrak{a} \cup \mathfrak{b} \in \mathcal{K}$.

2.11.10 Folge: Jeder nichttriviale Ring besitzt ein maximales Ideal.

2.11.11 Folge: Jeder nichttriviale Ring besitzt ein Primideal.

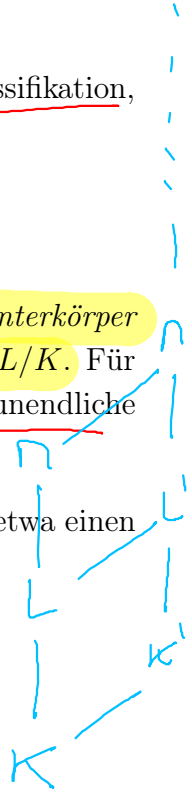
3 Körper

Körpertheorie ist das Studium von Körpererweiterungen, insbesondere ihrer Konstruktion, Klassifikation, und das Lösen von Gleichungen darin.

3.1 Körpererweiterungen

3.1.1 Definition: Ein Unterring K eines Körpers L, welcher selbst ein Körper ist, heisst ein *Unterkörper von L*. Dann heisst L ein *Oberkörper von K*, und wir sprechen von der *Körpererweiterung L/K*. Für Körpererweiterungen $M/L/K$ nennen wir L einen *Zwischenkörper von M/K*. Eine endliche oder unendliche Folge von Körpererweiterungen $\ldots/K_{i+1}/K_i/K_{i-1}/\ldots$ heisst ein *Körperturm*.

3.1.2 Bemerkung: Die Notation L/K bezeichnet hier kein neues mathematisches Objekt wie etwa einen Faktorraum, sondern dient nur als sprachliche Abkürzung.



3.1.3 Proposition: Jeder Körper K besitzt einen eindeutigen kleinsten Unterkörper. Dieser ist entweder isomorph zu $\mathbb{Q}$ oder zu $\mathbb{F}_p$ für eine eindeutige Primzahl p.

Bew.: Es existiert ein eindeutiger Ringhomo $\chi: \mathbb{Z} \to K$, $n \mapsto n \cdot 1_K$.
$\mathbb{Z}/\ker(\chi) \cong \mathrm{Bild}(\chi) \subset$ Integritätsbereich $\Rightarrow \ker(\chi)$ Primideal.
$\Rightarrow \ker(\chi) = \begin{cases} (0) \\ (p) \quad p \text{ prim.} \end{cases} \Rightarrow \mathrm{Bild}(\chi) \cong \begin{cases} \mathbb{Z} \\ \mathbb{F}_p \end{cases}$

Für jeden Unterkörper $K' \subset K$ ist $\mathrm{Bild}(\chi) \subset K'$!
χ injektiv $\Rightarrow \mathbb{Z} \subset K'$
$\Rightarrow \chi$ setzt sich fort zu $\mathbb{Q} \hookrightarrow K'$.

q.e.d.

3.1.4 Definition: Dieser Unterkörper heisst der *Primkörper von K*, und die Zahl

$$\mathrm{char}(K) := \begin{cases} 0 & \text{falls der Primkörper } \mathbb{Q} \text{ ist,} \\ p & \text{falls der Primkörper } \mathbb{F}_p \text{ ist,} \end{cases}$$

heisst die *Charakteristik von K*.

3.1.5 Proposition: Jeder Körperhomomorphismus $K \xrightarrow{\varphi} L$ ist injektiv, und wenn einer existiert, so ist $\mathrm{char}(K) = \mathrm{char}(L)$.

$K \xrightarrow{\sim} \mathrm{Bild}(\varphi) \subset L$.

Analog: Isomorphe Körper haben dieselbe Charakteristik.

3.1.6 Bemerkung: Durch einen Körperhomomorphismus $K \hookrightarrow L$ kann man K mit einem Unterkörper von L identifizieren. Man sollte dies aber nur dann tun, wenn der Homomorphismus später nicht mehr abgeändert wird.

3.1.7 Proposition: Für jede Körpererweiterung L/K und jede Teilmenge $A \subset L$ existiert ein eindeutiger kleinster Zwischenkörper von L/K, welcher A enthält. Dieser ist der Quotientenkörper des von A über K erzeugten Unterrings $K[A]$, besteht also aus den Elementen $\frac{f(a_1,\ldots,a_n)}{g(a_1,\ldots,a_n)}$ für alle $n \geqslant 0$, alle $a_1, \ldots, a_n \in A$, und alle $f, g \in K[X_1, \ldots, X_n]$ mit $g(a_1, \ldots, a_n) \neq 0$.

$K[A] = \{ f(a_1,\ldots,a_n) \mid \text{alle } f \in K[X_1,\ldots,X_n],\ a_1,\ldots,a_n \in A \} \subset K(A)$.

Vgl.: $K[X] \subset K(X)$

3.1.8 Definition: Dieser Zwischenkörper heisst *von A über K erzeugt* und wird bezeichnet mit $K(A)$. Für endlich viele Elemente $a_1, \ldots, a_n \in L$ schreiben wir auch $K(a_1, \ldots, a_n) := K(\{a_1, \ldots, a_n\})$ und nennen diesen Körper *endlich erzeugt über K*. Eine Körpererweiterung der Form $K(a)/K$ nennen wir *einfach*.

3.1.9 Proposition: (a) Für alle $a \in K$ gilt $K(a) = K$.

(b) Für alle $0 \leqslant m \leqslant n$ gilt $K(a_1, \ldots, a_n) = K(a_1, \ldots, a_m)(a_{m+1}, \ldots, a_n)$.

Beweis: Ü.

3.1.10 Beispiel: Der Körper $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\} \subset \mathbb{C}$.

3.2 Körpergrad

3.2.1 Definition: Der *Grad* einer Körpererweiterung L/K ist die Zahl

$$[L/K] \;:=\; \dim_K(L) \;\in\; \mathbb{Z}^{\geqslant 1} \cup \{\infty\}.$$

Eine Körperweiterung mit $[L/K] < \infty$ heisst *endlich*. Eine Körperweiterung vom Grad 2 heisst *quadratisch*, vom Grad 3 *kubisch*, vom Grad 4 *biquadratisch*.

3.2.2 Proposition: Es ist $[L/K] = 1$ genau dann, wenn $L = K$ ist.

3.2.3 Beispiel: Es ist $[\mathbb{C}/\mathbb{R}] = 2$ und $[\mathbb{R}/\mathbb{Q}] = \infty$.

3.2.4 Proposition: Für jeden Körperturm $M/L/K$ gilt

$$[M/K] \;=\; [M/L] \cdot [L/K].$$

Insbesondere ist M/K endlich genau dann, wenn M/L und L/K endlich sind.

3.2.5 Proposition: Jede endliche Körpererweiterung L/K vom Primzahlgrad ist einfach, und für jedes $a \in L \smallsetminus K$ gilt $L = K(a)$.

Beweis: $K \subsetneq K(a) \subset L$; $p = [L/K] = [L/K(a)] \cdot [K(a)/K]$ | Also ist $L = K(a)$. qed.
"1 ⟸ >1

3.2.6 Proposition: Für jede Körpererweiterung L/K vom Grad 2 mit $\mathrm{char}(K) \neq 2$ existiert ein $a \in L$ mit $L = K(a)$ und $b := a^2 \in K$. Wir können dieses a als *eine Quadratwurzel aus* b ansehen.

3.2.7 Vorsicht: Die Notation $a = \sqrt{b}$ ist sehr gefährlich wegen fehlender Eindeutigkeit! Nur in $\mathbb{R}^{\geqslant 0}$ sind Wurzeln eindeutig definiert.